AZ

ALGEBRAI MENNYISÉGEK

ÁLTALÁNOS ELMÉLETÉNEK ALAPVONALAI

IRTA

KŐNIG GYULA

BUDAPEST

KIADJA A MAGYAR TUDOMÁNYOS AKADÉMIA

1903

Ára 15 korona.

AZ

ALGEBRAI MENNYISÉGEK

ÁLTALÁNOS ELMÉLETÉNEK ALAPVONALAI

IRTA

KŐNIG GYULA

BUDAPEST

KIADJA A MAGYAR TUDOMÁNYOS AKADÉMIA

1903

219713

A M. T. AKADÉMIA
FŐTITKÁRI HIVATALA.

FRANKLIN-TÁRSULAT NYOMDAJA.

B 1977

Magyar Tudományos Akadémia
Könyvtára 728/1958 sz.

ELŐSZÓ.

Az algebrai mennyiségek általános elméletét, mint a mathematika alapvető fejezetét KRONECKER LIPÓT teremtette meg 1882-ben közzétett hires «Festschrift»-jében, mely már pontosan megállapítja az új tudománynak teljes tartalmát, czéljait és problemáit. Mindazonáltal az elmélet története messze visszanyúl. Elfátyolozva ugyan, de már sejthető GAUSS örökérdemű műveiben; döntő szempontjai pedig egymásután föllépnek LEJEUNE-DIRICHLET, KUMMER és DEDEKIND arithmetikai vizsgálataiban, ABEL, GALOIS és JORDAN algebrai kutatásaiban, PUISEUX, RIEMANN és WEIERSTRASS függvénytani alkotásaiban, valamint végre CAYLEY, CLEBSCH, GORDAN és NOETHER az algebra és geometria közös területét megvilágító tételeiben. Az a húsz év, mely a «Festschrift» megjelenése óta elmúlt, szintén igen lényeges eredményeket szolgáltatott, melyekből KRONECKER folytatólagos értekezései mellett leginkább kiemelendők HILBERT egyenesen alapvető tételei az osztórendszerekről, és HENSEL értékes dolgozatai.

Ha meggondoljuk továbbá, hogy a csoportelmélet és függvénytan új útjai, melyeket egyrészt KLEIN és LIE, másrészt FUCHS és POINCARÉ kezdeményeztek, az algebrai mennyi-

ségek általános elméletét szintén nem egyszer közelről érintik, bátran mondhatjuk, hogy az új tudományszaknak oly fontos és mindenfelé kiható szerepe jut a tiszta mennyiségtan körében, a minő ezenkívül talán csakis az infinitesimalis számítás módszereinek van még.

Bizonyára hálás föladatnak látszott ezen elméletnek, vagy pontosabb kifejezésben ez elmélet alaptételeinek rendszeres előadása, melynek viszonya az arithmetika és algebra meglévő kézi könyveihez, bár nem teljes analogiában, körülbelül az volna, mint valamely függvénytani munkáé a differenciál- és integrálszámítást tárgyaló művekhez. Hogy e föladat azonban nagyon nehéz is, azt ime közzéteendő kisérletemen magam is eléggé tapasztaltam. Hisz a módszertani kérdések mellett előbb elintézendő maradt az alapproblémák egész sora, a melyeknek megoldása vagy teljesen hiányzott, vagy csak a legspeciálisabb esetekben volt meg.

Épen ezen új vizsgálatok, melyek könyvem tartalmának több mint felét teszik, arra kényszerítettek, hogy rendszeresen és könyv alakjában adjam elő a tárgyat. Már nagyon is régóta foglalkozva ily irányban, mindjárt kezdetben beláttam, hogy egyes értekezések közzétételével igazában czélt érni nem lehet; mert a hogy ezek az alapproblemák egymást kölcsönösen feltételezik, ily értekezések mindig nehezen olvashatók és csak igen szűk kör érdeklődésére számíthatnak. Kezdettől fogva pedig arra is akartam törekedni, hogy — ha lehet ezen a téren ezt a kifejezést használni — mintegy népszerűsítsem KRONECKER módszereinek szellemét.

Így tehát oly könyv keletkezett, mely valójában csak az algebra és számelmélet első elemeinek ismeretét követeli, beleértve a determináns-elmélet alaptételeit, úgy hogy

az előrehaladott egyetemi tanúló is már haszonnal olvashatja, de a mely könyv a szakembernek is a régi és új eredményeket sokkal kényelmesebb alakban mutatja be, mint a hogy ez a tudományos folyóiratok hasábjain történhetett volna.

Túlságos kiterjedést nyerne ez az előszó, ha a munka tartalmát itt bármily rövidre fogott jelentésben összefoglalnám, és azért csak töredékesen érintem a legszükségesebbeket.

Az egész tárgyalás az általam «holoid»-, ill. «orthoid»-nak nevezett tartomány értelmezéséből indúl ki; a raczionális és egész, ill. a raczionális számok tartományának mintájára készült ezen értelmezés, és azért első pillanatra úgy látszik, mintha pótolhatók volnának a már használatban lévő kifejezésekkel. (Test, Rationalitätsbereich, Integritätsbereich etc.) Ez azonban nincs úgy; mert elkerülve az utóbbi fogalmak merevségét, az elméletnek sokkal egyszerübb fölépítését teszik lehetővé. Megszüntetik az arithmetika és geometria kellemetlen ellentétét, és a tárgyalás beosztását megkönnyítik azon lényeges körülmény alapján, hogy az orthoid (raczionális) a holoid (egész) specziális esetének tekinthető. E fogalomalkotásoknak megfelelőleg szétválik az elmélet «algebrai» és «arithmetikai» része.

Módszertani szempontból hangsúlyozni kívánom, hogy teljesen elemi bizonyítás alapján a KRONECKER-féle alaptételt (III. fej. 5—7. §.) az egész elmélet kiindúló pontjává lehetett tenni.

E tételhez csatlakozik — mint az elért új eredmények sarkköve — a «resolvens forma» fölállítása, mely a resultáns fogalmának arithmetikai általánosítása tetszés szerinti formarendszer esetére, és a mely jelesen ennek mintájára, mint az adott formák homogén, lineáris formája ábrázol-

ható. E mellett a «forma» szó használata — KRONECKER példáját követve — kiterjed a nem homogén esetre is.

A resolvens forma bevezetése egyrészt, az új határozatlanok «associatio»-jának KRONECKER-től származó alapgondolata, másrészt azután az eliminációnak a szó teljes értelmében általános elméletéhez vezetnek, a melyben az egyenletrendszer értelmezte sokaságok sokszorosságát sem hanyagoljuk már el. Így a kutatás hathatós eszközének jutunk birtokába, mely először is a függvénydeterminánsnak tisztán algebrai elméletét szolgáltatja. Külön fejezet tárgyalja azután az ú. n. speciális eliminácziò-elméletet, azaz a resultánsok és discriminánsok általános elméletét; az utóbbi teljesen új.

Az elméletnek a szó szűkebb értelmében arithmetikai részei a lineáris diophantikus problémák tárgyalásával nyernek csak szilárd alapot. E problema az oly egyenletrendszer általános megoldását követeli, melyben az egyes egyenletek alakja $\Sigma F_i X_i = F$, hol az F-ek adott, az X-ek pedig ismeretlen formák, melyekre nézve továbbá még követeljük, hogy együtthatóik bizonyos meghatározott, előre megadott holoid tartományba tartozzanak. Ezt a problémát az elemi műveletek véges és teljesen meghatározott sorával teljesen megoldjuk mindazon esetekre nézve, melyek az algebrai mennyiségek elméletében számba jönnek; jelesen akkor, midőn a formák együtthatói valamely orthoid tartományhoz tartoznak, vagy pedig raczionális és egész számok.

Az első esetből kifolyólag teljesen tárgyaljuk ezután NOETHER tételét az n-méretű térben.

Magától értetődik, hogy evvel az a fontos, eddig alig érintett kérdés, hogy két osztórendszer mikor æquivalens,

szintén elintézést nyer; sőt a «tartalmazás» általánosabb kérdése is teljesen meg van oldva.

Az egész algebrai mennyiségek elméletében teljesen azonos módszerek egyidőben fölölelik az általános arithmetika szigorú értelmében («absolute») egész mennyiségeket, valamint a bizonyos orthoid tartományra vonatkozólag («relative») egész mennyiségeket. A második esetben a többiek közt megkapjuk a függvénytan vagy geometria értelmében egészeknek nevezendő mennyiségeket is. A tárgyalásnak egyik sarkalatos pontja, hogy az ideális mennyiségek kezdettől fogva mint nemcsak a szorzásnak, de az összeadásnak is alávethető mennyiségek szerepelnek. Ezen az alapon új és egyszerű módszer épül, melylyel az alaprendszert bármily esetben valóban kiszámíthatjuk, és a mely első sorban az «æquivalentia-modulus» elméletét használja föl. Végre megtörténik az egész mennyiségek fölbontása törzsideálokra, az ide vonatkozó KRONECKER-féle eredmények lényeges helyesbítésével. Ezek ugyanis egy igen érdekes, mélyebbre menő tévedés következtében csakis a legegyszerűbb esetekben helyesek; pedig eddigelé csakis ezeket tárgyalták.

Minden egyébre nézve a tartalomjegyzékre utalok, melyből a munka tartalma és beosztása tisztán látható. Remélem, hogy a munka végén álló részletes tárgymutató az olvasónak igen nagy kényelmére lesz; különösen pedig megadja majd a szükséges útmutatásokat az új műszókra nézve, melyeknek bevezetése ott, a hol történt, teljességgel elkerülhetetlennek mutatkozott.

Tekintettel az «Encyclopädie der math. Wissenschaften» című most megjelenő munkára az irodalom fölsorolásában csak annyira mentem, hogy az egyes tárgyalt tételek birtokviszonyai tisztáztassanak.

Végül még igaz hálával emlékezem meg Kürschák József, Rados Gusztáv, Rados Ignácz és Stäckel Pál uraknak fáradhatatlan és fölötte értékes közreműködéséről, kik a kéziratot és a correcturákat átvizsgálták, valamint megemlítem azt is, hogy e munka egyidőben német fordításban is megjelenik Lipcsében B. G. Teubner kiadásában.

Budapesten, 1902. junius.

Kőnig Gyula.

TARTALOMMUTATÓ.

ELSŐ FEJEZET.

Bevezető alapfogalmak.

Lap

Szám, mennyiség, tartomány. 1. § ... 1
Az összeadás és szorzás közönséges törvénye. 2.—3. § ... 4
Holoid és orthoid tartományok. 4. § ... 7
Az oszthatóság holoid tartományokban. 5. § ... 10
A legnagyobb közös osztó. 6. § ... 14
Példa: A $[\sqrt{-k}]$ tartományok. 7.—9. § ... 17
Congruentiatartományok és modulusrendszerek. 10.—11. § ... 25
Relativ æquivalentia. 12. § ... 29

MÁSODIK FEJEZET.

A holoid tartományokból származó formák.

Formák és egész függvények. 1.—2. § ... 33
A formák tagjainak lexikographikus elrendezése. 3.—4. § ... 37
A derivált formák. 5.—6. § ... 41
A polynomiális tétel. 7. § ... 45
Homogén formák. 8.—9. § ... 46
Az elemi symmetrikus formák. 10.—12. § ... 49
A redukált formák. 13.—16. § ... 57
Az egész függvények. 17. § ... 65
Lineáris transformatio. Szabályos formák. 18.—19. § ... 68

HARMADIK FEJEZET.

A formák oszthatósága.

A közönséges osztási eljárás. 1. § ... 73
Az oszthatóság kriteriuma a formatartományban. 2.—3. § ... 75
Dedekind segédtétele. 4. § ... 77

Lap
KRONECKER alaptétele. 5.—7. § ... 81
Teljes tartományokból származó formák. 8.—11. § ... 88
Teljes tartományok mellérendelt orthoid tartományai. 12. § ... 95
A resultáns. 13.—17. § ... 97
Formarendszerek resolvens formája. 18. § ... 107
Az egyenletek elméletének problémája. 19.—21. § ... 113
A forma discriminánsa 22.—23. § ... 122
A resultáns és discrimináns mint symmetrikus forma 24.—25. § 127

NEGYEDIK FEJEZET.

Az algebrai mennyiségek.

A raczionális és egész formák felbontása tényezőkre 1.—2. § ... 133
Felbontás tényezőkre orthoid tartományban 3.—4. § ... 138
Az egyenlet problémájának új fogalmazása. Az adjunctio. 5.—7. § ... 143
Hyperorthoid tartományok. 8.—9. § ... 151
A GALOIS-féle tartomány. 10.—13. § ... 157
A genus-tartományok. 14.—15. § ... 167
Genus-tartományok, a melyeknek törzstartományai is már genus-tartományok. 16.—19. § ... 173
Raczionális tartományok. 20.—22. § ... 183
GALOIS elve. 23.—26. § ... 193
GAUSS alaptétele. 27.—28. § ... 203

ÖTÖDIK FEJEZET.

Az elimináczió általános elmélete.

Az alap-probléma. 1. § ... 209
KRONECKER elimináczió-módszere. 2.—4. § ... 212
Az $F_j=0$ rendszer megoldásainak összessége. 5.—8. § ... 223
Tiszta sokaságok főelőállítása. 9.—10. § ... 240
Tetszés szerinti sokaságok előállítása $m+1$ egyenlet segítségével. 11. § ... 246
Egyenletrendszerek, a melyeknek tartalma lineáris sokaságot alkot. 12.—13. § ... 250
A függvénydeterminánsa. 14.—18. § ... 255

HATODIK FEJEZET.

Resultánsok és discriminánsok.

(Ú. n. speczialis eliminácziò-elmélet.)

Lap

Általános formák és az ezekre vonatkozó kérdéstétel. 1.—2. § ... 274
A resultáns értelmezése és alapvető tulajdonságai. 3.—6. § ... 280
A resultáns recursiv képezése. 7.—10. § ... 290
A resultánsok szorzástétele. 11. § ... 304
Homogén formák rendszerének resultánsa. Invariáns-tulajdonság. 12. § ... 306
Homogén egyenletek rendszere. 13. § ... 310
Határozott és határozatlan közönséges rendszerek. 14.—17. § ... 315
A mennyiségek több rendszerének symmetrikus formái. 18.—21. § 328
A függvénydeterminánsirreducibilis volta. 22. § ... 339
A discriminánsalaptulajdonságai. 23.—26. § ... 341
A discriminánsinvariáns-tulajdonsága. 27. § ... 351
A megoldások sokszorossága. 28.—30. § ... 354

HETEDIK FEJEZET.

Lineáris diophantikus problémák.

(Általános tételek és az algebrai elmélet.)

A probléma felállítása. 1. § ... 364
Modulusrendszerek vagy osztórendszerek. 2.—4. § ... 368
Véges osztó-lánczok. 5.—7. § ... 380
Az algebrai és arithmetikai probléma elkülönítése. 8. § ... 389
A lineáris diophantikus rendszerek algebrai elmélete. 9. § ... 391
A főosztályhoz tartozó osztórendszerek (a melyeknek elemei orthoid tartományból származó formák). 10.—11. § ... 395
Noether tételének általánosítása. 12.—13. § ... 404
A gyökrendszerek charakteristikájának elmélete az «egyszerű» esetben. 14.—15. § ... 411
Hilbert tétele. 16. § ... 416

NYOLCZADIK FEJEZET.

A linearis diophantikus problémák arithmetikai elmélete.

Lap

Az absolut törzsrendszerek $[[1], x_1, \ldots, x_k]$-ban. 1.—4. § ... 419
Osztórendszerek mod. $(P^{(k)})$. 5. § ... 434
A resolvens formák elmélete mod. $(P^{(k)})$. 6.—8. § ... 438
Genus-tartományok mod. $(P^{(k)})$. 9. § ... 450
A homogén lineáris diophantikus egyenlet arithmetikai megoldása. A reductio elvei. 10.—14. § ... 454
Az általános eset. 15.—18. § ... 465
A singuláris eset. 19. § ... 477

KILENCZEDIK FEJEZET.

Az egész algebrai mennyiségek.

Bevezető megállapodások. 1. § ... 480
Az egész algebrai mennyiségek és formák. 2.—3. § ... 485
A primitiv egész algebrai formák. 4.—6. § ... 489
Az ideális mennyiségek associatiója. 7.—9. § ... 496
Az ideálok oszthatósági elmélete. 10.—13. § ... 507
A genus-tartomány igazi mennyiségeinek alaprendszere. 14.—16. § 517
A formák æquivalentia-modulus szerint való oszthatósága. 17.—20. § 526
Az alaprendszerek felállítására szolgáló általános módszer. 21—23. § 537
A genus-tartomány ideális mennyiségeinek alaprendszere. 24.—25. § ... 551
Az egész mennyiségek felbontása törzsideálokra. 26.—29. § ... 559
A genus discriminánsa. 30.—31. § ... 573

Név- és tárgymutató. ... 579

ELSŐ FEJEZET.

BEVEZETŐ ALAPFOGALMAK.

Szám, mennyiség, tartomány.

1. §. Minden a tiszta mennyiségtan körében történő vizsgálat alapja *a raczionális számok tartománya*, azaz a pozitiv és negativ, egész és tört számok összessége, hozzáértve még a zérust is.

A raczionális számok tartományának *tulajdonságait* kizárólag azon törvények összessége alkotja, melyek szerint az úgynevezett négy alapműveletben e számok összekapcsolása történik.

Szám a szó legáltalánosabb értelmében minden oly fogalom, melynek tartalma teljesen leirható a raczionális számok bizonyos sorozata segítségével, mely különben utolsó elemzésben a pozitiv egész számok sorozatával is pótolható. A szám — ismét a szó legáltalánosabb értelmében — *algebrai*, ha e teljes leirásnál a pozitiv egész számoknak csak véges sorozatát használjuk.

Az algebrai szám, valamint később az algebrai mennyiség ily értelmezése a dolog természete szerint csak ideiglenes és hézagos lehet; mert hiszen ezen egész munkának föladata, hogy az algebrai mennyiség fogalmát fölépitsük és tartalmát kifejtsük. Ez az értelmezés mindenesetre *túlságosan bő*, mert világos ugyan, hogy amaz a pozitiv egész számok valamely véges sorozatával történendő leirás úgy

értendő, hogy e számok tulajdonságainak csakis a négy alapműveletben való összekapcsolásuk veendő; de ebből még semmiképp sem tudjuk, hogy miféleek az új fogalomnak azon tulajdonságai, melyek teljes leírásában használandók. Mint ilyenek a négy alapművelettel analog kapcsolatok lesznek megállapítandók, a mi azonban épen már részletesebb tárgyalást igényel.

Mathematikai *mennyiség* az oly szám, melynek néhány meghatározó adata *határozatlan* marad. E meghatározó adatok természetesen ismét csak számok. A legegyszerűbb esetben valamely határozatlan egész vagy raczionális szám is mennyiség. (Mennyiség továbbá — ha a példa kedvéért a végzendő fogalomalkotásnak elejébe vágunk — az $x_1, \ldots x_m$ határozatlanoknak minden egész függvénye adott számbeli együtthatókkal). Rövidebb kifejezésmódot elérendők, végre még a «mennyiség» általánosabb fogalmába beleértjük a «szám»-ot is.

Algebrai mennyiség tehát végre az oly fogalom, melynek tartalmát a meghatározott vagy határozatlan egész számok véges sorozata teljesen megadja*.

Az arithmetika és algebra tárgyául e szerint általánosságban kijelölhető azon egész függvények elmélete, melyeknek együtthatói ismét algebrai mennyiségek.

Az ily módon tervbe vett fogalomalkotásokat azonban még tovább is megszorítjuk.

* Ily értelemben használjuk e munkában — KRONECKER szerint — a «mennyiség» és «algebrai mennyiség» kifejezéseket; de hozzáteendő, hogy az arithmetika és algebra körén kívül e kifejezéseknek tágabb értelmük van. Így mennyiség a tárgyaknak minden oly tulajdonsága, mely számok segítségével teljesen leírható. A függvénytanban algebrai függvényeknek nevezzük az oly mennyiségeket, melyeket a meghatározott és határozatlan számok véges sorozata értelmez, akkor is, midőn e számok nem algebrai számok.

Azon tartomány, melyben minden egyes vizsgálatunk majdan történik, azaz azon mennyiségek összessége, melyeket egyidőben áttekintünk, olyan legyen, hogy benne a raczionális számok tartományának jellemző tulajdonságai megmaradjanak. Azaz pontosabb kifejezésben *a vizsgálandó tartomány mennyiségei számára csakis oly kapcsolatokat állapítunk meg, melyeknek alaki törvényei teljesen egybehangzanak azokkal, melyeket a raczionális számok tartományában a négy alapmüvelet követ.*

Kényelmes lesz, ha e kapcsolatokat, a mennyiben egyáltalában léteznek, az új tartományban is az összeadás, kivonás, szorzás, ill. osztás nevével jelöljük.

Vizsgálataink kiinduló pontján csakis két tartomány áll rendelkezésünkre, az egész számok tartománya és a raczionális számok tartománya, mely tartományok tartalmát és tulajdonságait az elemekből ismerjük. Szoros módszertani következetességgel csak akkor beszélhetünk valamely új tartomány mennyiségeinek kapcsolásáról, ha e mennyiségeknek teljes értelmezése minden egyes esetben megtörtént; a mi különben, minthogy e kapcsolatok a vizsgálandó mennyiségek egyetlen «tulajdonságait» alkotják, épen csak e kapcsolási törvények megállapításával történhetik. Szóval minden további lépés valójában csak meghatározott, specziális új fogalom megalkotásával történhetik. Hogy azonban az ezzel járó folytonos és elég terjedelmes ismétléseket elkerüljük, a tartományoknak ama nagy osztályait, melyekkel folyton dolgunk lesz, egyszer mindenkorra jellemezzük és neveket adunk nekik. Ezt azonban most csak a legegyszerűbb esetekre végezzük; bonyolódottabb esetek tárgyalását, melyek kellő példák nélkül nehezebben tekinthetők át, későbbre tartva fönn magunknak.

Külön kiemelendő még, hogy e fejtegetések tulajdon-

képen még a mathematikai logika körébe tartoznak, és mint ilyenek, messze túlmenvén az arithmetika és algebra határain, az analizis tágabb keretében is érvényesíthetők.

Az összeadás és szorzás közönséges törvénye.

2. §. Legyen e szerint adva a mennyiségeknek bizonyos (véges vagy végtelen) sorozata *:

$$\alpha_1, \alpha_2, \alpha_3, \ldots,$$

melyeknek összessége az A tartományt alkotja.

Az A tartomány az összeadás közönséges törvényét követi, ha a következő föltételeknek megfelel:

a) Valamely adott megállapodás értelmében a tartomány két mennyisége α_1 és α_2 mindig meghatároz egy harmadik mennyiséget, σ-t, melyet az α_1 és α_2 összegének nevezünk és $\alpha_1+\alpha_2$-vel jelölünk.

b) Mindenkor

$$\alpha_1+\alpha_2=\alpha_2+\alpha_1$$

és

$$(\alpha_1+\alpha_2)+\alpha_3=\alpha_1+(\alpha_2+\alpha_3);$$

a mit ismeretes kifejezésmóddal élve úgy szokás kimondani, hogy az összeadás commutativ és associativ.

c) Ha α_1 és α_2 a tartomány bármely két mennyisége, akkor mindig van egy és csak egy olyan ξ mennyiség, hogy

$$\alpha_1+\xi=\alpha_2.$$

Ismeretes kifejezésmóddal élve ezt úgy szokás kimondani, hogy az összeadás megfordítása, a kivonás egyértelmű és mindig végrehajtható. Ekkor azt írjuk, hogy

$$\xi=\alpha_2-\alpha_1.$$

* A mutatók használata α_1 sat.) semmiképp se jelentse az elemek valami meghatározott sorozását és még kevésbbé azt, hogy a közönséges egész számok sorával ezen elemek kölcsönös egyértelmű vonatkozásban állanak. Egyszerűen kényelmi okokból használt jelzés.

Az $\alpha_1+\alpha_2+\cdots+\alpha_n$ összeget recursiv eljárással mint $(\alpha_1+\cdots+\alpha_{n-1})+\alpha_n$-t értelmezzük. Erről az összegről, a következtetés egy módjával, a melyet úgy látszik LEJEUNE-DIRICHLET adott meg először pontosan *, kimutatjuk, hogy az $\alpha_1, \alpha_2, \ldots, \alpha_n$ összeadandók sorrendjétől független.

Ha α bármely mennyiséget és 0 oly mennyiséget jelent, melyre nézve mindig

$$\alpha+0=\alpha,$$

akkor a már eddig felsorolt feltételekből következik, hogy *egy és csak egy ilyen tulajdonságú mennyiség van. Ezt «zérus»-nak nevezzük.* Ha ugyanis α_1 valamely meghatározott mennyiséget jelent, akkor 0 egyértelmű meghatározására minden esetre szolgálhat az

$$\alpha_1+0=\alpha_1$$

feltétel, és ha α_2 valamely más mennyiséget jelent, az

$$\alpha_1+\beta=\alpha_2$$

feltétel minden esetre megállapítja a β mennyiséget, és

$$\alpha_1+0+\beta=\alpha_1+\beta,$$

a miből végre:

$$\alpha_2+0=\alpha_2.$$

3. §. *Az* A *tartomány a szorzás közönséges törvényét követi*, ha kielégíti a következő feltételeket:

a) A tartomány két mennyisége: α_1 és α_2 bizonyos megállapodás értelmében mindig meghatároz egy harmadikat: π-t, a melyet az α_1 és α_2 mennyiségek szorzatának nevezünk és $\alpha_1\alpha_2$-vel jelölünk.

b) Mindenkor:

$$\alpha_1\alpha_2=\alpha_2\alpha_1$$

és

$$(\alpha_1\alpha_2)\alpha_3=\alpha_1(\alpha_2\alpha_3).$$

* Vorlesungen über Zahlentheorie von P. G. LEJEUNE-DIRICHLET, herausgegeben von R. DEDEKIND. IV. kiad. 3. l.

a mit ismeretes kifejezésmóddal élve úgy szokás kimondani, hogy a szorzás törvénye commutativ és associativ.

c) Ha az A tartomány egyszersmind az összeadás közönséges törvényét is követi, akkor

$$(\alpha_1 + \alpha_2)\alpha_3 = \alpha_1\alpha_3 + \alpha_2\alpha_3,$$

vagyis ebben az esetben — a mint azt ismeretes módon szokás kifejezni — a szorzás törvénye még distributiv is.

d) Vagy egyáltalában nincsen, vagy pedig, ha van, csak egy olyan singuláris δ mennyiség van, hogy

$$\delta\xi = \delta\eta,$$

ámbár a meghatározott ξ és η mennyiségek egymástól különbözők.

Ha α valamely tetszés szerinti mennyiség, akkor abból, hogy $\delta\xi = \delta\eta$, következik, hogy

$$(\delta\alpha)\xi = (\delta\alpha)\eta.$$

Megállapodásaink értelmében tehát, a tartománynak bármely mennyisége is α, mindig:

$$\delta\alpha = \delta.$$

Ezért ezt a singuláris δ mennyiséget 0-sal jelölhetjük. E jelt eddig csak abban az esetben használtuk, midőn a tartomány az összeadás közönséges törvényét is követi. De akkor

$$(\beta + 0)\alpha = \beta\alpha + 0\alpha = \beta\alpha;$$

tehát $0\alpha = 0$ és minthogy egynél több ilyen singuláris mennyiség nincsen, $\delta = 0$.

Ha tehát valamely tartomány a szorzás közönséges törvényét követi, akkor csak úgy lehetséges, hogy $\alpha\beta = 0$, ha vagy $\alpha = 0$, vagy pedig $\beta = 0$; mert, ha α nem zérus, akkor $\alpha\beta = 0$ és $\alpha . 0 = 0$-ból következik, hogy $\beta = 0$.

Még megemlítjük, hogy az $\alpha_1\alpha_2 \ldots \alpha_n$ szorzatot recursiv eljárással mint $(\alpha_1 \ldots \alpha_{n-1})\alpha_n$-t értelmezzük. A következtetés ama módjával, a melyre már az összeadásnál utal-

tunk, e szorzatról is kimutatható, hogy az $\alpha_1, \alpha_2, \ldots, \alpha_n$ tényezők sorrendjétől független.

Ha ε és ξ az A tartománynak két meghatározott a 0-tól különböző mennyisége, a melyeknek szorzata $\varepsilon\xi=\xi$, akkor bármely mennyiség legyen α, egyszersmind $\varepsilon\alpha=\alpha$. Ha ugyanis

$$\varepsilon\alpha=\beta$$

volna, a hol β az α-tól különböző, ebből, minthogy $\varepsilon\xi=\xi$, következnék, hogy

$$(\varepsilon\xi)\beta=(\varepsilon\xi)\alpha,$$

a mi csak úgy lehetséges, ha ellenkezésben feltevésünkkel $\varepsilon\xi=0$ volna. Az ε-tól különböző oly ε_1 mennyiség, a melyben meg volna az ε most részletezett tulajdonsága, egyáltalában nincsen, mert ekkor $\varepsilon\varepsilon_1=\varepsilon=\varepsilon_1$.

Az ε mennyiséget — ha az A tartományban egyáltalában előfordul — a tartomány *absolut egységének* nevezzük és 1-gyel jelöljük.

Holoid és orthoid tartományok.

4. §. *Holoidnak* * *nevezünk valamely tartományt, ha az összeadás és szorzás közönséges törvényét követi, az absolut egységet tartalmazza és az* 1 *ismételt összeadásából származó mennyiségsorozat*

$$1,\ 1+1,\ 1+1+1,\ \ldots$$

nem tartalmazza a 0 *mennyiséget.*

Egyelőre ezeknek a mennyiségeknek jelölésére fel-

* A «holoid» és «orthoid» új szóképzések arra valók, hogy kifejezzék a tartományok általános tulajdonságait s eredetüknek megfelelőleg arra emlékeztessenek, hogy az új tartományok az egész, ill. raczionális számok tartományának lényeges tulajdonságait megtartják. Az egyes valósággal megalkotott tartományokra megtartjuk a Gauss-Kronecker-féle terminologiát.

használhatjuk a közönséges egész számok jeleit ily módon:

$$(1), (2), (3), (4), \ldots, (m), \ldots$$

és azután rögtön felismerjük, hogy e sorozatban egyetlen egy mennyiség sem ismétlődik. Abból ugyanis, hogy (m) és $(m+k)$ ugyanazt a mennyiséget jelentik, szükségkép folyna, hogy:

$$(m+k)=(m)+(k)=(m),$$

azaz, hogy a vizsgált tartományban $(k)=0$.

Ebből azonban következik, hogy az (m) jel az m egész számmal azonosnak tekinthető, mert a (közönséges) összeadás és szorzás törvényei alapján megállapított tulajdonságok — az egyetlenek, melyek egyáltalában szóba kerülnek, — mindkét jelre nézve ugyanazok. Azaz pontos kifejezésben:

$$(m)+(n)=(m+n); \quad (m)(n)=(mn).$$

Továbbá még:

$$-1-1-\cdots=(-m)=-(m).$$

Ezt az eredményt még a következő módon is fogalmazhatjuk: *Minden holoid tartomány magában foglalja az egész számok tartományát*, azaz az összes egész számokat, beleértve a zérust is.

Azt mondjuk, hogy «az

$$\alpha\xi=\beta$$

egyenlet az adott tartományban megoldható», ha ebben található olyan ξ_1 mennyiség, a melyre nézve valóban $\alpha\xi_1=\beta$.

A tartomány *valódi holoid tartomány*, ha találhatunk benne oly két, a 0-tól különböző mennyiséget, a melyekre nézve az $\alpha\xi=\beta$ egyenlet nem oldható meg. A tartomány *orthoid* vagy *nem valódi holoid tartomány*, ha mindig van oly ξ_1 mennyiség, melyre nézve $\alpha\xi_1=\beta$, ha csak α a 0-tól különböző.

Az egész számok tartománya tehát valódi holoid tartomány, a raczionális számoké nem valódi holoid vagyis

orthoid tartomány. Az előbbinek jelölésére az [1], az utóbbiéra pedig az (1) symbolumot fogjuk használni.

Új mennyiségek hozzácsatolásával, «adjunctio»-jával minden holoid tartomány kibővíthető orthoid tartománynyá.

Az ujonnan hozzácsatolandó mennyiségeket (egyelőre még csak jelképileg) mindjárt a $\frac{\beta}{\alpha}$ alakban írhatjuk, hol α és β az eredeti holoid tartomány bármely két mennyisége, de α a 0-tól különböző. Megállapítjuk továbbá még azt is, hogy $\frac{\beta_1}{\alpha_1}$ és $\frac{\beta_2}{\alpha_2}$ csakis akkor jelentsenek különböző mennyiségeket, ha $\alpha_1\beta_2 - \alpha_2\beta_1$ a 0-tól különböző.

Valamely tartomány értelmezésénél az ily megállapítások feltétlenül jogosak és módszertani szempontból igen fontos segédeszközül szolgálnak új tartományok alkotásánál. De már itt is kiemeljük, hogy ez arra az újabb arithmetikai, ill. algebrai követelményre vezet, hogy a bővített tartomány minden mennyisége egyértelműleg meghatározott «canonicus» alakban állíttassék elő.

Ha a $\frac{\beta}{\alpha}$ «mennyiségek» tartományára az összeadás és szorzás következő törvényét állapítjuk meg:

$$\frac{\beta_1}{\alpha_1} + \frac{\beta_2}{\alpha_2} = \frac{\beta_1\alpha_2 + \beta_2\alpha_1}{\alpha_1\alpha_2},$$

$$\frac{\beta_1}{\alpha_1}\,\frac{\beta_2}{\alpha_2} = \frac{\beta_1\beta_2}{\alpha_1\alpha_2},$$

akkor a közönséges arithmetikában szokásos következtetéseket ismételve, felismerjük, hogy az összeadás és szorzás e törvénye «közönséges»; hogy az előbb adott értelmezés szerint nem különböző, vagyis «egyenlő» mennyiségek egymás helyébe téve, az összeadás vagy szorzás eredményét nem változtatják; továbbá, hogy a $\frac{0}{\alpha}$ mennyiség a zérus, az $\frac{\alpha}{\alpha}$ mennyiség az absolut egység és végre hogy a $\frac{\beta}{1}$ mennyiségek tulajdonságai ugyanazok, mint a β mennyiségekéi. A következőkben tehát $\frac{\beta}{1}$ helyett mindenütt

egyszerűbben β-t írhatunk. Ha β_1 a 0-tól különböző, akkor a

$$\frac{\beta_1}{\alpha_1}\xi = \frac{\beta_2}{\alpha_2}$$

egyenlet megoldása a

$$\xi = \frac{\alpha_1 \beta_2}{\alpha_2 \beta_1}$$

mennyiség; (α_1 és α_2 a feltevés szerint a 0-tól különböző). E mellett most $\frac{\beta}{\alpha}$ az $\alpha\xi = \beta$ egyenlet megoldása, vagyis a β-nak α-val való osztásánál föllépő eredmény.

Az így szerkesztett tartományt az eredeti holoid tartomány *mellérendelt* orthoid tartományának nevezzük. A mellérendelt tartomány egybeesik az eredetivel, ha ez nem valódi holoid, azaz már maga is orthoid tartomány. Ezentúl az eredeti holoid tartományt [A]-val, a mellérendelt orthoid tartományt pedig (A)-val fogjuk jelölni.

Mint e fejtegetésekből következik, *minden orthoid tartomány magában foglalja a raczionális számok tartományát.*

Az oszthatóság holoid tartományokban.

5. §. Ha α és β az adott holoid tartomány mennyiségei és az

$$\alpha\xi = \beta$$

egyenlet megoldható, akkor azt mondjuk, hogy α a β *osztója* és β az α *többszöröse.*

E szerint nem valódi holoid tartományokban minden mennyiség minden 0-tól különböző mennyiséggel osztható. Beszélhetünk tehát ebben az esetben is oszthatóságról; csakhogy itt az nem vezet a tartományban foglalt mennyiségeknek új fogalmi elkülönítésére.

Minden valódi holoid tartományban a 0 az egyetlen mennyiség, a mely a tartomány minden 0-tól különböző mennyiségével osztható. Ugyanis, ha γ ilyen mennyiség

volna, és γ nem zérus, akkor az osztható volna γ^2-vel is és $\gamma = \gamma^2 \xi_1$-ből következnék, hogy $1 = \gamma\xi_1$; γ tehát osztója volna az absolut egységnek. Továbbá még bármely a 0-tól különböző α-nak megfelelőleg bizonyos η mennyiség úgy volna meghatározható, hogy:

$$\alpha\eta = \gamma, \quad \alpha\eta\xi_1 = 1,$$

és így még

$$\alpha(\eta\xi_1\beta) = \beta.$$

Azaz az $\alpha\xi = \beta$ egyenlet mindig megoldható volna, és a tartomány nem volna valódi holoid tartomány.

Minden valódi holoid tartományban tehát valamely a 0-tól különböző mennyiség osztói a tartomány valódi részletsokaságát alkotják, azaz oly sokaságot, a mely még a 0 kizárása után sem foglalja magában a tartomány összes mennyiségeit.

Különösen kiemelendő: Ha α nem osztója β-nak, akkor $\mu\alpha$ sem osztója β-nak.

Az oszthatóság két elemi törvénye közvetetlenül az oszthatóság értelmezéséből következik. E törvények a következők:

I. *Ha γ osztható β-val és β osztható α-val, akkor γ is osztható α-val.*

II. *Ha β és γ osztható α-val, míg λ és μ a tartomány bármely két mennyisége, akkor $\lambda\beta + \mu\gamma$ is osztható α-val.*

Egységnek nevezzük a tartomány minden oly mennyiségét, a mely az absolut egységnek osztója. E definicziónak közvetetlen folyományai a következők:

A tartomány minden mennyisége minden egységgel osztható.

Két egység szorzata ismét egység.

Minden ε_1 egységhez ugyanis tartozik egy másik ε_2 egység oly módon, hogy $\varepsilon_1\varepsilon_2 = 1$. Igy tehát valóban

$$\alpha = \varepsilon_1(\varepsilon_2\alpha)$$

és

$$(\varepsilon_1\varepsilon_1')(\varepsilon_2\varepsilon_2') = 1.$$

A tartomány két mennyiségéről azt mondjuk, hogy *aequivalens* (vagy pontosabban, t. i. ellentétben a később bevezetendő relativ æquivalentiával *absolute aequivalens*), ha mindegyikük a másikkal osztható.

A tartomány két mennyisége tehát akkor és csak akkor æquivalens, ha mindegyikük a másikból úgy származik, hogy valamely egységgel megszorozzuk.

Ha ugyanis α és β æquivalensek, akkor az értelmezés szerint

$$\alpha = \beta\mu, \quad \beta = \alpha\nu.$$

Igy tehát vagy mind a kettő 0, vagy pedig mind a kettő a 0-tól különböző. Az utóbbi esetben azonban $\mu\nu = 1$ és ezért úgy μ mint ν egység. Viszont, ha $\alpha = \beta\varepsilon_1$ és $\varepsilon_1\varepsilon_2 = 1$, ezekből következik, hogy $\alpha\varepsilon_2 = \beta$.

Azt, hogy α æquivalens β-val, a következő jelöléssel fejezzük ki:

$$\alpha \sim \beta.$$

Hogy a holoid tartományra, vagy pedig annak egységeire pontosabban reá mutassunk, körülbelül a következő módon:

$$\alpha \sim \beta, \ [\mathrm{A}],$$

az majdnem mindenütt felesleges, mert az ezekre vonatkozó feltevések ugyanazon vizsgálat folyamában rendesen változatlanok maradnak.

Az æquivalentia fogalma az egyenlőség fogalmának bővítése. Egyenlő mennyiségek egyszersmind æquivalensek is és az æquivalentia jele ugyanazt az alaptörvényt követi, mint az egyenlőség jele. Ez az alaptörvény a következő:

Ha $\alpha \sim \beta$ és $\beta \sim \gamma$, akkor egyszersmind $\alpha \sim \gamma$.

A mennyiben a szorzást is tekintetbe veszszük, tovább fűzve az analogiát, még a következő tételeket nyerjük:

Ha $\alpha_1 \sim \beta_1$ *és* $\alpha_2 \sim \beta_2$, *akkor* $\alpha_1\alpha_2 \sim \beta_1\beta_2$.
Ha $\alpha_1\alpha_2 \sim \beta_1\beta_2$ *és* $\alpha_2 \sim \beta_2$, *de* β_2 *nem* 0, *akkor* $\alpha_1 \sim \beta_1$.

E tételek helyességéről úgy győződhetünk meg, ha bevezetjük az ε_1, ε_2 és $\varepsilon_1\varepsilon_2 = \varepsilon_3$ egységeket és az æquivalentia jele helyett az egyenlőség jelét használjuk. Igy pl. a második tételben $\alpha_1\alpha_2 = \beta_1\beta_2\varepsilon_3$, $\alpha_2 = \beta_2\varepsilon_2$; tehát $\alpha_1\beta_2\varepsilon_2 = \beta_1\beta_2\varepsilon_3$ és $\alpha_1\varepsilon_2 = \beta_1\varepsilon_3$. De minthogy $\varepsilon_3 = \varepsilon_1\varepsilon_2$, ebből végre következik, hogy $\alpha_1 = \beta_1\varepsilon_1$.

Még megjegyzendő, hogy az $\alpha \sim 0$ állításnak mindig következménye, hogy $\alpha = 0$.

A raczionális egész számok tartományában az egyetlen egységek $+1$ és -1. Ezért e tartományban két szám æquivalens volta egyszerűen csak azt fejezi ki, hogy e két szám vagy egyenlő egymással, vagy pedig csak az «előjelben» különbözik egymástól.

E felfogás szerint a raczionális számok tartományában, valamint minden nem valódi holoid tartományban a 0 kivételével az összes számok, ill. mennyiségek egységek. Az æquivalentia fogalma alapján tehát ezek a számok két osztályba válnak szét, a melyek közül az egyik csupán csak a 0-t, a másik pedig az összes többi számokat, ill. mennyiségeket foglalja magában.

Ha α a β osztója és az $\alpha \sim 1$, $\alpha \sim \beta$ relácziók közül egyik sem áll fenn, akkor α a β *valódi osztója.*

A holoid tartomány valamely mennyisége *irreducibilis*, ha nincsen valódi osztója.

Az irreducibilis mennyiségek vagy egységek, vagy pedig, ha nem azok, *valódi irreducibilis mennyiségek.*

E szerint az [1], azaz a raczionális egész számok tar-

tományának valódi irreducibilis mennyiségei a «természetes törzsszámok», 2, 3, 5, ...

Törzsmennyiségnek (prim-mennyiségnek) nevezünk valamely π mennyiséget akkor, ha sem 0, sem egység és bármely $\alpha\beta$ szorzat csak úgy osztható π-vel, ha vagy α, vagy pedig β osztható π-vel.

E szerint minden törzsmennyiség π egyszersmind irreducibilis is; mert ha $\pi=\pi_1\pi_2$ és sem π_1, sem pedig π_2 nem egység, akkor $\pi_1\pi_2$ oly π-vel osztható szorzat volna, a melynek egyik tényezője sem osztható π-vel. Ha ugyanis pl. π_1 osztható volna π-vel, akkor, minthogy π is osztható π_1-gyel, feltevésünk ellenére π_2-nek egységnek kellene lennie.

Az [1] tartományban a törzsmennyiségek egybeesnek a valódi irreducibilis mennyiségekkel és ezért azok ismét a természetes törzsszámok. (Lásd a következő §-nak V. tételét.)

Általánosságban minden törzsmennyiség irreducibilis is, de azért nem minden valódi irreducibilis mennyiség egyszersmind törzsmennyiség is, a mint ez már az e fejezet 9. §-ának végén tárgyalandó példából ki fog tünni.

A legnagyobb közös osztó.

6. §. Ha α és β a holoid tartomány két mennyisége és δ ugyanannak a tartománynak oly mennyisége, hogy α és β osztható δ-val, továbbá minden oly mennyiség, mely α és β osztója, a δ-nak is osztója, akkor δ-t az α és β *legnagyobb közös osztójának* nevezzük és (α, β)-val jelöljük.

Minden mennyiség, a mely $\sim \delta$-val, kielégíti a δ-ra kiszabott feltételeket. Ha pedig megfordítva úgy δ, mint δ' az α és β legnagyobb közös osztójára nézve megszabott követelményeknek megfelel, akkor δ osztható δ'-val és δ' oszt-

ható δ-val, azaz $\delta \sim \delta'$. A legnagyobb közös osztó meghatározása tehát, a mennyiben ilyen egyáltalában létezik, æquivalentia-meghatározás és azért úgy írjuk, hogy

$$(\alpha, \beta) \sim \delta.$$

Megemlítendő, hogy ha α bármely mennyiség, $(\alpha, 0) \sim \alpha$ és ha ε egység, akkor $(\alpha, \varepsilon) \sim 1$.

Teljesnek nevezzük az adott holoid tartományt akkor, ha a tartomány bármely két α és β mennyiségéből álló párhoz a tartományon belül meghatározhatunk oly δ mennyiséget, a mely α-nak és β-nak legnagyobb közös osztója.

Az elemekből ismeretes tételek szerint tehát a racionális egész számok tartománya teljes holoid tartomány.

Teljes holoid tartományokban a következő alapvető tételek érvényesek:

I. A tartomány tetszés szerinti n mennyiségének, α_1, $\alpha_2, \ldots, \alpha_n$-nek van legnagyobb közös osztója: δ abban az értelemben, hogy δ mindegyik α-nak osztója és viszont minden mennyiség, a mely az összes α-k osztója, osztója egyszersmind δ-nak is.

Ha ismét azt írjuk, hogy $(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim \delta$, akkor δ-t recursiv meghatározással a következő módon is adhatjuk meg:

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim ((\alpha_1, \alpha_2, \ldots, \alpha_{n-1}), \alpha_n),$$

a minek helyessége közvetetlenül a legnagyobb közös osztó értelmezéséből következik. Közvetetlenül világos továbbá az is, hogy

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim ((\alpha_1, \ldots, \alpha_k), (\alpha_{k+1}, \ldots, \alpha_n)).$$

II. Ép úgy világos, hogy, ha

$$\alpha_1 \sim \beta_1, \alpha_2 \sim \beta_2, \ldots, \alpha_n \sim \beta_n,$$

akkor mindig lesz:

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim (\beta_1, \beta_2, \ldots, \beta_n).$$

III. Továbbá

$$(\alpha_1\mu, \alpha_2\mu, \ldots, \alpha_n\mu) \sim (\alpha_1, \alpha_2, \ldots, \alpha_n)\mu.$$

A baloldali mennyiség ugyanis minden esetre többszöröse μ-nek és ezért ilyen alakú: $\delta\mu$. Hogy azonban $\delta\mu$ az $\alpha_1\mu, \alpha_2\mu, \ldots, \alpha_n\mu$ mennyiségeknek legnagyobb közös osztója lehessen, arra szükséges, hogy egyrészt minden egyes $\alpha\mu$ mennyiség osztható legyen $\delta\mu$-vel és így minden egyes α a δ-val; másrészt pedig, ha δ' az összes α-knak valamely közös osztója, szükséges, hogy $\delta\mu$ osztható legyen $\delta'\mu$-vel, azaz δ a δ'-val. Igy tehát valóban $\delta \sim (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

E tétel egyik fontos corollariuma a következő:

Ha $(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim \delta$ és $\alpha_i \sim \delta\beta_i$, akkor (kivéve azt az esetet, a melyben δ és így az összes α-k is egyenlők 0-sal) ebből következik, hogy

$$(\beta_1, \beta_2, \ldots, \beta_n) \sim 1.$$

Ha ugyanis $(\beta_1, \beta_2, \ldots, \beta_n) \sim \delta'$, akkor III-ból következik, hogy

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim \delta\delta';$$

tehát $\delta\delta' \sim \delta$ és $\delta' \sim 1$.

IV. *Ha* $(\mu, \nu) \sim 1$, *akkor* $(\alpha\mu, \nu) \sim (\alpha, \nu)$.

Ugyanis $\alpha\mu$ és ν legnagyobb közös osztója minden esetre $\alpha\mu$ és $\alpha\nu$-nek is közös osztója; tehát osztója egyszersmind a következő mennyiségnek is: $(\alpha\mu, \alpha\nu) \sim \alpha(\mu, \nu) \sim \alpha$. Ezért

$$(\alpha\mu, \nu) \sim (\alpha\mu, \alpha, \nu) \sim ((\alpha\mu, \alpha), \nu) \sim (\alpha, \nu).$$

Különösen, ha $(\mu, \nu) \sim 1$, akkor — ha r és s pozitiv egész számok — egyszersmind $(\mu^r, \nu^s) \sim 1$. Az előbbi szerint ugyanis:

$$(\mu^r, \nu) \sim (\mu^{r-1}, \nu) \sim \cdots \sim (\mu, \nu) \sim 1$$

és

$$(\mu^r, \nu^s) \sim (\mu^r, \nu^{s-1}) \cdots \sim (\mu^r, \nu) \sim 1.$$

V. *Ha* π *irreducibilis mennyiség és* $\alpha\beta$ *osztható* π*-vel,*

akkor már vagy α, vagy pedig β osztható π-vel; azaz teljes holoid tartományban minden irreducibilis mennyiség törzsmennyiség.

Mert, ha π irreducibilis, akkor vagy $(\gamma, \pi) \sim 1$, vagy pedig $(\gamma, \pi) \sim \pi$. Ha már mostan α nem osztható π-vel, akkor $(\alpha, \pi) \sim 1$. De, ha β sem osztható π-vel, akkor egyszersmind $(\beta, \pi) \sim 1$ és ezért a feltevés ellenére volna $(\alpha\beta, \pi) \sim (\alpha, \pi) \sim 1$.

Példa: A $[\sqrt{-k}]$ tartományok.

7. §. Az oly olvasó kedvéért, a ki legelőször csak ebben a tárgyalásban ismerkedik meg részletesebben az arithmetika és algebra általánosabb fogalomalkotásaival, a rendszeres tárgyalás megszakításával, szemléletének mintegy támogatására már itt mutatjuk be az oly holoid tartományok példáját, melyek bővítései ugyan a raczionális egész számok tartományának, de azért még sem mutatják e legegyszerűbb typusnak a legnagyobb közös osztóra vonatkozó tulajdonságait, jelesen már nem teljes holoid tartományok.

Az értelmezendő tartomány «számai» legyenek az (a, b) számpárok, a melyekben a és b közönséges egész számok. Az összeadás és szorzás kövessék a következő képletekben kifejezett törvényeket:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2 - k b_1 b_2, a_1 b_2 + a_2 b_1),$$

a hol k bizonyos meghatározott pozitiv egész számot jelent.

Hogy az összeadás és szorzás így megállapított törvényei «közönségesek», könnyen belátható.

Hogy mind a két törvény commutativ és associativ, az közvetetlenül világos, valamint az is, hogy a szorzás törvénye distributiv. A (0, 0) szám a tartomány egyetlen zérusa.

Ha ugyanis (a_1, b_1) különböző $(0, 0)$-tól, akkor abból, hogy

$$(a_1, b_1)(a_2, b_2) = (a_1, b_1)(a_3, b_3), \tag{1}$$

vagyis az

$$\begin{aligned} a_1a_2 - kb_1b_2 &= a_1a_3 - kb_1b_3, \\ a_1b_2 + a_2b_1 &= a_1b_3 + a_3b_1 \end{aligned}$$

egyenletekből, a melyek a következő alakban is írhatók:

$$\begin{aligned} a_1(a_2-a_3) - kb_1(b_2-b_3) &= 0, \\ b_1(a_2-a_3) + a_1(b_2-b_3) &= 0 \end{aligned} \tag{2}$$

következik, hogy

$$a_2-a_3=0, \quad b_2-b_3=0.$$

Tekintsük ugyanis a_2-a_3-mat és b_2-b_3-mat, mint ismeretleneket a (2) alatti lineáris homogén egyenletekben; akkor kiadódik, hogy értékeik egyenlők zérussal; mert az amaz egyenletek együtthatóiból alakított determináns: $a_1^2+kb_1^2$ feltevéseink alapján a zérustól különböző.

A tartomány magában foglalja az absolut egységet; ez $(1, 0)$. Ennek ismételt összeadásából származnak a $(2, 0)$, $(3, 0)$, ... számok; de a zérus sohasem.

E szerint tehát az a tartomány, a mely az összes (a, b) számokból áll, holoid tartomány; még pedig valódi holoid tartomány, mert pl. a

$$(2, 0)(x, y) = (1, 0)$$

egyenlet nem oldható meg benne. Annak feltételei ugyanis, hogy ez az egyenlet ki legyen elégítve, a következők:

$$2x = 1, \quad 2y = 0.$$

Ez pedig mutatja, hogy nincs olyan egész számokból összeállított (x, y) számpár, a mely amaz egyenletet kielégítené.

Hogy a tartomány számait lehetőleg egyszerűen jelölhessük (és egyszersmind lehetőleg egyszerűen le is írhassuk), vegyük tekintetbe, hogy az $(m, 0)$ és $(n, 0)$ számokra nézve a következők érvényesek:

$$\begin{aligned} (m, 0) + (n, 0) &= (m+n, 0), \\ (m, 0)(n, 0) &= (mn, 0), \end{aligned}$$

azaz, hogy e számok pontosan a közönséges egész számokra érvényes törvényeket követik. Ezért tehát a tartományon belül $(m, 0)$ helyett egyszerűen m-et írhatunk, mert e két szám «tulajdonságai» legalább annyira, a mennyire azok az m közönséges egész számokra vonatkozólag meg vannak állapítva, megegyeznek.

Vegyük továbbá tekintetbe, hogy

$$(0, 1)(a, b) = (-kb, a)$$

és különösen, hogy

$$(0, 1)(a, 0) = (0, a).$$

Ennek alapján lesz :

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + b(0, 1).$$

Most még egy a $(0, 1)$ jelölésére szolgáló külön jelt akarunk bevezetni ; támaszkodva arra a körülményre, hogy

$$(0, 1)(0, 1) = (-k, 0) = -k,$$

és csatlakozva az elemi algebra jelölés-módjához, azt írjuk :

$$(0, 1) = \sqrt{-k}.$$

Ezek után végre az (a, b) számot $a+b\sqrt{-k}$-val jelölhetjük és az $a+b\sqrt{-k}$ számok összekapcsolása az összeadásnál és szorzásnál «az algebra közönséges törvényei szerint» történik.

Ha mint itten feltételeztük, a és b az [1] tartományhoz tartozó számok, az $a+b\sqrt{-k}$ számok tartományát a $[\sqrt{-k}]$ symbolummal fogjuk jelölni.

A $[\sqrt{-k}]$ *tartomány egységeit* igen egyszerű módon határozhatjuk meg. Hogy $x+y\sqrt{-k}$ egység lehessen, arra szükséges, hogy a tartomány magában foglaljon oly $u+v\sqrt{-k}$ számot, a melyre nézve

$$(x+y\sqrt{-k})(u+v\sqrt{-k}) = 1,$$

és így evvel együtt egyszersmind

$$(x-y\sqrt{-k})(u-v\sqrt{-k}) = 1.$$

De akkor

$$(x^2+ky^2)(u^2+k^2v^2)=1$$

és minthogy a bal oldalon a tényezők közönséges egész számok, a melyek sohasem negativok, egyszersmind:

$$x^2+k^2y^2=1.$$

Innen kezdve a $k=1$ és $k>1$ esetek szétválasztandók.

Ha $k=1$, akkor lesz vagy $x=\pm 1$, $y=0$, vagy pedig $x=0$, $y=\pm 1$. A $[\sqrt{-1}]$ tartomány tehát a következő négy egységet tartalmazza: $1, -1, \sqrt{-1}, -\sqrt{-1}$. E tartomány az ú. n. *közönséges complex egész számok tartománya*, a melynek részletesebb tárgyalását itt mellőzzük *.

Ha $k>1$, akkor a közönséges egész számoknak $x=\pm 1$, $y=0$ rendszerei az egyetlenek, a melyek az $x^2+ky^2=1$ egyenletet kielégítik. Ezért a $k>1$ esetében a $[\sqrt{-k}]$ tartomány csupán csak ezt a két egységet tartalmazza: $1, -1$.

Eldöntendők, vajjon $u+v\sqrt{-k}$ osztója-e $a+b\sqrt{-k}$-nak, vegyük figyelembe e követelés szükséges és elegendő feltételét. Erre kell ugyanis, hogy meghatározhassunk két közönséges egész számot x-et és y-t, a melyekre nézve

$$a+b\sqrt{-k}=(u+v\sqrt{-k})(x+y\sqrt{-k}). \qquad (3)$$

Ez akkor lesz lehetséges, ha az

$$ux-kvy=a,\quad vx+uy=b$$

lineáris egyenletrendszer egész számokban megoldható.

Minden $a+b\sqrt{-k}$ szám osztóinak sora véges és meghatározható oly eljárással, a mely véges számú lépés után befejezéshez jut.

Ugyanis, ha fennáll (3), akkor egyszersmind lesz:

$$a-b\sqrt{-k}=(u-v\sqrt{-k})(x-y\sqrt{-k}) \qquad (4)$$

és így tehát

$$a^2+kb^2=(u^2+kv^2)(x^2+ky^2).$$

Ez mutatja, hogy az u^2+kv^2 közönséges egész szám

* L. pl. BACHMANN: Kreistheilung, Leipzig 1872, 150. lap.

$a^2 + kb^2$-nek osztója. Ha tehát $a^2 + kb^2$ pozitiv osztói $d_i (i=0, \ldots, n)$, akkor szükséges, hogy u és v kielégítsék az

$$u^2+kv^2 = d_i, \quad (i=0, 1, \ldots, n)$$

egyenletek valamelyikét. De minthogy ezek az egyenletek csak úgy elégíthetők ki, ha $u^2 \leqq d_i$, $v^2 \leqq d_i$, világos, hogy u, v számára véges számban kapunk megfelelő értékrendszereket. Az ezen értékrendszereknek külön-külön megfelelő $u+v\sqrt{-k}$ számokról azután a fennebbi eljárással eldöntendő, vajjon osztói-e $a+b\sqrt{-k}$-nak.

8. §. Ezek után részletesebben fogjuk megvizsgálni a $k=5$ esetet, azaz a $[\sqrt{-5}]$ tartományt, a melynek typikus jelentőségére legelőször DEDEKIND* figyelmeztetett. E tartomány ugyanis legegyszerübb példája a *nem teljes* holoid tartománynak.

Hogy ezt megmutassuk, határozzuk meg a

$$3,\ 9,\ 1-2\sqrt{-5},\ (1-2\sqrt{-5})^2 = -(19+4\sqrt{-5}),\ 3(1-2\sqrt{-5})$$

számok összes osztóit.

Az első esetben pl. meg kell oldanunk az $u^2+5v^2=d$ egyenleteket, a melyekben $d=1, 3, 9$. Ezek közül az elsőből nyerjük a $(\pm 1, 0)$, a harmadikból a $(\pm 2, \pm 1)$, $(\pm 3, 0)$ egész számú értékrendszereket, míg a második egyáltalában nem vezet egész számú értékrendszerhez.

Az előjelt mellőzve tehát csupán csak az

$$1 \text{ és } 3$$

osztókat nyerjük, mert a $(\pm 2, \pm 1)$ értékrendszer nem vezet osztóhoz. Hogy ez is osztóhoz vezessen, arra szükséges volna ugyanis, hogy legyen:

$$3 = (2+\sqrt{-5})(x+y\sqrt{-5}),$$

vagyis, hogy a

$$2x-5y=3,\ x+2y=0$$

* Zahlentheorie, 4. kiadás, 547. lap.

egyenletrendszernek x és y egész számú értékei feleljenek meg. Mint látni, azonban ennek az egyenletrendszernek megoldása:

$$x = \frac{2}{3}, \quad y = -\frac{1}{3}.$$

Ellenben csakugyan:

$$9 = (2+\sqrt{-5})(2-\sqrt{-5}).$$

Hasonló módon elvégezve a számítást a többi esetben is, végre azt találjuk, hogy az előjelt mellőzve:

3 osztói: 1, 3,

9 « 1, 3, $2\pm\sqrt{-5}$, 9

$1-2\sqrt{-5}$ « 1, $1-2\sqrt{-5}$,

$(1-2\sqrt{-5})^2$ « 1, $1-2\sqrt{-5}$, $2-\sqrt{-5}$, $2+3\sqrt{-5}$, $(1-2\sqrt{-5})^2$

$3(1-2\sqrt{-5})$ « 1, 3, $1-2\sqrt{-5}$, $2-\sqrt{-5}$, $4-\sqrt{-5}$, $3(1-2\sqrt{-5})$.

Ezek közül tehát 9 és $3(1-2\sqrt{-5})$ *oly számok, a melyeknek megállapodásaink értelmében legnagyobb közös osztójuk nincsen.* E két szám közös osztói ugyanis az előjelt mellőzve, a következők:

$$1,\ 3,\ 2-\sqrt{-5}$$

és így a 9 és $3(1-2\sqrt{-5})$ legnagyobb közös osztója csakis e számok egyike lehetne; még pedig az, a mely az összes többivel osztható. Ámde a három szám közül egyik sem osztható a másik kettővel és ezzel be van bizonyítva, hogy állításunk helyes*.

Még másképen, de ép oly feltünően mutatkozik a $[\sqrt{-5}]$ tartomány «nem teljes volta» abból a körülményből, hogy a 3 és $1-2\sqrt{-5}$ számoknak az egységen kívül nin-

* Igy tehát ez a két állítás, hogy α-nak és β-nak nincsen legnagyobb közös osztójuk és az, hogy legnagyobb közös osztójuk 1, nem jelenti ugyanazt. Ezt kiemeljük tekintettel arra a nem szabatos kifejezésmódra, melylyel az elemekben gyakran találkozunk.

csen közös osztójuk, míg mind a kettőnek négyzete osztható $2-\sqrt{-5}$-tel.

9. §. A $[\sqrt{-5}]$ tartománynak az előbbiekkel összefüggő tulajdonsága az, hogy a 3-*mal és* $2-\sqrt{-5}$-*tel osztható számainak összessége nem állítható elé mint egy bizonyos szám többszöröseinek összessége.*

Ama számok összessége ugyanis, tekintettel arra, hogy osztójuk 3, a $3x+3y\sqrt{-5}$ alakban lesz előállítható. Hogy azonban valamely ilyen alakú szám osztható legyen $2-\sqrt{-5}$-tel, szükséges, hogy meghatározhassunk két oly közönséges egész számot, u-t és v-t, a melyekre nézve

$$3x+3y\sqrt{-5} = (2-\sqrt{-5})(u+v\sqrt{-5}),$$

azaz

$$2u+5v=3x, \quad -u+2v=3y.$$

Így tehát

$$u = \frac{2x-5y}{3}, \quad v = \frac{x+2y}{3},$$

valamint

$$u-v+2y = \frac{x-y}{3}$$

is közönséges egész számok. Ebből következik, hogy x minden esetre ilyen alakú szám:

$$x=y+3w,$$

a hol w közönséges egész számot jelent. És minthogy x ilyen meghatározása mellett u és v mindig egész számok, a $[\sqrt{-5}]$ tartomány minden 3-mal *és* $2-\sqrt{-5}$-tel osztható száma ebben az alakban állítható elő:

$$(9w+3y) + 3y\sqrt{-5} = 9w+3(1+\sqrt{-5})y,$$

a hol y és w *tetszés szerinti* közönséges egész számokat jelentenek.

Ha pedig ezek a számok mind többszörösei volnának bizonyos meghatározott δ számnak, akkor δ szükségképen osztója volna azoknak a specziális számoknak is, a melyek

a $w=1$, $y=0$ és a $w=1$, $y=-2$ helyettesítésekből származnak, azaz 9-nek *és* $3(1-2\sqrt{-5})$-nek is. δ tehát vagy 1, vagy 3, vagy pedig $2-\sqrt{-5}$ volna. Ámde e számok többszörösei között vannak mindig olyanok is, a melyek *nem* oszthatók 3-mal *és* $2-\sqrt{-5}$-tel. Így már a 3 sem osztható $2-\sqrt{-5}$-tel sem pedig a $2-\sqrt{-5}$ a 3-mal.

A későbbi alkalmazás miatt még különösen kiemeljük, hogy *a*

$$3\alpha_1+(1-2\sqrt{-5})\,\alpha_2$$

számok összessége, a hol α_1 *és* α_2 *a* $[\sqrt{-5}]$ *tartomány tetszés szerinti számait jelentik, nem lehet azonos valamely a* $[\sqrt{-5}]$ *tartományban foglalt* δ *szám többszöröseinek összességével.*

Minthogy ama számok között a 3 és az $1-2\sqrt{-5}$ is előfordul, δ csakis ezeknek valamely közös osztója lehetne, azaz az előjelt mellőzve $=1$. De akkor szükséges, hogy α_1 és α_2 olyan értékeket is vehessenek föl, a melyekre nézve

$$3\alpha_1+(1-2\sqrt{-5})\,\alpha_2=1.$$

Négyzetre emelve azt látjuk, hogy α_1 és α_2 ugyanazon értékei mellett

$$9\alpha_1^2+6(1-2\sqrt{-5})\,\alpha_1\alpha_2+(1-2\sqrt{-5})^2\,\alpha_2^2=1.$$

Ámde itt α_1^2, $\alpha_1\alpha_2$, α_2^2 együtthatói — mint az előbb végrehajtott számításokból kitünik — mindannyian oszthatók $2-\sqrt{-5}$-tel. Ha tehát $[\sqrt{-5}]$ tartalmazna olyan α_1 és α_2 számokat, a melyek ezt a feltételt kielégítik, akkor 1-nek is oszthatónak kellene lennie $2-\sqrt{-5}$-tel, a mi pedig nem lehetséges, minthogy $2-\sqrt{-5}$ nem egység. Evvel állításunk be van bizonyítva.

Végre még azt is látjuk, hogy pl. $2-\sqrt{-5}$ *a* $[\sqrt{-5}]$ *tartományban irreducibilis ugyan, de nem törzsmennyiség;* mert sem 3, sem $1-2\sqrt{-5}$ nem osztható $2-\sqrt{-5}$-tel, míg szorzatuk osztható vele.

Congruentiatartományok és modulusrendszerek.

10. §. Az adott [A] tartományból egyszer mindenkorra kiválasztunk h meghatározott, a 0-tól különböző mennyiséget: M_1, M_2, ..., M_h-t, a melyeknek összfoglalatját $(M_1, M_2, \ldots, M_h)$ modulusrendszernek fogjuk nevezni. Az

$$\alpha_1 M_1 + \alpha_2 M_2 + \cdots + \alpha_h M_h$$

mennyiségek összességét, a hol $\alpha_1, \alpha_2, \ldots, \alpha_h$ *tetszés szerinti*, az [A] tartományba tartozó mennyiségeket jelentenek, *az* [A] *tartományból származó és az* $(M_1, \ldots, M_h)$ *modulusrendszer meghatározta congruentiatartománynak* fogjuk nevezni.

A modulusrendszert a benne foglalt mennyiségek száma szerint *h-tagúnak* nevezzük, a benne foglalt $M_1, M_2, \ldots, M_h$ mennyiségek pedig a modulusrendszer *elemei*.

A congruentiatartomány természetesen csak is oly mennyiségeket foglal magában, a melyek az [A] tartományhoz tartoznak. Két a congruentiatartományhoz tartozó mennyiség összege vagy szorzata ismét a congruentiatartományhoz tartozik.

Az [A] tartomány mennyiségeinek összessége akkor és csak akkor lehet azonos a congruentiatartomány mennyiségeinek összességével, ha ez magában foglalja az absolut egységet. Az 1 segítségével ugyanis az [A] tartomány minden mennyisége előállítható a kivánt alakban.

A congruentiatartományt *valódinak* nevezzük, ha nem tartalmazza az absolut egységet; tehát akkor és csak akkor, ha az [A] tartománynak valódi részletsokasága.

Az [A] tartomány két mennyisége, pl. λ és μ congruens az $(M_1, M_2, \ldots, M_h)$ modulusrendszerre vonatkozólag, ha $\lambda - \mu$ a modulusrendszer meghatározta congruentiatartományban foglaltatik, vagyis, ha [A]-ban vannak olyan α meny-

nyiségek, hogy

$$\lambda - \mu = \alpha_1 M_1 + \cdots + \alpha_h M_h.$$

Ezt a következő jelöléssel fejezzük ki:

$$\lambda \equiv \mu \,(\text{mod. } M_1, M_2, \ldots, M_h).$$

A mint közvetetlenül világos, ugyanezt a tényt a következő módon is fejezhetjük ki:

$$\lambda - \mu \equiv 0 \,(\text{mod. } M_1, M_2, \ldots, M_h).$$

A congruentia fogalma általánosítása az egyenlőség fogalmának. Egyenlő mennyiségek egyszersmind congruensek is és a congruentia jele részben követi az egyenlőség jelének törvényeit. Különösen:

I. *Ha* $\lambda \equiv \mu$ *és* $\mu \equiv \nu$, *akkor* $\lambda \equiv \nu$.

II. *Ha* $\lambda_1 \equiv \lambda_2$ *és* $\mu_1 \equiv \mu_2$, *akkor* $\lambda_1 \mu_1 \equiv \lambda_2 \mu_2$.

Mind a két esetben természetesen feltételezzük, hogy a meghatározó modulusrendszer mindig ugyanaz marad. Hogy bebizonyítsuk pl. a második tételt, csak a definiciónak megfelelőleg részletesen kell felírnunk, hogy

$$\lambda_1 = \lambda_2 + \alpha_1 M_1 + \cdots + \alpha_h M_h,$$

$$\mu_1 = \mu_2 + \beta_1 M_1 + \cdots + \beta_h M_h.$$

Ezekből közvetetlenül következik, hogy

$$\lambda_1 \mu_1 = \lambda_2 \mu_2 + \gamma_1 M_1 + \cdots + \gamma_h M_h.$$

Ennek a szorzásra vonatkozó tételnek megfordítása nem érvényes általánosan. A megfelelő pontos tétel a következő:

III. *Ha* $\lambda_1 \mu_1 \equiv \lambda_2 \mu_2$ *és* $\lambda_1 \equiv \lambda_2$, *akkor ezekből bármely* μ_1 *mennyiségre nézve akkor és csak akkor következik, hogy* $\mu_1 \equiv \mu_2$, *ha van az* [A] *tartományban oly* β *mennyiség, a melyre nézve* $\beta\lambda_1 \equiv 1$.

Ha van ilyen β mennyiség, akkor, minthogy $\lambda_1 \equiv \lambda_2$, lesz: $\beta\lambda_2 \equiv \beta\lambda_1 \equiv 1$; továbbá $\beta\lambda_1 \mu_1 \equiv \beta\lambda_2 \mu_2$, vagyis $\mu_1 \equiv \mu_2$.

Hogy ilyen β mennyiség nincsen, vagyis, hogy a

$$\beta\lambda_1 - \alpha_1 M_1 - \alpha_2 M_2 - \cdots - \alpha_h M_h = 1$$

egyenlet nem oldható meg oly módon, hogy $\beta, \alpha_1, \ldots, \alpha_h$ az [A] tartományhoz tartozó mennyiségek legyenek, az úgy is fejezhető ki, hogy e $h+1$-tagú modulusrendszer:

$$(\lambda_1, M_1, \ldots, M_h)$$

valódi congruentiatartományt határoz meg. De akkor a h-tagú $(M_1, \ldots, M_h)$ modulusrendszer meghatározta congruentiatartomány is valódi, mert minden benne foglalt mennyiség egyszersmind ama $h+1$-tagú modulusrendszer meghatározta congruentiatartományhoz is tartozik.

Ha tehát a μ_1 és μ_2 mennyiségeket úgy választjuk, hogy közülük az egyik az $(M_1, \ldots, M_h)$ meghatározta congruentiatartományhoz tartozzék, a másik pedig nem, a mi most mindig lehetséges, λ_1-et és λ_2-t pedig úgy, hogy mind a kettő $\equiv 0$ legyen (mod. $M_1, \ldots, M_h$), akkor lesz: $\lambda_1\mu_1 \equiv \lambda_2\mu_2$ a nélkül, hogy ebből $\mu_1 \equiv \mu_2$ következnék.

Két modulusrendszer $(M_1, \ldots, M_h)$ és $(N_1, \ldots, N_k)$ bizonyos módon meghatároz egy harmadikat

$$(M_1, \ldots, M_h, N_1, \ldots, N_k)\text{-t},$$

a mely tartalmazza az első kettőnek összes elemeit. A definiczió alapján az e modulusrendszer meghatározta congruentiatartomány nem változik, ha az esetleg ismétlődő elemeket csak egyszer tartjuk meg.

Ha már mostan

$$\lambda_1 \equiv \lambda_2 (\text{mod. } M_1, \ldots, M_h) \text{ és } \mu_1 \equiv \mu_2 (\text{mod. } N_1, \ldots, N_k),$$

akkor ezekből közvetetlenül következik, hogy

$$\lambda_1 \equiv \lambda_2, \ \mu_1 \equiv \mu_2 (\text{mod. } M_1, \ldots, M_h, N_1, \ldots, N_k).$$

Ez a congruentiára vonatkozó tételek következő bővítéséhez vezet:

Ha $\lambda \equiv \mu (\text{mod. } M_1, \ldots, M_h)$ *és* $\mu \equiv \nu (\text{mod. } N_1, \ldots, N_k)$,
akkor $\lambda \equiv \nu (\text{mod. } M_1, \ldots, M_h, N_1, \ldots, N_k)$.

Ha $\lambda_1 \equiv \lambda_2 (\text{mod. } M_1, \ldots, M_h)$ *és* $\mu_1 \equiv \mu_2 (\text{mod. } N_1, \ldots, N_k)$,
akkor $\lambda_1\mu_1 \equiv \lambda_2\mu_2 (\text{mod. } M_1, \ldots, M_h, N_1, \ldots, N_k)$.

Ha $\lambda_1\mu_1 \equiv \lambda_2\mu_2 (\text{mod. } M_1, \ldots, M_h)$ *és* $\lambda_1 \equiv \lambda_2 (\text{mod. } N_1, \ldots, N_k)$, *akkor ezekből bármely* μ_1 *mennyiségre nézve akkor és csak akkor következik, hogy* $\mu_1 \equiv \mu_2 (\text{mod. } M_1, \ldots, M_h, N_1, \ldots, N_k)$, *ha van az* [A] *tartományban oly* β *mennyiség, a melyre nézve*

$$\beta\lambda_1 \equiv 1 (\text{mod. } M_1, \ldots, M_h, N_1, \ldots, N_k).$$

Hogy ez utóbbi tétel igazságáról meggyőződjünk, egyszerűen ismételjük az előbbi bebizonyítást; csak a végén λ_1 s λ_2 számára oly mennyiség választandó, a mely $\equiv 0$ az $M_1, \ldots, M_h)$ modulusrendszerre vonatkozólag.

Ha az $(M_1, \ldots, M_h)$ és $(N_1, \ldots, N_k)$ modulusrendszerek azonosok, akkor újból az előbb felállított tételekhez jutunk.

11. §. E fogalomalkotásokra a legegyszerűbb példa a számelmélet elemeiből ismeretes congruentia-meghatározás. Itt Gauss használta először a congruentia elnevezést és annak jelét, míg az épen értelmezett általános fogalmak Kronecker-től származnak *.

Azokban a tárgyalásokban az [1] tartomány két számát congruensnek nevezik az egytagú (m) modulusrendszerre, vagy rövidebben az m modulusra vonatkozólag, ha különbségük osztható m-mel stb. Különösen minden 1-től különböző egész szám meghatároz egy valódi congruentiatartományt, a mely az m összes többszöröseiből és csakis ezekből áll.

Ebben a legegyszerűbb esetben további többtagú modulusrendszerek alkotása teljesen fölösleges. Legyenek ugyanis $m_1, m_2, \ldots, m_h$ közönséges egész számok és d a legnagyobb közös osztójuk, akkor mindig meghatározhatók olyan egész számok, a melyekre nézve

$$a_1 m_1 + \cdots + a_h m_h = d.$$

Az $(m_1, \ldots, m_h)$ modulusrendszer meghatározta congruentiatartomány tehát egyrészt csupán csak olyan számokat tar-

* Kivéve az igen kényelmes «congruentiatartomány» elnevezést.

talmaz, a melyek d-nek többszörösei és másrészt tartalmazza d-nek összes többszöröseit (mert $kd = ka_1 m_1 + \cdots + ka_h m_h$). E tartomány tehát azonos a (d) modulus meghatározta tartománynyal.

A raczionális számok tartománya, (1) nem ad alkalmat valódi congruentia-meghatározásra. Ha ugyanis $(r_1, r_2, \ldots, r_h)$ e tartományban modulusrendszer volna, akkor, minthogy már az $r_1 x = 1$ egyenlet is megoldható raczionális számokban, e modulusrendszerre vonatkozólag az összes számoknak congruenseknek kellene lenniök. A megfelelő congruentiatartomány tehát mindig egybeesnék magával (1)-gyel.

Teljesen ugyanaz érvényes minden orthoid tartományra.

Hogy a viszonyok nem minden tartományban olyan egyszerűek mint [1]-ben, már az előbb példaképen tárgyalt $[\sqrt{-5}]$ tartomány esetéből is látható. Ebben a kéttagú $(3, 1-2\sqrt{-5})$ modulusrendszer meghatározta congruentiatartomány a $3\alpha_1 + (1-2\sqrt{-5})\alpha_2$ számok összessége, a melyről épen (a 9. §. végén) bebizonyítottuk, hogy nem állítható elő semmiféle egytagú modulus segítségével.

A congruentia fogalma arithmetikai vizsgálatokban azért fontos, mert módot nyujt az [A] tartomány mennyiségeinek osztályokba való sorozására úgy, hogy egy osztályba sorozzuk az összes egy bizonyos meghatározott mennyiséggel congruens, vagy — a mi ugyanaz — az összes egymás között congruens mennyiségeket.

Relativ æquivalentia.

12. §. Valamely adott [A] holoid tartomány oly

$$\pi_1, \pi_2, \ldots$$

részletsokaságát, a mely tartalmazza az [A] tartomány minden egységét, valamint bármely benne előforduló két mennyi-

ség szorzatát is, de nem tartalmazza a 0-t, *aequivalentiatartománynak* nevezzük. *Valódi* az æquivalentiatartomány akkor, ha a 0 kizárása után is van az [A] tartományban oly mennyiség, melynek szorzata az æquivalentiatartomány bármely mennyiségével *nem* tartozik ebbe a tartományba.

Orthoid tartomány tehát sohasem adhat alkalmat valódi æquivalentiatartományok alkotására, mert azokban a zérus kizárása után minden mennyiség egységnek tekintendő.

Ha az [A] holoid tartományról a 4. §-ban leírt eljárás szerint áttérünk a mellérendelt orthoid (A) tartományra és az épen most jellemzett æquivalentiatartományt Π-vel jelöljük, akkor az összes $\frac{\alpha}{\pi}$ mennyiségek, a melyekben α az [A] tartomány és π a Π tartomány bármely mennyiségét jelenti, ismét holoid tartományt alkotnak, a melyet [A | Π]-vel jelölhetünk.

E tartomány holoid, mert mind az összeadás törvénye:

$$\frac{\alpha_1}{\pi_1} + \frac{\alpha_2}{\pi_2} = \frac{\alpha_1 \pi_2 + \alpha_2 \pi_1}{\pi_1 \pi_2},$$

mind a szorzás törvénye:

$$\frac{\alpha_1}{\pi_1} \frac{\alpha_2}{\pi_2} = \frac{\alpha_1 \alpha_2}{\pi_1 \pi_2}$$

benne közönséges; továbbá, mert úgy α, mint π helyébe tehető az absolut egység és így tehát ez a tartomány is tartalmazza az absolut egységet és az ennek ismételt összeadása révén származó mennyiségeket: 1, 2, 3, . . ., a melyek sorában — mint közvetetlenül látni — a 0 nem fordul elő.

Ha [A] *valódi holoid tartomány,* Π *valódi aequivalentiatartomány és van az* [A]*-ban oly* γ *mennyiség, mely a* Π *egy mennyiségének sem osztója, — még pedig csakis ebben az esetben — az* $\frac{\alpha}{\pi}$ *mennyiségek is valódi holoid tartományt alkotnak.*

E tartományban minden egyes π mennyiség egység, mert $\pi \frac{1}{\pi} = 1$. Ebből világos, hogy $\frac{1}{\pi}$ is egység. Hogy azonban $\frac{\alpha}{\pi}$ is egység, tehát

$$\frac{\alpha}{\pi} \frac{\alpha'}{\pi'} = 1$$

lehessen, az $\alpha\alpha' = \pi\pi'$ egyenlőség miatt szükséges és elegendő hogy α az [A] tartományon belül osztója legyen $\pi\pi'$-nek, vagyis: *Az* [A | Π] *tartomány egységei tehát az összes* $\frac{\varphi}{\pi}$ *alakú számok, hol* φ *a* Π *valamely mennyiségének osztója.*

Ha tehát γ az [A] tartomány oly mennyisége, a mely az előbb kimondott föltételnek megfelel, akkor a $\gamma\xi = 1$ egyenlet az új tartományban sem oldható meg. Ha ugyanis ezt az egyenletet kielégítené $\xi = \frac{\beta}{\pi}$, akkor $\gamma\beta = \pi$ volna és γ feltevésünk ellenére az [A] tartományban osztója volna π-nek.

Evvel látjuk, hogy a föntebb adott tétel föltételei elegendők. Hogy egyszersmind szükségesek, kiviláglik a következő megjegyzésekből. Ha az [A] tartomány bármely γ mennyiségére csakugyan fönnáll egy $\gamma\beta = \pi$ alakú egyenlet, akkor az [A | Π] tartományban értendő

$$\frac{\gamma_1}{\pi'} \xi = \frac{\gamma_2}{\pi''}$$

egyenletnek a $\gamma_1 \beta_1 = \pi_1$ értelmezte mennyiségek bevezetése után rögtön fölírható megoldása is:

$$\xi = \frac{\gamma_2 \beta_1 \pi'}{\pi_1 \pi''}.$$

Figyelembe veendő végre, hogy, ha nem valódi æquivalentiatartománynyal van dolgunk, az [A]-nak bármely γ mennyisége föllép mint az æquivalentiatartomány valamely mennyiségének osztója.

Minden æquivalentiatartomány tartalmazza az [A] tar-

tomány egységeit. Ezek magukban tehát az [A]-ból származó «legkisebb» æquivalentiatartományt alkotják, a melyet E-vel fogunk jelölni. Közvetetlenül világos, hogy [A | E] azonos [A]-val.

A Π æquivalentiatartományra vonatkozólag *relative aequivalensnek* akkor nevezzük az [A] tartomány két mennyiségét, pl. α-t és β-t, ha ebben a Π tartományban meghatározhatunk két mennyiséget, π_1-et és π_2-t, a melyekre nézve $\pi_1 \alpha = \pi_2 \beta$.

Ezt a következő módon fejezzük ki:

$$\alpha \sim \beta, [A], \Pi,$$

a hol az æquivalentia meghatározásának alapjára vonatkozó pontosabb adatok el is maradhatnak, ha azok a vizsgálat folyamában változatlanok maradnak.

Közvetetlenül látni, hogy az æquivalentiára vonatkozó már előbb (5. §.) lehozott három alaptörvény itt is érvényes.

Ha Π egybeesik E-vel, akkor a relativ æquivalentia átmegy az absolut æquivalentiába.

Hogy e fogalomalkotás mennyire fontos, csak később fog kiderülni; itt azonban csak egészen jelentéktelen példák állanak rendelkezésünkre. [1]-ből pl. mint æquivalentiatartományt kiemelhetjük az összes $\pm 2^k (k \geqq 0)$ alakú számokat úgy, hogy két egész szám akkor lesz relative æquivalensnek tekintendő, ha az egyik közülük a másikból úgy származik, hogy ezt valamely $\pm 2^k$ alakú számmal megszorozzuk. A bővített [A | Π] tartomány ebben az esetben mindazokból a raczionális számokból áll, a melyeknek nevezője 2-nek valamely hatványa.

Az æquivalentia fogalma újból általánosítható, ha a Π tartomány értelmezésénél elejtjük azt az egy föltételt, hogy Π az [A] minden egységét tartalmazza. Elég, ha ezt itt egyszerűen megemlítjük.

MÁSODIK FEJEZET.

A HOLOID TARTOMÁNYBÓL SZÁRMAZÓ FORMÁK.

Formák és egész függvények.

1. §. Legyen adva az [A] holoid tartomány. E tartomány mennyiségeiből és az x új határozatlanból alkotjuk az

$$A_0 + A_1 x + A_2 x^2 + \cdots + A_m x^m$$

«mennyiségeket», hol $A_0, A_1, \ldots, A_m$ az eredeti [A] tartomány mennyiségei. E mennyiségeket ismét egy tartományba foglaljuk össze oly módon, hogy ha

$$B_0 + B_1 x + B_2 x^2 + \cdots + B_n x^n$$

egy második ilyen mennyiség, a két mennyiség összegének ill. szorzatának az

$$(A_0 + B_0) + (A_1 + B_1) x + (A_2 + B_2) x^2 + \cdots$$

és

$$A_0 B_0 + (A_0 B_1 + A_1 B_0) x + (A_0 B_2 + A_1 B_1 + A_2 B_0) x_2 + \cdots + A_m B_n x^{m+n};$$

mennyiségeket nevezzük; azaz, az összeadást és szorzást ama szabályok szerint hajtjuk végre, a melyek az algebra elemeiből mint az x hatványai szerint rendezett kifejezésekre vonatkozó szabályok ismeretesek. Ezen az alapon világos, hogy az eredetileg adott mennyiség felfogható mint az $A_0, A_1 x, \ldots, A_m x^m$ tagok összege. Elvileg ugyan az összeadás és szorzás törvényeinek megállapítása előtt e mennyiséget mint az $(A_0, A_1, \ldots, A_m, x)$ mennyiségek complexusát kellett volna felírnunk, a mi azonban e megállapodásaink után mindjárt felesleges bonyolításnak bizonyul.

Képezésüknek megfelelőleg két ilyen mennyiség akkor és csak akkor egyenlő egymással, ha az [A] tartomány mennyiségei, a melyeket alkotásuknál felhasználtunk, az ú. n. együtthatók, rendre egyenlők; tehát

$$A_0 = B_0,\ A_1 = B_1,\ \ldots,\ A_m = B_m,$$

és így azoknak száma is mindkét esetben ugyanaz.

Ezek után közvetetlenül felismerjük, hogy az így alkotott mennyiségek összessége valódi holoid tartomány; még pedig akkor is, ha az [A] tartomány nem valódi holoid, azaz orthoid tartomány. Az így értelmezett mennyiségek ugyanis az összeadás és szorzás közönséges törvényét követik; a tartomány magában foglalja (az [A] tartomány összes mennyiségeivel együtt) az absolut egységet és az ebből alkotott $1, 2, 3, \ldots$ sorozat nem tartalmazza a zérust, mert hiszen m és 0 az értelmezés szerint különböző mennyiségek. Hogy a tartomány végre *valódi* holoid tartomány, világos abból, hogy az

$$F\xi = 1$$

egyenlet nem oldható meg, ha F nem tartozik a szűkebb [A] tartományhoz, vagyis — a mint azt másképen is akarjuk kifejezni — az x határozatlant tartalmazza. Ebben az esetben ugyanis F alakja a következő:

$$F = A_0 + A_1 x + \cdots + A_m x^m,$$

a hol $m > 0$ és $A_m \neq 0$.

Ha $F\xi = 1$, semmi esetre sem lehetséges, hogy $\xi = 0$, és így ξ alakja a következő:

$$\xi = B_0 + B_1 x + \cdots + B_n x^n,$$

a hol $n \geqq 0$ és $B_n \neq 0$. Ámde akkor

$$F\xi = A_0 B_0 + \cdots + A_m B_n x^{m+n},$$

hol $m + n > 0$ és $A_m B_n \neq 0$. E mennyiség pedig nem lehet $= 1$, mert az x határozatlant valóban tartalmazza.

Az így képezett tartományt röviden $[A, x]$-szel fogjuk jelölni.

2. §. Közvetetlenül világos, hogy e fogalomalkotás egy új második, harmadik stb. határozatlan bevezetésével tovább folytatható.

Legyenek a rendre egymásután bevezetendő határozatlanok: $x_1, x_2, \ldots, x_m$. Akkor $[A]$-ból először származik majd az $[A, x_1]$ tartomány és minthogy ez valódi holoid tartomány, ebből az x_2 határozatlan hozzácsatolása után egy új bővített tartomány, a melyet $[A, x_1, x_2]$-vel fogunk jelölni és így tovább, míg végre az

$$[A, x_1, x_2, \ldots, x_m]$$

tartományhoz jutunk. Minthogy az összeadást és szorzást ezekben a tartományokban is az elemi algebra szabályai szerint végezhetjük, valamely ezekhez tartozó mennyiség x_m hatványai szerint rendezett kifejezésében az együtthatókat összegeknek tekinthetjük és ha a szorzásokat valóban elvégezzük, ilyen alakú kifejezést nyerünk:

$$A_0 U_0 + A_1 U_1 + A_2 U_2 + \cdots + A_k U_k,$$

a hol az $A_0, A_1, \ldots$ együtthatók az eredeti $[A]$ tartomány mennyiségei és az U-k az $x_1, x_2, \ldots, x_m$ határozatlanok különböző hatványszorzatai, azaz ilyen alakú mennyiségek:

$$x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}.$$

Az $[A, x_1, x_2, \ldots, x_m]$ tartomány mennyiségeinek ez az alakja közvetetlenül mutatja, hogy a sorrend, a melyben az $x_1, \ldots, x_m$ határozatlanokat a tartomány alkotására felhasználtuk, magára a tartományra nézve egészen közömbös és hogy a határozatlanok $(x_1, x_2, \ldots, x_m)$ rendszerének hozzácsatolása által A-tól egyetlen egy lépéssel is eljuthatunk $[A, x_1, x_2, \ldots, x_m]$-hez.

Az $[A, x_1, x_2, \ldots, x_m]$ tartomány mennyiségeit (az $[A]$

tartományból származó) formáknak, vagy pedig az $x_1, x_2, \ldots, x_m$ *határozatlanok egész függvényeinek nevezzük.*

E két elnevezés szoros kapcsolatban áll az ujonnan alkotott mennyiségeknek két elvileg különböző felfogásával.

Valóságban az x határozatlanok használata tisztán csak átmeneti jelölés. A tartomány két mennyiségéből,

$$A_0U_0 + \cdots + A_kU_k \text{ és } B_0U_0 + \cdots + B_lU_l$$

összeadás és szorzás révén nyerünk egy harmadikat,

$$C_0U_0 + C_1U_1 + \cdots + C_rU_r,$$

melyben az együtthatók $(C_0, C_1, \ldots)$ rendszere bizonyos meghatározott módon az összeadások és szorzások sora segítségével alkotandó az $(A_0, A_1, \ldots)$ és $(B_0, B_1, \ldots)$ együtthatók rendszereiből. Az $U_0, U_1, \ldots$ hatványszorzatok itt csak arra szolgálnak, hogy egyszerű módon jellemezzék azt a törvényt, a mely szerint a különböző $A_0, A_1, \ldots, B_0, B_1, \ldots$ együtthatók felhasználandók; ezeknek az együtthatóknak a kitevők $(g_1, \ldots, g_m)$ rendszere által kifejezett «helyi értéket» kölcsönöznek. E szerint a kérdéses formákat $(A_0, \ldots, A_k)$-val is jelölhetnők; csakhogy akkor az összeadás és szorzás törvényét igen bonyolódott módon kellene kifejeznünk. A mennyiben tehát ama határozatlanokat *csak* azért vezetjük be, hogy az új mennyiségek összekapcsolását a legegyszerűbb módon írhassuk le, beszélünk *az* $x_1, \ldots, x_m$ *határozatlanok formáiról, a melyekben tehát csupán csak az* $A_0, A_1, \ldots$ *együtthatók és ezeknek* $(g_1, \ldots, g_m)$ *jellemezte helyi értékei jönnek tekintetbe.*

Az «$x_1, \ldots, x_m$ egész függvénye» kifejezésnek az általános mathematikai nyelvhasználat szerint egész más az értelme. Itt ugyanis $x_1, \ldots, x_m$ a szónak bizonyos szűkebb értelmében jelentenek határozatlanokat, a mennyiben az [A] tartományok, vagy pedig valamely az [A]-t magában foglaló bővebb [A'] tartomány bármely mennyiségei lehetnek, és így

tetszés szerinti meghatározott «értékeket» vehetnek fel. *Az egész függvény azután kifejezése valamely speciális törvénynek, a melynek alapján* $x_1, \ldots, x_m$ *értékeiből, a* $\xi_1, \ldots, \xi_m$ *mennyiségekből meghatározunk egy* $m+1$*-edik mennyiséget, az egész függvény értékét* *.

Az $U_g = x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}$ hatványszorzat *dimensiója* $g_1 + g_2 + \cdots + g_m$, *foka* x_i*-re vonatkozólag* g_i.

Az

$$A_0 U_0 + A_1 U_1 + \cdots + A_k U_k$$

forma vagy egész függvény dimensiója n' és x_i-re vonatkozó foka n_i, ha n', ill. n_i a legnagyobb raczionális egész szám azok közül, a melyek mint $U_0, U_1, \ldots, U_k$ dimensiói, ill. fokai szerepelnek. Természetesen csak azokra az U-kra kell itt tekintettel lennünk, a melyek a forma (egész függvény) kifejezésében valóban előfordulnak, azaz a melyeknek együtthatója nem 0.

A formák tagjainak lexikographikus elrendezése.

3. §. Egy határozatlant tartalmazó formákban a tagoknak természetes sorrendjét szolgáltatja közvetetlenül azoknak a határozatlan növekedő vagy fogyó hatványai szerint

* Hogy a mathematikai irodalomban a «forma» kifejezést eddig legtöbbnyire mint a homogén egész függvények elnevezését használták, nem elég ok arra, hogy itt végig ne ragaszkodjunk ahhoz a pontos fogalmi elkülönítéshez, a melyre legelőször Kronecker hívta fel a figyelmet «Festschrift»-jében. Az elnevezések összetévesztésétől alig lehet tartani. Másrészt nem csak módszertani szempontból nagy becsű a jelentésnek ily elvi elkülönítése, a mely már az elnevezésben is nyilvánul, hanem következetes terminologiának megállapítása más alapon lehetetlen. E nélkül le kellene mondanunk ily rövid és találó elnevezésekről, mint pl. ez: «egész forma» (midőn az együtthatók egész számok).

való elrendezése. E rendezési elv GAUSS-tól* származó következetes kibővítése az $x_1, x_2, \ldots, x_m$, számra nézve m határozatlant tartalmazó formák esetére a következő. Az

$$A_g x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m} \text{ és } A_h x_1^{h_1} x_2^{h_2} \ldots x_m^{h_m}$$

két tag közül a *magasabb* legyen az első, ha $g_1 > h_1$; ha pedig $g_1 = h_1$, akkor, ha $g_2 > h_2$; általánosságban, ha $g_1 = h_1$, $g_2 = h_2, \ldots, g_{i-1} = h_{i-1}$, akkor, ha $g_i > h_i$. Minthogy a hasonló (azaz ugyanazt a hatványszorzatot tartalmazó) tagok már összevontaknak tekintendők, ez az elv a tagoknak teljesen meghatározott elrendezését szolgáltatja, a legalacsonyabbtól kezdve a legmagasabbig.

Valamely tag magasságát első sorban az egész számok $(g_1, g_2, \ldots, g_m)$ complexusa jellemzi. Ha azonban vizsgálataink egyszerre csak meghatározott számú formára vonatkoznak, a melyek közül ismét mindegyik csak meghatározott számú tagból áll, e magasságot egyetlen egész számmal is jellemezhetjük. E czélból válaszszuk a t pozitiv egész számot nagyobbnak minden g_i kitevőnél, mely a különböző formák különböző tagjaiban előfordul.

Akkor az $A_g x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}$ tag magasságát teljesen megadja a

$$g = g_1 t^{m-1} + g_2 t^{m-2} + \cdots + g_i t^{m-i} + \cdots + g_m \qquad (1)$$

szám. Valamely más tagra nézve legyen

$$h = h_1 t^{m-1} + h_2 t^{m-2} + \cdots + h_i t^{m-i} + \cdots + h_m$$

és $g_1 = h_1, \ldots, g_{i-1} = h_{i-1}$, g_i és h_i ellenben különbözők legyenek egymástól; akkor, mint az állításunk szerint szükséges, $g-h$ és $g_i - h_i$ előjelei ugyanazok lesznek. Ugyanis

$$g-h = (g_i - h_i) t^{m-i} + (g_{i+1} - h_{i+1}) t^{m-i-1} + \cdots + g_m - h_m,$$

vagyis

* Demonstratio nova altera stb. Werke, III. köt. 36. lap.

$$\frac{g-h}{g_i-h_i} = t^{m-i} + \left(\frac{g_{i+1}-h_{i+1}}{g_i-h_i}\, t^{m-i-1} + \cdots + \frac{g_m-h_m}{g_i-h_i} \right).$$

Minthogy a $g_{i+1}, \ldots, g_m, h_{i+1}, \ldots, h_m$ számok közül egyik sem negativ és mindannyian kisebbek t-nél, a jobb oldalon a zárójelben álló kifejezés az előjelt mellőzve nem nagyobb mint

$$\frac{t-1}{|g_i-h_i|}(t^{m-i-1}+\cdots+1) = \frac{t^{m-i}-1}{|g_i-h_i|},$$

azaz kisebb t^{m-i}-nél és ebből következik, hogy valóban

$$\frac{g-h}{g_i-h_i} > 0.$$

Látni, hogy a g számnak az (1) alatti alakban való előállítása tulajdonképen annak felírása oly számrendszerben, a melynek alapszáma t, a hol azután $g_1, g_2, \ldots, g_m$ egyszerűen a «számjegyek», a melyeket e felírásban használunk. A formák különböző tagjaira nézve karakterisztikus *magassági számok*, $0, g^{(1)}, g^{(2)}, \ldots$ e szerint nem negativ egész számokból álló sorozatot alkotnak, a mely általánosságban hézagos. Válaszszuk pl. t-t $N+1$-nek, ha az összes formák dimensiója legfeljebb N; akkor a számjegyeknek oly $(g_1, g_2, \ldots, g_m)$ rendszere, melyben $g_1+g_2+\cdots+g_m > N$, nem léphet fel, mert ez megfelelne olyan tagnak, melynek dimensiója N-nél magasabb.

4. §. Az épen nyert rendezési elv figyelemre méltó és módszertani szempontból igen fontos kapcsolatra vezet, a mely az n határozatlant és az egy határozatlant tartalmazó formák közt fennáll *.

Ha csak olyan formákat vizsgálunk, a melyeknek dimensiója nem magasabb N-nél, akkor az

* KRONECKER, Über die symmetrischen Functionen, Berl. Mon. Ber. 1880. 938. lap. Grundzüge einer arithmetischen Theorie der algebraischen Grössen (= Festschrift) 4. §. Crelle Journal, 92. köt.

$$F(x_1, x_2, \ldots, x_m) = \Sigma A_g x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}$$

formával együtt teljesen meg van határozva az

$$f(x) = \Sigma A_g x^g$$

forma is, ha t-t oly számnak választjuk, a mely $> N$ és g-t (1) szerint határozzuk meg. Ha pedig csupán csak olyan g-kre szorítkozunk, a melyek a meghatározás e módja mellett magassági számok lehetnek, a melyekre nézve tehát a t alapszámhoz tartozó számrendszerben a számjegyek összege nem nagyobb N-nél; akkor viszont $f(x)$ is meghatározza az $F(x_1, x_2, \ldots, x_m)$ formát, mert g-vel együtt meg vannak adva a g_i-k is.

Igy tehát *oly kölcsönösen egyértelmü vonatkozáshoz jutottunk, a mely fennáll az* [A] *tartományból származó N-nél nem magasabb dimensiójú* $F(x_1, \ldots, x_m)$ *formák és oly ugyanabból az* [A] *tartományból származó* $f(x)$ *formák között, a melyekben csupán csak olyan kitevők fordulnak elő, a melyek az épen taglalt értelemben mint magassági számok szerepelhetnek.*

Különösen, ha $F_1, F_2, \ldots, F_k$ bármely ilyen formák és $F = F_1 F_2 \ldots F_k$ dimensiója N, úgy hogy F_i dimensiója ennél semmi esetre sem lehet magasabb, akkor egyszersmind lesz

$$f = f_1 f_2 \cdots f_k,$$

hol $f, f_1, f_2, \ldots, f_k$ az x határozatlannak ama formái, a melyek $F, F_1, F_2, \ldots, F_k$ formáknak megfelelnek; mert hasonló tagoknak mindig ismét hasonló tagok felelnek meg. Abból, hogy

$$(x_1^{g_1} x_2^{g_2} \ldots x_m g^m)(x_1^{h_1} x_2^{h_2} \ldots x_m^{h_m}) = x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m},$$

az is következik, hogy

$$x^g x^h = x^i;$$

és minthogy e szerint *a szorzás folyamata mind a két esetben ugyanazoknak a müveleteknek az együtthatókon való végrehajtását követeli, f is megfelel F-nek és evvel együtt jól rendezett alakban lép fel.*

A derivált formák.

5. §. Ha az $F(x_1, x_2, \ldots, x_m)$ formába x_i helyébe x_i+h_i-t teszszük, hol h_i új határozatlant jelent, akkor F-et h_i hatványai szerint rendezhetjük, hol azután az együtthatók ismét az $x_1, \ldots, x_m$ határozatlanok formái lesznek. Az itt h_i együtthatójaként fellépő formát F-nek x_i szerint vett *(első) deriváltjának** nevezzük és F'_{x_i}-vel, vagy pedig $\frac{\partial F}{\partial x_i}$-vel jelöljük.

Az Xx_i^k egytagú, a hol X valamely az x_i-t *nem* tartalmazó forma, a következő módon fejthető ki:

$$X(x_i+h_i)^k = Xx_i^k + kXx_i^{k-1}h_i + Gh_i^2. \qquad (1)$$

Hogy e kifejtés érvényes $k=1$ esetében, közvetetlenül világos és általános érvényessége a binomiális tétel nélkül is, teljes inductio segítségével bebizonyítható. Ha a kifejtés érvényes valamely k-ra nézve, akkor hozzácsatolván az x_i+h_i tényezőt, $k+1$-re nézve lesz:

$$X(x_i+h_i)^{k+1} = Xx_i^{k+1} + (k+1)Xx_i^k h_i + G_1 h_i^2.$$

Ha tehát X az x_i határozatlant nem tartalmazza, akkor mindig:

$$\frac{\partial}{\partial x_i}(Xx_i^k) = kXx_i^{k-1}.$$

* Ugyanez a képezési mód fellép tudvalevőleg a differenciálszámolás elemeiben is és a $\frac{\partial}{\partial x_i}$ műveleti symbolum használata kényelmesnek mutatkozik itt is. E symbolumot azonban természetesen — tekintet nélkül történeti vagy analitikai jelentésére — egységes jelként kell felfognunk. Ha az algebra alapvető tételeit teljesen meg akarjuk érteni, akkor a törvényeket, a melyeket ez a művelet követ, elemi jellemük daczára röviden ki kell itt fejtenünk; már azért is, hogy megmutassuk, miszerint ekkor semmiféle elméletünk körét túllépő segédeszközre nincs szükségünk.

Minthogy továbbá F az

$$F = X_0 + X_1 x_i + X_2 x_i^2 + \cdots + X_{n_i} x_i^{n_i}$$

alakban írható, lesz:

$$F(\ldots, x_i + h_i, \ldots) = F(\ldots, x_i, \ldots) + \frac{\partial F}{\partial x_i} h_i + H_1 h_i^2.$$

Ha valamely második formára nézve hasonlóképen

$$G(\ldots, x_i + h_i, \ldots) = G(\ldots, x_i, \ldots) + \frac{\partial G}{\partial x_i} h_i + H_2 h_i^2,$$

akkor e két kifejtés összeadásából és szorzásából kiadódik a derivatio két alaptörvénye:

$$\frac{\partial}{\partial x_i}(F+G) = \frac{\partial F}{\partial x_i} + \frac{\partial G}{\partial x_i} \qquad \text{(I)}$$

és

$$\frac{\partial}{\partial x_i}(FG) = F\frac{\partial G}{\partial x_i} + G\frac{\partial F}{\partial x_i}. \qquad \text{(II)}$$

Hogy az

$$F(\ldots, x_i + h_i, \ldots) = F_0 + F_1 h_i + F_2 h_i^2 + \cdots + F_{n_i} h_i^{n_i} = \sum_{k=0}^{n_i} F_k h_i^k$$

identitásban, a hol

$$F_0 = F, \quad F_1 = \frac{\partial F}{\partial x_i},$$

a h_i^k-k együtthatóiként fellépő további formákat is mint deriváltakat határozhassuk meg, helyettesítsük a következőket:

$$x_i + h_i = z_i, \quad h_i = z_i - x_i,$$

úgy hogy azután lesz:

$$F(\ldots, z_i, \ldots) = \sum_{k=0}^{n_i} F_k (z_i - x_i)^k.$$

Ha már mostan általánosságban *azt a formát, a mely F-ből úgy származik, hogy ezt l-szer ismételve alávetjük a derivatio folyamatának, az F x_i (ill. z_i) szerint vett l-dik deriváltjának nevezzük és* $\frac{\partial^l F}{\partial x_i^l}$*-vel, ill.* $\frac{\partial^l F}{\partial z_i^l}$*-vel jelöljük*, akkor (I)

szerint az ismételt derivatiót a jobb oldalon tényleg végrehajthatjuk és a következőt nyerjük:

$$\frac{\partial^l F}{\partial z_i^l} = \sum_{k=l}^{n_i} k(k-1)\ldots(k-l+1)\, F_k (z_i - x_i)^{k-l}.$$

Ha ebben z_i helyébe x_i-t teszszük, akkor, minthogy a jobb oldalon csak az a tag nem tünik el, a melyben $k=l$, végre lesz

$$\frac{\partial^l F}{\partial x_i^l} = l!\, F_l$$

és így kifejtésünk a következő lesz*:

$$F(\ldots, x_i + h_i, \ldots) = \sum_{k=0}^{n_i} \frac{1}{k!} \frac{\partial^k F}{\partial x_i^k} h_i^k. \qquad (2)$$

6. §. Tegyük most már az $F(x_1, x_2, \ldots, x_m)$ formában az összes $x_1, x_2, \ldots, x_m$ határozatlanok helyébe az

$$x_1 + h_1, x_2 + h_2, \ldots, x_m + h_m$$

összegeket, a hol $h_1, \ldots, h_m$ új határozatlanok és rendezzük $F(x_1 + h_1, \ldots, x_m + h_m)$-et a h-k hatványszorzatai szerint. Hogy a $h_1^{k_1} h_2^{k_2} \ldots h_m^{k_m}$ ezen elrendezés mellett származó együtthatóját meghatározhassuk, a következő módon járunk el. Tegyük először csak x_1 helyébe az $x_1 + h_1$ összeget és határozzuk meg $h_1^{k_1}$ együtthatóját; ebben az együtthatóban ismét csak x_2 helyébe tegyük az $x_2 + h_2$ összeget és határozzuk meg $h_2^{k_2}$-nek együtthatóját és így tovább, míg végre az utoljára nyert együtthatóban x_m helyébe $x_m + h_m$-et teszszük és meghatározzuk $h_m^{k_m}$ együtthatóját. Ez az eljárás mint $h_1^{k_1} h_2^{k_2} \ldots h_m^{k_m}$ együtthatóját az

* hol még megjegyzendők a következő symbolikus jelölések: $0! = 1$, $\frac{\partial^0 F}{\partial x_i^0} = F$.

$$\frac{1}{k_m!}\frac{\partial^{k_m}}{\partial x_m^{k_m}}\left(\frac{1}{k_{m-1}!}\frac{\partial^{k_{m-1}}}{\partial x_{m-1}^{k_{m-1}}}\left(\cdots\left(\frac{1}{k_1!}\frac{\partial^{k_1}}{\partial x_1^{k_1}}\right)\cdots\right)\right),$$

vagyis az

$$\frac{1}{k_m!\,k_{m-1}!\ldots k_1!}\frac{\partial^{k_m}}{\partial x_m^{k_m}}\cdots\frac{\partial^{k_1}F}{\partial x_1^{k_1}}$$

kifejezést szolgáltatja.

Az így nyert eredmény jelentéséből közvetetlenül világos, hogy *a*

$$\frac{\partial^{k_1}}{\partial x_1^{k_1}},\ldots,\frac{\partial^{k_m}}{\partial x_m^{k_m}}$$

müveletek sorrendje fölcserélhető. Továbbá *az ismételten elvégzendő*

$$\frac{\partial}{\partial x_1},\ldots,\frac{\partial}{\partial x_m}$$

elemi müveletek is bármely sorrendben hajthatók végre, mert az előbbiek szerint bármely G formára nézve

$$\frac{\partial}{\partial x_i}\frac{\partial G}{\partial x_j}=\frac{\partial}{\partial x_j}\frac{\partial G}{\partial x_i}.$$

Ennek megfelelőleg $h_1^{k_1}h_2^{k_2}\ldots h_m^{k_m}$ épen nyert együtthatóját rövidebben így is írhatjuk:

$$\frac{1}{k_1!\,k_2!\ldots k_m!}\frac{\partial^k F}{\partial x_1^{k_1}\partial x_2^{k_2}\ldots\partial x_m^{k_m}},\quad(k=k_1+k_2+\cdots+k_m)$$

és így az

$$F(x_1+h_1,\ldots,x_m+h_m)=\sum\frac{1}{k_1!\ldots k_m!}\frac{\partial^k F}{\partial x_1^{k_1}\ldots\partial x_m^{k_m}}h_1^{k_1}\ldots h_m^{k_m}\quad(3)$$

kifejtés keletkezik, a hol a jobb oldalon a summatio kiterjesztendő a nem negativ $k_1,\ldots,k_m$ egész számok mindama rendszereire, a melyek a

$$k=k_1+k_2+\cdots+k_m\leqq n'$$

feltételt kielégítik. Itt n' az F forma dimensióját jelenti az $x_1,\ldots,x_m$ határozatlanokra vonatkozólag.

A polynomiális tétel.

7. §. Az előbbiek alkalmazása a specziális

$$F = (x_1+x_2+\cdots+x_m)^n$$

formára szolgáltatja a *polynomiális tételt.*

Ekkor ugyanis, ha $k=k_1+k_2+\cdots+k_n$,

$$\frac{\partial^k F}{\partial x_1^{k_1}\,\partial x_2^{k_2}\ldots\partial x_m^{k_m}} = n(n-1)\ldots(n-k+1)(x_1+x_2+\cdots+x_m)^{n-k}$$

és így

$$(x_1+h_1+x_2+h_2+\cdots+x_m+h_m)^n=$$

$$=\sum \frac{n(n-1)\ldots(n-k+1)}{k_1!\,k_2!\ldots k_m!}(x_1+x_2+\cdots+x_m)^{n-k}h_1^{k_1}h_2^{k_2}\ldots h_m^{k_m},$$

vagy pedig, ha még bevezetjük az új

$$h_0=x_1+x_2+\cdots+x_m$$

határozatlant és az

$$n-k=k_0$$

jelölést használjuk, úgy hogy azután

$$\frac{n(n-1)\ldots(n-k+1)}{k_1!\,k_2!\ldots k_m!} = \frac{n!}{k_0!\,k_1!\ldots k_m!},$$

végre lesz

$$(h_0+h_1+\cdots+h_m)^n=\sum \frac{n!}{k_0!\,k_1!\ldots k_m!}h_0^{k_0}h_1^{k_1}\ldots h_m^{k_m}.$$

$$(k_0+k_1+\cdots+k_m=n,\ k_i=0,\ 1,\ 2,\ldots,\ n)$$

Az itt fellépő együtthatók, az ú. n. polynomiális együtthatók — mint származásuk mutatja — pozitiv raczionális és egész számok. A legegyszerűbb ($m=1$) esetben a binomiális együtthatókat még a következő alakokban is írjuk:

$$\frac{n!}{k_0!\,k_1!} = \binom{n}{k_0} = \binom{n}{k_1},$$

hol a két kifejezés identikus volta közvetetlenül abból következik, hogy $k_0+k_1=n$.

Még megállapodunk abban, hogy a symmetria kedvéért legyen

$$\binom{n}{0} = 1;$$

és figyelembe veszszük a következő közvetetlenül igazolható relációt:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Homogén formák.

8. §. Valamely forma *homogén*, ha összes tagjainak dimensiója ugyanaz. Bármely formában mindazokat a tagokat, a melyeknek dimensiói egyenlők, egy-egy részletösszegbe foglalhatjuk össze és ezért azt a következő alakban írhatjuk:

$$F = \Phi_0 + \Phi_1 + \cdots + \Phi_r + \cdots + \Phi_n,$$

a hol Φ_r oly homogén forma, a melynek dimensiója r. Ebből azután az új x_{m+1} határozatlant bevezetve, előállíthatjuk az $x_1, \ldots, x_m, x_{m+1}$ határozatlanoknak következő

$$\Phi = \Phi_0 x_{m+1}^n + \Phi_1 x_{m+1}^{n-1} + \cdots + \Phi_r x_{m+1}^{n-r} + \cdots + \Phi_n$$

homogén formáját, a melynek dimensiója n és a mely az *F-nek megfelelő* homogén forma.

A tagok száma, melyek Φ_n-ben előfordulhatnak, ugyanaz, mint a különböző

$$x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m} \qquad (k_1 + k_2 + \cdots + k_m = n)$$

formák száma, azaz ama különböző nem negativ egész számokból álló rendszerek száma, a melyek a

$$k_1 + \cdots + k_m = n$$

feltételt kielégítik. Ha meg vannak adva m és n, akkor e szám véges számú kisérlettel meghatározható és ezért egyelőre $\{m, n\}$-nel jelölhető. Közvetetlenül világos, hogy

$$\{m, 0\} = 1,$$
$$\{m, 1\} = m.$$

Általánosságban pedig

$$\{m, n\} = \{m-1, n\} + \{m, n-1\},$$

mert itt a jobb oldalon az első helyen áll azon tagoknak száma, a melyek nem tartalmazzák pl. x_m-et és azután az x_m-et tartalmazó tagoknak száma épen annyi mint valamely olyan az $x_1, \ldots, x_m$ határozatlanokat tartalmazó homogén forma tagjainak száma, a melynek dimensiója $n-1$.

Ennek alapján teljes inductio segítségével bebizonyíthatjuk, hogy $\Phi_n(x_1, \ldots, x_m)$-ben a *lehetséges tagok száma*,

$$\{m, n\} = \binom{m+n-1}{n}.$$

Hogy ez az $m=1$ és $n=0$ vagy 1 esetében igaz, közvetetlenül világos; ha pedig megengedjük, hogy igaz mindaddig, míg $m+n$ kisebb bizonyos meghatározott N számnál, akkor

$$\{m, n+1\} = \{m-1, n+1\} + \{m, n\} = \binom{m+n-1}{n+1} + \binom{m+n-1}{n} = \binom{m+n}{n+1}.$$

Ez pedig mutatja, hogy képletünk akkor is érvényes, ha $m+n=N$ és evvel be van bizonyítva általános érvényessége is.

A lehetséges tagok száma oly $F(x_1, \ldots, x_m)$ formában, a melynek dimensiója n, a következő:

$$(m+1, n) = \binom{m+n}{n};$$

mert annak meg kell egyeznie a Φ tagjainak számával. Ha pedig ezt a számot mint $\Phi_0, \Phi_1, \ldots, \Phi_n$ tagszámainak összegét értelmezzük, a következő relációt nyerjük:

$$\binom{m+n}{n} = 1 + \binom{m}{1} + \cdots + \binom{m+r-1}{r} + \cdots + \binom{m+n-1}{n}.$$

9. §. *Az $F(x_1, x_2, \ldots, x_m)$ forma akkor és csak akkor homogén és n-ed dimensiójú, ha*

$$F(tx_1, tx_2, \ldots, tx_m) = t^n F(x_1, x_2, \ldots, x_m).$$

Hogy minden homogén forma Φ_r valóban eleget tesz ilyen

relációnak, közvetetlenül világos. Ha pedig viszont $F=\sum_{i=1}^{k} \Phi_i$, és így

$$F(tx_1, tx_2, \ldots, tx_m) = \sum_{i=1}^{k} \Phi_i(tx_1, tx_2, \ldots, tx_m),$$

akkor, ha F eleget tesz az adott relációnak, egyszersmind lesz:

$$t^n F(x_1, x_2, \ldots, x_m) = \sum_{i=1}^{k} t^i \Phi_i(x_1, x_2, \ldots, x_m)$$

és ha ebben összehasonlítjuk t egyenlő hatványainak együtthatóit mind a két oldalon, azt találjuk, hogy

$$\Phi_i = 0, \quad (i \neq n), \quad \Phi_n = F.$$

Végre még megemlítjük a következő Euler-től származó képletsorozatot, a mely érvényes oly $\Phi(x_1, x_2, \ldots, x_m)$ homogén formára nézve, a melynek dimensiója n:

$$n(n-1)\ldots(n-k+1)\Phi = \sum_{i_k=1}^{m} \ldots \sum_{i_1=1}^{m} x_{i_1} x_{i_2} \ldots x_{i_k} \frac{\partial^k \Phi}{\partial x_{i_1} \partial x_{i_2} \ldots \partial x_{i_k}}. \quad \text{(I)}$$

Hogy a legegyszerübb esetben, midőn $k=1$, valóban

$$n\Phi = \sum_{i=1}^{m} x_i \frac{\partial \Phi}{\partial x_i}, \quad \text{(I}a\text{)}$$

azt közvetetlenül a jobb oldalon kijelölt müveleteket végrehajtásával láthatjuk. A sorozat általános képletét a teljes inductio segítségével igazoljuk. Fölteszszük, hogy a képlet bizonyos k-ra nézve érvényes; akkor Φ minden k-dik deriváltja oly $n-k$-dik dimensiójú forma, a melyre nézve (Ia) szerint a következő érvényes:

$$(n-k) \frac{\partial^k \Phi}{\partial x_{i_1} \partial x_{i_2} \ldots \partial x_{i_k}} = \sum_{i_{k+1}=1}^{m} x_{i_{k+1}} \frac{\partial x^{k+1}}{\partial x_{i_1} \ldots \partial x_{i_k} \partial x_{i_{k+1}}}.$$

Ha ezt (I)-be behelyettesítjük, közvetetlenül nyerjük a a $k+1$ esetének megfelelő képletet.

Vegyük még figyelembe a következő, bármely mennyiségek közt fennálló identitást:

$$\sum_{i_k=1}^{m} \cdots \sum_{i_2=1}^{m} \sum_{i_1=1}^{m} c_{i_1} c_{i_2} \cdots c_{i_k} = (c_1+c_2+\cdots+c_m)^k,$$

a melyről közvetetlenül világos, hogy $k=1$ esetében érvényes és a melynek általános érvényessége a teljes inductio segítségével úgy bizonyítható be, hogy

$$\sum_{i_{k+1}=1}^{m} c_{i_{k+1}} = c_1+c_2+\cdots+c_m$$

-mel szorzunk. Ennek alapján az EULER-féle képleteket e közvetetlenül megérthető és gyakran kényelmesnek mutatkozó

$$n(n-1)\ldots(n-k+1)\Phi = \left(x_1\frac{\partial}{\partial x_1} + x_2\frac{\partial}{\partial x_2} + \cdots + \frac{\partial}{\partial x_m}\right)^k \Phi \quad (\text{II})$$

symbolikus alakban írhatjuk.

Az elemi symmetrikus formák.

10. §. Ha valamely F formában a $z_1, z_2, \ldots, z_r$ határozatlanok helyébe rendre a $z_{i_1}, z_{i_2}, \ldots, z_{i_r}$ határozatlanokat teszszük, hol az $i_1, i_2, \ldots, i_r$ számok az $1, 2, \ldots, r$ számokat bármely tetszőleges sorrendben jelentik, vagy — a mint ezt röviden szoktuk kifejezni — az F formára a

$$\begin{pmatrix} z_1 & z_2 & \cdots & z_r \\ z_{i_1} & z_{i_2} & \cdots & z_{i_r} \end{pmatrix}$$

substitutiót alkalmazzuk, akkor evvel tulajdonképen a forma együtthatóit cseréljük fel egymással bizonyos törvény szerint.

Valamely F formát *a* $z_1, z_2, \ldots, z_r$ *határozatlanok symmetrikus formájának* nevezzük, ha mindig

$$F(z_{i_1}, z_{i_2}, \ldots, z_{i_r}) = F(z_1, z_2, \ldots, z_r),$$

azaz, ha a forma az összes ilyen substitutiók alkalmazása mellett változatlan marad.

Az F forma a $z_1, \ldots, z_r$ határozatlanokon kívül természetesen még más $u_1, u_2, \ldots, u_s$ határozatlanokat is tartalmazhat, a melyekre a föntebbi állítás nem vonatkozik. Ha

az S symmetrikus formát az $u_1, \ldots, u_s$ hatványszorzatai szerint rendezzük:

$$S(z_1, z_2, \ldots, z_r, u_1, u_2, \ldots, u_s) = \Sigma S_j(z_1, z_2, \ldots, z_r)U_j,$$

akkor egyszersmind

$$S(z_{i_1}, z_{i_2}, \ldots, z_{i_r}, u_1, u_2, \ldots, u_s) = \Sigma S_j(z_{i_1}, z_{i_2}, \ldots, z_{i_r})U_j$$

és minthogy az értelmezés szerint a bal oldalon álló kifejezések egyenlők, ebből következik, hogy

$$S_j(z_{i_1}, z_{i_2}, \ldots, z_{i_r}) = S_j(z_1, z_2, \ldots, z_r),$$

azaz, hogy az u-k hatványszorzatai szerint való kifejtésnél minden együttható külön is a $z_1, z_2, \ldots, z_r$ határozatlanoknak symmetrikus formája.

11. §. A symmetrikus formák általános elméletében alapvető jelentőségük van az ú. n. *elemi symmetrikus formáknak*. Ezek a

$$P^{(k)}(z) = (z-x_{k+1})(z-x_{k+2}) \ldots (z-x_m) \qquad (I)$$

formából származnak, a melyet röviden $P^{(k)}(z)$-vel fogunk jelölni. Közvetetlenül belátható, hogy ez a szorzat alakjában felírt forma $x_{k+1}, x_{k+2}, \ldots, x_m$-ben symmetrikus. Ha tehát z hatványai szerint rendezünk, minden együttható is ilyen lesz, és

$$P^{(k)}(z) = z^{m-k} - \mathfrak{f}_1^{(k)} z^{m-k-1} + \cdots + (-1)^r \mathfrak{f}_r^{(k)} z^{m-k-r} + \cdots + (-1)^{m-k} \mathfrak{f}_{m-k}^{(k)}$$

megadja $\mathfrak{f}_1^{(k)}, \ldots, \mathfrak{f}_{m-k}^{(k)}$-t mint az $x_{k+1}, \ldots, x_m$ határozatlanoknak elemi symmetrikus formáit.

Könnyen felismerhető, hogy ezeknek kifejtett alakja, a melyet azonban tulajdonképen nem használunk,

$$\mathfrak{f}_r^{(k)} = \Sigma x_{i_{k+1}} x_{i_{k+2}} \ldots x_{i_{k+r}},$$

a hol a summatio kiterjesztendő az összes a $k+1, \ldots, m$ számokból alkotható különböző combinatiókra, azaz az összes $i_{k+1}, \ldots, i_m$ rendszerekre, melyek a $k+1, \ldots, m$ számokból úgy alkothatók, hogy nem csupán az elrendezésben különbözők.

A $k=0$ esetében, midőn az alkotandó formákban az összes x-ek fellépnek, a lehető egyszerű jelölés kedvéért a felső indexeket elhagyjuk. Végre pedig a könnyebb összefoglalás kedvéért még legyen: $\mathfrak{f}_0^{(k)}=1$. Akkor:

$$P^{(k)}(z)=\sum_{r=0}^{m-k}(-1)^r\,\mathfrak{f}_r^{(k)}\,z^{m-k-r},$$

$$P(z)\quad=\sum_{r=0}^{m}(-1)^r\,\mathfrak{f}_r\,z^{m-r}.$$

A $z=u+x_{k+i}$ transformatio a következőre vezet:

$$P^{(k)}(u+x_{k+i})=\sum_{r=0}^{m-k}(-1)^r\,\mathfrak{f}_r^{(k)}(u+x_{k+i})^{m-k-r},$$

a hol a bal oldalon — mint közvetetlenül látni — u mint tényező szerepel. Ha tehát a jobb oldalon u hatványai szerint rendezünk, az u-tól mentes tagnak 0-nak kell lennie. E megjegyzés alapján világos, hogy érvényes a következő alapvető azonosság:

$$\sum_{r=0}^{m-k}(-1)^r\,\mathfrak{f}_r^{(k)}\,x_{k+i}^{m-k-r}=P^{(k)}(x_{k+i})=0,\qquad (i=1,2,\ldots,m-k)\qquad (\mathrm{II})$$

$k=0$ esetében

$$\sum_{r=0}^{m}(-1)^r\mathfrak{f}_r\,x_i^{m-r}=P(x_i)=0,\qquad (i=1,2,\ldots,m)\qquad (\mathrm{II}_0)$$

E kettő ismét, mint majd kimutatjuk, a következő *identitásra* vezet:

$$|\,x_{k+i}^{m-k-j}\,|=\prod_{r,\,s}(x_r-x_s),\quad \begin{pmatrix} i,j=1,2,\ldots,m-k,\\ r,s=k+1,\ldots,m,\\ r<s\end{pmatrix},\qquad (\mathrm{III})$$

vagyis — a mint ezt még kifejezhetjük — a bal oldalon álló determináns explicit kiszámítására. Különösen, ha $k=m-2$, akkor valóban

$$\begin{vmatrix} x_{m-1} & 1\\ x_m & 1\end{vmatrix}=x_{m-1}-x_m.$$

Igy tehát a tétel általános bebizonyítására a teljes inductiót használhatjuk. A kiszámítandó determináns i-dik

sora részletesen kiírva a következő:

$$x_{k+i}^{m-k-1},\ x_{k+i}^{m-k-2},\ \ldots,\ x_{k+i}^{m-k-j},\ \ldots,\ x_{k+i},\ 1.$$

Ha tehát a második, ..., j-dik, ..., utolsó előtti és utolsó oszlop elemeit rendre a következőkkel szorozzuk:

$$-\mathfrak{f}_1^{(k+1)},\ldots,\ (-1)^{j-1}\mathfrak{f}_{j-1}^{(k+1)},\ldots,(-1)^{m-k-2}\mathfrak{f}_{m-k-2}^{(k+1)},\ (-1)^{m-k-1}\mathfrak{f}_{m-k-1}^{(k+1)}$$

és azután az első oszlophoz hozzáadjuk, akkor az így átalakított determinánsban c_{i1} * a következő lesz:

$$\sum_{r=0}^{m-k-1}(-1)^r\mathfrak{f}_r^{(k+1)}\,x_{k+i}^{m-k-r-1}=P^{(k+1)}(x_{k+i}),$$

és így az első sorban

$$c_{11}=P^{(k+1)}(x_{k+1})=(x_{k+1}-x_{k+2})(x_{k+1}-x_{k+3})\ldots(x_{k+1}-x_m)$$

és a többi sorban $c_{i1}=0,\ (i\neq 1)$. A determináns tehát felbomlik $P^{(k+1)}(x_{k+1})$ és egy az $x_{k+2},\ldots,x_m$-ből hasonló módon alakított determináns szorzatára, a melyről már feltettük, hogy (III) szerint kiszámítható, és így

$$|\,x_{k+i}^{m-k-j}\,|=P^{(k+1)}(x_{k+1})\prod_{r,s}(x_r-x_s),\qquad \left(\begin{matrix}i,j=1,2,\ldots,m-k\\ r,s=k+2,\ldots,m\\ r<s\end{matrix}\right),$$

a hol a jobb oldalról közvetetlenül felismerhető, hogy azonos (III)-nak jobb oldalával.

A különbségek ama szorzatának négyzetét $\Delta(x_{k+1},\ldots,x_m)$-mel, vagy Δ_k-val fogjuk jelölni és ennek alapján az épen nyert eredményt a következő új és leginkább használt alakban írjuk:

$$|\,x_{k+i}^{m-k-j}\,|^2=\Delta(x_{k+1},\ldots,x_m)=\Delta_k,\quad (i,j=1,2,\ldots,m-k)\qquad (\mathrm{III}a)$$

* Hacsak lehetséges, a szemlélés támogatására a determinánsokat mindig a $|\,c_{ij}\,|$ alakban fogjuk felírni, úgy hogy c_{ij} jelentse az i-dik sornak azt az elemét, a mely a j-dik oszlopban áll. A determinánsokat helykimélés szempontjából legtöbbnyire nem írjuk a részletes alakban, a mit azután a kevésbbé gyakorlott olvasó mindig maga is megtehet.

12. §. Ugyanez a módszer vezet *a következő általánosabb* $m(m-1)\ldots(m-e+1)$*-edik fokú determináns értékének meghatározásához*:

$$|x_{i_1}^{j_1} x_{i_2}^{j_2} \ldots x_{i_e}^{j_e}|, \quad \begin{pmatrix} i_1, i_2, \ldots, i_e = 1, 2, \ldots, m \\ i_r \neq i_s \\ 0 \leqq j_r \leqq m-r \end{pmatrix},$$

hol a szemlélet megrögzítésére* az első sorban legyen $i_1=1, i_2=2, \ldots, i_e=e$ és az első sor elemei mint az x-ek hatványszorzatai magasságuk szerint legyenek rendezve. Különösen $c_{11}=x_1^{m-1} x_2^{m-2} \ldots x_e^{m-e}$ és minthogy e megállapodások alapján c_{11} az egész determinánst jellemzi, ezt gyakran

$$[x_1^{m-1} x_2^{m-2} \ldots x_e^{m-e}]$$

-vel fogjuk jelölni. Ezen kívül természetesen a sorok sorrendjét, azaz az $(i_1, i_2, \ldots, i_e)$ rendszerek sorrendjét is meg kell állapítanunk; a mennyiben pedig ez nem történt meg, a determináns előjele határozatlan marad.

Hogy ezt a determinánst kiszámíthassuk, azt bizonyos sajátságos symbolikus determináns alakjában fogjuk írni. Legyen ugyanis e symbolikus determináns első sora a következő:

$$x_1^{m-1}[x_2^{m-2} \ldots x_e^{m-e}],\ x_1^{m-2}[x_2^{m-2} \ldots x_e^{m-e}], \ldots,$$
$$x_1[x_2^{m-2} \ldots x_e^{m-e}], [x_2^{m-2} \ldots x_e^{m-e}],$$

míg az i-dik sor az elsőből x_1-nek x_i-vel való felcserélése révén keletkezzék. A determináns tehát most m sorból és m oszlopból áll; de úgy hogy minden egyes eleme a zárójeles kifejezés jelölte determináns elemeinek egész schémáját jelenti, a melyek közül mindegyikhez még az elől álló tényező hozzácsatolandó. Minden egyes elem tehát egy-egy $(m-1)\ldots(m-e+1)$-edik fokú determináns-schéma jelképe

* Az itt felhasznált $(i_1, \ldots, i_e)$ rendszerek tulajdonképen az $1, \ldots, n$ elemeknek ismétlés nélküli e-tagú variációi.

és ha azokat a leírt módon egymás mellé sorozzuk, akkor — mint az közvetetlenül belátható — a kiszámítandó determináns származik.

Minthogy továbbá a zárójeles kifejezés minden egyes sorban végig mindenütt ugyanaz, azon azonos átalakítás, a mely szerint valamely oszlopnak bármely tényezővel megszorzott elemeit valamely más oszlop megfelelő elemeihez hozzáadjuk, itt sem fogja megváltoztatni a determináns értékét; mert ez ugyanaz, mintha a valóságos determinánsban az oszlopok egész sorának bizonyos tényezőkkel megszorzott elemeit az oszlopok más sorának megfelelő elemeihez adnók hozzá.

Ha tehát a symbolikusan felírt determináns 2-dik, . . ., m-dik oszlopát a következőkkel megszorozzuk:

$$-f_1^{(1)},\ f_2^{(1)},\ \ldots,\ (-1)^{m-1} f_{m-1}^{(1)}$$

és azután az első oszlophoz hozzáadjuk (I) és (II) alapján nyerjük, hogy

$$c_{11} = P^{(1)}(x_1)\,[x_2^{m-2} \ldots x_e^{m-e}],\ c_{i1} = 0, \qquad (i>1).$$

Ha már mostan az így átalakított determináns 3-dik, . . ., m-dik oszlopát a következőkkel megszorozzuk:

$$-f_1^{(2)},\ f_2^{(2)},\ \ldots,\ (-1)^{m-2} f_{m-2}^{(2)}$$

és azután a második oszlophoz hozzáadjuk, lesz:

$$c_{22} = P^{(2)}(x_2)\,[x_2^{m-2} \ldots x_e^{m-e}]_{(1,2)},\ c_{i2} = 0, \qquad (i>2).$$

a hol a zárójelhez hozzácsatolt (1, 2) jel azt jelenti, hogy x_1 felcserélendő x_2-vel.

Ezt az eljárást ugyanazon a módon folytatva általánosságban az r-dik oszlopot úgy fogjuk átalakítani, hogy

$$c_{rr} = P^{(r)}(x_r)\,[x_2^{m-2} \ldots x_e^{m-e}]_{(1,r)},\ c_{ir} = 0, \qquad (i>r)$$

lesz.

Akkor azonban a keresett determináns az

$$[x_2^{m-2} \dots x_e^{m-e}]_{(1,r)}, \quad (r=1, 2, \dots, m)$$

determinánsok szorzata, a hol minden egyes determináns minden eleme még előbb a megfelelő $P^{(r)}(x_r)$-rel, vagy pedig, minthogy e determinánsok foka $(m-1) \dots (m-e+1)$, az maga $(P^{(r)}(x_r))^{(m-1)\dots(m-e+1)}$-vel megszorzandó.

Igy tehát

$$[x_1^{m-1} x_2^{m-2} \dots x_e^{m-e}] = [x_1^{m-1}]^{(m-1)\dots(m-e+1)} \prod_{r=1}^{m} [x_2^{m-2} \dots x_e^{m-e}]_{(1,r)}, \quad \text{(IV)}$$

mert

$$P^{(1)}(x_1)\, P^{(2)}(x_2) \dots P^{(m-1)}(x_{m-1}) = \prod_{\substack{r,s \\ r<s}} (x_r - x_s),$$

$$\left(\begin{matrix} r, s=1, 2, \dots, m \\ r<s \end{matrix}\right)$$

és a különbségek e szorzata a már bevezetett irásmód szerint $[x_1^{m-1}]$-vel jelölhető.

Ez közvetetlenül a *kérdéses determináns következő általános meghatározásához* vezet:

$$[x_1^{m-1} x_2^{m-2} \dots x_e^{m-e}] = \pm [x_1^{m-1}]^{\varphi(m,e)} \quad \text{(V)}$$

$$\varphi(m, 1) = 1, \quad \varphi(m, 2) = 2m - 3$$

$$\varphi(m, e) = \frac{e(2m-e-1)}{2} (m-2)(m-3) \dots (m-e+1). \quad (e>2)$$

Az előjel természetesen a determináns soraira vonatkozólag megállapított sorrendtől függ. Teljes inductióval ki lesz mutatható, hogy (V) általánosan érvényes; mert $e=1$ esetében a két oldal formálisan is megegyezik. Ha feltételezzük, hogy (V) valamely $e-1$ esetében érvényes, akkor most már általánosságban

$$[x_2^{m-2} \dots x_e^{m-e}]_{(1,r)} = \pm X_r^{\varphi(m-1, e-1)},$$

a hol X_r az $x_1, x_2, \dots, x_m$ határozatlanokból az x_r kizárá-

sával alkotható különbségek szorzatát jelenti. Minthogy $x_r - x_s$ az X_r és X_s kivételével minden X_i-ben egyszer fordul elő, lesz

$$\prod_{r=1}^{m} [x_2^{m-2} \dots x_e^{m-e}]_{(1,r)} = \pm [x_1^{m-1}]^{(m-2)\varphi(m-1,e-1)}$$

és ezért

$$[x_1^{m-1} x_2^{m-2} \dots x_e^{m-e}] = \pm [x_1^{m-1}]^{(m-1)(m-2)\dots(m-e+1)+(m-2)\varphi(m-1,e-1)}.$$

Ez szolgáltatja * $\varphi(m, e)$-nek a következő képletben megadott recursiv meghatározási módját:

$$\varphi(m, e) = (m-1) \dots (m-e+1) + (m-2)\varphi(m-1, e-1),$$

a mely a legegyszerűbb esetekben (V)-tel megegyezőleg a következőket szolgáltatja:

$$\varphi(m, 2) = 2m-3, \quad \varphi(m, 3) = 3(m-2)^2,$$

míg általánosságban, midőn $e > 3$,

$$\varphi(m, e) = (m-1) \dots (m-e+1) + \\ + (m-2)\frac{(e-1)(2m-e-2)}{2}(m-3) \dots (m-e+1)$$

$$= \left(m-1 + \frac{(e-1)(2m-e-2)}{2}\right)(m-2) \dots (m-e+1),$$

a mi szintén azonos (V)-nek megfelelő adatával.

Végre e determináns négyzetét az

$$[x_1^{m-1} x_2^{m-2} \dots x_e^{m-e}]^2 = \Delta^{\varphi(m,e)} \qquad \text{(VI)}$$

képlet szolgáltatja, hol $\Delta(x_1, x_2, \dots, x_m)$ helyett rövidebben Δ-t írtunk.

* Ha már meg van állapítva, hogy a kérdéses determináns ama különbségszorzatnak hatványa, akkor — Rados Gusztáv collegám egy szóbeli közlése szerint — a $\varphi(m, e)$ egész szám értékét közvetetlenül úgy nyerhetjük, hogy e determinánsnak, mint az $x_1, \dots, x_m$ határozatlanok formájának dimensióját direkt úton kiszámítjuk.

A redukált formák.

13. §. KRONECKER-től* származó egyik alapvető tétel szerint *az* $x_1, x_2, \ldots, x_m$ *határozatlanoknak minden formája, F egy és csak egy redukált formával,* azaz *egy*

$$\sum_{(j)} \mathfrak{F}_j x_1^{j_1} x_2^{j_2} \ldots x_{m-1}^{j_{m-1}} \qquad (0 \leqq j_r \leqq m-r;\ r=1, \ldots, m-1)$$

*alakú kifejezéssel egyenlő, hol*** $\mathfrak{F}_j$ *az* $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ *«elemi symmetrikus formák formája»*, vagyis más szóval $\mathfrak{F}_j$ *ilyen alakú kifejezés:*

$$\mathfrak{F}_j = \sum_{(g)} C_g \mathfrak{f}_1^{g_1} \mathfrak{f}_2^{g_2} \ldots \mathfrak{f}_m^{g_m},$$

a hol ismét C_g *az eredeti* $F(x_1, \ldots, x_m) = \sum_{(h)} A_h x_1^{h_1} x_2^{h_2} \ldots x_m^{h_m}$ *forma együtthatóinak «raczionális és egész lineáris formája»,*

azaz

$$C_g = \sum_{(h)} k_h A_h,$$

a melyben a k_h*-k raczionális és egész számokat jelentenek.*

Egy határozatlan esetében a tétel elveszti ugyan tartalmát, de azért mégis helyes, mert akkor egyszerűen $x_1 = \mathfrak{f}_1$

Két határozatlan, x_1 és x_2 esetében a jellemzett átalakítás közvetetlenül elvégezhető. Először mindenütt $x_2 = \mathfrak{f}_1 - x_1$ teendő és azután az

$$x_1^2 - \mathfrak{f}_1 x_1 + \mathfrak{f}_2 = 0$$

identitás alapján, a mely ebben az alakban is írható:

* «Über die verschiedenen Sturm'schen Reihen». Mon. Ber Berl. Ak. Febr. 1873. Werke I. köt. 323. lap.

** Azt a kifejezést, a mely az $F(x_1, \ldots, x_m)$ formából származik, ha az $x_1, \ldots, x_m$ határozatlanok helyébe az $X_1, \ldots, X_m$ mennyiségeket helyettesítjük, röviden az $X_1, \ldots, X_m$ mennyiségek formájának nevezzük. Valamely forma «raczionális és egész», ha együtthatói raczionális és egész számok.

$$x_1^k - \mathfrak{f}_1 x_1^{k-1} + \mathfrak{f}_2 x_1^{k-2} = 0 \qquad (k \geqq 2)$$

mindenünnen, a hol $k \geqq 2$, formálisan eltávolíthatjuk x_1^k-t és így közvetetlenül a redukált formához jutunk.

Általánosságban a redukált forma felállításához a teljes inductio vezet.

Ha F-et x_1 hatványai szerint rendezzük, akkor minden egyes együtthatója az $x_2, \ldots, x_m$ határozatlanok formája esz, a melyről felteszszük, hogy a

$$\sum_{(j)} \mathfrak{F}_j^{(1)} x_2^{j_2} \ldots x_{m-1}^{j_{m-1}} \qquad (0 \leqq j_r \leqq m-r)$$

alakban írható fel, hol $\mathfrak{F}_j^{(1)}$ az $\mathfrak{f}_1^{(1)}, \ldots, \mathfrak{f}_{m-1}^{(1)}$ elemi symmetrikus formák formája és együtthatói az adott forma együtthatóinak raczionális és egész lineáris formái. Ámde, ha felhasználjuk a

$$(z - x_1)(z^{m-1} - \mathfrak{f}_1^{(1)} z^{m-2} + \mathfrak{f}_2^{(1)} z^{m-3} - \ldots) = z^m - \mathfrak{f}_1 z^{m-1} + \mathfrak{f}_2 z^{m-2} - \ldots$$

identitásból származó további identitásokat:

$$\begin{aligned}
&x_1 + \mathfrak{f}_1^{(1)} = \mathfrak{f}_1, \\
&x_1 \mathfrak{f}_1^{(1)} + \mathfrak{f}_2^{(1)} = \mathfrak{f}_2, \\
&\ldots\ldots\ldots \\
&x_1 \mathfrak{f}_{r-1}^{(1)} + \mathfrak{f}_r^{(1)} = \mathfrak{f}_r, \\
&\ldots\ldots\ldots \\
&x_1 \mathfrak{f}_{m-2}^{(1)} + \mathfrak{f}_{m-1}^{(1)} = \mathfrak{f}_{m-1},
\end{aligned}$$

melyek még így is írhatók:

$$\begin{aligned}
\mathfrak{f}_1^{(1)} &= \mathfrak{f}_1 - x_1, \\
\mathfrak{f}_2^{(1)} &= \mathfrak{f}_2 - \mathfrak{f}_1 x_1 + x_1^2, \\
&\ldots\ldots\ldots \\
\mathfrak{f}_r^{(1)} &= \mathfrak{f}_r - \mathfrak{f}_{r-1} x_1 + \mathfrak{f}_{r-2} x_1^2 - \mathfrak{f}_{r-3} x_1^3 + \cdots + (-1)^r x_1^r, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\mathfrak{f}_{m-1}^{(1)} &= \mathfrak{f}_{m-1} - \mathfrak{f}_{m-2} x_1 + \mathfrak{f}_{m-3} x_1^2 + \cdots + (-1)^{m-1} x_1^{m-1},
\end{aligned}$$

akkor $\mathfrak{F}_j^{(1)}$ helyébe lép az $x_1, \mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_{m-1}$ formája, a melynek együtthatói állításunknak megfelelnek. Ha végre az

$$x_1^m - \mathfrak{f}_1 x_1^{m-1} + \mathfrak{f}_2 x_1^{m-2} - \cdots + (-1)^m \mathfrak{f}_m = 0$$

identitás alapján mindenünnen eltávolítjuk x_1^{m+k}-t, a hol $k \geqq 0$, a felsorolt tulajdonságoknak megfelelő redukált forma keletkezik.

Hogy *csak egy ilyen* redukált forma van, az egy határozatlan esetében közvetetlenül világos; általánosságban pedig ismét a teljes inductio segítségével bebizonyítható.

A jelzett müveletek, melyek a redukált formához vezetnek, ugyanis megfordíthatók. Ha t. i. a redukált formában $\mathfrak{f}_m$ helyett ismét x_1-et vezetjük be, azután pedig $\mathfrak{f}_1, \ldots, \mathfrak{f}_{m-1}$ helyett $\mathfrak{f}_1^{(1)}, \ldots, \mathfrak{f}_{m-1}^{(1)}$-et, és végre x_1 hatványai szerint rendezünk, megkapjuk ismét F-et, x_1 hatványai szerint rendezve a

$$\sum_{(j)} \mathfrak{F}_j^{(1)} x_2^{j_2} \ldots x_{m-1}^{j_{m-1}} \qquad (0 \leqq j_r \leqq m-r)$$

alakú együtthatókkal.

Ha most már F számára két különböző redukált forma léteznek, ugyan így az F-nek egy második, szintén x_1 hatványai szerint rendezett alakját nyernők bizonyos

$$\sum_{(j)} \overline{\mathfrak{F}}_j^{(1)} x_2^{j_2} \ldots x_{m-1}^{j_{m-1}}$$

együtthatókkal, melyek az előbbiekkel minden esetre rendre egyenlők; de *azonosan* egyenlők, mert az $x_2, \ldots, x_m$, számra nézve $m-1$ határozatlannak redukált formái.

Tehát az $F(x_1, \ldots, x_m)$-nek megfelelö és különbözőnek föltételezett két redukált forma azonos.

14. §. *Ha a redukálandó forma $x_{k+1}, \ldots, x_m$-re nézve symmetrikus,* — a mely esetben azt $S^{(k)}(x_1, \ldots, x_m)$-mel fogjuk jelölni, — *akkor a redukált formából kiesnek mindazok a tagok, a melyekben $x_{k+1}, \ldots, x_m$ explicite fordulna elő.*

Hogy ezt bebizonyítsuk, az $S^{(k)}$-nak megfelelő redukált formát az $x_{k+1}, \ldots, x_m$ határozatlanok hatványszorzatai szerint rendezzük, a mi ily alakú identitásra vezet:

$$\Phi_h x_{k+1}^{h_{k+1}} \ldots x_{m-1}^{h_{m-1}} + \cdots + \Phi_j x_{k+1}^{j_{k+1}} \ldots x_{m-1}^{j_{m-1}} + \cdots + \Phi_0 - S^{(k)} = 0,$$

a hol a Φ együtthatók még csak $x_1, \ldots, x_k, \mathfrak{f}_1, \ldots, \mathfrak{f}_m$-et tartalmazzák.

Ha ebben az identitásban $x_{k+1}, \ldots, x_m$ helyébe $x_{r_{k+1}}, \ldots, x_{r_m}$-et teszszük, a hol $r_{k+1}, \ldots, r_m$ a $k+1, \ldots, m$ számok bármely permutációját jelentheti, akkor az identitás ilyen marad; de ekkor egy Φ sem változik és feltevésünk szerint $S^{(k)}$ sem. Igy tehát $(m-k)!$ reláczió származik, a melyek mint a $\Phi_h, \ldots, \Phi_j, \ldots, \Phi_0 - S_k$ meghatározására szolgáló homogén lineáris egyenletek foghatók fel, a mely mennyiségek száma szinte $(m-k)!$

Ámde ennek az egyenletrendszernek determinánsa: $[x_{k+1}^{m-k-1} x_{k+2}^{m-k-2} \ldots x_{m-1}]$ ismét a 0-tól különböző mennyiség; tehát

$$\Phi_j = 0, \quad (j>0); \quad \Phi_0 = S^{(k)},$$

a mi épen bebizonyítandó volt.

A $k = 0$ esetére ebből kiadódik *a symmetrikus formáknak az elemi symmetrikus formákból való előállítására vonatkozó főtétel, vagyis részletesebben:*

Minden $S(x_1, \ldots, x_m)$ symmetrikus forma előállítható mint az $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ elemi symmetrikus formák formája, a melyben az együtthatók az S-ben fellépő együtthatóknak racziónális és egész, homogén lineáris formái.

Ezt az előállítást elvileg a redukált forma kiszámítása szolgáltatja. A specziális módszerek egész sora, a melyeket itt tovább nem fejtegetünk, szolgál ennek az eljárásnak rövidítésére és egyszersmind reávezet a megfelelő redukált formának $S(x_1, \ldots, x_m)$ által megadott tulajdonságaira.

Az előbbiből folyó további fontos következtetés a következő tételbe foglalható össze.

Az $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$ *elemi symmetrikus formák egymástól függetlenek.* E rövid kifejezéssel a következő tényt akarjuk előadni: *Ily alakú identitás*

$$\sum_{(g)} A_g \mathfrak{f}_1^{g_1} \mathfrak{f}_2^{g_2} \ldots \mathfrak{f}_m^{g_m} = 0,$$

csak úgy állhat fenn, ha az összes A_g *együtthatók egyenlők* 0*-sal; bárhogy is válaszszuk azt a holoid* $[A]$ *tartományt, a melyhez az* A_g *együtthatók tartoznak.* Itt a dolog természetének megfelelőleg csak azt tételezzük fel, hogy $x_1, x_2, \ldots, x_m$ *új* határozatlanok; tehát nem talán az $[A]$ tartományhoz tartozó mennyiségek. Ezt a messzeható tételt a következőkben mint *Gauss elvét* fogjuk idézni, mert GAUSS mutatott reá először annak fontosságára az algebra bizonyító módszereiben *.

Ilyen identitás ugyanis, a melyben nem tünnek el az összes A_g-k, a 0 előállítására szolgáló redukált forma volna, a mely különböznék attól, a melyben az összes A_g-k egyenlők zérussal és így — a mint az magától értetődik — a zérust szolgáltatja. Ilyen második redukált forma azonban — a mint azt bebizonyítottuk — nem lehetséges.

15. §. Az elemi symmetrikus formák épen kifejtett tulajdonságával — a mint azt alkalmas helyen (V. fej. 15. §.) a függvénydeterminánsok elméletében meg fogjuk mutatni — szorosan kapcsolatos az

$$|\mathfrak{f}_{rs}|, \quad (r, s = 1, \ldots, m)$$

determináns értékének meghatározása, a hol

$$\mathfrak{f}_{rs} = \frac{\partial \mathfrak{f}_r}{\partial x_s}.$$

* «Demonstratio nova altera». Werke III. köt.

E czélból kiindulunk a 10. §-ban felállított

$$P(z) = (z-x_1)\ldots(z-x_m) = \sum_{r=0}^{m}(-1)^r \mathfrak{f}_r\, z^{m-r}$$

identitásból. Ha ebben x_s szerint deriválunk, lesz:

$$\frac{\partial}{\partial x_s} P(z) = \sum_{r=1}^{m}(-1)^r \mathfrak{f}_{rs}\, z^{m-r}, \qquad (1)$$

a hol még

$$\frac{\partial}{\partial x_s} P(z) = -\prod_{h=1}^{m}{}^{(s)}(z-x_h),$$

ha a $\prod_{h=1}^{m}{}^{(s)}$ jel arra utal, hogy a szorzatot a $h=s$-nek megfelelő tényező kihagyásával alkossuk. Legyen még

$$P'(z) = \frac{\partial}{\partial z} P(z) = \sum_{i=1}^{m}\prod_{h=1}^{m}{}^{(i)}(z-x_h),$$

akkor, ha (1)-ben z helyébe x_i-t helyettesítjük, azt találjuk, hogy

$$\sum_{r=1}^{m}(-1)^{r-1}\mathfrak{f}_{rs}\, x_i^{m-r}$$

vagy $P'(x_i)$-vel, vagy pedig 0-sal egyenlő a szerint, a mint i egyenlő s-sel, vagy pedig s-től különböző. Ez oly meghatározás, a mely, ha a δ_{gh} jelt avval a jelentéssel vezetjük be, hogy

$$\delta_{gg} = 1,\ \delta_{gh} = 0, \qquad (g \neq h),$$

a következő egységes alakban írható:

$$\sum_{r=1}^{m}(-1)^{r-1}\mathfrak{f}_{rs}\, x_i^{m-r} = \delta_{is}\, P'(x_i), \qquad (i, s = 1, 2, \ldots, m) \qquad (D)$$

Ebből a determinánsok szorzástétele alapján közvetetlenül következik, hogy

$$\left|(-1)^{r-1}\mathfrak{f}_{rs}\right|\left|x_i^{m-r}\right| = \prod_{i=1}^{m} P'(x_i), \qquad (i, r, s = 1, 2, \ldots, m),$$

vagy pedig, minthogy a jobb oldalon $x_i - x_j$ kétszer-kétszer, még pedig ellenkező előjellel fordul elő, hogy

$$= (-1)^{\frac{m(m-1)}{2}} \prod_{r,s} (x_r - x_s)^2. \quad (r<s).$$

Ha már mostan a bal oldalon minden oszlopban elhagyjuk $(-1)^{r-1}$-et $(r = 1, \ldots, m)$ és ennek megfelelőleg a jobb oldalon $(-1)^{\frac{m(m-1)}{2}}$-et, lesz:

$$|f_{rs}|\,|x_i^{m-r}| = \prod_{r,s} (x_r - x_s)^2,$$

vagy pedig tekintettel a 11. §. (III) alatti relációjára, végre

$$|f_{rs}| = |x_i^{m-j}| = \prod_{r,s} (x_r - x_s), \quad (i,j,r,s=1,\ldots,m).$$

16. §. Be fogjuk most bizonyítani *a determinánsok elméletébe tartozó* következő egyszerű, de sokszorosan hasznos *lemmát*:

Ha az

$$A = |a_{rs}|, \quad B = |b_{ij}|, \quad (i,j,r,s=1,\ldots,m)$$

determinánsokra nézve az első determináns oszlopainak compositiója a második determináns soraival azt szolgáltatja, hogy

$$\sum_{k=1}^{m} a_{ks} b_{ik} = \delta_{is}, \tag{1}$$

akkor az első determináns sorainak compositiója a másodiknak oszlopaival azt adja, hogy

$$\sum_{k=1}^{m} a_{rk} b_{kj} = \delta_{rj}, \tag{2}$$

a hol a δ jel értelme az előbb megállapított.

Az (1) alatt felállított egyenletek, a melyeknek száma m^2, közvetetlenül lineáris egyenletekből álló m egyenletrendszernek tekinthetők, a melyek egyenként i valamely értékére nézve a b_{ik} $(k = 1, \ldots, m)$ menyiségeket szolgáltatják; még pedig, ha az a_{rs}, b_{ij} elemek adjungált aldeterminánsait a szokott módon A_{rs}-sel és B_{ij}-vel jelöljük, akkor lesz:

$$Ab_{ik} = \sum_{s=1}^{m} \delta_{is} A_{ks} = A_{ki}$$

és

$$A \sum_{k=1}^{m} a_{rk} b_{kj} = \sum_{k=1}^{m} a_{rk} A_{jk} = \delta_{rj} A,$$

a miből, minthogy $AB = 1$, tehát A nem zérus, valóban a (2) alatt felállított relációk következnek.

Most már az $[A, x_1, \ldots, x_m]$ holoid tartományról — mint az az első fejezet 4. §-a szerint meg van engedve — áttérünk a megfelelő orthoid tartományra és ekkor a

$$|(-1)^{r-1} \mathfrak{f}_{rs}| \text{ és } \left| \frac{x_i^{m-r}}{P'(x_i)} \right|, \quad (i, r, s = 1, 2, \ldots, m)$$

determinánsokban olyanokat ismerünk fel, a melyek az előbbi §. (*D*) relációja szerint az épen bebizonyított lemmának megfelelnek. Igy tehát közvetetlenül nyerjük a KRONECKER-től* származó következő relációkat:

$$\sum \frac{(-1)^{r-1} \mathfrak{f}_{rk} x_k^{m-j}}{P'(x_k)} = \delta_{rj}, \qquad (E)$$

a melyekből, ha $r=1$, különös esetként az ú. n. EULER-féle képletek adódnak ki. Ugyanis közvetetlenül látni, hogy

$$\mathfrak{f}_{1k} = \frac{\partial \mathfrak{f}_1}{\partial x_k} = 1,$$

és így ebben az esetben lesz:

$$\sum_{k=1}^{m} \frac{x_k^{m-j}}{P'(x_k)} = \delta_{1j}. \qquad (E')$$

Ha (E)-ben x^{m-1}-ve szorzunk és azután az $r=1, \ldots, m$ ese-

* «Über die symmetrischen Functionen». Mon. Ber. Berl. Ak. 1880. 948. lap. (Werke IV. köt.)

teknek megfelelő egyenleteket összeadjuk, még a következőket nyerjük:

$$\sum_{k=1}^{m} \frac{x_k^{m-j} \sum_{r=1}^{m} (-1)^{r-1} \mathfrak{f}_{rk} x^{m-r}}{P'(x_k)} = x^{m-j}. \qquad (j=1, \ldots, m)$$

Ebben azonban a 15. §. szerint

$$\Sigma (-1)^{r-1} \mathfrak{f}_{rk} x^{m-r} = \prod_{h=1}^{m(k)} (x - x_h) = P_k(x),$$

a hol még az $x-x_h$, $(h=1, \ldots, m)$ tényezőkből az $x-x_k$ kizárásával alkotott szorzat rövid jelölésére bevezettük a $P_k(x)$ jelt és így végre a

$$\sum_{k=1}^{m} \frac{x_k^{m-j} P_k(x)}{P'(x_k)} = x^{m-j} \qquad (j=1, \ldots, m) \qquad (L')$$

képlethez jutunk, a mely közvetíteni fogja az átmenetet az egész függvények elméletére, különösen azoknak meghatározására adott értékekből, e fejezet 2. §-a értelmében.

Az egész függvények.

17. §. A

$$P(x) = \prod_{k=1}^{m} (x - x_k)$$

értelmezés közvetetlen következménye, hogy

$$\frac{\partial}{\partial x} P(x) = P'(x) = \sum_{k=1}^{m} P_k(x),$$

és így

$$P'(x_k) = P_k(x_k)$$

mint a 0-tól különböző adódik ki, míg

$$P_k(x_h) = 0; \qquad (h \pm k)$$

tehát

$$\frac{P_k(x_h)}{P'(x_k)} = \delta_{hk}.$$

Ez nemcsak az előbbi fejtegetéstől független úton vezet (L')-hez, hanem mindjárt az abban foglalt, de formálisan általánosabb *Lagrange-féle interpoláczió-képlethez* is.

Ha ugyanis

$$f(x) = A_0 + A_1 x + \cdots + A_{m-1} x^{m-1}$$

x-nek oly egész függvénye, a melynek foka nem éri el m-et és a mely $x = x_k$-ra nézve $(k = 1, \ldots, m)$ az $f(x_k)$ értéket veszi fel, akkor

$$f(x) = \sum_{k=r}^{m} \frac{f(x_k)\, P_k(x)}{P'(x_k)}. \qquad (L)$$

Hogy a jobb oldalon álló kifejezés $x = x_k$-ra nézve valóban mindig $f(x_k)$-val egyenlő, közvetetlenül világos; hogy pedig annak $f(x)$-szel teljesen meg kell egyeznie, a következő alapvető tételből következik:

Egy és csak egy oly egész függvény van, a melynek foka nem éri el m-et és a mely x-nek m különböző értékére nézve adott értékeket vesz fel.

E feltételek alapján az egész függvény együtthatóira nézve a következő egyenletek állanak fönn:

$$A_0 + A_1 x_k + A_2 x_k^2 + \cdots + A_{m-1} x_k^{m-1} = f(x_k). \qquad (k = 1, \ldots, m).$$

Ezek az A_i-k meghatározására szolgáló oly lineáris egyenletrendszert alkotnak, melynek determinánsa, $[x_1^{m-1}]$ nem tünik el és így az A_i-k egyértelmű meghatározását szolgáltatja.

Meg kell azonban jegyeznünk, hogy még akkor is, ha az x_k és $f(x_k)$ mennyiségek mindannyian az [A] tartományhoz tartoznak, a megfelelő egész függvény együtthatói általánosságban olyanok lesznek, a melyek csak a bővített (A) tartományban foglaltatnak. (Pl. az az elsőfokú egész függvény, a melyre nézve $f(3) = 3$, $f(9) = 7$, lesz: $\frac{2}{3} x + 1$).

Ugyanazt a tételt még a következő módon is fogalmazhatjuk:

Ha $\xi_1, \xi_2, \ldots, \xi_{n+1}$ *különböző mennyiségek és* $f(x)$ *oly egész függvény, a melynek foka nem magasabb n-nél és a melynek nem tünik el minden együtthatója, akkor az* $f(\xi_1)$, $f(\xi_2), \ldots, f(\xi_{n+1})$ *mennyiségek nem lehetnek mind zérusok.*

Ellenkező esetben 0 és $f(x)$ két oly különböző egész függvény volna, a mely mind a kettő alacsonyabb fokú $n+1$-nél és x-nek $n+1$ különböző értékére nézve egyenlő értékeket vesz fel.

A tétel utóbb adott alakja közvetetlenül a következő általánosításhoz vezet:

Legyen $F(x_1, x_2, \ldots, x_m)$ *az* $x_1, x_2, \ldots, x_m$ *határozatlanoknak oly egész függvénye, a melynek dimensiója nem nagyobb n-nél és a melynek nem tünik el minden együtthatója; legyen továbbá*

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{i,n+1} \qquad (i=1, \ldots, m)$$

a mennyiségek m sorozata, mely sorozatok egyenként $n+1$ *különböző mennyiségből állanak, akkor ezekből kiválaszthatunk oly*

$$\xi_{1r_1}, \xi_{2r_2}, \ldots, \xi_{mr_m} \qquad (r_i=1, \ldots, n+1)$$

értékrendszert, a melyre nézve

$$F(\xi_{1r_1}, \xi_{2r_2}, \ldots, \xi_{mr_m})$$

nem tünik el.

Az ($m=1$ esetére épen bebizonyított) tétel általános érvényessége könnyen bizonyítható a teljes inductio segítségével.

Ha ugyanis x_m hatványai szerint rendezünk:

$$F(x_1, x_2, \ldots, x_m) = X_0 + X_1 x_m + \cdots + X_n x_m^n,$$

akkor az ellenkező esetben az összes

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{i,n+1} \qquad (i=1, \ldots, m-1)$$

értékrendszerekre nézve az $x_1, \ldots, x_{m-1}$, számra nézve $m-1$ határozatlan összes X_i függvényeinek, a melyeknek dimensiói ismét $\leqq n$, el kellene tünniök, a mi az $m-1$ esetére érvényesnek feltételezett tétellel ellenkeznék.

Végül még a tételnek a következő csak formálisan különböző alakját adjuk, a melyben leggyakrabban szokott alkalmaztatni:

Legyen $F_1, F_2, \ldots, F_k$ *az* $x_1, \ldots, x_m$ *határozatlanoknak akárhány az* [A] *tartományból származó, 0-tól különböző formája; akkor meghatározhatunk akárhány valamely az* [A] *tartományban foglalt határtalan mennyiségsorozathoz tartozó* $\xi_1, \ldots, \xi_m$ *rendszert, egyebek között akárhány olyant is, a mely raczionális és egész számokból áll, a melyekre nézve*

$$F_i(\xi_1, \xi_2, \ldots, \xi_m) \qquad (i=1, 2, \ldots, k)$$

a zérustól különböző.

E czélból csak $F = F_1 F_2 \ldots F_k$-t kell képeznünk és ha ennek a formának vagy egész függvénynek dimensiója n, a $\xi_{ij}\,(i=1, \ldots, m; j=1, \ldots, n+1)$ mennyiségeket úgy kell választanunk, hogy a $\xi_{i1}, \xi_{i2}, \ldots, \xi_{i,n+1}$ sorozat csak különböző mennyiségeket tartalmazzon. Ezek közt minden esetre találkozik egy a kiszabott feltételeknek megfelelő értékrendszer. Ha tehát [A]-ból a mennyiségek valamely határtalan sorozatát, mint pl. a raczionális egész számokét, kiemeljük, már ebben is találhatjuk az értékrendszereknek oly határtalan sorozatát, a melyek a kiszabott feltételeknek megfelelnek.

Lineáris transformatio. Szabályos formák.

18. §. Az

$$x_i = u_{i1} y_1 + u_{i2} y_2 + \cdots + u_{im} y_m \qquad (i=1, 2, \ldots, m) \qquad (T)$$

képletek meghatározta *(homogén) lineáris transformatio* (vagy *substitutio*) átvezeti az $F(x_1, \ldots, x_m)$ formát, ha t. i. F-ben min-

den x_i helyébe egyszerűen (T) megfelelő egyenletének jobb oldalát helyettesítjük, az $y_1, \ldots, y_m$ határozatlanokat tartalmazó $\overline{F}(y_1, \ldots, y_m)$ *transformált formába*, a melyet némelykor $T(F)$-fel is fogunk jelölni. Az u_{ij} mennyiségeket, a melyeket a *transformatio együtthatóinak* nevezünk, tekintsük az [A] tartomány mennyiségeinek. Az

$$U = |u_{ij}| \qquad (i,j=1,\ldots,m)$$

determináns, a melyet *mindig 0-tól különbözőnek tételezünk fel, a lineáris transformatio determinánsa*

Ha a (T) alatti egyenleteket y szerint megoldjuk, nyerjük az

$$y_j = \frac{U_{1j}x_1 + U_{2j}x_2 + \cdots + U_{mj}x_m}{U} \qquad (T^{(-1)})$$

képletek meghatározta *recziprok lineáris transformatiót*, a hol U_{ij} a szokott módon az u_{ij} elem adjungált aldeterminánsát jelenti. (Itt ugyan az U nevező miatt már általánosságban az orthoid (A) tartományra mentünk át; ez azonban csak kényelmességi szempontból történik, hogy a nevező elkerülésével járó hosszadalmas írásmódot rövidítsük. Ez a $(T^{(-1)})$ recziprok transformatio — mint közvetetlenül világos — $\overline{F}(y_1, \ldots, y_m)$-et ismét átvezeti $F(x_1, \ldots, x_m)$-be.

Az eredeti $F(x_1, \ldots, x_m)$ *forma és a transformált* $\overline{F}(y_1, \ldots, y_m)$ *forma dimensiói egyenlők.* Ha F és $\overline{F}$ dimensiói pl. n és $\overline{n}$ volnának, akkor — a mint $\overline{F}$ kifejezése közvetetlenül mutatja — a transformatio a dimensiót nem emelheti fel; minden esetre tehát $\overline{n} \leqq n$. Minthogy azonban az (A) tartományban F tekinthető az eredeti és F a transformált formának, egyszersmind $n \leqq \overline{n}$ és ebből következik, hogy $n = \overline{n}$.

Az utasítás, a melyet a lineáris transformatio végrehajtására adtunk, továbbá mindjárt azt is mutatja, hogy a *transformált forma együtthatói a transformatio együtthatói-*

nak az [A] *tartományból származó formái, a melyeknek dimensiója nem haladja túl az eredeti forma dimensióját.*

Ha a (T)-nek $F(x_1, \ldots, x_m)$-re való alkalmazása révén származó $\overline{F}(y_1, \ldots, y_m)$ formára újból valamely lineáris transformatiót alkalmazunk, a mely meg van adva a következő módon:

$$y_j = v_{j1}z_1 + v_{j2}z_2 + \cdots + y_{jm}z_m, \qquad (T')$$

akkor bizonyos harmadik forma: $\overline{\overline{F}}(z_1, \ldots, z_m)$ származik, a melyet azonban az

$$x_i = w_{i1}z_1 + \cdots + w_{ij}z_j + \cdots + w_{im}z_m \qquad (T'')$$

lineáris transformatiót alkalmazván, közvetetlenül F-ből is nyerhetünk, ha

$$w_{ij} = u_{i1}v_{1j} + u_{i2}v_{2j} + \cdots + u_{im}v_{mj}.$$

Mert, hogy $\overline{\overline{F}}$-et nyerjük, F-be az x_i-k helyébe be kell helyettesítenünk a (T) egyenletek jobb oldalait és az ebből származó formába az y_j-k helyébe a (T') egyenletek jobb oldalait.

Itt a w_{ij} mennyiségek szerkezete értelmében és a determinánsok szorzás-tétele alapján a (T'') transformatio determinánsa:

$$|w_{ij}| = |u_{ij}||v_{ij}|.$$

Két (vagy több) lineáris transformatio egymásutánja tehát ismét lineáris transformatio és ennek az eredő transformatiónak determinánsa az egyes transformatiók determinánsainak szorzata.

19. §. Ha az $F(x_1, \ldots, x_m)$ forma, a melynek dimensiója n, az x_i^n tagot a 0-tól különböző együtthatóval tartalmazza, akkor azt *x_i-re nézve szabályosnak* mondjuk; *szabályosnak* pedig — minden hozzátétel nélkül — akkor nevezzük, ha minden határozatlanra nézve szabályos.

Könnyen bizonyíthatjuk be a következő tételt:

Legyen $F_1, F_2, \ldots, F_k$ az $x_1, \ldots, x_m$ határozatlanoknak

akárhány formája, akkor van akárhány oly lineáris transformatio, a melynek együtthatói raczionális és egész számok, determinánsaik pedig egyenlők eggyel és a melyek az összes adott formákat szabályos formákba viszik át.

Legyen részletesebben írva:

$$F_i = \sum_{(g)} A_g^{(i)} x_1^{g_1} x_2^{g_2} \dots x_m^{g_m}. \qquad (i=1, \dots, k).$$

Ha erre a következő specziális lineáris transformatiót alkalmazzuk:

$$x_1 = y_1, \quad x_j = u_{j1} y_1 + y_j, \qquad (j=2, \dots, m)$$

a melynek determinánsa, ha fenn is tartjuk az u_{j1} mennyiségek alkalmas meghatározását, ettől függetlenül egyenlő 1-gyel, akkor lesz:

$$\bar{F}_i = \sum_{(g)} A_g^{(i)} y_1^{g_1} (u_{21} y_1 + y_2)^{g_2} \dots (u_{m1} y_1 + y_m)^{g_m}$$

és y_1^n együtthatója ebben

$$\Sigma A_g^{(i)} u_{21}^{g_2} u_{31}^{g_3} \dots u_{m1}^{g_m}, \qquad (I)$$

a hol a summatio kiterjesztendő mindazokra a tagokra, a melyekben $g_1 + g_2 + \dots + g_n = n$; de az y_j^n-et $(j \geqq 2)$ tartalmazó tagok együtthatói ugyanazok lesznek, mint az x_j^n-et tartalmazó tagok együtthatói F_i-ben. Az előbbi § végén felállított tétel szerint az $u_{21}, \dots, u_{m-1}$ mennyiségeket mint raczionális és egész számokat úgy választhatjuk, hogy az összes (I) alatti kifejezések $(i=1, \dots, k)$, a 0-tól különböző értékeket vegyenek fel, azaz az $\bar{F}_1, \dots, \bar{F}_k$ formák y_1-re nézve szabályosak legyenek.

Evvel azonban a bebizonyítás lényeges részét már elintéztük. Ha ugyanis ezen a módon sikerült az adott formákat olyanokká átalakítani, a melyek bizonyos számú, pl. l határozatlanra nézve szabályosak, akkor valamely új transformatio, a mely ismét az adott specziális alaknak megfelel, oly transformált formákat fog szolgáltatni, a me-

lyek bizonyos $l+1$-edik határozatlanra nézve szabályosak, míg azoknak a tagoknak az együtthatói, a melyek amaz l határozatlan n-dik hatványait tartalmazzák, egyáltalában változatlanok maradnak úgy, hogy az új formák ezekre nézve is és így mindössze $l+1$ határozatlanra nézve szabályosak.

Igy tehát végre oly formákhoz jutunk, a melyek az összes határozatlanokra nézve szabályosak; még pedig oly lineáris transformatio segítségével, a mely mint azoknak a specziális transformatióknak egymásutánja könnyen állítható elő. Közvetetlenül felismerjük, hogy az u mennyiségekkel együtt ennek az eredő transformatiónak együtthatói is raczionális és egész számok és hogy determinánsa, mint olyan determinánsok szorzata, a melyek közül mindegyik egyenlő egygyel, ismét egygyel egyenlő.

Az «általános» (homogén) lineáris transformatiót szintén az

$$x_i = u_{i1} y_1 + u_{i2} y_2 + \cdots + u_{im} y_m \quad (i=1, \ldots, m) \quad (T)$$

egyenlet definiálja, a hol azonban most a transformatio együtthatóit, az u_{ij}-ket új határozatlanoknak kell tekintenünk. A transformált forma együtthatói akkor az u_{ij} határozatlanoknak az [A] tartományból származó formái és minden forma az általános transformatio végrehajtása után szabályossá válik, mert a kérdéses együtthatók akkor sem egyenlők zérussal, ha az u_{ij}-k helyébe az előbb meghatározott specziálisabb értékeket teszszük; így tehát az «általános» esetben is a 0-tól különböző formák lesznek.

HARMADIK FEJEZET.

A FORMÁK OSZTHATÓSÁGA.

A közönséges osztási eljárás.

1. §. Az [A] tartomány, a mely most is kiinduló pontunk, vonatkozással a benne uralkodó oszthatósági viszonyokra, csak akkor tekinthető *jól értelmezettnek,* ha van olyan módszer, a melylyel a $\beta x = \alpha$, $(\beta \neq 0)$ elsőfokú egyenlet teljes discussióját véges számú lépésben tudjuk elintézni; azaz a melylyel az ép említett módon dönthetünk a felett, vajjon α osztható-e β-val és ha igen, az mindjárt szolgáltatja a $\xi = \beta'$ értéket is (α-nak β-ra vonatkozólag *complementáris* osztóját). Ilyen az elemek szerint az [1] tartomány és ilyen minden orthoid tartomány, mert ebben az esetben a keresett mennyiség közvetetlenül az $\frac{\alpha}{\beta}$ alakban van megadva.

Első feladatunk megmutatni azt, hogy [A]-val együtt mindig az $[A, x_1, x_2, \ldots, x_m]$ is az adott értelemben jól meghatározott tartomány. E czélból csupán csak az elemekből ismeretes közönséges osztási eljárást kell szabatosan fogalmaznunk. Minthogy a dolog lényege szerint itt ismét a teljes inductiót alkalmazzuk, még külön kiemeljük, hogy már az [A] tartomány is tartalmazhat akárhány határozatlant. Ha az x határozatlan hozzácsatolásával az $[A, x]$ tartományra megyünk át, akkor ama közönséges osztási eljárás tartalmát a következő tétel fejezi ki:

Legyen

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_m$$
$$G = B_0 x^n + B_1 x^{n-1} + \cdots + B_n$$

(a hol $m \geqq n$, $A_0 \neq 0$, $B_0 \neq 0$*) az* [A, x] *tartomány két formája; tehát* A_i, B_j az [A] *tartományhoz tartozó mennyiségek, akkor az* [A, x] *tartományban mindig van egy és csakis egy olyan* Q *forma, hogy*

$$R = B_0^{m-n+1} F - GQ$$

x*-ben legfölebb* $n-1$*-edik fokú forma.*

Q-t és R-t itt a «B_0^{m-n+1} F-nek G-vel való osztásában» fellépő *hányadosnak*, ill. *maradéknak* nevezzük.

A felállított feltétel szerint Q foka nem lépheti túl $m-n$-t, mert különben R foka legalább is $m+1 \geqq n+1$; de Q foka $m-n$-nél alacsonyabb sem lehet, mert különben GQ foka nem érné el m-et és így R m-edfokú lenne. Ha tehát ilyen Q forma egyáltalában van, az csak a következő alakú lehet:

$$Q = Q_0 x^{m-n} + Q_1 x^{m-n-1} + \cdots + Q_{m-n}, \qquad (I)$$

a hol $Q_0 \neq 0$. Minthogy R-ben $x^n, x^{n+1}, \ldots, x^m$ együtthatójának 0-nak kell lennie, a Q_i mennyiségek meghatározására a következő lineáris egyenletrendszert nyerjük:

$$B_0^{m-n+1} A_i = B_i Q_0 + B_{i-1} Q_1 + \cdots + B_0 Q_i,$$
$$(i = 0, 1, \ldots, m-n)$$

a mely a Q_i mennyiségeket valóban mint az [A] tartomány mennyiségeit egyértelműleg határozza meg; mert az ismeretlenek együtthatóiból alkotott determináns, B_0^{m-n+1} a zérustól különböző. Q_i-t ebből nyerjük:

$$B_0^{m-n+1} Q_i = D_i, \qquad (Ia)$$

a hol a jobb oldalon álló D_i mennyiségről közvetetlenül látni, hogy osztható B_0^{m-n+1}-vel; mert determináns alakjában előállítva, $i+1$-edik oszlopának minden eleme osztható B_0^{m-n+1}-vel.

A Q_i mennyiségek e meghatározása után az

$$R = R_0 x^{n-1} + R_1 x^{n-2} + \cdots + R_{n-1}$$

forma együtthatói a következő módon adódnak ki közvetetlenül:

$$R_j = B_0^{m-n+1} A_{m-n+j+1} - B_{j+1} Q_{m-n} - B_{j+2} Q_{m-n-1} - \cdots, \quad (j=0, 1, \ldots, n-1) \qquad \text{(II)}$$

a hol a Q_i-k értékei (Ia)-ból helyettesítendők.

Az oszthatóság kriteriuma a formatartományban.

2. §. *Annak szükséges és elegendő feltételei, hogy az*

$$F = A_0 x^m + \cdots + A_m \quad (A_0 \neq 0)$$

forma osztható legyen a

$$G = B_0 x^n + \cdots + B_n \quad (B_0 \neq 0)$$

formával a következők: Szükséges, hogy $m \geqq n$ legyen, továbbá, hogy az előbbi §-ban értelmezett $R_j (j=0, \ldots, n-1)$ mennyiségek mind ellünjenek és végül, hogy az ugyanott értelmezett Q_i mennyiségek oszthatók legyenek B_0^{m-n+1}-vel

Hogy ugyanis

$$F = GH$$

lehessen, a hol H ismét az $[A, x]$ tartomány formája, valóban szükséges, hogy $m \geqq n$ legyen és az osztási eljárásból származó

$$B_0^{m-n+1} F = GQ + R$$

reláczió az oszthatóság tényét kifejező

$$B_0^{m-n+1} F = GB_0^{m-n+1} H$$

relációval oly módon egyezzék meg, hogy

$$R = 0, \quad Q = B_0^{m-n+1} H$$

legyen.

Valóban szükséges tehát, hogy $R_j = 0$ legyen és ha H részletesen írva a következő:

$$H = H_0 x^{m-n} + \cdots + H_{m-n},$$

egyszersmind

$$Q_i = B_0^{m-n+1} H_i$$

legyen.

Evvel az oszthatóság kérdését az $[A, x]$ tartományból átvittük az $[A]$ tartományba, és így tehát akkor is, ha az adott formák az $[A, x_1, \ldots, x_m]$ tartományhoz tartoznak, annak a kérdésnek a vizsgálata, vajjon az egyik osztható-e a másikkal, visszavezethető a megfelelő vizsgálatra az $[A, x_1 \ldots, x_{m-1}]$ tartományban, és így tovább végre a megfelelő vizsgálatra az $[A]$ tartományban.

3. §. *A lineáris transformatio módszere alapján lehetséges, hogy F-nek G-vel való oszthatóságának kérdését az* $[A, x_1, \ldots, x_m]$ *tartományból közvetetlenül az* $[A]$ *tartományba vigyük át.* Ezt a következő egyszerű meggondolás mutatja:

Legyen T oly lineáris transformatio, a melynek együtthatói raczionális és egész számok és determinánsa egyenlő egygyel, akkor (a II. fej. 18. és 19. §-a alapján) abból, hogy

$$F = GH,$$

következik, hogy egyszersmind

$$\overline{F} = \overline{G}\,\overline{H}$$

és viszont. Az oszthatóság kérdése tehát akár a transformált $\overline{G}$ és $\overline{H}$ formákon dönthető el. Az idézett helyen azonban bebizonyítottuk, hogy ama lineáris transformatio együtthatói mint raczionális és egész számok oly módon választhatók, hogy a $\overline{G}$ forma szabályossá, azaz olyanná váljék, a melynek legmagasabb tagjában, $\overline{B}_0 y_1^n$-ben, a hol most már n egyenlő a forma dimensiójával, a $\overline{B}_0$ együttható az $[A]$ tartomány valamely 0-tól különböző mennyisége. Q-nak $\overline{B}_0^{m-n+1}$-vel való oszthatósága tehát feltételezi, hogy összes együtthatói oszthatók legyenek azzal és így már most a kérdést valóban az $[A]$ tartományban döntjük el.

A szabályos formák definicziójából közvetetlenül kö-

vetkezik, hogy *két forma G és H szorzata x_1-re nézve csak akkor lehet szabályos, ha a G és H formák maguk is x_1-re nézve szabályosak.*

Ugyanis, ha

$$G = G_0 x_1^n + \cdots + G_n,$$

$$H = H_0 x_1^p + \cdots + H_p$$

és így

$$GH = G_0 H_0 x_1^{n+p} + \cdots + G_n H_p,$$

akkor ez az utóbbi forma csak úgy lehet szabályos, ha dimensiója egyenlő fokával x_1-ben, azaz $n+p$-vel. De arra szükséges, hogy $G_0 H_0$ és evvel együtt G_0 és H_0 is az [A] tartományhoz tartozzanak és a 0-tól különbözők legyenek. Másrészt pedig G és H dimensiója minden esetre n, ill. p. Az első tag ugyanis mutatja, hogy G és H dimensiói legalább is ezek; ha pedig csak az egyiknek dimensiója is ezeken túlmenne, szorzatuk dimensiója már magasabb volna $n+p$-nél. G és H tehát valóban szabályos formák.

Az épen bebizonyított tételnek következő fogalmazása az oszthatóságra vonatkozó elemi vizsgálatokban való jelentését mutatja.

Valamely bizonyos határozatlanokra nézve szabályos forma osztói csak olyan formák lehetnek, a melyek ugyanazokra a határozatlanokra nézve maguk is szabályosak.

Dedekind segédtétele *.

4. §. Legyen

$$a_0, a_1, \ldots, a_m$$

$m+1$ mennyiség, a mely valamely holoid tartományhoz tar-

* «Über einen arithmetischen Satz von Gauss». Mittheilungen der deutschen mathematischen Gesellschaft in Prag. 1892. 1. lap.

Ezt a tételt, valamint a később az 5. §-ban tárgyaltakat, a me-

tozik; (vagy általánosabban valamely oly tartományhoz, a melynek mennyiségei az összeadás és szorzás közönséges törvényét követik). Alkossuk meg azután az a mennyiségek összes oly hatványszorzatait, a melyeknek dimensiója $n+1$, a hol n valamely nem negativ raczionális és egész számot jelent:

$$P_r = a_0^{r_0} a_1^{r_1} \ldots a_m^{r_m},$$

a hol tehát ismét az r-ek oly nem negativ raczionális és egész számok, a melyek az

$$r_0 + r_1 + \cdots + r_m = n + 1$$

relácziót kielégítik. A P_r hatványszorzatok száma itt ugyanaz, mint a lehetséges tagok száma $m+1$ határozatlannak oly homogén formájában, melynek dimensiója $n+1$; tehát a II. fej. 8. §-a szerint $\binom{m+n+1}{n+1}$.

Alkossuk másrészt az $a_0, \ldots, a_m$ mennyiségekből a következő $m+n+1$ sorból és $n+1$ oszlopból álló schémát, a belőle alkotandó determinánsok miatt úgy nevezett (determináns-) *matrixot:*

$$\| a_{i-j} \|, \quad (i=1, \ldots, m+n+1;\ j=1, \ldots, n+1) \qquad (M)$$

a hol a_r helyébe zérust kell tennünk, ha r negativ szám, vagy pedig nagyobb m-nél. E matrix törvénye — mint az adott meghatározásból kiolvasható — részletesen kifejtve a következő: A j-dik oszlop a sorok sorrendjében a következő mennyiségeket tartalmazza: $j-1$-szer a zérust, azután $a_0, a_1, \ldots, a_m$-et és végre $n-j+1$-szer ismét a zérust. A jobb áttekinthetőség kedvéért a matrixot kivételesen még részletesen is kiírjuk:

lyek itt mint elemi identitások lépnek fel, DEDEKIND mély, de fölötte bonyolódott meggondolások alapján nyeri, a melyek a tőle származó «modulusok elméletébe» tartoznak.

$$\begin{Vmatrix} a_0 & & & & \\ a_1 & a_0 & & & \\ . & a_1 & . & & \\ . & . & . & . & \\ . & . & . & . & a_0 \\ a_m & . & . & . & a_1 \\ & a_m & . & . & . \\ & & & . & . \\ & & & & a_m \end{Vmatrix}, \qquad (M)$$

a hol az üres (még nem is pontozott) helyek zérussal töltendők be. E matrix közvetetlenül meghatározza a

$$D_s = |a_{i-j}| \quad \begin{pmatrix} i=s_0, s_1, \ldots, s_n, j=1, \ldots, n+1 \\ s_h=1, 2, \ldots, m+n+1 \end{pmatrix}$$

determinánsokat, a melyeknek száma, ha mint lényegesen egymástól különbözőket csak azokat számláljuk meg, a melyek nem csupán a matrixból vett sorok sorrendjében különböznek egymástól, ismét egyenlő $\binom{m+n+1}{n+1}$-tel; mert hiszen az $m+n+1$ sorból mindig $n+1$-et kell választanunk. Hogy e determinánsokat teljesen, azaz az előjelre vonatkozólag is meghatározzuk, mint további feltételt a következőt vezethetjük be:

$$s_0 < s_1 < \cdots s_n.$$

Ha a P_r és D_s mennyiségeket bármely

$$P_\varrho, \; D_\sigma \qquad \left(\varrho, \sigma = 1, 2, \ldots, \binom{m+n+1}{n+1}\right)$$

sorrendben írjuk, akkor érvényes a következő tétel:

Minden egyes P_ϱ mennyiség a D_σ mennyiségeknek raczionális és egész, homogén lineáris formája, azaz:

$$P_\varrho = \sum_{\sigma=1}^{\nu} k_{\varrho\sigma} D_\sigma, \qquad \left(\nu = \binom{m+n+1}{n+1}\right)$$

a hol a $k_{\varrho\sigma}$ együtthatók raczionális és egész számok.

Hogy e tétel megfordítható, azaz, hogy D_σ a P_ϱ-kból megfelelő módon állítható elő, magától értetődik; mert a determináns definíciója épen ezt az előállítást szolgáltatja.

Hogy bebizonyítsuk a kimondott tételt és a P_ϱ mennyiségeket a jellemzett alakban valóban elő is állítsuk, a teljes inductiót használjuk.

Föltételezzük, hogy az előállítás módja meg van adva, ha $m+n$ kisebb bizonyos meghatározott N számnál és kifejtjük azt azután az $m+n=N$ esetére. Ez elég, mert, ha $m+n=0$, a tétel helyessége közvetetlenül belátható. Ekkor m-nek és n-nek 0-nak kell lennie; tehát csak egy a_0 mennyiség van és a P_ϱ-k sorozata az egyetlen a_0 mennyiségre szorítkozik, valamint a D_σ mennyiségek sorozata is csupán csak az egyetlen a_0 mennyiségből áll; ama matrixnak ugyanis ebben az esetben csak egy sora és egy oszlopa van és így tehát hasonlóképen csupán csak az egyetlen a_0 elemből áll.

Hogy a tételt általánosságban bebizonyíthassuk, két esetet különböztetünk meg a szerint, a mint a kiszámítandó P mennyiség a_0-t mint tényezőt tartalmazza, vagy pedig nem. Az első esetben írhatjuk, hogy

$$P_0 = a_0 P'.$$

Akkor P' az $a_0, \ldots, a_m$ mennyiségek oly hatványszorzata, a melynek dimensiója $n=(n-1)+1$ és így tehát az erre az esetre helyesnek feltételezett tétel szerint mint bizonyos könnyen jellemezhető (M') matrixból származó D' determinánsok raczionális és egész, homogén lineáris formája állítható elő. A mennyiségeknek felhasznált sorozata itt ugyanaz, mint az előbbi: $a_0, a_1, \ldots, a_m$; csak n helyébe lépett $n-1$. (M') úgy származik (M)-ből, hogy ebből az első sort és oszlopot elhagyjuk. Minden D' determinánsból, ha elébe mint első sort csupa 0-t írunk és azután mint első oszlopot olyant írunk, a melyben az első sorban a_0 áll, a többi sorban pe-

dig azok az elemek, a melyek M első oszlopában ugyanabban a sorban állanak, oly D determináns származik, a melynek értéke származási törvényénél fogva $a_0 D'$. Ha tehát — a mint feltételeztük — P' a D'-k raczionális és egész, homogén lineáris formája, akkor $a_0 P' = P$ ugyanily formája az $a_0 D'$-knek, vagyis a D-knek.

A *második* esetben, a hol P az a_0 mennyiséget egyáltalában nem tartalmazza, P az $a_1, \ldots, a_m$, számra nézve $m = (m-1) + 1$ mennyiség oly hatványszorzata, a melynek dimensiója $n+1$ marad és így tehát a helyesnek feltételezett tétel szerint mint bizonyos könnyen jellemezhető (M'') matrixból származó D'' determinánsok raczionális és egész, homogén lineáris formája állítható elő. Az itt felhasznált mennyiségek sorozata: $a_1, \ldots, a_m$, a hol tehát a_0 elmaradt. (M'') úgy származik (M)-ből, ha ebből az első sort elhagyjuk és a többiekben a_0 helyébe mindenütt a zérust teszszük. Ha tehát D''-ben, mindazokra a helyekre, a hol eredetileg a_0 állott, a 0 helyébe ismét a_0-t írjuk, származik a megfelelő D determináns és $D'' - D$ oly P hatványszorzatok raczionális és egész, homogén lineáris formája lesz, a mely az a_0 tényezőt tartalmazza; tehát az előbb bebizonyított részlettétel szerint époly formája a D determinánsoknak is. Ezért ugyanez áll D''-re és végre P-re nézve is, úgy hogy evvel a felállított tétel általánosan is be van bizonyítva.

Kronecker alaptétele*.

5. §. Először a tétel egyik speciális de alapvető esetét fogjuk bebizonyítani. Legyen, csatlakozva az előbbi §-ban használt jelölésekhez,

* «Zur Theorie der Formen höherer Stufe». Ber. Berl. Akad. 1883. 957. lap. (Werke, II. köt. 417. lap).

Ezt a tételt KRONECKER csak a «Festschrift» kiadása után ta-

$$f(x) = a_0 x^m + \cdots + a_m,$$
$$g(x) = b_0 x^n + \cdots + b_n,$$

x két formája, a melyeknek együtthatói az [A] tartományhoz tartoznak*; e két forma ismét x hatványai szerint rendezett szorzata pedig legyen:

$$f(x)\,g(x) = c_0 x^{m+n} + \cdots + c_{m+n}.$$

Az a, b, c együtthatók között azután a következő relációk állanak fenn:

$$a_t b_0 + a_{t-1} b_1 + \cdots + a_{t-n} b_n = c_t,$$
$$(t = 0, 1, \ldots, m+n),$$

a hol ismét a_r helyébe zérus teendő, ha r negativ szám, vagy nagyobb m-nél.

látta, a miért is abban nincsen felhasználva. E tétel — úgy látszik — egész észrevétlen maradt mindaddig, míg DEDEKIND az előbb idézett helyen az 5. §-ban tárgyalt speciális esetet nem fedezte fel újból önállóan és ezután különösen HURWITZ annak fontosságára rámutatott («Über die Theorie der Ideale». Nachr. d. kgl. Ges. der Wiss. zu Göttingen 1894. 290. lap.).

Ez annál különösebb, minthogy MOLK («Sur une notion générale, qui comprend celle de la divisibilité etc.» Acta math. 6. k. 71. old.) már használja a tételt és maga KRONECKER amaz értekezése bevezetésében a tétel fontosságára a következő szavakkal mutat reá: «Ama törekvésem, hogy kifürkészszem a formák elméletének legegyszerűbb alapjait, már régen vezetett engem oly kérdésre, a mely látszólag egészen elemi, de a melyet mindamellett előbb még sem tudtam elintézni».

E tételnek minden segédelmélet nélküli és teljesen elemi fogalmazása és bebizonyítása, a melyet itt előadunk, megengedi, hogy azt az elmélet kiinduló pontjául válaszszuk, a mi valóban meglepően egyszerűvé és átlátszóvá teszi az egész rendszert.

* Megjegyezzük még egyszer, hogy itt, valamint a következő §-ban az [A] tartomány tulajdonságai közül csak azt használjuk fel, hogy mennyiségei az összeadás és szorzás közönséges törvényét követik.

Ha ezen egyenletek közül kiválasztjuk azokat, a melyekben

$$t = s_0, s_1, \ldots, s_n,$$

és ismeretleneknek bennük a $b_0, \ldots, b_n$ mennyiségeket tekintjük, akkor bármely b_j-re nézve lesz:

$$D_s b_j = \sum_{t=0}^{m+n} Q_{jt}^{(s)} c_t,$$

a hol D_s teljesen ugyanazt a determinánst jelenti, mint az előbbi §-ban és a $Q_{jt}^{(s)}$-ek, mint D_s első aldeterminánsai az $a_0 \ldots a_m$ mennyiségeknek oly raczionális és egész homogén formái, a melyeknek dimensiója n.

Ha már mostan a_i az $a_0, \ldots, a_m$ mennyiségek bármelyike, akkor továbbá lesz:

$$D_s a_i b_j = \sum_{t=0}^{m+n} Q_{jt}^{(s)} a_i c_t,$$

a hol az $a_i Q$-k az a-k oly raczionális és egész homogén formái, a melyeknek dimensiója $n+1$. Minthogy azonban az a-k minden oly hatványszorzata, a melynek dimensiója $n+1$, a $D_\sigma \left(\sigma = 1, \ldots, \nu;\ \nu = \binom{m+n+1}{n+1}\right)$ determinánsok raczionális és egész, homogén lineáris formája, végre, ha az épen nyert kifejezésbe $a_i Q$ minden egyes tagjának helyébe ezeket a formákat behelyettesítjük és azután az összes ugyanazt a D_σ-t tartalmazó tagokat egyesítjük, *az együtthatók bármely $a_i b_j$ szorzatára nézve a következő identitásokat nyerjük:*

$$D_s a_i b_j = \sum_{\sigma=1}^{\nu} L_{ij\sigma}^{(s)} D_\sigma, \qquad (1)$$

a hol az $L_{ij\sigma}^{(s)}$-k a $c_0, \ldots, c_{m+n}$ mennyiségek raczionális és egész, homogén lineáris formái és D_s helyébe a D_σ sorozat bármely determinánsát tehetjük, a minek következtében természetesen csupán csak az $L_{ij\sigma}^{(s)}$ formák, vagy pontosabban az ezekben együtthatókként szereplő raczionális és egész számok megváltoznak.

Az így nyert eredmény épen KRONECKER alaptétele a legegyszerűbb esetre, egy határozatlan két formájának esetére. A további tárgyalás világosabb lesz, ha a tételt előbb legáltalánosabb alakjában mondjuk ki.

6. §. *Legyen*

$$F_j = \Sigma A_g^{(j)} x_1^{g_1} \ldots x_m^{g_m} \qquad (j=1, 2, \ldots, k)$$

az $x_1, \ldots, x_m$ *határozatlanoknak* k *zérustól különböző formája (a melyeknek együtthatói az* [A] *holoid tartomány mennyiségei); e formák szorzata pedig:*

$$F = F_1 \ldots F_k = \Sigma C_g x_1^{g_1} \ldots x_m^{g_m};$$

legyen továbbá

$$P_i = A_{i_1}^{(1)} A_{i_2}^{(2)} \ldots A_{i_k}^{(k)}$$

k *oly együttható szorzata, a melyek közül mindegyik másmás* F_j *formából van véve:*

Akkor mindig van a mennyiségeknek oly $H_1, H_2, \ldots, H_\nu$ *sorozata, a melyek az* $A^{(1)}, \ldots, A^{(k-1)}$ *mennyiségek zérustól különböző raczionális és egész homogén formái és a mennyiségeknek oly további* $L_{i\sigma}^{(s)}$ *sorozata, a melyek a* C_g *mennyiségek raczionális és egész homogén lineáris formái, úgy hogy*

$$H_s P_i = \sum_{\sigma=1}^{\nu} L_{i\sigma}^{(s)} H_\sigma. \qquad (s=1, \ldots, \nu) \qquad (K)$$

Egy határozatlan két formájának esetében ez pontosan az épen bebizonyított tétel és a H mennyiségek ekkor ama D_σ determinánsok, a melyek közül a_0^{n+1} a zérustól különböző, míg az esetleg eltünő D-k a tétel végleges fogalmazásából egyszerűen elhagyhatók.

Feladatunk most megállapítani ama H_σ és $L_{i\sigma}^{(s)}$ mennyiségeket, a melyek a (K) relácziókat kielégítik. E mellett az egész problémát mindenekelőtt visszavezethetjük arra az esetre, a melyben a formák csak egy határozatlant tartalmaznak.

Ha ugyanis a II. fej. 3. és 4. §-ában előadott fejtegetések értelmében

$$g = g_1 t^{m-1} + g_2 t^{m-2} + \cdots + g_m$$

és $x_1^{g_1} \ldots x_m^{g_m}$ helyébe x^g-t írjuk, akkor az $F_1, \ldots, F_k$ és F formákból a következők származnak:

$$f_g = \Sigma A_g^{(j)} x^g$$
$$f = f_1 \cdots f_k = \Sigma C_g x^g,$$

a hol a C_g-k ugyanazon a módon állítandók elő az $A_g^{(j)}$-ből, mint előbb. Ha tehát sikerül e formák esetében a megfelelő H_σ és $L_{i\sigma}^{(s)}$ mennyiségek alkotásának törvényét megállapítani, akkor ez érvényes lesz az F_j formák esetében is.

Erre a végleges törvényre a teljes inductio segítségével juthatunk.

Feltételezzük, hogy ez a törvény k-nál kevesebb forma esetére ismeretes és azután megállapítjuk k forma esetére. Minthogy két forma esetére a probléma már valóban meg van oldva, ezen az úton általánosságban, azaz bármely k-ra nézve is meg lesz oldható.

Ha előbb $k-1$ formára, $f_1, \ldots, f_{k-1}$-re szorítkozunk, jelöljük ezeknek szorzatát $\bar{f}$-fel, azaz legyen

$$\bar{f} = f_1 \cdots f_{k-1} = \Sigma \bar{C}_g x^g.$$

Ha ennek megfelelőleg

$$\bar{P}_i = A_{i_1}^{(1)} \ldots A_{i_{k-1}}^{(k-1)},$$

akkor feltevésünk értelmében van a mennyiségeknek oly $\bar{H}_1, \ldots, \bar{H}_{\bar{\nu}}$ sorozata, a melyek az $A^{(1)}, \ldots, A^{(k-2)}$ mennyiségeknek a zérustól különböző raczionális és egész homogén formái és a mennyiségeknek oly további $\bar{L}_{i\sigma'}^{(u)}$ sorozata, a melyek a $\bar{C}_g$ mennyiségek raczionális és egész homogén lineáris formái úgy, hogy

$$\bar{H}_u \bar{P}_i = \sum_{\sigma'=1}^{\bar{\nu}} \bar{L}_{i\sigma}^{(u)} \bar{H}_{\sigma'}. \quad (u=1, \ldots, \bar{\nu}) \tag{1}$$

Ha most az alaptételt, a mely két forma esetére már szintén be van bizonyítva, alkalmazzuk az $\bar{f}$ és f_k formákra, a melyeknek szorzata

$$\bar{f} f_k = f = \Sigma C_g x^g,$$

azt találjuk, hogy van a mennyiségeknek oly $h_1, \ldots, h_{\nu'}$ sorozata, a melyek a $\bar{C}_g$, és így az $A^{(1)}, \ldots, A^{(k-1)}$ mennyiségeknek a zérustól különböző raczionális és egész homogén formái és a mennyiségeknek oly további $l_{gi_k\tau}^{(t)}$ sorozata, a melyek a C_g mennyiségek raczionális és egész homogén lineáris formái úgy, hogy

$$h_t \bar{C}_g A_{i_k}^{(k)} = \sum_{\tau=1}^{\nu} l_{gi_k\tau}^{(t)} h_\tau. \quad (t=1, \ldots, \nu') \tag{2}$$

Ha már mostan (1)-et megszorozzuk $h_t A_{i_k}^{(k)}$-val, akkor a jobb oldalon ezt a szorzást az $\bar{L}_{i\sigma'}^{(u)}$ formákon belül hajthatjuk végre, a mi csupa raczionális és egész együtthatókkal ellátott olyan alakú tagra fog vezetni, mint a milyenek a (2) alattiak. Ha azután egyesítjük azokat a tagokat, a melyek ugyanazt a $\bar{H}_{\sigma'} h_\tau$ szorzatot tartalmazzák, az együtthatók ismét a C_g mennyiségek raczionális és egész homogén lineáris formái lesznek, a melyeket $L_{i\sigma'\tau}^{(u,t)}$-vel jelölhetünk, úgy hogy

$$\bar{H}_u h_t \bar{P}_i = \sum_{\sigma=1}^{\bar{\nu}} \sum_{\tau=1}^{\nu'} L_{i\sigma'\tau}^{(u,t)} \bar{H}_{\sigma'} h_t. \quad (u=1, \ldots, \bar{\nu}, t=1, \ldots, \nu').$$

Ha végre a $\nu = \nu' \bar{\nu}$ számmal lévő $\bar{H}_u h_t$ mennyiségeket bármely sorrendjükben $H_1, \ldots, H_s, \ldots, H_\nu$-vel jelöljük és $L_{i\sigma'\tau}^{(u,t)}$ helyébe az egyszerűbb $L_{i\sigma}^{(s)}$-et írjuk, akkor evvel meg van a bebizonyítandó tétel; mert a $\bar{H}_u$ és h_t mennyiségek és ezekkel együtt szorzataik, a H_s-ek is mindannyian a zérustól különbözők.

7. §. Felhasználva a már előbb használt $\delta_{ii}=1$, $\delta_{ij}=0$ $(i \neq j)$ jeleket, az alaptétel megadta (K) relácziókat még a

következő alakra is hozhatjuk:

$$\sum_{\sigma=1}^{\nu} (L_{i\sigma}^{(s)} - \delta_{s\sigma} P_i) H_\sigma = 0$$

és minthogy a H_σ mennyiségek a zérustól különbözők, ebből következik, hogy az e mennyiségek együtthatóiból alkotott determinánsnak el kell tünnie. Igy tehát nyerjük, hogy

$$(-1)^\nu \, | L_{i\sigma}^{(s)} - \delta_{s\sigma} P_i | = 0 ; \quad {\scriptstyle (s, \sigma = 1, \ldots, \nu)}$$

ebben pedig mindjárt az *alaptétel egy második* hasonlóan fontos alakja rejlik:

Az együtthatóknak minden P_i szorzata kielégít oly

$$P_i^\nu + A_1^{(i)} P_i^{\nu-1} + \cdots + A_k^{(i)} P_i^{\nu-k} + \cdots + A_\nu^{(i)} = 0 \qquad (K')$$

identitást, a melyben $A_k^{(i)}$ az adott formák szorzatában előforduló C_g együtthatók oly raczionális és egész homogén formája, a melynek dimensiója k. A raczionális és egész számok, a melyek a $A_k^{(i)}$-kben mint együtthatók szerepelnek, természetesen a P_i, azaz az $A_{i_1}^{(i)}, \ldots, A_{i_k}^{(k)}$ mennyiségek választása szerint változnak.

Hogy ezt beláthassuk, csak azt kell figyelembe vennünk, hogy az L-ek a C_g-k raczionális és egész homogén lineáris formái és így ama determináns minden eleme ép olyan formája a C_g-knek és P_i-nek. A fődiagonális elemei továbbá az egyetlenek, a melyekben $\delta_{s\sigma}$ a 0-tól különböző, és így P_i bennük valóban előfordul. Ha tehát $(-1)^\nu$-vel szorzunk és azután P_i fogyó hatványai szerint rendezünk, P_i^ν együtthatója egyenlő lesz 1-gyel és minthogy az egész determináns a C_g-k és P_i ν-dik dimensiójú formája, $P_i^{\nu-k}$ együtthatója szükségképen oly $A_k^{(i)}$ forma, a mely a felsorolt tulajdonságokat mutatja.

Teljes tartományokból származó formák.

8. §. Feltételezzük most, hogy az [A] tartomány, a mely a megvizsgálandó formák együtthatóit szolgáltatja, *teljes holoid tartomány*. Ha tehát A és B a tartomány bármely két mennyisége, akkor az I. fej. 6. §-ában adott definicció szerint mindig van egy, szintén az [A] tartományhoz tartozó D mennyiség, a mely A és B legnagyobb közös osztója, azaz oly tulajdonságú, hogy összes osztói és csakis ezek A és B osztói. Az itt magától értetődik, hogy D «meghatározását» az absolut æquivalentia (I. fej. 5. §.) értelmében gondoljuk.

Valamely teljes tartomány, mint ilyen csak akkor tekinthető *jól értelmezettnek*, ha rendelkezünk olyan módszerrel, a melynek segítségével az abban foglalt bármely két mennyiség legnagyobb közös osztójának meghatározását véges számú lépésben végezhetjük. Ez az [1] tartomány esetében az arithmetika elemei szerint és nyilván minden orthoid tartomány esetében is lehetséges.

Teljes tartományok esetében mindenekelőtt az épen tárgyalt alaptétel különösen egyszerű alakot vesz fel.

Ha ugyanis a 6. §. (K) identitásaiban előforduló H_s mennyiségek legnagyobb közös osztója

$$(H_1, \ldots, H_\nu) \sim H,$$

tehát

$$H_s = HH'_s$$

és

$$(H'_1, \ldots, H'_\nu) \sim 1;$$

akkor amaz identitásokból a H osztót teljesen eltávolíthatjuk és nyerjük, hogy

$$H'_s P_i = \sum_{\sigma=1}^{\nu} L_{i\sigma}^{(s)} H'_\sigma. \qquad (s=1, \ldots, \nu)$$

Legyen másrészt a C_g mennyiségek legnagyobb közös osztója

$$(C_1, \ldots, C_g, \ldots) \sim C,$$

akkor az $L_{i\sigma}^{(s)}$ mennyiségek, továbbá ezekkel együtt a $H_s' P_i$ mennyiségek és végre

$$(H_1' P_i, \ldots, H_r' P_i) \sim P_i$$

oszthatók C-vel. Ha tehát

$$P \sim (P_1, \ldots, P_i, \ldots)$$

az összes P_i-k legnagyobb közös osztója, akkor P osztható C-vel és viszont C P-vel. Az utóbbi következik a szorzat definíciójából, a mely szerint minden egyes C_g mennyiség a P_i-k raczionális és egész, homogén lineáris formája és így tehát osztható P-vel. Ezek szerint

$$C \sim P$$

és evvel, csatlakozva a 6. §-ban használt jelölésekhez, azt találtuk, hogy *az F_i formák együtthatóiból alkotott*

$$P_i = A_{i_1}^{(1)} A_{i_2}^{(2)} \ldots A_{i_k}^{(k)}$$

szorzatok és az ama formák szorzatában előforduló C_g együtthatók legnagyobb közös osztója ugyanaz.

Ez a tétel (egyelőre csak teljes tartományok esetében) mély betekintést enged a formák szorzatának szerkezetébe; mert mutatja, hogy a szorzat bizonyos tulajdonságai változatlanok maradnak, ha a tényezőkként szereplő formákat bármely módon is építjük fel az adott együtthatókból. Ezt pontosabban a következő tétel fejezi ki, a melyet a következőkben mint *a teljes tartományokból származó formákra vonatkozó alaptételt* fogunk idézni.

Legyen

$$A_0^{(i)}, A_1^{(i)}, \ldots, A_g^{(i)}, \ldots \qquad (i=1, \ldots, k)$$

a mennyiségeknek valamely teljes holoid tartományból telszés szerint választott k sorozata; legyenek továbbá

$$U_0^{(i)}, U_1^{(i)}, \ldots, U_g^{(i)}, \ldots \qquad (i=1, \ldots, k)$$

letszés szerinti határozatlanoknak bármely hatványszorzatai, a hol azonban az egy sorban állók egymástól különbözők, azaz $U_g^{(i)}$ *csak akkor* $= U_h^{(i)}$, *ha* $g = h$; *végre pedig legyen*

$$F_i = \sum_{(g)} A_g^{(i)} U_g^{(i)} \qquad (i = 1, \ldots, k)$$

és

$$F = \prod_{i=1}^{k} F_i = \sum_{(h)} C_h V_h,$$

a hol tehát a V_h*-k a szorzás után fellépő összes hatványszorzatokat jelentik: akkor*

$$C \sim (C_1, \ldots, C_h, \ldots)$$

amaz U hatványszorzatok választásától teljesen független, az absolut aequivalentia-meghatározás értelmében nem változó (invariáns) mennyiség.

Az előbbi szerint ugyanis C mindig æquivalens a P_i mennyiségek legnagyobb közös osztójával; F-ben pedig ezek szerepelnek mint a C_h együtthatók, ha egyszerűen az $U_g^{(i)}$-ket mindenütt különböző határozatlanoknak tekintjük, azaz az F_i formákat mint különböző határozatlanok lineáris formáit állítjuk elő.

Ha tehát majd valamely forma jelölésére a részletesebb $\Sigma A_g x_1^{g_1} \ldots x_m^{g_m}$ kifejezés helyett gyakran a $\Sigma A_g U_g$ kifejezést használjuk, ez az írásmód nemcsak mint rövidített jelölés mutatkozik hasznosnak, hanem egyszersmind arra is utal, hogy a formák oly tulajdonságaival van dolgunk, a melyek az U_g hatványszorzatok választásától függetlenek. Akkor azonban $U_0, U_1, \ldots$ mindig *különböző* hatványszorzatoknak tekintendők, mert különben a forma hasonló tagjait egyesítenünk kellene és így a forma már «nem épülne fel az együtthatók $A_0, A_1, \ldots$ sorozatából».

9. §. *Valamely formát primitivnek, vagy egységformá-*

nak nevezünk, ha együtthatóinak legnagyobb közös osztója ~ 1*.

Közvetetlenül világos, hogy a forma így értelmezett tulajdonsága ismét kizárólag az együtthatók tulajdonsága. Azok a primitiv formák, a melyeknek dimensiója 0, az [A] tartomány egységei.

Ha tehát

$$F = \sum_{(g)} A_g U_g$$

valamely tetszés szerinti forma és

$$(A_0, A_1, \ldots, A_g, \ldots) \sim A,$$

tehát

$$A_g = AA'_g$$

és

$$(A'_0, A'_1, \ldots, A'_g, \ldots) \sim 1;$$

akkor végre lesz

$$F = A \sum_{(g)} A'_g U_g,$$

hol a jobb oldalon a második tényező származásánál fogva primitiv forma.

Minden a teljes holoid [A] *tartományból származó F forma tehát egy primitiv forma és egy az* [A] *tartományba tartozó mennyiség szorzata.* Ennek alapján írjuk, hogy $F = AX$

* Magától értetődik, hogy itt figyelembe veendő, miszerint már az alapul felvett teljes holoid tartomány is tartalmazhat határozatlanokat, a melyek azután az együtthatókba tartoznak. Ha pl. később ki fog tünni, hogy az $[1, x]$ tartomány teljes, akkor

$$x + xy,$$

mint y-nak az $[1, x]$ tartományból származó formája nem lesz primitiv, mert mind a két együtthatója x és így ezt a mennyiséget, a mely az æquivalentia-meghatározás értelmében 1-től különbözőnek mutatkozik, a két együttható legnagyobb közös osztójának kell tekintenünk.

Primitiv ellenben $x + xy$ mint (az x és y határozatlanoknak) az [1] tartományból származó formája.

és X-et alkalmilag «az F primitiv formájának» fogjuk nevezni.

Az alaptétel egyszerű következménye azután a következő fontos tétel:

Primitiv formák szorzata ismét primitiv forma.

Ha ugyanis két forma esetében

$$X = \Sigma A_g U_g, \quad Y = \Sigma B_g V_g$$

és

$$(A_0, A_1, \ldots) \sim 1, \quad (B_0, B_1, \ldots) \sim 1,$$

akkor, ha még

$$XY = \Sigma C_g W_g,$$

a C_g együtthatók legnagyobb közös osztója C, az alaptétel szerint lesz

$$C \sim (\ldots, A_i B_j, \ldots)$$

Ha itt az I. fej. 6. §-ában előadott, a legnagyobb közös osztóra vonatkozó tételeket alkalmazzuk, akkor különösen a legnagyobb közös osztó ott második helyen I. alatt álló recursiv meghatározásának módját ismételten alkalmazva, azt találjuk, hogy C az

$$(A_i B_0, A_i B_1, \ldots, A_i B_j, \ldots) \qquad (i=0, 1, \ldots)$$

legnagyobb közös osztók legnagyobb közös osztója. Ezek pedig így is írhatók:

$$A_i (B_0, B_1, \ldots, B_j, \ldots) \sim A_i,$$

tehát

$$C \sim (A_0, A_1, \ldots, A_i, \ldots) \sim 1,$$

a mi bebizonyítandó volt.

Ha már mostan $X_1, X_2, \ldots, X_k$ primitiv formák, akkor az előbbiek szerint primitiv forma $X_1 X_2$, tehát $X_1 X_2 X_3$ és í. t. és végre az $X_1 X_2 \ldots X_k$ szorzat is.

10. §. *Ha $F=AX$ és $G=BY$, továbbá F osztható G-vel, akkor már A is osztható B-vel és X az Y-nal.* E tétel megfordítása nyilvánvalóan helyes. Természetes, hogy itt X és Y

F és G primitiv formáit és A és B az [A] tartomány mennyiségeit jelentik.

Feltevésünk értelmében $F = GH$, a hol ismét írhatjuk, hogy $H = CZ$; így tehát

$$F = AX = (BC)(YZ).$$

Itt YZ primitiv forma; tehát F együtthatóinak legnagyobb közös osztója egyszer A, azután ismét BC, úgy hogy

$$A \sim BC.$$

A tehát osztható BC-vel és így — a mint azt állítottuk — B-vel is. Másrészt pedig BC osztható A-val, úgy hogy $\frac{BC}{A} = K$ az [A] tartomány egyik mennyisége és ezért

$$X = Y(KZ),$$

vagyis X osztható Y-nal.

Mint a bebizonyított tétel egyszerű corollariumait a következő igen gyakran alkalmazott és közvetetlenül belátható tételeket soroljuk fel:

Ha $F = AX$ osztható a primitiv Y formával, akkor már F primitiv formája, X is osztható Y-nal.

Primitiv formák osztói csupán csak primitiv formák lehetnek.

11. §. Legyen már most

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_m,$$
$$G = B_0 x^n + B_1 x^{n-1} + \cdots + B_n,$$

(a hol $m \geqq n$) az $[A, x]$ tartomány két formája tehát A_i és B_j az [A] tartomány mennyiségei, a melyről most feltételezzük, hogy teljes; akkor teljes analogiában az elemekből ismeretes Euklides-féle algorithmussal, a mely a raczionális és egész számok körében a legnagyobb közös osztó meghatározására szolgál, a közönséges osztási eljárás segítségével a következő identitásokat vezethetjük le, a melyek egyszersmind a bennük előforduló R formák értelmezésére is szolgálnak:

$$
\begin{aligned}
K_0 F &= G\ Q_1 + R_1 \\
K_1 G &= R_1 Q_2 + R_2 \\
K_2 R_1 &= R_2 Q_3 + R_3 \\
&\cdots\cdots\cdots \\
K_i R_{i-1} &= R_i Q_{i+1} + R_{i+1} \qquad (E) \\
&\cdots\cdots\cdots \\
K_{l-1} R_{l-2} &= R_{l-1} Q_l + R_l \\
K_l R_{l-1} &= R_l Q_{l+1}.
\end{aligned}
$$

Ezekben az identitásokban K_i jelentse R_i legmagasabb együtthatójának ama hatványát, a melylyel a közönséges osztási eljárás értelmében meg kell szoroznunk az R_{i-1} formát, hogy ezt az eljárást alkalmazva, csak az [A] tartományba tartozó együtthatókat nyerjünk, Q_{i+1} és R_{i+1} pedig egyszerűen jelentsék a hányadost, ill. a maradékot, a mely fellép, ha $K_i R_{i-1}$-et osztjuk R_i-vel. Akkor $R_1, R_2, \ldots$ az $[A, x]$ tartomány formái, a melyeknek foka x-ben nem lehet nagyobb mint $n-1, n-2, \ldots$ Az eljárást tekintsük befejezettnek, *ha* R_l *az utolsó maradék, a mely a* 0*-tól különböző;* ha ez az eljárás valahogy oly R_l maradékhoz vezetne, a mely nem tartalmazza x-et, de nem is 0, akkor az utolsó identitásban felvehetjük, hogy $K_l = R_l$, $Q_{l+1} = R_{l-1}$ és így lesz $R_{l+1} = 0$.

Ha már mostan, úgy mint előbb $F = AX$, $G = BY$ *és* $R_l = CZ$ *(a hol, ha* R_l *az* x *határozatlant nem tartalmazza,* $Z = 1$*-nek veendő), akkor* Z *az* X *és* Y *legnagyobb közös osztója.*

Ezt a következő egyszerű megjegyzésekből következtethetjük. F és G és így tehát X és Y minden közös osztója (E) szerint egyszersmind $R_1, R_2, \ldots$-nek és így tehát végre R_l-nek is osztója; X és Y minden közös osztója azonban primitiv (10. §.) és így Z-nek is osztója. Viszont pedig Z-nek minden osztója $K_{l+1} R_{l+1}$-nek is osztója és mivel primitiv, már osztója R_{l-1}-nek, épúgy R_{l-2}-nek és így to-

vább; tehát végre osztója G-nek és F-nek és így X-nek és Y-nak is.

Ebből közvetetlenül következik, *hogy az* $F=AX$, $G=BY$ *formák legnagyobb közös osztója az*

$$(A, B)(X, Y)$$

alakban állítható elő, hol (A, B) a feltevés szerint meghatározható, mert [A] jól meghatározott teljes tartomány és (X, Y) épen az a Z mennyiség, a melynek meghatározására az (E)-ben definiált EUKLIDES-féle algorithmus tanít.

Kimondhatjuk tehát egész általánosan:

A teljes [A] *tartományból származó* $[A, x_1, \ldots, x_m]$ *forma-tartomány ismét teljes tartomány.*

[A]-ról rendre $[A, x_1]$-re, $[A, x_1, x_2]$-re, ... áttérve azt találjuk, hogy ez az állítás helyes és evvel egyszersmind oly szabályt nyerünk, a mely szerint bármely két forma legnagyobb közös osztója valóban meghatározható.

Teljes tartományok mellérendelt orthoid tartományai.

12. §. Ha (az I. fej. 4. §-a szerint) az [A] tartományról átmegyünk a mellérendelt orthoid (A) tartományra, *valamely mennyiséget röviden orthoidnak vagy holoidnak fogunk nevezni,* a szerint, a mint az az (A), vagy pedig az [A] tartományhoz tartozik és épúgy *orthoid, ill. holoid forma* legyen az olyan forma, a melynek együtthatói orthoid, ill. holoid mennyiségek *.

Ha az [A] tartomány teljes, akkor *minden orthoid mennyiség bizonyos jellemző alakra hozható.* Minden egyes ilyen

* Csak a raczionális és egész melléknévi jelzőkre kell gondolnunk, a melyek az (1) és [1] tartományokban általánosan használatosak. Ennek megfelelőleg valamely orthoid mennyiség egyszersmind holoid is lehet.

mennyiség ugyanis a $\frac{P}{Q}$ alakban állítható elő, hol P és Q holoid mennyiségek és $(P, Q) \sim 1$. Az (A) tartományhoz tartozó mennyiség alakja minden esetre $\frac{M}{N}$, a hol M és N az [A] mennyiségei. Ha már mostan $(M, N) \sim D$, tehát

$$M = DP,\ N = DQ,\ (P, Q) \sim 1,$$

akkor valóban lesz $\frac{M}{N} = \frac{P}{Q}$.

E megállapodások alapján a következő tételhez jutunk:

Ha az [A] *tartomány teljes és* $A_0, A_1, \ldots, A_k$ *e tartományhoz tartozó mennyiségek, z pedig az* (A) *tartomány valamely mennyisége, a melyre nézve*

$$A_0 z^k + A_1 z^{k-1} + \cdots + A_k = 0, \qquad (1)$$

akkor $A_0 z$ *szükségképen az* [A] *tartományhoz tartozik. Különösen, ha* A_0 *egység, akkor már z maga is holoid mennyiség*

Az előbbiek szerint z alakja minden esetre $\frac{P}{Q}$, a hol $(P, Q) \sim 1$; ha tehát (1)-ben Q^k-val szorzunk, nyerjük, hogy

$$A_0 P^k + A_1 P^{k-1} Q + \cdots A_k Q^k = 0.$$

$A_0 P^k$ tehát osztható Q-val és, minthogy $(P, Q) \sim 1$, A_0 is osztható Q-val és így $A_0 z = \frac{A_0 P}{Q}$ holoid mennyiség.

Ugyanez az egyenlet mutatja, hogy $A_k Q^k$ és így A_k is osztható P-vel. Ebből következik:

Hogy valamely $z = \frac{P}{Q}$ *orthoid mennyiség kielégíthesse az* (1) *egyenletet, szükséges, hogy P az* A_k*-nak és Q az* A_0*-nak osztója legyen.*

Ha az (1) és [1] tartományokkal van dolgunk, úgy hogy az $A_0, \ldots, A_k$ mennyiségek raczionális és egész számok, akkor ez a tétel szolgáltatja *azoknak a raczionális számoknak teljes meghatározását, a melyek az* (1) *egyenletnek «gyökei»*; mert minden 0-tól különböző raczionális és egész számnak csak véges számú osztója van, és így minthogy az $A_k = 0$ eset könnyen elkerülhető, véges számú kisérlet

megadja azokat a raczionális számokat, a melyek az adott feltételeknek megfelelnek.

Ha az (A) *tartományon belül*

$z^m+\cdots+A_m=(z^k+M_1z^{k-1}+\cdots+M_k)(z^{m-k}+N_1z^{m-k-1}+\cdots+N_{m-k})$

és $A_1, \ldots, A_m$ *holoid mennyiségek, akkor az* $M_1, \ldots, M_k$, $N_1, \ldots, N_{m-k}$ *mennyiségeknek is holoid mennyiségeknek kell lenniök.*

Ha ugyanis az adott szorzatra a KRONECKER-féle alaptételt alkalmazzuk, azt találjuk, hogy M_i és N_j (mint $1 . M_i$ és $1 . N_j$ együttható-szorzatok) oly egyenletet elégítenek ki, a melyben M_i ill. N_j legmagasabb hatványának együtthatója 1, míg az összes többi együttható holoid mennyiség. Így tehát az előbbiek szerint az összes M_i és N_j mennyiségeknek holoid mennyiségeknek kell lenniök.

Különösen az (1) tartományban ily alakú felbontás esetében az $A_1, \ldots, A_m$ együtthatókkal együtt az M_i és N_j együtthatók is raczionális és egész számok.

Ez a GAUSS-tól származó tétel* történetileg kiinduló pontja volt az algebrai mennyiségek általános elméletének.

A resultáns.

13. §. Most az utolsó fejtegetésekben fentartott feltevést, hogy az [A] tartomány teljes, ismét elejtjük. Ez azért is fontos, mert az algebrai mennyiségek elméletében fellépő tartományok — mint azt már az I. fej. 8. és 9. §-ában tárgyalt egyszerű példa mutatta — általánosságban *nem* teljesek. A két eset között fennálló jellemző különbség a következő tényben rejlik:

Ha A az [A] tartomány valamely mennyisége, G pedig

* Disquisitiones arithmeticæ 42. cz.

az $[A, x]$ tartomány oly irreducibilis mennyisége, a mely nem osztója A-nak, akkor teljes tartományok esetében AF-fel együtt F is osztható G-vel; mert hiszen $(A, G) \sim 1$ és így $(AF, G) \sim G$-ből következik, hogy egyszersmind $(F, G) \sim G$. Ha ellenben az $[A]$ tartomány nem teljes, akkor jóllehet, hogy AF osztható G-vel, nem szükséges, hogy F is osztható legyen G-vel.

Ha ismét az épen idézett példára, a $[\sqrt{-5}]$ tartományra térünk vissza, akkor pl. 3 nem osztható a $2-\sqrt{-5}$ irreducibilis mennyiséggel, de $3 \cdot 3$ igenis osztható. Hogy oly G mennyiségek esetében, a melyek az x-et valóban tartalmazzák, a viszonyok hasonlók, ép oly könnyen mutatható ki. Igy pl.

$$G = 3x + (1 - 2\sqrt{-5})$$

— mint az közvetetlenül belátható — irreducibilis és

$$F = (2 - \sqrt{-5})\, x + (4 - \sqrt{-5})$$

nem osztható G-vel, noha

$$(2 - \sqrt{-5})\, F = 9x + 3(1 - 2\sqrt{5})$$

avval osztható.

Azt a kérdést, vajjon F osztható-e G-vel, tehát a következő módon kell általánosítanunk: Vannak-e az $[A]$ tartományban oly A mennyiségek, hogy AF oszthatóvá válik G-vel? Ámde $[A]$ az $[A, x_1, \ldots, x_m]$ tartományban foglalt æquivalentia-tartomány és így a felállított kérdés még így is fogalmazható: Van-e az $[A]$ æquivalentia-tartományra vonatkozólag oly F-fel æquivalens mennyiség, a mely osztható G-vel?

Az $[A, x_1, x_2, \ldots, x_m]$ tartomány mennyiségeinek relativ æquivalentiája az $[A]$ æquivalentia-tartományra vonatkozólag épen absolut æquivalentia abban a tartományban, a mely származik $[A, x_1, \ldots, x_m]$-ből, ha nevezőkként az $[A]$ tartomány mennyiségeit használjuk, azaz az orthoid (A)

tartományból származó $[(A), x_1, \ldots, x_m]$ formatartományban. Ezt az eredményt még egyszerűbben fogalmazhatjuk.

Áttérünk a holoid [A] tartományról a mellérendelt orthoid (A) tartományra és megvizsgáljuk a formák oszthatóságát még akkor is, ha holoidok, a bővített $[(A), x_1, \ldots, x_m]$ tartományban. Ez a tartomány teljes, mert minden orthoid tartomány, tehát (A) is teljes és így, ha a kérdést ebben az általánosított alakban állítjuk fel, alkalmazhatjuk az előbb kifejtett módszereket.

Mint az algebrai mennyiségek elméletének czélja egyenesen az tűzhető ki, hogy az eredeti vizsgálatok alapjául szolgáló tartományt új fogalomalkotásokkal oly módon bővítsük, hogy egyrészt bizonyos feladatoknak, a melyek az eredeti tartományban nem oldhatók meg, az új tartományban legyen megoldásuk, másrészt pedig, hogy az eredeti tartomány mennyiségeinek bizonyos tulajdonságai megmaradjanak változatlanul az új tartományban is. Legalább is azok a törvények maradjanak meg, a melyek szerint az eredeti tartomány mennyiségeinek összeadása és szorzása megy végbe úgy, hogy, ha ezeket a műveleteket a bővített tartományban az eredeti tartomány mennyiségeire alkalmazzuk, eredményül ugyanazokat a mennyiségeket nyerjük, mint előbb. Csakis ekkor mondjuk, hogy az új, bővített tartomány *tartalmazza* vagy *magában foglalja* az eredeti tartományt. Ez az eset beáll tényleg, ha [A]-ról (A)-ra térünk át.

Figyelmeztetünk azonban arra, hogy [A] mennyiségeinek bizonyos más tulajdonságai megváltoznak. (A)-ban ugyanis minden A mennyiség osztható minden más a 0-tól különböző B mennyiséggel; e mennyiségeknek az oszthatóságra vonatkozó tulajdonságai itt tehát egészen mások. Ez utal bizonyos új, igen fontos fogalomalkotásra, az [A] tartomány oly bővítésére, hogy az új tartomány teljes legyen,

de e mellett az [A] mennyiségeinek az oszthatóságra vonatkozó tulajdonságai megmaradjanak. Ennek az alapproblémának tárgyalása azonban még további segédeszközökre támaszkodik és ezért csak később (a IX. fejezetben) lesz elintézhető.

14. §. Legyen már most

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_m,$$
$$G = B_0 x^n + B_1 x^{n-1} + \cdots + B_n$$

két forma, a melyeknek együtthatói a holoid [A] tartományhoz tartoznak. Ha azután az orthoid (A) tartományra megyünk át (a mely [A]-val egybe is eshetik), akkor F és G egyszersmind az $[(A), x]$ tartománynak is formái és mint ilyeneknek van legnagyobb közös osztójuk. Az (A) tartomány minden mennyisége æquivalens 1-gyel; ama legnagyobb közös osztó tehát vagy 1, vagy pedig valamely x-et tartalmazó igazi forma. E két eset szétválasztása reávezet a resultáns fontos alapfogalmára.

Ha (F, G) az x valamely igazi formájával æquivalens, tehát

$$(F, G) \sim D = D_0 x^k + D_1 x^{k-1} + \cdots + D_k,$$

akkor

$$F = D\overline{V}, \quad G = -D\overline{U}$$

és

$$-\overline{U} = \overline{P}_0 x^{n-k} + \overline{P}_1 x^{n-k-1} + \cdots + \overline{P}_{n-k},$$
$$\overline{V} = \overline{Q}_0 x^{m-k} + \overline{Q}_1 x^{m-k-1} + \cdots + \overline{Q}_{m-k},$$

a hol D, $\overline{U}$ és $\overline{V}$ együtthatói az (A) tartományhoz tartoznak. Igy tehát

$$UF + \overline{V}G = 0.$$

Minthogy D legalább is elsőfokú, tehát $k \geqq 1$, azért $m-k \leqq m-1$ és $n-k \leqq n-1$. Hogy tehát (F, G) az æquivalentia értelmében az 1-től különböző lehessen, szükséges, hogy meghatározhassunk két oly formát,

$$-U = P_0 x^{n-1} + \cdots + P_{n-1},$$
$$V = Q_0 x^{m-1} + \cdots + Q_{m-1},$$

AKADÉMIA KÖNYVTÁR

a melynek együtthatói nem mindannyian egyenlők 0-sal és az

$$UF + VG = 0$$

relációt kielégítik. Ez a lényegében EULER-től származó eljárás a következő P és Q meghatározására szolgáló egyenletrendszert adja:

$$\begin{aligned} A_0 P_0 \quad &+ B_0 Q_0 \quad = 0 \\ A_1 P_0 + A_0 P_1 \quad &+ B_1 Q_0 + B_0 Q_1 \quad = 0 \\ &\cdots\cdots\cdots\cdots \\ A_m P_{n-1} \quad &+ B_n Q_{m-1} = 0, \end{aligned}$$

a hol a rendszer általános, $k+1$-dik egyenlete a következő módon jellemezhető:

$$\Sigma A_i P_r + \Sigma B_j Q_s = 0$$

$$\left(\begin{matrix} i=0, 1, \ldots, m;\ j=0, 1, \ldots, n;\ r=0, 1, \ldots, n-1;\ s=0, 1, \ldots, m-1 \\ i+r=k,\ j+s=k \end{matrix}\right)$$

és k rendre $0, 1, \ldots, m+n-1$ lehet.

Így tehát oly homogén, lineáris egyenletrendszerhez jutottunk, a melyben úgy az egyenletek, mint az ismeretlenek száma $m+n$ és ezek az ismeretlenek, a P és Q együtthatók csak akkor nem lesznek mindannyian 0-sal egyenlők, ha az egyenletek együtthatóiból alkotott determináns, az ú. n. *Sylvester-féle determináns* * eltünik.

* SYLVESTER, «On a general method of determining by mere inspection the derivatives from two equations of any degree», Phil. Mag. 1840. febr. 132. lap. — Az «Encyclopädie d. math. Wiss.» (I. k. 246. lap sub 88 és 89) helytelen adataival szemben még megjegyezzük, hogy RICHELOT «Nota ad theoriam eliminationis pertinens» című dolgozatában SYLVESTER eredményeit már határozottan idézi (Journ. f. Math. 21. k.). Körülbelül négy évvel később HESSE ugyanezt a determinánst állítja fel («Über die Endgleichung etc.» Journ. f. Math. 27. Werke 83. lap), de csodálatos módon két elődje közül egyikről sem emlékezik meg.

Ennek az

$$R = \begin{vmatrix} A_0 & & & B_0 & & & \\ A_1 & A_0 & & B_1 & B_0 & & \\ . & A_1 & & . & B_1 & . & \\ . & . & A_0 & . & . & . & \\ A_m & . & A_1 & . & . & . & B_0 \\ & A_m & . & . & . & . & B_1 \\ & & . & B_n & . & . & . \\ & & . & & & & . \\ & & A_m & & & & B_n \end{vmatrix}$$

determinánsnak a törvénye egyszerűen a következő módon fejezhető ki: A j-dik oszlopban ($j=1, \ldots, n$) $j-1$ zérus után állanak az $A_0, A_1, \ldots, A_m$ elemek, a melyekre ismét $n-j$ zérus következik; az $n+k$-dik oszlopban ($k=1, \ldots, m$) $k-1$ zérus után következnek a $B_0, B_1, \ldots, B_n$ elemek és ezek után ismét $m-k$ zérus.

Ha viszont ez a determináns zérus a nélkül, hogy egyúttal A_0 és B_0 is eltünnének, akkor tudvalevőleg vannak a P és Q együtthatók oly értékrendszerei, a melyeknek értékei nem tünnek el mindannyian és a felállított egyenletrendszert kielégítik; még pedig olyanok is, a melyekben ezek mind az A_i és B_j mennyiségek raczionális és egész formái. Az

$$UF + VG = 0$$

relácziő értelmében azonban VG-nek oszthatónak kell lennie F-fel és UF-nek G-vel. Ha már mostan $(F, G) \sim 1$ volna, akkor V volna oszható F-fel és U a G-vel. Ha azonban pl. A_0 nem 0, akkor V az x-ben legfölebb $m-1$-edfokú lehetne és csak úgy lehetne osztható F-fel, ha azonosan zérus. Így tehát ebben az esetben szükséges, hogy $VG=0$ legyen. Ámde sem V nem tünhetik el, mert akkor eltünnének az összes P és Q együtthatók, valamint az sem lehetséges, hogy $G=0$, mert ebből

következnék, hogy $(F, G) \sim F$, holott F mint m-edfokú forma nem lehet ~ 1-gyel.

Az R mennyiség eltünése tehát szükséges és elegendő feltétele annak, hogy az F és G formáknak, a melyekben A_0 és B_0 nem egyidőben egyenlők 0-sal, az (A) tartományból származó $[(A), x]$ formatartományban az æquivalentia értelmében az 1-től különböző legnagyobb közös osztója legyen.

15. §. Az R mennyiség *az F és G formáknak az x határozatlanra vonatkozó resultánsa,* a hol ez a pontosabb, x-re vonatkozó megjelölés el is hagyható, ha ennek következtében kétértelműség nem áll elő. Ebben az esetben jelölésére szolgáljon

$$\text{Res.}\,(F, G),$$

a hol azután $\text{Res.}\,(G, F) = (-1)^{mn}\,\text{Res.}\,(F, G)$, a mint azt az értelmezés alapjául szolgáló determináns közvetetlenül mutatja. Minthogy az F és G formák még további határozatlanokat is tartalmazhatnak, általánosabb vizsgálatokban pontosabb jelölésre van szükségünk, a melyet, tekintettel későbbi fejtegetésekre, a következő módon állapítunk meg:

$$\text{Res.}\begin{pmatrix} F, & G \\ x, & 1 \end{pmatrix}.$$

Ha már az [A] tartomány maga is oly formák tartománya, a melyek általánosságban a holoid $[\bar{A}]$ tartományból származnak, azaz $[A] = [\bar{A}, x_1, \ldots, x_m]$, akkor, ha A_0 és B_0 nem egyidőben egyenlők zérussal, az F és G resultánsának eltünése arra mutat, hogy van olyan

$$D = D_0 x^k + D_1 x^{k-1} + \cdots + D_k$$

legnagyobb közös osztójuk, a hol a $D_0, \ldots, D_k$ mennyiségek alakja $\frac{\bar{D}_i}{E_i}$, $\bar{D}_i$ és E_i az [A] tartományhoz tartoznak és legalább egy a $\bar{D}_0, \ldots, \bar{D}_{k-1}$ mennyiségek közül, valamint az E_i mennyiségek valamennyien különbözők a zérustól. Ha tehát az E_i mennyiségek szorzata E, akkor EF-nek és EG-nek

ez az osztójuk van:

$$D' = D'_0 x^k + D'_1 x^{k-1} + \cdots + D'_k,$$

a hol a D'_i-k az [A] tartomány mennyiségei és a $D'_0, \ldots, D'_{k-1}$ közül ismét legalább egy különböző a zérustól. Ha már most az $[(\bar{A}), x_1, x_2, \ldots, x_m]$ formatartományban $(F, G) \sim 1$ volna, E-nek oszthatónak kellene lennie D'-vel, a mi lehetetlen, mert E az x határozatlant nem tartalmazza.

Ha pedig viszont (F, G) az æquivalentia-meghatározás értelmében az $[(\bar{A}), x_1, x_2, \ldots, x_m]$-re vonatkozólag nem egy, ebből közvetetlenül következik, hogy van egy D alakú osztó és hogy a resultáns eltünik.

Ezek alapján a resultáns *első alaptulajdonságát* a következőben fejezhetjük ki:

Ha $F = A_0 x^m + \cdots$, $G = B_0 x^n + \cdots$ *két oly forma, a melyeknek együtthatói az* [A] *tartományból származó formák és* A_0 *és* B_0 *nem egyidőben egyenlők zérussal, akkor* F *és* G *resultánsának eltünése szükséges és elegendő feltétele annak, hogy áttérve az orthoid* (A) *tartományból származó formákra,* F *és* G *legnagyobb közös osztója az* x*-et valóban tartalmazó forma legyen.*

Az eddigiek szerint világos, hogy az átmenet a holoid [A] tartományról az orthoid (A) tartományra csak akkor szükséges, ha az [A] tartomány nem teljes. Ha [A] teljes tartomány, akkor tartalmaz oly A mennyiséget, hogy AF és AG bizonyos az [A] tartományból származó, x-et tartalmazó H formával osztható. A-nak vehetjük pl. ama legnagyobb közös osztóban előforduló nevezők szorzatát. Ámde akkor F és G osztható a H primitiv formájával és ez különböző az 1-től.

Az eddig előadottaknak lényeges tartalmát már a következő egyszerű tétel foglalja magában:

Az [A] *orthoid tartományból származó* F *és* G *formák-*

nak, a melyek valamely határozatlanra nézve szabályosak, akkor és csak akkor van az 1*-től különböző legnagyobb közös osztójuk, ha arra a határozatlanra vonatkozó resultánsuk eltünik.*

Mert az e határozatlan szerint rendezett formákban sem A_0, sem B_0 nem egyenlő zérussal és minthogy F és G minden valódi osztójának (e fej. 3. §-a szerint) szintén szabályosnak kell lennie, a legnagyobb közös osztónak, ha nem 1, tartalmaznia kell ama határozatlant.

16. §. A resultáns *második alaptulajdonsága* egyszerű következménye a determináns alakjában való előállításának.

Ha az R determinánsban (14. §.) az i-dik sort megszorozzuk x^{m+n-i}-vel és az így nyert elemeket hozzáadjuk a változatlan utolsó sorhoz, akkor ennek elemei rendre a következők lesznek:

$$Fx^{m-1},\ Fx^{n-2},\ \ldots,\ F,\ Gx^{m-1},\ Gx^{m-2},\ \ldots,\ G.$$

Ez vezet *az R mennyiség következő előállítására:*

$$R = G_1 F + F_1 G,$$

a hol G_1 az x-ben legfölebb $n-1$-edfokú és ép úgy F_1 legfölebb $m-1$-edfokú; F_1 és G_1 együtthatói itt az A és B együtthatók raczionális és egész formái.

A következőkben mindenütt megengedjük, hogy a formák együtthatói az orthoid (A) tartományhoz tartozzanak és az æquivalentia-meghatározást hasonlóképen erre a tartományra fogjuk vonatkoztatni. A resultáns első alaptulajdonságát azután még így is fogalmazhatjuk, hogy $R \sim 1$-ből következik $(F, G) \sim 1$ és viszont.

Ha már mostan R a 0-tól különböző, azaz $R \sim 1$, akkor (F_1, G_1) is ~ 1. Az ellenkező esetben F_1 és G_1 legnagyobb közös osztója, noha igazi forma, mégis osztója volna R-nek, a mi lehetetlen. De akkor sem F_1, sem G_1 nem lehet zérus.

Ha pl. volna $F_1 = 0$, tehát $R = G_1 F$, akkor G_1 nem lehetne 0 és R osztható volna F-fel.

Ha $R=0$, akkor $(F, G) \sim D$ oly forma, a mely tartalmazza x-et és azután lesz:

$$F = DF', \quad -G = DG', \quad (F', G') \sim 1,$$

vagyis

$$0 = G'F + F'G.$$

Bármely

$$r = gF + fG$$

relációból, a melyben f foka x-ben nem magasabb $m-1$-nél és g-é $n-1$-nél, továbbá f és g a 0-tól különbözők és r nem tartalmazza x-et, és végre még $(f, g) \sim 1$, következik, hogy

$$r \sim R;$$

azaz annak eldöntésére, vajjon (F, G) valóban tartalmazza-e az x határozatlant az r mennyiség ép úgy használható, mint R. Ennek bebizonyítására vegyük figyelembe, hogy az

$$r = gF + fG, \quad R = FG_1 + F_1 G$$

relációkból még következik, hogy

$$(gF_1 - fG_1)\ F = rF_1 - Rf,$$

a hol a jobb oldal, a melynek F-fel oszthatónak kellene lennie, x-ben legfölebb $m-1$-edfokú. Így tehát szükséges, hogy legyen

$$rF_1 - Rf = 0,$$
$$gF_1 - fG_1 = 0.$$

De akkor $r=0$-ból közvetetlenül következik, hogy $R=0$ és viszont $R=0$-ból, mert r osztható (F, G)-vel és ez a mennyiség ebben az esetben x-et tartalmazza, következik, hogy $r=0$. Ez épen az, a mit az $r \sim R$ æquivalentia kifejez.

17. §. Ha ismét $(F, G) \sim D$, tehát $\left(\frac{F}{D}, \frac{G}{D}\right) \sim 1$, akkor $\frac{F}{D}$ és $\frac{G}{D}$ resultánsa, R' oly el nem tünő forma, a mely nem tartalmazza x-et és a melyre nézve

$$DR' = UF + VG;$$

azaz F és G legnagyobb közös osztója bizonyos x-et nem

tartalmazó mennyiséggel való megszorzása után mint F és G homogén, lineáris formája állítható elő.

Itt R', valamint az U és V együtthatók kellően választott tényező hozzácsatolásával holoid formákba vihetők át.

Ezt az eredményt különösen akkor fogjuk alkalmazni, ha az eredeti [A] tartomány holoid; mert akkor D-t abban az alakban írhatjuk, a mely (F, G) számára az [A] tartományból származó formatartományban létezik.

Hogy még itt sem mehetünk tovább, azaz, hogy D maga nem állítható elő mint F és G homogén, lineáris formája, a következő egyszerű példa is már mutatja, a hol alapul az [1] tartományt választottuk. Az $x+2$ és $x+4$ formák legnagyobb közös osztója 1 és

$$2 = (x+4) - (x+2).$$

Ily alakú reláczió:

$$1 = U(x+2) + V(x+4)$$

azonban nem állhat fenn, mert akkor a jobb oldalon az x-től független tagnak $2a+4b$ alakúnak és 1-gyel egyenlőnek kellene lennie; és így 1-nek oszthatónak kellene lennie 2-vel.

Formarendszerek resolvens formája.

18. §. A következő vizsgálat menete legegyszerűbb lesz akkor, ha a tárgyalandó formákról felteszszük, hogy valamely teljes holoid [A] tartományból származnak. Hogy a nyert eredményeket azután más esetekre is alkalmazhassuk, csak azt kell figyelembe vennünk, hogy akkor az összes együtthatók benne vannak a mellérendelt orthoid (A) tartományban, és minthogy minden orthoid tartomány teljes, evvel az eredmény oly fogalmazását nyerjük, a mely érvényes marad akkor is, ha az alapul felvett holoid [A] tartomány nem teljes.

Legyen már most

$$F_j(x_1, x_2, \ldots, x_m) \qquad (j=1, \ldots, k)$$

k forma, mely a teljes holoid [A] tartományból származik. Annak eldöntésére, vajjon ezeknek a formáknak legnagyobb közös osztója magához az [A] tartományhoz tartozik-e, vagy pedig az $x_1, \ldots, x_m$ határozatlanoknak legalább egyikét tartalmazza, legegyszerűbb lesz, ha az F_j formákat oly racionális és egész számú együtthatókkal ellátott lineáris transformatiónak vetjük alá, a melynek determinánsa egyenlő egygyel (II. fej. 19. §.) és a mely az összes formákat olyanokba vezeti át, a melyek az összes új y_1 határozatlanokra nézve szabályosak. Ez a lineáris transformatio a kérdéses tulajdonságot nem érinti, mert — mint közvetetlenül látni — a transformált formák legnagyobb közös osztóját úgy állíthatjuk elő, hogy ugyanazt a lineáris transformatiót alkalmazzuk az eredeti formák legnagyobb közös osztójára. Minthogy azonban szabályos formák minden osztója is szabályos, kérdésünk evvel arra van visszavezetve, vajjon ama formáknak van-e egyáltalában olyan osztójuk, a mely tartalmazza y_1-et. Ez a transformatio, a mely KRONECKER kifejezése szerint a formák rendszerét «az esetleges körülményektől megszabadítja», ugyanaz, a mit a geometria nyelvén affinitásnak szokás nevezni; még pedig olyan, a melyben «a végtelenben fekvő elemek» az eldöntendő kérdésekben tovább nem jönnek tekintetbe.

Hogy a jelölést túlságosan ne bonyolítsuk, legyenek F_j és x_i már a transformált formák, ill. határozatlanok.

Ha már mostan u_j és u_j' $(j=1, \ldots, k)$ a határozatlanok két új sorozata, akkor a

$$\sum_{j=1}^{k} F_j u_j \quad \text{és} \quad \sum_{j=1}^{k} F_j u_j'$$

formáknak akkor és csak akkor lesz az x_1-et tartalmazó legnagyobb közös osztójuk, ha ugyanaz az eset áll fenn az F_j formákra is. Az F_j formáknak az új u_j és u_j' határozatlanok segítségével való formális összefoglalása igen messzevágó jelentőségű; KRONECKER * használta legelőször és azért KRONECKER-féle eliminációs-elvnek akarjuk nevezni.

Ezeket az új formákat is az $x_1, \ldots, x_m$ határozatlanok formáiként fogjuk fel, a melyeknek együtthatói azonban most az $[A, u_1, \ldots, u_k, u_1', \ldots, u_k']$ holoid tartományhoz tartoznak. Mint ilyenek azonban az $F_1, \ldots, F_k$ formákkal együtt szabályosak, azaz x_i legmagasabb hatványának együtthatója az $x_1, \ldots, x_m$ határozatlanoktól független mennyiség. Így tehát

$$\text{Res.}\begin{pmatrix} \Sigma F_j u_j, & \Sigma F_j u_j' \\ x_1 \quad , & 1 \end{pmatrix} = R_0 U_0 + R_1 U_1 + \cdots,$$

a hol $U_0, U_1, \ldots$ az u és u' határozatlanok különböző hatványszorzatait jelentik, míg az R-ek az $[A, x_2, \ldots, x_m]$ tartomány mennyiségei és $R_0, R_1, \ldots$ *eltünése szükséges és elegendő feltétele annak, hogy az F_j formáknak oly legnagyobb közös osztójuk legyen, a mely x_1-et valóban tartalmazza.*

Legyen már most

$$(F_1, \ldots, F_k) \sim D, \quad F_j = F_j D,$$

úgy hogy

$$(\bar{F}_1, \ldots, \bar{F}_k) \sim 1$$

és továbbá

$$\text{Res.}\begin{pmatrix} \Sigma \bar{F}_j u_j, & \Sigma \bar{F}_j u_j' \\ x_1 \quad , & 1 \end{pmatrix} = F_1^{(1)} U_0 + F_2^{(1)} U_1 + \cdots,$$

akkor nem tünhetnek el az összes $F_1^{(1)}, F_2^{(1)}, \ldots$ mennyiségek. A resultánsnak a 16. §-ban kimutatott második alaptulajdonsága szerint azután

* Festschrift 10. §.

$$F_1^{(1)}U_0+F_2^{(1)}U_1+\cdots=G_1\Sigma\bar{F}_j u_j+H_1\Sigma\bar{F}_j u_j'$$

és ha ebben a különböző U_l hatványszorzatok együtthatóit összehasonlítjuk, minden egyes $F_{j_1}^{(1)}$ mennyiség az $\bar{F}_j$-k homogén lineáris formája, vagyis az I. fej. 10. §-ában értelmezett jelöléssel

$$F_{j_1}^{(1)}\equiv 0\,(\text{mod. } \bar{F}_1,\ldots,\bar{F}_k), \qquad (j_1=1,\ldots,k_1)$$

és így

$$DF_{j_1}^{(1)}\equiv 0\,(\text{mod. } F_1,\ldots,F_k). \qquad (j_1=1,\ldots,k_1).$$

Megjegyzendő, hogy az $F_{j_1}^{(1)}$ mennyiségek az $x_2,\ldots,x_m$ oly formái, a melyek az [A] tartományból származnak.

Az $F_{j_1}^{(1)}$ formákról ismét feltételezhetjük, hogy $x_2,\ldots,x_m$-re nézve szabályosak. Ha nem volna így, akkor arra, hogy szabályos formákat nyerjünk, elég az $x_2,\ldots,x_m$ határozatlanok oly $T^{(1)}$ lineáris transformatióját alkalmaznunk, a melynek együtthatói raczionális és egész számok és determinánsa egyenlő egygyel. Ezt a transformatiót azonban mindjárt kezdettől fogva az F_j formákon végezhetjük el ama transformatio után, a mely ezeket a formákat szabályos formákba viszi át. E mellett az eddigi eredmények csak annyiban változnak, hogy a tárgyalás közben értelmezett, $D, F_1^{(1)}, F_1^{(2)},\ldots$ mennyiségek is már mint a $T^{(1)}$ transformatióval átalakított formák lépnek fel.

Ha már mostan az

$$F_{j_1}^{(1)}(x_2,\ldots,x_m) \qquad (j_1=1,\ldots,k_1)$$

formákkal ép úgy bánunk el, legyen

$$(F_1^{(1)},\ldots,F_{k_1}^{(1)})\sim D^{(1)},$$

$$F_{j_1}^{(1)}=D^{(1)}\bar{F}_{j_1}^{(1)},$$

$$\text{Res.}\begin{pmatrix}\Sigma\bar{F}_{j_1}^{(1)}u_{j_1}^{(1)}, & \Sigma\bar{F}_{j_1}^{(1)}v_{j_1}^{(1)}\\ x_2 \quad , & 1\end{pmatrix}=F_1^{(2)}U_0^{(1)}+F_2^{(2)}U_1^{(1)}+\cdots,$$

akkor e formák

$$F_{j_2}^{(2)}(x_3, \ldots, x_m) \qquad (j_2=1, \ldots, k_2)$$

rendszerére nézve ismét áll, hogy

$$D^{(1)}F_{j_2}^{(2)} \equiv 0 \,(\text{mod. } F_1^{(1)}, \ldots, F_{k_1}^{(1)})$$

és végre, hogy

$$DD_1F_{j_2}^{(2)} \equiv 0 \,(\text{mod. } F_1, \ldots, F_k).$$

Ezt az eljárást ezen a módon folytatva, a formák

$$F_{j_{h-1}}^{(h-1)}(x_h, \ldots, x_m) \qquad (j_{h-1}=1, \ldots, k_{h-1})$$

rendszeréről, ha

$$(F_1^{(h-1)}, \ldots, F_{k_{h-1}}^{(h-1)}) \sim D^{(h-1)},$$

$$F_{j_{h-1}}^{(h-1)} = D^{(h-1)}\bar{F}_{j_{h-1}}^{(h-1)}$$

és

$$\text{Res.}\begin{pmatrix} \Sigma\bar{F}_{j_{h-1}}^{(h-1)}u_{j_{h-1}}^{(h-1)}, & \Sigma\bar{F}_{j_{h-1}}^{(h-1)}v_{j_{h-1}}^{(h-1)} \\ x_h \quad , & 1 \end{pmatrix} =$$

$$= F_1^{(h)}U_0^{(h-1)} + F_2^{(h)}U_1^{(h-1)} + \cdots,$$

általánosságban a formák oly

$$F_{j_h}^{(h)}(x_{h+1}, \ldots, x_m) \qquad (j_h=1, \ldots, k_h)$$

rendszeréhez jutunk, a melyekben az $x_1, \ldots, x_h$ határozatlanok már nem fordulnak elő, míg $x_{h+1}, \ldots, x_m$-re nézve szabályosak; tehát vagy e határozatlanokat valóban tartalmazzák, vagy pedig dimensiójuk 0, azaz minden határozatlantól mentesek. Mindaddig, míg ez az eset az összes formákra nem áll be, a jellemzett eljárást folytathatjuk és ha nem előbb minden esetre m lépés után, általánosságban pedig — mondjuk — r lépés után oly

$$F_{j_r}^{(r)} \qquad (j_r=1, \ldots, k_r)$$

mennyiségekhez jutunk, a melyek a határozatlanoktól teljesen mentesek és így az [A] tartományhoz tartozó mennyiségek.

Ha még

$$D^{(h)} \sim (F_1^{(h)}, F_2^{(h)}, \ldots, F_{k_h}^{(h)})$$

és különösen $h=r$ esetében

$$F_{j_r}^{(r)} = D^{(r)} C_{j_r} \qquad (j_r=1, \ldots, k_r),$$

akkor végre *azt találjuk, hogy*

$$DD^{(1)} \ldots D^{(r)} C_{j_r} \equiv 0 \,(\text{mod. } F_1, \ldots, F_k), \qquad (\bar{R})$$

vagy pedig, ha ezeket az új $w_1, w_2, \ldots$ *határozatlanok segítségével összefoglaljuk, hogy*

$$DD^{(1)} \ldots D^{(r)} \sum_{j_r=1}^{k_r} C_{j_r} w_{j_r} \equiv 0 \,(\text{mod. } F_1, \ldots, F_k), \qquad (R)$$

a hol $D^{(h)}$ $(h=1, \ldots, r-1)$ *az* $x_{h+1}, \ldots, x_m$ *határozatlanoknak oly formáját jelenti, a mely* $x_{h+1}, \ldots, x_m$*-re nézve szabályos, míg* $D^{(r)}, C_{j_r}$ *az* [A] *tartomány mennyiségei és* $1 \leqq r \leqq m$.

Az (R) bal oldalán álló formát, ama fontos szerepénél fogva, mely neki az algebrai egyenletrendszerek elméletében jut, *az* F_i *formarendszer resolvens formájának* nevezzük. Különösen megjegyezzük, hogy e resolvens forma ama tulajdonsága, a melyet (R) kifejez, fennáll még akkor is, ha a formák dimensiója részben, vagy pedig mindegyiké 0. Az utóbbi esetben az eredmény természetesen triviális. Ugyanis, ha

$$(A_1, \ldots, A_k) \sim D, \quad A_i = DC_i,$$

akkor (R) átmegy ebbe a magától értetődő relációba:

$$D \sum_{i=1}^{k} C_i w_i = \sum_{i=1}^{k} A_i w_i.$$

Azt is látjuk, hogy (R) érvényes marad még akkor is, ha az F_i formákat eredeti alakjukban újabb lineáris transformatio nélkül megtartjuk; csakhogy ekkor $D, D^{(1)}, \ldots, D^{(r-1)}$-nek nincs meg a fennebb jellemzett speciális szabályos alakjuk. Hogy ezt belássuk, csak a transformált formákra vonatkozó (R) congruentiára a recziprok transformatiót kell alkalmaznunk.

Ha végre a holoid [A] tartomány nem teljes, akkor az

(R) congruentiát, vagy pedig az ennek megfelelő

$$DD^{(1)} \dots D^{(r)} \sum_{j_r=1}^{k_r} C_{j_r} w_r = \sum_{i=1}^{k} G_i F_i$$

identitást minden esetre fölállíthatjuk a megfelelő orthoid (A) tartományban. Akkor mindegyik $D^{(h)}$ forma ilyen alakú lesz: $\frac{\overline{D}^{(h)}}{A_h}$, a hol $\overline{D}^{(h)}$ együtthatói már az [A] tartományhoz tartoznak és egyetlen A_h sem zérus. Ha tehát $A_1 A_2 \dots A_r$ oly többszörösével szorzunk, hogy úgy a C_{j_r} mennyiségek, mint a G_i-k együtthatói holoidokká válnak, akkor a nem teljes tartományok esetére nyerjük a megfelelő

$$A\overline{D}\overline{D}^{(1)} \dots \overline{D}^{(r)} \sum_{j_r=1}^{k_r} C_{j_r} w_r \equiv 0 \,(\text{mod. } F_1, \dots, F_k). \qquad (\overline{R})$$

congruentiát, a hol a bal oldalon álló mennyiség, és így minden tényezője is különbözik a 0-tól.

Az egyenletek elméletének problémája.

19. §. Ha $F_j(x_1, \dots, x_m)$, $(j=1, \dots, k)$ ismét a holoid [A] tartományból származó formák, akkor az egyenletek és egyenletrendszerek elméletének általános problémáját, a mely ebben a fogalmazásban — a mit különösen kiemelünk — az úgynevezett diophantikus egyenletek esetére is kiterjeszkedik,* a következő módon fogalmazhatjuk:

(a) *Meghatározandók az* [A] *tartományhoz tartozó mindamaz* $x_i = \xi_i$, $(i=1, \dots, m)$ *értékrendszerek, a melyekre nézve* $F_j(\xi_1, \dots, \xi_m)$, $(j=1, \dots, k)$ *egyenlővé válik zérussal.*

Ekkor a «formákról» átmentünk az «egész függvényekre». Ezt az átmenetet megokolja a dolog természete:

* Sőt a mi gondolatmenetünk szerint tulajdonképen csakis diophantikus egyenletekre. A classikus egyenlet-problémára úgy jutunk, ha alapul mint holoid tartományt a complex számok összességét veszszük fel.

mert minden ilyen ξ_i rendszer az F egész függvény egy egy alapvető tulajdonságát, egy-egy úgynevezett «zérushelyét» szolgáltatja. Azonban tekintettel az elvi felfogásra mindjárt megjegyezzük, hogy ugyanez a probléma oly módon is fogalmazható, hogy teljesen a formák elméletének körében maradhassunk. E fogalmazás a következő:

(b) *Meghatározandók az* [A] *tartományhoz tartozó mindama* $\xi_i (i=1, \ldots, m)$ *értékrendszerek, a melyekre nézve*

$$F_j(x_1, \ldots, x_m) \equiv 0 (\text{mod. } x_1-\xi_1, x_2-\xi_2, \ldots, x_m-\xi_m). \quad (j=1, \ldots, k).$$

Hogy a ξ_i értékrendszerek (a)-ban és (b)-ben kimondott tulajdonsága ugyanaz, közvetetlenül belátjuk, ha az

$$F_j(x_1, \ldots, x_m) = F_j(\xi_1+x_1-\xi_1, \ldots, \xi_m+x_m-\xi_m)$$

formát az $x_1-\xi_1, \ldots, x_m-\xi_m$ mennyiségek hatványszorzatai szerint kifejtjük és az eredményt az

$$F_j(x_1, \ldots, x_m) \equiv F_j(\xi_1, \ldots, \xi_m) (\text{mod. } x_1-\xi_1, \ldots, x_m-\xi_m)$$

alakban írjuk. Így közvetetlenül belátjuk, hogy az (a) feltételt kielégítő ξ_i értékrendszerek kielégítik a (b) feltételt is. Ha pedig viszont ξ_i valamely a (b) feltételt kielégítő értékrendszer, akkor lesz

$$F_j(x_1, \ldots, x_m) \equiv 0 (\text{mod. } x_1-\xi_1, \ldots, x_m-\xi_m),$$

vagy pedig részletesebben kiírva:

$$F_j(x_1, \ldots, x_m) = G_1(x_1-\xi_1) + \cdots + G_m(x_m-\xi_m),$$

a hol feltételezhetjük, hogy úgy az F_j, mint a G formák az $x_1-\xi_1, \ldots, x_m-\xi_m$ mennyiségek hatványszorzatai szerint vannak rendezve. Akkor azonban, a jobb oldalon az a tag, a melynek dimensiója 0, egyenlő 0-sal; így tehát szükséges, hogy $F_j(\xi_1, \ldots, \xi_m)$ egyenlő legyen 0-sal.

Minden ilyen $\xi_1, \ldots, \xi_m$ értékrendszert az $F_j=0$ egyenletrendszer «megoldásának» vagy pedig «gyökének», ill. «gyökrendszerének» nevezzük. Az $x_1, \ldots, x_m$ határozatlanok akkor az egyenletrendszerben fellépő «ismeretlenek».

Valamely $F=0$ egyenlet dimensiója, valamint bizonyos x_i ismeretlenre vonatkozó foka ugyanazok a számok, a melyeket az F forma esetében így neveztünk.

Az egy ismeretlent tartalmazó m-edfokú

$$F(x)=A_0 x^m+A_1 x^{m-1}+\cdots+A_m=0$$

egyenletre nézve a következő elemi tételek érvényesek, a melyeket folyton alkalmazunk.

I. *Az* $F(x)=0$ *egyenletnek* ξ *akkor és csak akkor gyöke, ha az* $F(x)$ *forma osztható* $x-\xi$*-vel.*

Ez nem más, mint az (a)-ban és (b)-ben kiszabott feltételek egyenlőértékű voltáról szóló tétel a most fenforgó speciális esetben.

II. *A holoid* [A] *tartományon belül, a melyhez az* $F(x)=0$ *egyenlet együtthatói is tartoznak (hol ezek nem tünnek el mind), ennek az egyenletnek* m*-nél több különböző gyöke sohasem lehet.*

Ha η_i $(i=1,\ldots,m+1)$ $m+1$ oly érték volna, a mely az egyenletet kielégíti, akkor

$$A_0\eta_i^m+\cdots+A_m=0 \qquad (i=1,\ldots,m+1)$$

oly homogén lineáris egyenletrendszer lenne, a mely az $A_0,\ldots,A_m$ együtthatók meghatározására szolgálhatna és minthogy ennek az egyenletrendszernek determinánsa,

$$[\eta_i^m]=\prod_{r,s}(\eta_r-\eta_s) \qquad \left(\begin{smallmatrix} r,s=1,\ldots,m+1 \\ r<s \end{smallmatrix}\right)$$

a II. fej. 11. §-a szerint a 0-tól különböző, ebből feltevésünk ellenére következnék, hogy az egyenlet összes együtthatói eltünnek.

20. §. Ha a formák rendszerére — vagy a mint azt most még másképp is mondhatjuk — az $F_j=0$ egyenletrendszerre oly lineáris transformatiót alkalmazunk, a melynek együtthatói raczionális és egész számok, determinánsa pedig egy, nyerjük a transformált $\bar{F}_j=0$ egyenletrendszert, és közvetetlenül belátható, hogy az eredeti és a transformált

egyenletrendszert egyszerre tekinthetjük megoldottnak; mert az átmenetet az egyiknek megoldásairól a másikéira lineáris egyenletrendszer közvetíti. Még pedig, ha $\xi_1, \ldots, \xi_m$ az $F_j=0$ valamely megoldása, akkor a ξ-k bizonyos meghatározott raczionális és egész, homogén lineáris formáinak rendszere $\bar{F}_j=0$-nak megoldása és viszont.

Feltehetjük tehát, hogy az $F_j=0$ egyenletrendszert már úgy «készítettük elő», a mint azt az előbbiekben a resolvens-forma meghatározására tettük; azután mindenütt az erre vonatkozó eredményeket alkalmazhatjuk. E mellett még az a további egyszerűsítés is belép, hogy mindig abban a formatartományban mozoghatunk, mely az orthoid (A) tartományból származik; mert a

$$\Sigma \frac{A'_g}{E'_g} x_1^{g_1} \ldots x_m^{g_m}=0 \quad \text{vagy} \quad \Sigma \frac{A_g}{E} x_1^{g_1} \ldots x_m^{g_m}=0$$

minden megoldása kielégíti egyszersmind a

$$\Sigma A_g x_1^{g_1} \ldots x_m^{g_m}=0$$

egyenletet is, a melynek együtthatói holoidok és viszont. Ebben E a E'_g-k szorzata és ezekkel együtt a zérustól különböző. A mennyiben tehát a probléma további tárgyalásában oly egyenletek fordulnának elő, a melyeknek együtthatói orthoidok, ezeket egyenlő nevezővel írhatjuk és azután a nevező teljesen elmaradhat. A következőkben feltételezzük, hogy ez már mindenütt megtörtént.

Akkor a 18. §. (R) congruentiája közvetetlenül mutatja, hogy *az* $F_j=0$ *egyenletrendszer minden megoldása szükségképen a*

$$D=0,\ D^{(1)}=0, \ldots,\ D^{(r-1)}=0$$

egyenletek egyikének is megoldása.

Minthogy F_j, ha azt bizonyos a zérustól különböző mennyiséggel megszorozzuk, oszthatóvá válik D-vel, $D=0$

minden megoldása egyszersmind az $F_j=0$ rendszer megoldása is. Általánosságban azonban D holoid mennyiség, a mely az x határozatlanokat egyáltalában nem is tartalmazza és természetesen nem is zérus; azaz a $D=0$ egyenletnek akkor egyetlen megoldása sincs.

Ha általánosságban $D^{(h)}$ az $x_{h+1}, \ldots, x_m$ változóknak igazi formája és $\xi_{h+1}, \ldots, \xi_m$ a $D^{(h)}=0$ egyenlet egyik megoldása, akkor ezeket az értékeket behelyettesítvén, az $F_{j_h}^{(h)}(j_h=1, \ldots, k_h)$ egész függvények eltünnek. E szerint tehát az

$$\overline{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$$

formáknak van egy $G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m)$ legnagyobb közös osztójuk *.

Ha most továbbá $x_h=\xi_h$ a

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m) = 0$$

* A $G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m)$ jelölés arra utaljon, hogy $G_1^{(h)}$ az x_h oly formája, melynek együtthatóit a $\xi_{h+1}, \ldots, \xi_m$ értékrendszer meghatározza ugyan, de *a nélkül*, hogy volna oly $\Gamma(x_h, x_{h+1}, \ldots, x_m)$ forma, melyből mindig — *kivétel nélkül* — származtatható $G_1^{(h)}$ az $x_{h+1}=\xi_{h+1}, \ldots, x_m=\xi_m$ helyettesítés segítségével. Hogy ily kivételek mikép keletkeznek, azt igen egyszerűen mutatja a következő példa:

Az

$$(x-a)(x-b) \quad \text{és} \quad (x-a+y-z)(x-b+z)$$

formák legnagyobb közös osztója, ha y és z értékei kielégítik az $y-z=0$ egyenletet, $x-a$ ha t. i. $y=z\neq 0$; ellenben $(x-a)(x-b)$, ha $y=z=0$.

Az $\overline{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h-1}, \ldots, \xi_m)$ formák legnagyobb közös osztója tehát az absolut æquivalentia értelmében meghatározott

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m)$$

forma, melyet azonban nem lehet a $G_1^{(h)}(x_h, \xi_{h+1}, \ldots, \xi_m)$ alakban írni. E mellett annak a körülménynek, hogy $G_1^{(h)}$ csakis az absolut æquivalentia értelmében meghatározott forma, nincs különös jelentősége. Hogy $G_1^{(h)}$ mint forma teljesen meg legyen adva, kiköthetjük például, hogy x_h legmagasabb hatványának együtthatója az egység legyen.

egyenlet megoldása, az $\bar{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$ függvények akkor és csak akkor tünnek el, ha x_h helyébe ilyen ξ_h-t teszünk*.

Tehát

$$F_{j_{h-1}}^{(h-1)} = D^{(h-1)} \bar{F}_{j_{h-1}}^{(h-1)}$$

ismét csak ebben az esetben tünhetik el (az ennek megfelelő megoldásokat átmenetileg első fajú megoldásoknak akarjuk nevezni), vagy pedig akkor, ha $D^{(h-1)}=0$. Az utóbbi lehetőségből származó megoldásokat azonban nem veszszük tovább tekintetbe, mert azokat már a $D^{(h-1)}=0$ egyenlet tárgyalásával kapcsolatban állítottuk elő.

Ha már most az $F_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)=0$ egyenleteknek nincsen elsőfajú megoldásuk, akkor az

$$\bar{F}_{j_{h-2}}^{(h-2)}(x_{h-1}, \xi_h, \ldots, \xi_m)$$

formáknak ξ_h egyetlen értékére nézve sem lehet közös osztójuk; tehát az $\bar{F}_{j_{h-2}}^{(h-2)}=0$ egyenleteknek egyetlen megoldásuk sem lehet. E szerint $x_{h-1}=\xi_{h-1}, \ldots, x_m=\xi_m$ csak akkor lehet

$$F_{j_{h-2}}^{(h-2)} = D^{(h-2)} \bar{F}_{j_{h-2}}^{(h-2)} = 0$$

megoldása, ha egyszersmind kielégíti $D^{(h-2)}=0$-t is, a mit ismét nem fogunk tovább tekintetbe venni.

Így tovább következtetve látjuk, hogy az eredeti egyenletrendszernek csak $D^{(h)}=0$ ama megoldásai felelnek meg, a melyek a

* Ugyanis, ha ξ_h a $G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m)=0$ egyenlet egyik gyöke, akkor $G_1^{(h)}$ és evvel együtt $\bar{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$ is osztható $x_h-\xi_h$-val, és így $\bar{F}_{j_{h-1}}^{(h-1)}(\xi_h, \xi_{h+1}, \ldots, \xi_m) = 0$.

Ha viszont az utóbbi egyenletek fennállanak, akkor minden egyes $\bar{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$ az $x_h-\xi_h$-val osztható, tehát legnagyobb közös osztójuk, $G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m)$ is és így ebben az esetben $G_1^{(h)}(\xi_h \mid \xi_{h+1}, \ldots, \xi_m) = 0$.

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m) = 0$$

egyenletet is kielégítik és így az

$$F_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m) = 0$$

rendszernek is megoldásai. Azokat a megoldásokat, a melyek már $D^{(h-1)}=0$-ból kiadódnak, itt nem vettük tekintetbe.

Ha $\xi_h, \ldots, \xi_m$ egyik ilyen megoldás, akkor az

$$\bar{F}_{j_{h-2}}^{(h-2)}(x_{h-1}, \xi_h, \ldots, \xi_m)$$

formáknak van egy közös tényezőjük

$$G_2^{(h)}(x_{h-1} \mid \xi_h, \ldots, \xi_m).$$

Ha továbbá ξ_{h-1} ismét a megfelelő egyenlet egyik gyöke, ugyanazon a módon tovább haladva, végre *az* $F_j=0$ *egyenletrendszer ama megoldásait, a melyek egyszersmind a* $D^{(h)}=0$ *egyenletet is kielégítik, az egyenletek következő lánczából nyerjük:*

$$D^{(h)}(x_{h+1}, x_{h+2}, \ldots, x_m) = 0$$
$$G_1^{(h)}(x_h \mid x_{h+1}, \ldots, x_m) = 0$$
$$G_2^{(h)}(x_{h-1} \mid x_h, \ldots, x_m) = 0$$
$$\ldots\ldots\ldots\ldots$$
$$G_h^{(h)}(x_1 \mid x_2, \ldots, x_m) = 0,$$

a hol $G_i^{(h)}$ *képezéséből kitünik, hogy* x_{h-i}*-re nézve szabályos forma.*

Az egyenletrendszer evvel elért egyszerűsítése lényeges. Ennek alapján egyszerre mindig csak egy egyenlettel van dolgunk; először egy olyannal, a mely esetleg még több ismeretlent tartartalmaz. Ha azután $\xi_h, \ldots, \xi_m$ ennek az első egyenletnek egyik megoldása, akkor a megfelelő ξ_{h-1}-nek ki kell elégítenie a

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m) = 0$$

egyenletet, a melyben csak *egy* ismeretlen van, továbbá a a megfelelő ξ_{h-2}-nek a

$$G_2^{(h)}(x_{h-1} \mid \xi_h, \ldots, \xi_m) = 0$$

egyenletet és így tovább. Akkor és csak akkor nyerünk megoldást, ha az így értelmezett összes egyenletek megoldhatók.

21. §. Az $F_j = 0$ egyenletrendszer megoldásainak összességét, a mennyiben ilyenek egyáltalában vannak, a $D^{(h)} = 0$ egyenletek szerint, a melyek közül egyet minden egyes megoldás kielégít, különböző complexusokba sorozhatjuk, a hol azonban semmiképen sincsen kizárva az, hogy egy és ugyanaz a megoldás egyszerre több complexusba is tartozzék.

A megoldásoknak a $D^{(h)} = 0$ egyenlethez tartozó complexusát az jellemzi, hogy olyan megoldása, a melyre nézve $x_{h+1} = \xi_{h+1}, \ldots, x_m = \xi_m$, csak véges számban lehet. Ez közvetetlen következménye a 19. §-ban bebizonyított amaz elemi tételnek, hogy valamely egy ismeretlent tartalmazó m-edfokú egyenletnek, a melynek együtthatói bizonyos holoid tartomány mennyiségei, hacsak együtthatói mind el nem tünnek, e tartományon belül soha sem lehet m-nél több gyöke.

Az értékrendszerek összessége, a mely $(x_{k+1}, x_{k+2}, \ldots, x_m)$-ből származik, ha $x_{k+1}, \ldots, x_m$ helyébe egymástól függetlenül a holoid [A] tartomány egy-egy tetszés szerinti mennyiségét teszszük, *az* [A] *tartományból származó* $m-k$*-szoros sokaság* legegyszerűbb esete (a hol ennek a kifejezésnek értelme a tetszés szerinti [A] tartományra való vonatkozása miatt általánosabb, mint közönségesen); minden egyes $(\xi_{k+1}, \xi_{k+2}, \ldots, \xi_m)$ értékrendszer pedig *a sokaság egy eleme*. A megoldásoknak a $D^{(h)} = 0$ egyenlethez tartozó complexusa e szerint olyan, hogy az $(x_{h+2}, \ldots, x_m)$

sokaság minden elemének csak a megoldásoknak véges száma felel meg; még pedig, ha a $D_h=0$ egyenlet foka m_{h+1} és a $G_1^{(h)}=0, \ldots, G_h^{(h)}=0$ egyenletek foka $x_h, \ldots, x_1$-re nézve legfölebb $m_h, \ldots, m_1$*, e szám $m_1 m_2 \ldots m_{h+1}$-nél nagyobb sohasem lehet, de lehet egyenlő 0-sal is.

E ténynek különös jelentősége van akkor, ha az adott holoid [A] tartomány olyan, hogy minden azon belül alkotott (egy ismeretlent tartalmazó) egyenletnek van gyöke. Vajjon vannak-e ilyen tartományok, az egyelőre még eldöntetlen marad**.

Ebben az esetben a megoldások ama complexusában, a mely a $D^{(h)}=0$ egyenletnek megfelel, az $(x_{h+2}, \ldots, x_m)$ sokaság minden elemének legalább is egy, legfeljebb pedig $m_1 \ldots m_{h+1}$ megoldás felel meg; akkor is az adott definicziót bővítve, a megoldásoknak e complexusát *az* [A] *tartományból származó* $m-h-1$*-szeres sokaságnak* nevezzük.

Minden esetre lehetséges, hogy az itt tárgyalt általános egyenletrendszer esetében (a hol az egyenletek száma egészen tetszés szerinti) az összes $D^{(h)}$-k a határozatlanoktól szabadok, úgy hogy az egyenletrendszernek egyáltalában nincsen megoldása, a mint azt pl. már a legegyszerűbb eset, n ismeretlent tartalmazó $n+1$ lineáris egyenlet mutatja. Ha pedig vannak megoldásai, ezek $m-h-1$-szeres sokaságokban válnak külön, a hol h a $0, 1, \ldots, m-1$ értékeket veheti fel. A «0-szoros» sokaság a $\xi_1, \ldots, \xi_m$ oly vé-

* A $G_1^{(h)}=0$ egyenlet foka nem lehet nagyobb az $F_{l_{h-1}}^{(h-1)}$ formák bármelyikének fokánál s ú. t.

** Később ki fog tünni, hogy ilyen tartománynak legalább is az úgynevezett algebrai számok összességét kell tartalmaznia. Ez az algebrai számok értelmezésének (IV. fej. 6. §.) közvetetlen következménye. Az analizis körében a complex számok összessége ilyen tartomány.

ges számú értékrendszeréből áll, a melyek az adott egyenletrendszernek megoldásai.

A forma discriminánsa.

22. §. Legyen $F = A_0 x^m + \cdots$, $G = B_0 x^n + \cdots$ két az $[A, x_1, \ldots, x_m, x]$-ből származó holoid igazi forma és G az F osztója. Hogy eredményeinkbe, úgy mint előbb, a nem teljes holoid tartományokat is belévonhassuk, az oszthatóság fogalmát itt is arra a formatartományra vonatkoztatjuk, a mely az orthoid (A) tartományból származik. *G-t az F k-szoros osztójának* nevezzük, ha F még osztható G^k-val, de G^{k+1}-vel már nem osztható. Abban a különös esetben, midőn $k > 1$, *G-t többszörös osztónak nevezzük.* Az ily többszörös osztóra nézve a következő tétel érvényes:

Az F formának akkor és csak akkor van többszörös igazi osztója, ha F és $F' = \frac{\partial F}{\partial x}$ legnagyobb közös osztója tartalmazza az x határozatlant.

Az $F = G^k H$ föltevésből közvetetlenül következik, hogy $F' = G^k H' + kG^{k-1} HG'$; ha tehát $k > 1$, akkor úgy F, mint F' legalább is G-vel osztható.

Ha pedig viszont F és F' legnagyobb közös osztója D és D az x határozatlant tartalmazza úgy, hogy D' a 0-tól különböző, akkor abból, hogy

$$F = DK, \quad F' = DK_1, \quad (K, K_1) \sim 1,$$

még tovább következik, hogy

$$F' = DK' + D'K$$

és minthogy F' osztható D-vel, az is, hogy

$$D'K = DK_2.$$

De akkor szükséges, hogy

$$D_1 \sim (D, K)$$

valóban tartalmazza x-et; mert máskülönben, ha K-t mint

x formáját fogjuk fel, K_2 osztható volna K primitiv formájával és így D' x-re vonatkozólag legalább is egyenlőfokú volna D-vel. Ámde D' foka x-ben egy egységgel alacsonyabb, mint D-é; ezért tehát úgy D, mint K az igazi D_1 formát tartalmazza mint osztót és így F legalább is D_1^2-vel lesz osztható. Az orthoid $D = \frac{\bar{D}_1}{A}$ formáról, mint azt már ismételten kifejtettük, ismét a holoid $\bar{D}_1$ formára térünk át, a mely hasonlóképen többszörös osztója F-nek.

Hogy tehát kriteriumát találjuk annak, vajjon F-nek van-e többszörös osztója, csak

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_{m-1} x + A_m$$

és

$$\frac{\partial F}{\partial x} = mA_0 x^{m-1} + (m-1) A_1 x^{m-2} + \cdots + A_{m-1}$$

legnagyobb közös osztóját kell megvizsgálnunk. Erre szolgál e két forma resultánsa. Ez, hacsak $m>1$, a SYLVESTER-féle determináns alakjában (14. §.) közvetetlenül meg van adva. Csak a következőket kell abba behelyettesítenünk:

$$n = m-1, \quad B_0 = mA_0, \quad B_1 = (m-1)A_1, \ldots, \quad B_{m-1} = A_{m-1}.$$

Minthogy azután közvetetlenül látni, hogy A_0 az első sor minden elemében mint tényező szerepel, az a determináns elé tehető. Az azután fellépő determinánst *az (elsőnél magasabb fokú) F forma discriminánsának* fogjuk nevezni és Dscr. F-fel, szükség esetében pedig Dscr. $\binom{F}{x}$-szel jelölni.

A discriminánsdefinicióját tehát a

$$\text{Res.}\left(F, \frac{\partial F}{\partial x}\right) = A_0 \text{ Dscr. } F$$

reláczió szolgáltatja; részletesen kiírva pedig a discriminánsa lesz:

$$
\begin{vmatrix}
1 & & & & m & & & \\
A_1 & A_0 & & & (m-1)A_1 & mA_0 & & \\
. & A_1 & . & & & (m-1)A_1 & . & \\
. & . & . & A_0 & & . & . & mA_0 \\
. & . & . & . & A_{m-1} & . & . & (m-1)A_1 \\
. & . & . & . & & . & . & . \\
A_m & . & . & . & & A_{m-1} & & . \\
 & A_m & . & . & & & & . \\
 & & . & . & & & & . \\
 & & & A_m & & & & A_{m-1}
\end{vmatrix} \qquad (D)
$$

Hogy e discriminánsnak mindjárt oly alakját nyerjük, a mely a következőkben alapvető fontosságúnak fog mutatkozni, megjegyezzük, hogy kifejtésében kétféle tagot különböztethetünk meg: olyanokat, a melyekben A_0 előfordul és olyanokat, a melyek A_0-t nem tartalmazzák. Az első fajú tagok összege legyen $A_0\Phi$, a hol Φ az $A_0, \ldots, A_m$ mennyiségek raczionális és egész formája. A másik fajhoz tartozó tagok összegét közvetetlenül nyerjük, ha ama determinánsban A_0 helyébe 0-t teszünk. Ebben az esetben az első és második sorban csak a

$$c_{11}=1, \quad c_{1m}=m,$$
$$c_{21}=A_1, \quad c_{2m}=(m-1)A_1$$

elemek maradnak a 0-tól különbözők. $A_0=0$ esetében tehát Dscr. F két tényező szorzatába megy át, a melyek közül az első $-A_1$, a második pedig

$$(-1)^{m-2}A_1 \,\text{Dscr.}\,(F-A_0x^m).$$

E tényezőkre való felbomlás közvetetlenül világossá válik, ha az m-dik oszlopot az első és második közé írjuk, a mi csak azt a változást idézi elő, hogy a determinánshoz $-1)^{m-2}$ mint tényező járul hozzá; a közvetetlen megszemlélés pedig mutatja, hogy a második tényezőképen fellépő determináns az

$$A_1 x^{m-1} + A_2 x^{m-2} + \cdots + A_m = F - A_0 x^m$$

forma és ennek x szerint vett deriváltjának resultánsa. Ennek alapján *a discriminánsra nézve a következő alapvető identitást* nyerjük:

$$\text{Dscr.}(F) = A_0 \Phi + (-1)^{m-1} A_1^2 \text{ Dscr.}(F - A_0 x^m), \qquad (D_1)$$

hol F foka $m > 1$.

A másodfokú forma discriminánsa $4A_0A_2 - A_1^2$.

23. §. A resultánsra vonatkozó fejtegetésekkel párhuzamosan a discriminánsnak is két fontos alaptulajdonságát nyerjük, a melyek közül az *elsőt* a következő tétel adja meg.

Az $F(x)$ forma discriminánsa akkor és csak akkor lünik el, ha e formának oly többszörös osztója van, a mely x-et valóban tartalmazza, vagy pedig az A_0 és A_1 együtthatók egyidőben zérusok.

A mennyiben az alapul felvett [A] tartomány nem volna teljes, az oszthatóság itt is arra a formatartományra vonatkozik, a mely az orthoid (A) tartományból származik.

Ha A_0 különböző a 0-tól, az F és $\frac{\partial F}{\partial x}$ formák resultánsa akkor fog csak eltünni, ha eltünik az F forma discriminánsa, és így a felállított tétel $A_0 \neq 0$ esetére érvényes. Ha azonban $A_0 = 0$ és A_1 is egyenlő a 0-sal, akkor (D_1) szerint $\Delta = \text{Dscr.}(F)$ is egyenlő a 0-sal. Ha pedig viszont $A_0 = 0$ és egyszersmind $\Delta = 0$, akkor vagy A_1-nek, vagy pedig — minthogy $A_0 = 0$ — a most F-fel azonos

$$F - A_0 x^m = A_1 x^{m-1} + \cdots + A_m$$

forma discriminánsának egyenlőnek kell lennie 0-sal. Az F formának tehát, ha $A_1 \neq 0$, valóban van többszörös osztója.

A második alaptétel a következő:

Az elsőnél magasabb fokú $F(x)$ forma discriminánsa kielégíti egy

$$\Delta = GF + G_1 \frac{\partial F}{\partial x}$$

identitást, a melyben G és G_1 az x két oly formája, a melynek együtthatói az eredeti $A_0, A_1, \ldots, A_m$ együtthatók racionális és egész formái.

E tétel bebizonyítása első példáját mutatja majd egy hasonló esetekben mindenütt alkalmazható és ezért igen messzevágó módszer alkalmazásának.

A $\text{Res.}\left(F, \frac{\partial F}{\partial x}\right) = A_0 \Delta$-ra nézve a 16. §. szerint minden esetre hasonló identitás áll fenn. Ez, ha $\frac{\partial F}{\partial x}$ helyébe F'-et írunk, a következő:

$$A_0 \Delta = HF + H_1 F'.$$

Ez az identitás az együtthatók minden rendszerére nézve érvényes, tehát akkor is, ha A_m helyébe az $A_m - F(u)$ mennyiséget teszszük *. Ez nem változtat semmit sem A_0-on, sem F'-en, míg $F(x)$ átmegy $F(x) - F(u)$-ba. Δ-ból, H-ból és H'-ból származzanak így a $\Delta^{(u)}$, $H^{(u)}$ és $H_1^{(u)}$ formák. Akkor

$$A_0 \Delta^{(u)} = H^{(u)} \big(F(x) - F(u)\big) + H_1^{(u)} F',$$

vagy pedig, minthogy $F(x) - F(u)$ osztható $x-u$-val,

$$A_0 \Delta^{(u)} \equiv H_1^{(u)} F' \pmod{x-u}.$$

Ha ebben $F'(x)$-et és $H_1^{(u)}$-t $x-u$ hatványai szerint kifejtjük, lesz:

$$F'(x) = F'(u+x-u) = F'(u) + \cdots, \quad H_1^{(u)} = H_2^{(u)} + \cdots,$$

és így

$$A_0 \Delta^{(u)} - H_2^{(u)} F'(u) \equiv 0 \pmod{x-u}.$$

Minthogy ez a mennyiség azonban x-et egyáltalában nem tartalmazza és mégis osztható $x-u$-val, annak 0-sal kell egyenlőnek lennie. Itt u mint új határozatlan jele szerepelt; helyébe tehát ismét x-et írhatjuk és akkor nyerjük, hogy

$$A_0 \Delta^{(x)} = H_2^{(x)} F'(x)$$

* Ezt a fontos substitutiót legelőször KRONECKER alkalmazta a resultánsra (Festschrift, 20. §.).

Ez az identitás érvényes marad akkor is, ha az $A_0, A_1, \ldots, A_m$ mennyiségeket határozatlanokként fogjuk fel. E felfogás alapján azonban

$$F'(x) = mA_0 x^{m-1} + (m-1)A_1 x^{m-2} + \cdots + A_{m-1}$$

x-nek oly primitiv formája, a melynek együtthatói az $[[1], A_0, A_1, \ldots]$ tartományhoz tartoznak; $A_0 \Delta^{(x)}$-szel együtt tehát már $\Delta^{(x)}$-nek is oszthatónak kell lennie $F'(x)$-szel és így lesz

$$\Delta^{(x)} = G_1 F'(x),$$

a hol G_1 az $A_0, \ldots, A_m$, x mennyiségek raczionális és egész formája.

A $\Delta^{(x)}$ másrészt úgy származik Δ-ból, hogy A_m helyébe az $A_m - F(x)$ mennyiségeket helyettesítjük. Ha tehát $\Delta^{(x)}$-et $F(x)$ hatványai szerint kifejtjük, lesz

$$\Delta^{(x)} = \Delta - GF,$$

és így

$$\Delta = GF + G_1 F',$$

a mi bebizonyítandó volt. Ez az identitás akkor is helyes, ha az A-k határozatlan mennyiségek; tehát érvényesnek kell maradnia akkor is, ha az A-k az [A] tartomány tetszés szerinti mennyiségei.

A resultáns és discriminánsmint symmetrikus forma.

24. §. Legyen úgy mint a II. fej. 11. §-ában

$$P(z) = (z-x_1)(z-x_2)\ldots(z-x_m) =$$
$$= z^m - \mathfrak{f}_1 z^{m-1} + \mathfrak{f}_2 z^{m-2} - \cdots + (-1)^m \mathfrak{f}_m,$$

a hol $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ az $x_1, \ldots, x_m$ elemi symmetrikus formáit jelentik és hasonlóképen még

$$Q(z) = (z-y_1)(z-y_2)\dots(z-y_n) =$$
$$= z^n - \mathfrak{g}_1 z^{n-1} + \mathfrak{g}_2 z^{n-2} - \dots + (-1)^n \mathfrak{g}_n,$$

a hol $\mathfrak{g}_1, \dots, \mathfrak{g}_n$ az $y_1, \dots, y_n$ elemi symmetrikus formái és vizsgáljuk meg az

$$\bar{F}(z) = A_0 P(z), \quad \bar{G}(z) = B_0 Q(z)$$

formákat.

E két forma resultánsa a 14. §. szerint mindjárt determináns alakjában írható; még pedig, ha az egyes oszlopokban fellépő A_0 és B_0 tényezőket a determináns elé írjuk, lesz: Res. $(\bar{F}, \bar{G}) =$

$$= A_0^n B_0^m \begin{vmatrix} 1 & & & & 1 & & \\ -\mathfrak{f}_1 & \cdot & & & -\mathfrak{g}_1 & \cdot & \\ \mathfrak{f}_2 & \cdot & \cdot & & \mathfrak{g}_2 & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -\mathfrak{f}_1 & \cdot & \cdot & \cdot \\ (-1)^m \mathfrak{f}_m & \cdot & \cdot & \mathfrak{f}_2 & (-1)^n \mathfrak{g}_n & \cdot & \cdot \\ & \cdot & \cdot & \cdot & & \cdot & \cdot \\ & & \cdot & \cdot & & & \cdot \\ & & & (-1)^m \mathfrak{f}_m & & & (-1)^n \mathfrak{g}_n \end{vmatrix}.$$

Ha e determináns első sorát megszorozzuk x_k^{m+n-1}-vel, általánosságban pedig az i-dik sort x_k^{m+n-i}-vel és az így származó sorokat az utolsóhoz hozzáadjuk, akkor $\frac{\text{Res.}(\bar{F}, \bar{G})}{A_0^n B_0^m}$-et oly Γ determináns alakjában nyerjük, a melynek utolsó sora a következő elemekből áll:

$$c_{m+n,\,j} = x_k^{n-j} P(x_k) = 0 \qquad (j = 1, 2, \dots, n)$$

$$c_{m+n,\,n+j'} = x_k^{n-j'} Q(x_k). \qquad (j' = 1, \dots, m).$$

Tehát a

$$\text{Res.}(\bar{F}, \bar{G}) = A_0^n B_0^m \Gamma$$

képletben a Γ determináns minden esetre az x és y elemeknek raczionális és egész formája és az utolsó sor elemei-

nek meghatározása értelmében a

$$Q(x_k) = (x_k - y_1)(x_k - y_2) \ldots (x_k - y_n)$$

formával osztható.

$Q(x_k)$ és $Q(x_l)$ legnagyobb közös osztója azonban 1. Az ugyanis sem x_k-t, sem pedig x_l-et nem tartalmazhatja; $Q(x_k)$-ban tehát e legnagyobb közös osztó az x_k minden egyes hatványához tartozó együttható osztója lesz, és mert itt x_k^n-nek együtthatója az egység, végre 1-gyel egyenlő. Ezért $\frac{\text{Res.}(F, G)}{A_0^n B_0^m}$ osztható $\prod_{k=1}^{m} Q(x_k)$-val is és ebből végre:

$$\text{Res.}(F, G) = C A_0^n B_0^m \prod_{k=1}^{m} Q(x_k).$$

Könnyű felismerni, hogy ebben $C=1$. Ugyanis Res. (F, G) eredeti alakjából közvetetlenül következik, hogy az a tag, a melynek dimensiója az y határozatlanokban a legmagasabb, $(-1)^{mn} A_0^n B_0^m \mathfrak{g}_n^m = (-1)^{mn} A_0^n B_0^m (y_1 y_2 \ldots y_n)^m$, míg a most nyert kifejezésből, ha tekintetbe veszszük $Q(x_k)$-nak értékét, következik, hogy ama tagok, a melyeknek dimensiója a legmagasabb, minden esetre bennfoglaltatnak a

$$C A_0^n B_0^m (-1)^{mn} (y_1 \ldots y_n)^m$$

kifejezésben. Így tehát szükséges, hogy C az x-ektől szabad legyen és az előbb meghatározott taggal, a melynek dimensiója a legmagasabb, megegyezzék, a miből épen $C=1$ következik.

Ez az eredmény még így is írható:

$$\text{Res.}(F, G) = A_0^n B_0^m \Pi(x_k - y_l). \qquad \binom{k=1, \ldots, m}{l=1, \ldots, n}$$

A bal oldalon álló kifejezés úgy az x-ek, mint az y-ok elemi symmetrikus formáinak oly formája, melyet ez az identitás teljesen meghatároz. Ugyanis az $\mathfrak{f}$-ek és $\mathfrak{g}$-k két oly formája, melyek mindegyike egyenlő a jobb oldalon álló szorzattal,

okvetetlenül azonos. Valóban a II. fej. 14. §. szerint először az $\mathfrak{f}$-ek valamely hatványszorzatának együtthatói mind a két formában ugyanazok lesznek; ezek az együtthatók pedig a $\mathfrak{g}$-k raczionális és egész formái és ezekben is ugyanazon tétel szerint az egyes megfelelő együtthatóknak egyenlőknek kell lenniök.

Ha tehát — tekintet nélkül $\mathfrak{f}_i$ és $\mathfrak{g}_j$ jelentésére — az

$$\mathfrak{f}_i = \frac{(-1)^i A_i}{A_0}, \quad \mathfrak{g}_j = \frac{(-1)^j B_j}{B_0}$$

helyettesítést végezzük, nemcsak az $\overline{F}(z)$ és $\overline{G}(z)$ formák mennek át az «általánosabb»

$$F(z) = A_0 z^m + A_1 z^{m-1} + \cdots + A_m$$
$$G(z) = B_0 z^n + B_1 z^{n-1} + \cdots + B_n$$

formákba, hanem Res. $(\overline{F}, \overline{G})$ is Res. (F, G)-be és így evvel *két forma resultánsának következő fontos symbolikus előállítását* nyerjük:

$$\text{Res.}(F, G) = A_0^n B_0^m \Pi(x_k - y_l) \cdot \binom{k=1,\ldots,m}{l=1,\ldots,n}. \qquad (R_1)$$

E képlet értelmében a resultáns meghatározása úgy megy végbe, hogy a jobb oldalon álló formát először mint az $\mathfrak{f}$ *és* $\mathfrak{g}$ *elemi symmetrikus formák formáját állítjuk elő és azután ezek helyébe a következőket helyettesítjük:*

$$\mathfrak{f}_i = \frac{(-1)^i A_i}{A_0}, \quad \mathfrak{g}_j = \frac{(-1)^j B_j}{B_0}.$$

Ha az F és G formák szerepet cserélnek, akkor ép úgy nyerjük, hogy

$$\text{Res.}(G, F) = A_0^n B_0^m \Pi(y_l - x_k) = (-1)^{mn} A_0^n B_0^m \Pi(x_k - y_l);$$

tehát ismét lesz:

$$\text{Res.}(F, G) = (-1)^{mn} \text{Res.}(G, F).$$

Végre még a $\mathfrak{g}_j$-k értékeit már a

$$B_0(x_k - y_1)(x_k - y_2)\ldots(x_k - y_l) = B_0(x_k^n - \mathfrak{g}_1 x^{n-1} + \cdots + (-1)^n \mathfrak{g}_n)$$

részletszorzatokba vezethetjük be és akkor nyerjük a resultánsnak

$$\text{Res.}\,(F, G) = A_0^n \prod_{k=1}^{m} G(x_k) \qquad (R_2)$$

második symbolikus alakját, a melyet ép úgy kell értelmeznünk, mint a fentebbit. Ép úgy származik

$$\text{Res.}\,(G, F) = B_0^m \prod_{l=1}^{n} F(y_l)$$

és így

$$\text{Res.}\,(F, G) = (-1)^{mn} B_0^m \prod_{l=1}^{n} F(y_l) \qquad (R_3)$$

is.

25. §. A discriminánsnak hasonló előállításához jutunk, ha tekintetbe veszszük, hogy az $F(z)$ és $F'(z)$ resultánsából úgy származik, ha ebből az A_0 tényezőt elhagyjuk; (R_2)-ből tehát közvetetlenül következik, hogy

$$\text{Dscr.}\, F = A_0^{m-2} \prod_{k=1}^{m} F'(x_k). \qquad (\Delta_2)$$

Ha (Δ_2)-t a

$$\bar{F}(z) = A_0 P(z) = A_0 \left(z^m - \mathfrak{f}_1 z^{m-1} + \cdots + (-1)^m \mathfrak{f}_m\right),$$

formára alkalmazzuk, akkor, minthogy

$$P'(x_k) = (x_k - x_1) \ldots (x_k - x_{k-1})(x_k - x_{k+1}) \ldots (x_k - x_m),$$

továbbá lesz

$$\text{Dscr.}\, \bar{F} = A_0^{2m-2} \prod_{k=1}^{m} P'(x_k)$$

$$= (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} \prod_{\substack{r,s \\ r<s}}^{(r,s=1,\ldots,m)} (x_r - x_s)^2.$$

Ha ebben Dscr. $\bar{F}$ az e mennyiség előállítására felállított determináns-alakot jelenti, akkor a következtetésnek ugyanaz a módja érvényes, a mely a resultánsnak (R_1) alatti előállítására vezetett és ennek megfelelőleg lesz:

$$\text{Dscr. } F = (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} \prod_{\substack{r,s \\ (r,s=1,\ldots,m \\ r<s)}} (x_r - x_s)^2, \qquad (\Delta_1)$$

a mely meghatározást ép úgy kell értelmeznünk, mint előbb (R_1)-et. Ha pedig még tekintetbe veszszük a II. fej. 11. §-ának eredményeit, lesz

$$\text{Dscr. } F = (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} [x_1^{m-1}]^2 =$$

$$= (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} \Delta(x_1, x_2, \ldots, x_m). \qquad (\Delta_1')$$

NEGYEDIK FEJEZET.

AZ ALGEBRAI MENNYISÉGEK.

A raczionális és egész formák felbontása tényezőkre.

1. §. A raczionális és egész számok tartományában, [1]-ben fennállanak először is azok az oszthatósági törvények, a melyek teljes holoid tartományokban egyáltalában érvényesek; de ezeken felül az arithmetika elemei még a következő alapvető tételekre tanítanak, a melyeket itt egyszerűen csak idézünk:

I. A 0 kivételével minden raczionális és egész számnak ugyanolyan osztói csak véges számmal vannak és ezek a kisérletek véges sorával meghatározhatók.

II. A 0 és ± 1 kivételével minden raczionális és egész szám mint törzsszámok szorzata állítható elé; még pedig úgy, hogy ez az előállítás az æquivalentia értelmében egyértelműen meghatározott.

A második tételre vonatkozólag még megjegyezzük, hogy két raczionális és egész szám k és k' akkor és csak akkor æquivalens, ha $k' = \pm k$. A tétel pontosabb fogalmazása tehát a következő: Ha $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ és $n = q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$ is, a hol $p_1, p_2, \dots, q_1, q_2, \dots$ törzsszámok, akkor szükségképen $r = s$, továbbá $p_1 \sim q_{i_1}$, $p_2 \sim q_{i_2}$, $\dots$, $p_r \sim q_{i_r}$, a hol az $i_1, i_2, \dots, i_r$ számok az $1, \dots, r$ számokat jelentik bizonyos meghatározott sorrendben. Magától értetődik, hogy p-vel együtt $-p$-t is törzsszámnak kell tekintenünk, valamint az is, hogy $a_1 = b_{i_1}$ stb.

A raczionális és egész formák $[[1]x_1, \ldots, x_m]$ tartományában pontosan az ezekkel analog tételek állanak fenn. Először is:

Minden raczionális és egész formának ugyanolyan osztói csak véges számmal vannak és ezek a kisérletek véges sorával meghatározhatók.

Legyenek

$$F=\sum_{(g)} k_g x_1^{g_1}\ldots x_m^{g_m},\quad F_1=\sum_{(g')} k'_{g'} x_1^{g'_1}\ldots x_m^{g'_m},\quad F_2=\sum_{(g'')} k''_{g''} x_1^{g''_1}\ldots x_m^{g''_m}$$

ilyen formák és

$$F=F_1 F_2.$$

Ha F dimensiója n, az F_1 osztó dimensiója nem lehet ennél magasabb és így rendre azokat az osztókat kell meghatároznunk, a melyeknek dimensiója $0, 1, \ldots, n$. Ha azután F_1 dimensiója k, F_2-é lesz $n-k$. Elég tehát, ha meghatározzuk azokat az osztókat, a melyek dimensiója nem magasabb $\frac{n}{2}$-nél és e mellett feltételezzük, hogy $n>0$; mert oly forma, a melynek dimensiója 0, raczionalis és egész szám; osztói pedig ugyanolyan számok, a melyeknek sorozata közvetetlenül felírható.

Ha F most igazi formát jelent, akkor F 0-dik dimensiójú osztói raczionális és egész számok, a melyek mint a k_g együtthatók legnagyobb közös osztójának osztói ismeretesek; számuk tehát ismét véges.

Hogy már most meghatározhassuk az l-dik dimensiójú osztókat is, írjuk F_1-et és F_2-t mint $x_1, \ldots, x_m$ «általános» formáit, a melyeknek dimensiói az adottak:

$$F_1=\sum_{(g')} k'_{g'} x_1^{g'_1}\ldots x_m^{g_m},\quad F_2=\sum_{(g'')} k''_{g''} x_1^{g''_1}\ldots x_m^{g''_m};$$

azaz tegyük az első formában $g'_1, \ldots, g'_m$ helyébe az összes raczionális és egész értékrendszereket, a melyekre nézve $g'_1+\cdots+g'_m\leqq l$ és épúgy a második formában $g''_1, \ldots, g''_m$ he-

lyébe mindazokat az értékrendszereket, a melyekre nézve $g'_1+\cdots+g'_m \leqq n-l$, a k'_g, k''_g együtthatókat pedig tekintsük ismeretlen, azaz meghatározandó mennyiségeknek.

Hogy már most $F=F_1F_2$ lehessen, KRONECKER tételének a III. fejezet 7. §-ában adott (K') fogalmazása szerint szükséges, hogy minden $k'_g k''_g$ együttható-szorzat egy-egy identitást elégítsen ki, a mely, ha röviden $z = k'_g k''_g$-t írunk, a következő:

$$z^\nu + h_1 z^{\nu-1} + \cdots + h_\nu = 0,$$

a hol $h_1, \ldots, h_\nu$ az $F_1F_2=F$ együtthatóinak ismeretes raczionális és egész formái, tehát ismeretes raczionális és egész számok. Ámde ez csak akkor lehetséges, ha úgy k'_g, mint k''_g az utolsó el nem tünő h együttható osztója, vagy pedig $h_\nu=0$ esetében legalább egyikük 0. És így, minthogy sem az összes k', sem az összes k'' számok nem lehetnek mind zérusok, ezek az összes $k'_g k''_g$ szorzatok számára fönnálló egyenletek egybevetése után a meghatározott értékeknek csak véges sorát vehetik fel. A mondottak az F_1 és F_2 formákra is állanak. Vajjon valamely így meghatározott F_1 formának valóban egy $F=F_1F_2$ reláczió a következménye-e, még nem bizonyos; e felett azonban minden egyes esetben egyszerű osztással dönthetünk. Tételünk szerint tehát az F osztóinak teljes sorozata véges számú lépés után felállítható. Meg kell azonban jegyeznünk, hogy itt ismét F_1 és $-F_1$ és csakis ezek tekintendők az æquivalentia értelmében nem különbözőknek *.

* Más módszer F osztóinak meghatározására, a mely a LAGRANGE-féle interpoláczió-képletből indul ki, KRONECKER-től származik («Festschrift», §. 4). A szöveg fejtegetései ennél elvileg egyszerűbbek, mert mi nem használjuk fel az F egész függvény értékeit és így a formák elméletébe nem tartozó segédeszközt sem vettünk igénybe. A fellépő rendkívül hosszadalmas számítások rövidítésére szolgáló

2. §. Minthogy $[[1], x_1, \ldots, x_m]$ teljes holoid tartomány, ebben az irreducibilis mennyiség fogalma egybe esik a törzsmennyiség fogalmával. E mennyiségeket, a melyek vagy törzsszámok, vagy pedig igazi formák és akkor minden esetre primitivek, *törzsformáknak, törzsosztóknak* fogjuk nevezni.

Minden ± 1-től különböző formának legalább is egy törzsosztója van. Ha F-nek (az æquivalentia értelmében) különböző osztói csupán csak 1 és F, akkor F maga is törzsforma. Ellenkező esetben van F-nek egy az 1-től és F-től különböző osztója G, a mely tehát nem osztható F-fel, míg G összes osztói F-nek is osztói. G osztóinak száma tehát kisebb, mint F osztóinak száma. G azonban ismét vagy törzsforma, vagy pedig valamely az 1-től és G-től különböző G_1 formával osztható. Ennek az eljárásnak folytatása így a formák bizonyos

$$F, G, G_1, \ldots, G_s$$

sorozatához fog vezetni. Az eljárásnak azonban szükségképen véget kell érnie, mert az osztók száma mindig kisebbé válik. Így tehát $s+1$ lépés után G_s-nek törzsformának kell lennie.

Ha már most F a P_1 törzsformával osztható, akkor vagy lesz $F = \pm P_1$, azaz $F \sim P_1$; vagy pedig $F = P_1 F_1$ és ha F_1 ismét a P_2 törzsformával osztható úgy, hogy $F_1 = P_2 F_2$, akkor lesz $F = P_1 P_2 F_2$ és így tovább. Végre tehát

$$F \sim P_1 P_2 \ldots P_r,$$

a hol ez az eljárás ismét megszakad, azaz r meghatározott positiv egész szám, mert az $F_1, F_2 \ldots$ osztóinak száma mindig kisebb lesz úgy, hogy végre $F_r = 1$. Ha azután

eljárást ismertetett RUNGE (Journ. f. Math. 99. köt. 89. l.). Táblázatok készítésére az alaptétel alkalmazása vezet, mert meghatározott dimensiójú formákra nézve, a h formák mindig ugyanazok maradnak.

egyszersmind

$$F \sim Q_1 Q_2 \dots Q_s$$

volna, a hol $Q_1, Q_2, \dots$ ismét törzsformák, akor $F \sim Q_1 Q_2 \dots Q_s$-nek oszthatónak kell lennie P_1-gyel; tehát vagy Q_1, vagy pedig $Q_2 \dots Q_s$ lesz akkor osztható P_1-gyel. Ha nem áll be az első eset, vagy Q_2-nek, vagy pedig $Q_3 \dots Q_s$-nek kell oszthatónak lennie P_1-gyel s így tovább; szükséges tehát, hogy minden esetre egy Q_{i_1} törzsforma osztható legyen P_1-gyel. Ámde Q_{i_1}-nek, mint irreducibilis mennyiségnek csak ez a két különböző osztója van: $1, Q_{i_1}$; szükségképen tehát

$$P_1 \sim Q_{i_1}$$

és ép úgy $P_2 \sim Q_{i_2}$ s így tovább és egyszersmind $r = s$. Evvel megvan *a tényezőkre való felbontásra vonatkozó alaptétel* a raczionális és egész formatartományra nézve:

A 0, ± 1 *kivételével minden raczionális és egész forma előállítható mint ép olyan törzsformák szorzata; még pedig ez az előállítás az aequivalentia értelmében egyértelműen meghatározott.*

Minthogy æquivalens formák csak az előjelben különbözhetnek egymástól, *a most megvizsgált tartományban* ebből a tételből következik az előbb bebizonyított tétel is, a mely az osztók véges számára vonatkozik. Ha az esetleg többszörösen előforduló törzsosztókat összefoglaljuk, F előállítása lesz

$$F \sim P_1^{a_1} P_2^{a_2} \dots P_h^{a_h}$$

és ebből látjuk, hogy F minden osztójának a

$$G \sim P_1^{b_1} P_2^{b_2} \dots P_h^{b_h} \qquad (b_h \leqq a_h)$$

alakban előállíthatónak kell lennie.

Felbontás tényezőkre orthoid formatartományban.

3. §. Ha valamely (A) orthoid tartományból indulunk ki és megvizsgáljuk az ebből származó $[(A), x_1, \ldots, x_m]$ formatartományt, akkor ebben az AF és BF formák æquivalensek, ha A és B az (A) tartomány két a 0-tól különböző mennyisége; mert ebben az esetben a már többször fejtegetett æquivalentia-meghatározás szerint $A \sim 1$ és $B \sim 1$.

Ebben a tartományban tehát valamennyi igazi lineáris forma törzsforma. Ilyen lineáris forma, L semmi esetre sem lehet osztható magasabb dimensiójú formákkal. Minden egyes osztója tehát vagy (A)-nak valamely a 0-tól különböző mennyisége és így ~ 1-gyel, vagy pedig valamely L_1 linearis forma. De akkor szükséges, hogy $L = AL_1$-ben az A mennyiség (A)-hoz tartozzék és ne legyen 0; így tehát $A \sim 1$ és $L_1 \sim L$.

Általánosabban továbbá, *ha G a 0-tól különböző F formának osztója és G dimensiója ugyanaz mint F-é, F mindig $\sim G$-vel.* Szükséges ugyanis, hogy $F = AG$-ben A az (A) tartományhoz tartozzék, tehát $A \sim 1$ legyen.

Ha az F forma sem törzsforma, sem pedig az (A) tartomány mennyisége (tehát sem 0, sem pedig ~ 1), akkor okvetetlenül lesznek oly valódi osztói, a melyeknek dimensiója kisebb mint az F-é és legalább is egyenlő 1-gyel. Ezek közt van minden esetre egy legkisebb dimensiójú forma P_1. Ennek törzsformának kell lennie, mert bármelyik osztója egyszersmind F-nek is volna osztója. Ha pedig ez P_1-nek valódi osztója, dimensiója kisebb lenne mint a P_1-é, a mi a feltevéssel ellenkezik.

Ha már most $F = P_1 F_1$, akkor F_1 dimensiója kisebb mint F-é. Azután ismét nyerjük, hogy $F_1 = P_2 F_2$ és így tovább. Ennek az eljárásnak azonban véges számú lépés után meg

kell szakadnia; ha nem előbb, legalább is akkor, ha lineáris formához jutunk és ez még a legkedvezőtlenebb esetben is $n-1$ lépés után beáll, ha n az F dimensióját jelenti.

Így tehát ismét ezt a tételt nyertük:

Minden igazi orthoid forma mint ugyanolyan törzsformák szorzata állítható elé; még pedig ez az előállítása az aequivalentia értelmében egyértelműen meghatározott.

Ugyanis $F \sim P_1 \ldots P_r$-ből és $F \sim Q_1 \ldots Q_s$-ből teljesen úgy mint előbb következik, hogy $r=s$, $P_1 \sim Q_{i_1}$, mert az alapul szolgáló formatartomány ismét teljes tartomány.

Az előbbi következtetéseket tehát szóról-szóra ismételve, azt találjuk, hogy *minden a 0-tól különböző formának csak véges számú nem aequivalens osztója van.*

Itt azonban mindjárt a követett gondolatmenet lényeges hézagára akarunk reámutatni. E tétel csak ú. n. *existentia-bizonyítást* szolgáltat, mert minden utasítás híján van, a mely szerint a formát mint törzsformák szorzatát előállíthatnók. A míg azonban az (A) tartomány minden további meghatározása hiányzik, ez nem is lehetséges.

Az (A) tartományból származó formatartományt tehát csak akkor fogjuk *jól értelmezettnek* tekinteni, ha van olyan utasításunk, a mely szerint véges számú lépésben bármely a 0-tól különböző formának megfelelőleg oly törzsformára jutunk, a melylyel az osztható. Hogy evvel azután már a törzsformák szorzata alakjában való előállítás is megvan és F nem æquivalens osztóinak sorozatát is felállíthatjuk, az világos.

További vizsgálataink szilárd alapját ismét a következő tétel szolgáltatja:

Minden a 0-tól különböző raczionális forma a műveletek véges számával előállítható mint ugyanolyan törzsformák szorzata.

E tétel abból a megjegyzésből következik, hogy minden raczionális forma a

$$\sum_{(g)} \frac{k_g}{l} x_1^{g_1} \dots x_m^{g_m} = \frac{k}{l} \sum k'_g x_1^{g_1} \dots x_m^{g_m}$$

alakban írható, a hol k a k_g raczionális és egész számok legnagyobb közös osztója úgy, hogy

$$(\dots, k'_g, \dots) \sim 1.$$

Minden raczionális forma tehát egy raczionális szám és egy raczionális és egész primitiv forma szorzata és így evvel az utóbbival æquivalens. Ha ezt X-szel jelöljük és abban az értelemben, a melyet a raczionális és egész formák törzsformákra való felbontásánál megállapítottunk,

$$X \sim P_1 P_2 \dots P_r,$$

akkor a raczionális formatartományban is

$$F \sim P_1 P_2 \dots P_r$$

az F forma felbontása törzsformákra. Itt ugyanis $F \sim X$, és minden egyes P igazi forma, mert X mint primitiv forma egyetlen törzsszámmal sem osztható; végre pedig P a raczionális formatartományban is irreducibilis. Ha ugyanis P két igazi forma szorzata volna, ezeket minden esetre ismét a $\frac{k_1}{l_1} X_1$ és $\frac{k_2}{l_2} X_2$ alakban írhatnók, hol k_1, l_1, k_2, l_2 egész számok és X_1, X_2 raczionális és egész primitiv formák. Így tehát volna

$$l_1 l_2 P = k_1 k_2 X_1 X_2,$$

továbbá, minthogy $X_1 X_2$ is primitiv, $k_1 k_2 = \pm l_1 l_2$ és

$$P = \pm X_1 X_2;$$

P tehát a feltevés ellenére a raczionális és egész formák tartományában is fel volna bontható.

Az egyetlen egy határozatlant tartalmazó forma, valamint bármely szabályos forma esetében még különösen megjegyezzük, hogy az æquivalens formák közül mindig azt választjuk, a melyben valamely z határozatlan legmagasabb

hatványának együtthatója 1. Ha azután

$$F \sim F_1 F_2 \ldots F_s$$

F bármely felbontása, továbbá

$$F = A_0 z^m + A_1 z^{m-1} + \cdots,$$

$$\bar{F} = z^m + \frac{A_1}{A_0} z^{m-1} + \cdots$$

és az $F_1, F_2, \ldots, F_s$ formáknak hasonlóképen megfelelnek $\bar{F}_1, \bar{F}_2, \ldots, \bar{F}_s$, akkor lesz

$$\bar{F} = \bar{F}_1 \bar{F}_2 \ldots \bar{F}_s;$$

mert $\bar{F}$ minden esetre így állítható elő:

$$\bar{F} = C\bar{F}_1 \bar{F}_2 \ldots \bar{F}_s$$

és az együtthatók összehasonlításából közvetetlenül kitünik, hogy $C=1$.

4. §. A P-re vonatkozólag előbb bebizonyított tétel a következő módon mondható ki:

Ha P a raczionális és egész formák tartományában irreducibilis, akkor irreducibilis a raczionális formák tartományában is.

Az igazi formákra vonatkozólag bebizonyított tételhez még csak azt az esetet kell hozzácsatolnunk, a melyben P törzsszám. A tétel akkor is érvényes, mert a raczionális formatartományban ekkor $P \sim 1$.

Ebből már most közvetetlenül következtethetjük, hogy *úgy a raczionális, mint a raczionális és egész formatartományban végtelen sok törzsforma van, a melyek dimensiója tetszés szerint választható.*

Eisenstein-tól* származó egyik tétel szerint ugyanis a

$$z^m + c_1 z^{m-1} + \cdots + c_{m-1} z + c_m$$

forma, a melyben $c_1, \ldots, c_{m-1}$ oly egész számok, a melyek valamely szabadon választott p törzsszámmal oszthatók, míg

* Journal f. Math. 59. köt. 160. old.

c_m osztható ugyan p-vel, de nem p^2-tel, a racionális és egész és így a racionális formák tartományában is mindig irreducibilis.

Ha ennek ellenkezője történnék, ama formát szükségképen ily szorzat alakjában írhatnók:

$$(z^g + k_1 z^{g-1} + \cdots + k_g)(z^{m-g} + k'_1 z^{m-g-1} + \cdots + k'_{m-g}).$$

Ha most már k'_j a $j<0$ esetben a 0-t és k'_0 az 1-et jelenti az együtthatók összehasonlításából a következők származnak:

$$k_g k'_{m-g} = c_m$$
$$k_{g-1} k'_{m-g} + k_g k'_{m-g-1} = c_{m-1}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$k_1 k'_{m-g} + k_2 k'_{m-g-1} + \cdots + k_g k'_{m-2g+1} = c_{m-g+1}$$
$$k'_{m-g} + k_1 k'_{m-g-1} + \cdots + k_{g-1} k'_{m-2g+1} + k_g k'_{m-2g} = c_{m-g}$$

Ámde, minthogy c_m osztható ugyan p-vel, de nem p^2-vel, a k_g, k'_{m-g} számok közül az egyik és csak is az egyik osztható p-vel. Az általánosság megszorítása nélkül feltehetjük, hogy pl. k_g a p-vel osztható szám; az ellenkező esetben csak a két tényezőt kell egymással felcserélnünk. De akkor, minthogy a második egyenlőségben úgy c_{m-1} mint k_g osztható p-vel, míg k'_{m-g} avval nem osztható, k_{g-1}-nek is osztathónak kell lennie p-vel. Épúgy következik a harmadik egyenlőségből, hogy $k_{g-2}, \ldots$ és így tovább és végre k_1 is osztható p-vel. De akkor az utolsó egyenlőség szerint a megvizsgált formára vonatkozó feltevéssel ellenmondásban k'_{m-g} is osztható volna p-vel, c_m pedig p^2-vel és evvel a tétel be van bizonyítva.

Mint e tétel egyszerű corrolariumát a gyakori alkalmazás kedvéért még felemlítjük a következő tételt:

Bármely p törzsszámra nézve a

$$z^{p-1} + z^{p-2} + \cdots + z + 1$$

forma úgy a racionális, mint a racionális és egész formatartományban irreducibilis.

A forma reducibilis vagy irreducibilis volta ugyanis változatlan marad, ha alkalmazzuk a $z=y+1$ transformatiót. De akkor, minthogy

$$(z-1)(z^{p-1}+\cdots+z+1)=z^p-1$$

egyszersmind lesz

$$y\left((y+1)^{p-1}+\cdots+1\right)=(y+1)^p-1=$$
$$=y^p+\binom{p}{1}y^{p-1}+\binom{p}{2}y^{p-2}+\cdots+\binom{p}{1}y$$

és így tehát

$$(y+1)^{p-1}+\cdots+1=y^{p-1}+\binom{p}{1}y^{p-2}+\cdots+\binom{p}{2}y+\binom{p}{1}$$

Eisenstein tétele szerint irreducibilis forma.

Az egyenlet problémájának új fogalmazása. Az adjunctio.

5. §. Az

$$F(z)=A_0z^n+A_1z^{n-1}+\cdots+A_n=0$$

egyenletet *az orthoid* (A) *tartományból származó egy ismeretlent tartalmazó n-ed fokú egyenletnek* fogjuk nevezni, ha az A együtthatók az orthoid (A) tartományból származnak és A_0 a 0-tól különböző, a mikor A_0 az általánosság megszorítása nélkül 1-nek is vehető. Ha a tartomány a 3. §. értelmében jól értelmezett, akkor *az ilyen egyenlet megoldását az* (A) *tartományban* elintézett problémának kell tekintenünk, mert a $z=\xi_1$ megoldásnak megfelel az $F(z)$ forma egy lineáris osztója $z-\xi_1$ és viszont. Ha tehát $F(z)$-t az (A)-ból származó formatartományban fel tudjuk bontani irreducibilis tényezőkre, akkor minden elsőfokú tényezőnek, és csakis ezeknek, megfelel egy-egy megoldás.

Ha azonban $F(z)$ felbontása egyáltalában nem szolgáltat elsőfokú tényezőket, akkor az $F(z)=0$ egyenletnek az adott (A) tartományban nincsen megoldása és a megelőző

fejtegetések szerint ez az eset magasabb fokú irreducibilis formák egy végtelen sorozatára nézve áll be már akkor is, ha az orthoid tartomány az (1).

Az $F(z) = 0$ egyenletet az (A) *tartományban irreducibilisnek nevezzük, ha az $F(z)$ forma az* (A) *tartományban irreducibilis.*

Az épen fejtegetett tény új fogalomalkotás követelésére vezet, a mely a legegyszerűbb esetben már a mathematika elemeiben is fellép, midőn kapcsolatban a másodfokú egyenlet «megoldásával» a valós quadratikus irraczionálitásokat és a complex számokat bevezetjük.

Ezt a követelést közvetetlenül a következő módon fogalmazhatjuk:

Az adott orthoid (A) *tartomány úgy bővítendő, hogy az* (A)*-ban megoldhatatlan $F(z)=0$ egyenlet a bővített tartományban megoldhatóvá váljék.* Követeljük e mellett, hogy a bővített tartomány az eredeti tartomány összes mennyiségeit «tartalmazza». E kijelentés értelmét már a III. fej. 13. §-ának végén fejtegettük.

Elég, ha csupán csak az irreducibilis egyenleteket vizsgáljuk. Mert, ha $F_1(z)$ az $F(z)$ irreducibilis tényezője és az $F_1(z) = 0$ egyenletnek a bővített tartományban van megoldása, akkor ez kielégíti az $F(z) = 0$ egyenletet is.

Az új mennyiségek, a melyek a bővített tartományban megvannak, de (A)-ban nincsenek meg, *az* (A) *tartományhoz adjungált mennyiségek;* maga a tartománynak bővítése *az új mennyiségek «adjunctio»-ja;* az $F(z) = 0$ egyenlet «bizonyos mennyiségek adjunctiója után megoldhatóvá válik». Első feladatunk tehát az lesz, hogy valamely adott irreducibilis egyenletnek megfelelőleg megtaláljuk azokat a mennyiségeket, a melyeknek adjunctiója az egyenletet megoldhatóvá teszi; továbbá, hogy ezeket a mennyiségeket a

lehetőleg legegyszerűbb módon jellemezzük. Első tekintetre ugyan az egyenlet problémája ebben a fogalmazásban csak formális feladatot állít elénk, valóban azonban a mathematikai kutatás mezejét kimérhetetlenül bővíti.

6. §. Az $F(z)=0$ egyenletet, a melyről feltételezzük, hogy irreducibilis — mint már említettük — a

$$z^n+A_1 z^{n-1}+A_2 z^{n-2}+\cdots+A_n=0$$

alakban írjuk és hozzá — tisztán formálisan — adjungáljuk az (A)-nak mindig n mennyiségéből alkotott

$$\{C_0', C_1', \ldots, C_{n-1}'\}, \quad \{C_0'', C_1'', \ldots, C_{n-1}''\}, \ldots$$

complexusokat. (Az olvasó figyeljen itt a complex számok bevezetésével fennálló analogiára, a hol az alapul szolgáló egyenlet $z^2+1=0$.) Ezeknek az új mennyiségeknek összessége mindazokból a complexusokból áll, a melyeket nyerünk, ha a C-knek az (A)-ban foglalt bármely értékeket tulajdonítunk; kettő közülük, pl. a részletesen kiírtak a definiczió szerint akkor és csak akkor egyenlők, ha a megfelelő helyeken álló elemek mindig ugyanazok; azaz, ha $C_0'=C_0'', \ldots, C_{n-1}'=C_{n-1}''$.

Ezek az új mennyiségek úgy válnak «tartomány»-nyá, ha azokat bizonyos «tulajdonságok»-kal felruházzuk, azaz megállapítjuk a kapcsolások bizonyos módjait, a melyeket mindjárt összeadásnak és szorzásnak fogunk nevezni.

Két

$$\gamma_1=\{C_0', C_1', \ldots, C_{n-1}'\}$$
$$\gamma_2=\{C_0'', C_1'', \ldots, C_{n-1}''\}$$

mennyiség *összegének és szorzatának* definiczióját legyen a következő:

Alkossuk a

$C_0'+C_1'z+\cdots+C_{n-1}'z^{n-1}$ és $C_0''+C_1''z+\cdots+C_{n-1}''z^{n-1}$

formák összegét és szorzatát és azután a maradékot, a mely fellép, ha az így származó formákat elosztjuk $F(z)$-vel:

$$(C_0'+C_0'')+(C_1'+C_1'')\,z+\cdots+(C_{n-1}'+C_{n-1}'')\,z^{n-1},$$
$$Q_0+Q_1 z+\cdots+Q_{n-1}z^{n-1};$$

azután legyen:

$$\gamma_1+\gamma_2=\{(C_0'+C_0''),\,(C_1'+C_1''),\,\ldots,\,(C_{n-1}'+C_{n-1}'')\}$$
$$\gamma_1\gamma_2=\{Q_0,\,Q_1,\,\ldots,\,Q_{n-1}\}.$$

Hogy az így értelmezett összeadás és szorzás commutativ és associativ, az utóbbi művelet pedig distributiv is, közvetetlenül abból a körülményből következik, hogy e műveleteket valóban a megfelelő formákon hajtjuk végre, a hol ama törvények tényleg érvényesek; az új mennyiségeket pedig egyértelműleg az így összeg- vagy szorzatként nyert formák együtthatóiból határozzuk meg.

Az is majdnem közvetetlenül világos, hogy a $\gamma_1+\xi=\gamma_2$ egyenlet mindig megoldható és hogy ennek csak egy gyöke van. Részletesen írva

$$\xi=\{X_0,\,X_1,\,\ldots,\,X_{n-1}\},$$

és ekkor szükséges, hogy

$$C_0'+X_0=C_0'',\,\ldots,\,C_{n-1}'+X_{n-1}=C_{n-1}'',$$

azaz

$$\xi=\{(C_0''-C_0'),\,(C_1''-C_1'),\,\ldots,\,(C_{n-1}''-C_{n-1}')\}$$

legyen.

E szerint a $\{0,0,\ldots,0\}$ mennyiség az új tartomány «zérus»-a.

Továbbá a szorzás értelmezéséből következik, hogy, ha az $\{1,0,\ldots,0\}$ mennyiséget megszorozzuk γ-val, a szorzat ismét γ lesz. Ama mennyiség az új tartomány absolut egysége, a melyet röviden mindjárt 1-gyel jelölünk, valamint a zérust 0-sal.

Hogy a $\gamma_2\xi=\gamma_1$ egyenletnek is, ha γ_2 a zérustól különböző, egy és csak egy gyöke van, a következőképen bizonyítjuk az $F(z)$ forma irreducibilis voltából.

A γ_2-nek megfelelő

$$G(z) = C_0'' + C_1'' z + \cdots + C_{n-1}'' z^{n-1}$$

forma a 0-tól különböző és minthogy $F(z)$ irreducibilis, $F(z)$ és $G(z)$ legnagyobb közös osztója æquivalens az egygyel. $F(z)$ és $G(z)$ resultánsa, R tehát az (A) tartomány valamely 0-tól különböző mennyisége. A III. fej. 16. §-ában nyert $R = G_1 F + F_1 G$ relációt tehát, ha azt R-rel elosztjuk, a

$$(X_0' + X_1' z + \cdots + X_{n-1}' z^{n-1})(C_0'' + C_1'' z + \cdots + C_{n-1}'' z^{n-1}) + \\ + (Y_0 + Y_1 z + \cdots + Y_{n-2} z^{n-2}) F(z) = 1 \quad (D)$$

alakra hozhatjuk és így tehát, ha

$$\xi' = \{X_0', X_1', \ldots, X_{n-1}'\},$$

a definiczió szerint lesz

$$\gamma_2 \xi' = 1$$

és, ha még $\xi = \gamma_1 \xi'$, egyszersmind

$$\gamma_2 \xi = \gamma_1.$$

Ha még ugyancsak $\gamma_2 \eta = \gamma_1$ volna, ebből következnék, hogy

$$\gamma_2 (\xi - \eta) = 0,$$

azaz, hogy a γ_2 és $\xi - \eta$ szorzatának megfelelő forma osztható $F(z)$-vel. Ámde a γ_2-nek megfelelő $G(z)$ formára nézve, mint azt már előbb megemlítettük, $(F(z), G(z)) \sim 1$; így tehát már a $\xi - \eta$-nak megfelelő formának oszthatónak kell lennie $F(z)$-vel. Ez pedig csak más kifejezése annak a ténynek, hogy $\xi - \eta = 0$, azaz $\xi = \eta$.

A $\gamma = \{C_0, C_1, \ldots, C_{n-1}\}$ *mennyiségek tartománya tehát ismét orthoid;* mert világos végre, hogy az $1, 1+1, \ldots$ mennyiségek közt, a melyek általános alakja részletesen kiírva: $\{m, 0, \ldots, 0\}$, nincsen meg a 0. E tartomány «magában foglalja» az eredetileg adott (A) tartományt oly módon, hogy az (A) tartomány C mennyisége és az új tartomány $\{C, 0, \ldots, 0\}$ mennyisége az összes itt tekintetbe veendő tulajdonságaikban megegyeznek.

Hogy már most az új tartomány mennyiségeit lehetőleg egyszerűen leírhassuk, a $\{0, 1, 0, \ldots, 0\}$ mennyiség jelölésére, a melyben csak C_1 a 0-tól különböző, még pedig 1-gyel egyenlő, az egyszerű α jelt használjuk. A szorzás kivitele azután mutatja, hogy

$$\alpha^k = \{0, \ldots, 0, 1, 0, \ldots, 0\} \quad (0 \leqq k \leqq n-1),$$

a hol csak a $k+1$-edik helyen álló C_k elem különbözik a 0-tól, még pedig 1-gyel egyenlő. Hogy ezt belássuk, csak az osztási maradékot kell képeznünk, a mely fellép, ha z^k-t elosztjuk $F(z)$-vel.

Ép úgy lesz azután

$$C_k \alpha^k = \{0, \ldots, 0, C_k, 0, \ldots, 0\}$$

és így tehát végre $\{C_0, C_1, \ldots, C_{n-1}\}$-et a

$$C_0 + C_1 \alpha + \cdots + C_{n-1} \alpha^{n-1}$$

alakban írhatjuk.

Hogy ép úgy meghatározhassuk α^n-t is, z^n-t el kell osztanunk $F(z) = z^n + A_1 z^{n-1} + \cdots + A_n$-nel. Akkor

$$z^n = F(z) - A_1 z^{n-1} - \cdots - A_n;$$

tehát

$$\alpha^n = \{-A_n, -A_{n-1}, \ldots, -A_1\}$$

és

$$\alpha^n + A_1 \alpha^{n-1} + \cdots + A_n = 0;$$

α tehát a bővített tartományban az egyenlet gyöke.

7. §. Ezt a bővített orthoid tartományt most már röviden úgy jellemezhetjük, hogy (A)-*ból az α adjunctiója révén származik* és ennek megfelelőleg (A, α)-val fogjuk jelölni. E tartomány áll az összes $C_0 + C_1 \alpha + \cdots + C_{n-1} \alpha^{n-1}$ mennyiségekből, a hol a C-k az eredeti tartomány tetszés szerinti mennyiségei; az új mennyiségek tulajdonságait, azaz a négy alapművelet szerinti kapcsolataikat pedig az alapúl felvett definiciókkal szintén megállapítottuk. Ugyanezekből következik, hogy az (A) tartományhoz tartozó mennyiségek

«tulajdonságai», ha azokat az (A, α) tartomány mennyiségeinek tekintjük, teljesen változatlanok maradnak, azaz ily mennyiségek összeadása, szorzása mind a két esetben ugyanarra az eredményre vezet. Evvel egyszersmind igazolva van a 0 és 1 jeleknek már előbb történt változatlan átvétele.

A most bevezetett mennyiségeket «(A)-*ra vonatkozólag*» *algebrai mennyiségeknek* fogjuk nevezni; absolut algebrai mennyiségeknek vagy röviden «*algebrai mennyiségeknek*» pedig akkor, ha (A) valamely $[(1), x_1, \ldots, x_m]$ formatartomány mellérendelt orthoid tartománya; ha végre (A) a raczionális számok tartománya, akkor e mennyiségeket *algebrai számoknak* nevezzük.

Az itt előadott fejtegetéseknek messze ható elvi jelentőségük van. Mindenek előtt bizonyítékát szolgáltatják annak, hogy az $F(z) = 0$ irreducibilis egyenletnek «*van*» egy α gyöke abban a pontosabb értelemben, hogy van oly orthoid tartomány, mely magában foglalja az (A) tartományt és egy oly α mennyiséget, melyre nézve $F(\alpha)=0$. A tétel e fogalmazásánál az $F(z)$ irreducibilis volta már nem lényeges; de ha föntartjuk az irreducibilis $F(z)$ föltevését, még a következő fontos eredményhez jutunk:

Bármely orthoid tartomány, mely magában foglalja az (A) *tartományt és egy oly* α *mennyiséget, mely az* (A)*-ban irreducibilis* $F(z)=0$ *gyöke, tartalmazza az egész előbb értelmezett* (A, α) *tartományt.*

Az ily orthoid tartomány tartalmazza minden esetre az összes $C_0+C_1\alpha+\cdots+C_{n-1}\alpha^{n-1}$ alakú mennyiségeket, hol a C-k (A)-hoz tartoznak. Két ily mennyiség összege, különbsége, szorzata és hányadosa pedig ép úgy alkotandó, mint az (A, α)-ban, a mi az első három esetben az összeg és szorzat a 6. §-ban adott értelmezéséből, a hányados esetében pedig ugyancsak a 6. §. (D) képletéből világos, a mennyiben az

ott mod. $F(z)$ congruens mennyiségek, ha z helyébe α-t teszszük, $F(\alpha)=0$ miatt egyenlők lesznek.

De az összes így alkotott $C'_0 + C'_1\alpha + \cdots + C'_{n-1}\alpha^{n-1}$, $C''_0 + C''_1\alpha + \cdots + C''_{n-1}\alpha^{n-1}$, ... különbözők is, mihelyt a megfelelő helyeken álló C együtthatók nem mind ugyanazok. Az ellenkező esetben volna ugyanis a $K_0, \ldots, K_{n-1}$ együtthatóknak (A)-ból vett oly rendszere, hogy

$$K_0 + K_1\alpha + \cdots + K_{n-1}\alpha^{n-1} = 0$$

a nélkül, hogy minden K zérus volna. De

$$K(z) = K_0 + K_1 z + \cdots + K_{n-1} z^{n-1}$$

és az irreducibilis $F(z)$ legnagyobb közös osztója 1; és így volna két az (A)-ból származó $F_1(z)$ és $G_1(z)$ forma, melyeknek fokszáma legfölebb $n-1$, ill. $n-2$ és melyekre nézve

$$G(z)\,F(z) + F_1(z)\,K(z) = 1.$$

De ebből következnék, ha z helyébe α-t teszszük,

$$F_1(\alpha)\,K(\alpha) = 1$$

és minthogy $K(\alpha)=0$, volna $1=0$, a mi orthoid tartományban lehetetlen.

A bebizonyított eredményt most már röviden úgy fogalmazhatjuk, hogy *az előbb értelmezett* (A, α) *tartomány a «legkisebb» orthoid tartomány, a mely* (A) *bővítésével alkotva, az* (A)*-ban irreducibilis* $F(z)=0$ *egyenlet egy gyökét tartalmazza.*

Hogy a fejtegetett fogalomalkotást egy legegyszerűbb példán részletezzük, az $x^2=2$ egyenlet α gyöke pl. oly mennyiség, a melynek fogalmi tartalmát teljesen a raczionális és egész számok tartományában fejtjük ki. E mellett α és $-\alpha$ különböző mennyiségek ugyan, de annak a kérdésnek, hogy a kettő közül melyik 2-nek positiv és melyik negativ négyzetgyöke, nincsen értelme; α és $-\alpha$ ugyanis *nem mérő mennyiségek,* azaz nem olyanok, a melyek a valós vagy pedig a complex számok tartományának valamely meghatározott he-

lyével azonosítandók. Ha azonban $\sqrt{2}$ viszont ama meghatározott pozitiv vagy negativ valós szám, a melyet az analizisben határértékként értelmezünk, akkor ebben megvannak α összes «tulajdonságai», de azon felül még olyanok is, a melyekre az algebrai mennyiségek elméletében nem leszünk tekintettel; különösen az, hogy $\pm\sqrt{2}$ «nagyságára nézve» minden raczionális számmal összehasonlítható.

Az α-nak minden az algebrai mennyiségek elméletében kifejtett «tulajdonsága» egyszerűen oly identikus reláczió, a melybe α is belép és az meg fogja tartani érvényességét még akkor is, ha analitikai meggondolásokra áttérve α helyébe ama határértéket teszszük.

Ha valamely algebrai mennyiség nem algebrai szám, azaz definiczióiában határozatlanok is szerepelnek, azt *algebrai függvénynek* is fogjuk nevezni. Az «algebrai függvény» fogalmi tartalmát az analizissel szemben teljesen ugyanazon a módon szűkebbre kell szabnunk, mint azt a szám esetére épen kifejtettük.

Hyperorthoid tartományok.

8. §. Az algebrai mennyiségek elméletében elvileg algebrai és arithmetikai módszereket kell megkülönböztetnünk; mely elvi különbség most már a következő módon fejezhető ki egész pontosan.

Az *algebra* megvizsgálja a valamely orthoid tartományból származó formákat, a melyeknek tartományában nemcsak hogy mindig van legnagyobb közös osztó, hanem ez — a mint tudjuk — megállapított algorithmus segítségével véges számú lépésben meg is határozható. Az adott $F_1, \ldots, F_k$ formáknak más felbontását tényezőkre nem is használja,

mint azt, mely két-két ily forma legnagyobb közös osztójának létezéséből következik.

Az *arithmetika* megvizsgálja a valamely holoid vagy orthoid tartományból származó formákat arra az esetre, hogy azok mindig mint véges számmal lévő irreducibilis formák szorzatai állíthatók elő.

Ebben a felfogásban — de a dolog lényege szerint is — az arithmetika területe a magasabb, a mely csak az algebrai módszereknek kifejtése után vizsgálható tüzetesen. Az algebrai mennyiségek elméletének előadásában azonban, a melyet e könyv tervbe vett, alig volna tanácsos az algebrai és arithmetikai módszerek e szigorú elkülönítését valóban keresztülvinni, a mit eddig se tettünk. Ez ellen szól ugyanis az a fontos körülmény, hogy az ide tartozó fogalmak felépítésénél csakis a raczionális, illetőleg raczionális és egész formákból mint olyanokból indulhatunk ki, a melyek már eleinte valóban megalkothatók és ezeket már belé kell vonnunk a magasabb algebrai képződmények definiczijába ; ámde már ezeknek a formáknak, sőt a legegyszerűbb, a raczionális és egész számok tartományának vizsgálata is úgy «algebrai», mint «arithmetikai» módszerek alkalmazására szorul.

Mindezek daczára nem felesleges megmutatni, hogy az algebrai mennyiségek elméletében az algebrai és arithmetikai rész ily szigorú elkülönítése csakugyan keresztülvihető. Noha az erre szükséges fogalomalkotást a következőkben nem igen fogjuk használni, mégis helyén lesz, hogy azt röviden vázoljuk.

A megelőző fejtegetésekben feltételeztük, hogy az (A) tartomány «jól értelmezett» és ennek alapján feltételezhettük azt is, hogy az $F(z) = 0$ egyenlet irreducibilis. E feltevésnek most már el kell maradnia és $F(z)$ felbonthatóságát tényezőkre csak akkor fogjuk megengedni, ha $F(z)$-

nek és valamely a műveletek véges sorából keletkezett $G(z)$ formának van az 1-től különböző legnagyobb közös osztója.

Ekkor azonban a 6. §-ban képezett (A, α) tartomány általánosságban már *nem* lesz orthoid tartomány, mert a $\gamma_2 \xi = \gamma_1$ egyenlet megoldása lényegesen másképp alakul.

Ha a 0-tól különböző γ_2 mennyiségnek megfelelő $G(z) = C_0'' + \cdots + C_{n-1}'' z^{n-1}$ forma olyan, hogy $(G(z), F(z)) \sim 1$, akkor az összes ott elvégzett következtetések megtartják érvényességüket és a $\gamma_2 \xi = \gamma_1$ egyenletnek egy és csak egy gyöke lesz.

Ha azonban $(G(z), F(z)) \sim D(z)$ a z-t valóban tartalmazó forma, akkor $D(z)$ az $F(z)$ valódi osztója, (mert $G(z)$ alacsonyabb fokú mint $F(z)$ és nem 0); így tehát $F(z) = D(z) F_1(z)$, $G(z) = D(z) G_1(z)$. De akkor a 6. §. (D) egyenletének helyébe bizonyos

$$(X_0' + \cdots + X_{n-1}' z^{n-1})(C_0'' + \cdots + C_{n-1}'' z^{n-1}) + (Y_0 + \cdots + Y_{n-2} z^{n-2}) F(z) = 0$$

reláczió lép, a melyben

$$X_0' + \cdots + X_{n-1}' z^{n-1} = F_1(z);$$

tehát az X' együtthatók nem tünhetnek el mindannyian. Ha ismét

$$\xi' = \{X_0', \ldots, X_{n-1}'\},$$

akkor $\gamma_2 \xi' = 0$, noha sem γ_2, sem pedig ξ' nem zérus; γ_2 a Weierstrass-tól származó kifejezésmód szerint *a zérus valódi osztója*. Vajjon valamely γ_2 mennyiség a zérus osztója-e, azt egyszerűen $D(z) \sim (G(z), F(z))$ képezése alapján dönthetjük el. *γ_2 a zérus valódi osztója, ha $G(z)$-nek és $F(z)$-nek az 1-től különböző legnagyobb közös osztója van*.*

Ha már most γ_2 a zérus valódi osztója, a $\gamma_2 \xi = \gamma_1$ egyenletnek vagy egyáltalában nincsen gyöke, vagy pedig

* Ha $F(z)$ irreducibilis, akkor épen 0 a 0 «egyetlen» osztója, tehát valódi osztója a 0-nak akkor nincsen; ha azonban $F(z)$ reducibilis, a zérusnak mindig vannak valódi osztói.

végtelen sok gyöke van. Ugyanis, ha ξ_1 annak egyik gyöke és μ az (A, α) tartomány valamely mennyisége, akkor egyszersmind lesz $\gamma_2(\xi_1 + \mu\xi') = \gamma_2 \xi_1 = \gamma_1$.

Ha γ_2 a zérus valódi osztója, tehát $\gamma_2\xi' = 0$, noha $\xi' \neq 0$, abból, hogy van oly ξ_1 mennyiség, a melyre nézve

$$\gamma_2 \xi_1 = \varepsilon,$$

továbbá az is következik, hogy

$$\gamma_2 \xi' \xi_1 = \varepsilon\xi' = 0;$$

tehát ε is a zérus osztója és akkor a $\gamma_2 \xi = A$ egyenletnek, a hol A valamely a 0-tól különböző mennyiség az (A)-ból, soha sem lesz megoldása; $\gamma_2 \xi$ ugyanis a megelőzők szerint a zérus valódi osztója, A azonban nem az.

Ép úgy nincsen megoldása a $\gamma_2 \xi = \varepsilon$ egyenletnek sem, ha $E(z)$ az ε-nek megfelelő forma és $E(z)$ nem osztható $D(z) \sim (F(z), G(z))$-vel. $\gamma_2 \xi_1 - \varepsilon = 0$ ugyanis egyszerűen azt a tényt fejezi ki, hogy

$$(X_0' + \cdots + X_{n-1}' z^{n-1}) G(z) - E(z)$$

osztható $F(z)$-vel, tehát $D(z)$-vel is.

Ha ellenben $E(z)$ osztható $D(z)$-vel, tehát $E(z) = D(z) E_1(z)$, akkor az a követelés, hogy

$$(X_0' + \cdots + X_n' z^{n-1}) G_1(z) - E_1(z)$$

osztható legyen $F_1(z)$-vel, meghatározza az X' együtthatóknak oly rendszerét, a melyek nem tünnek el mind. Ugyanis, minthogy $(G_1(z), F_1(z)) \sim 1$, minden esetre van két oly a 0-tól különböző forma, Φ és Ψ, a melyekre nézve

$$\Phi G_1 + \Psi F_1 = 1,$$

tehát

$$\Phi E_1 G_1 + \Psi E_1 F_1 = E_1.$$

Itt ΦE_1 nem osztható F_1-gyel, mert különben E_1 is osztható volna F_1-gyel, tehát E is F-fel; pedig E a z-ben csak $n-1$-edfokú. ΦE_1 tehát annál kevésbbé osztható F-fel. A ΦE_1-nek

megfelelő $\xi_1 = \{X_0', \ldots, X_{n-1}'\}$ mennyiség tehát nem lehet csupa eltünő elemből alkotva.

Ebben az esetben tehát oly ξ_1 mennyiség meghatározását nyertük, a melyre nézve $\gamma_2 \xi_1 = \varepsilon$. Hogy ez ξ-re nézve is álljon, tehát $\gamma_2 \xi = \varepsilon$ legyen, szükséges, hogy legyen

$$\gamma_2 (\xi - \xi_1) = 0$$

és ez egyszersmind elegendő is. Szükséges tehát, hogy $\xi_1 - \xi$ megfeleljen oly $X(z)$ formának, a melyre nézve GX oszthatóvá válik F-fel. Erre elegendő és szükséges, hogy $G_1 X$ osztható legyen F_1-gyel. Minthogy azonban $(F_1, G_1) \sim 1$, X-nek oszthatónak kell lennie $F_1(z)$-vel. Ha tehát megállapítjuk, hogy $X = F_1(z) H_1(z)$, a hol elég feltételeznünk, hogy H_1 foka $n-1$, akkor megkapjuk az összes oly $\xi - \xi_1$ mennyiségeket, a melyek a $\gamma_2(\xi - \xi_1) = 0$ egyenletet kielégítik és evvel közvetetlenül az összes mennyiségeket, a melyek a $\gamma_2 \xi = \varepsilon$ egyenletet kielégítik. Számuk természetesen határtalan.

Így tehát a következő általános eredményre jutottunk:

Legyenek a γ és ε mennyiségeknek megfelelő formák $G(z)$ és $E(z)$, akkor a $\gamma\xi = \varepsilon$ egyenletnek egy és csak egy megoldása van, ha $(G, F) \sim 1$; ha ellenben $(G, F) \sim D$ olyan forma, a mely z-t valóban tartalmazza, a $\gamma\xi = \varepsilon$ egyenletnek végtelen sok megoldása van, vagy pedig egyáltalában nincsen megoldása, a szerint, a mint $E(z)$ osztható, vagy pedig nem osztható D-vel.

9. §. Hogy most ismét rövid kifejezésmódra tegyünk szert, az oly tartományok számára, a melyek az orthoid tartományoktól csak a $\gamma\xi = \varepsilon$ egyenlet viszonyaira tekintettel különbözők, melléknévi jelzést vezetünk be.

Valamely tartomány hyperorthoid, ha az összeadás közönséges törvényét követi, az absolut egységet tartalmazza, az $1, 1+1, 1+1+1, \ldots$ mennyiségek sorozatában a zérus nem

fordul elő és a szorzás törvénye, mint a szorzás «közönséges» törvényének (I. fej. 3. §.) általánosítása röviden a következő módon fogalmazható:

a) és *b)* A szorzás commutativ, associativ és distributiv.

c) Az $\alpha x = \beta$ egyenletnek egy és csak egy megoldása van, ha nincsen oly a 0-tól különböző δ mennyiség, a melyre nézve $\alpha\delta = 0$. Oly α mennyiség, a melyre nézve $\alpha\delta = 0$ a nélkül, hogy $\delta = 0$, a zérus osztója; még pedig a zérus *valódi* osztója, ha a 0-tól különböző.

Az orthoid tartomány tehát a hyperorthoid tartomány általánosabb fogalomalkotásában benne van és úgy származik, ha a tartomány mennyiségei között a zérus valódi osztói nem fordulnak elő. Ezeket singuláris mennyiségeknek kell tekintenünk és mint ilyen az orthoid tartományban épen csak a zérus marad meg.

A hyperorthoid tartományok általános elméletét e könyvben tovább nem fejtegetjük; csak azt akarjuk még megjegyezni, hogy kifejtésével* lehetségessé válik a «végtelen kicsiny» és «végtelen nagy» mennyiségek vizsgálata az algebrai mennyiségek elméletének módszereivel és ennek keretén belül.

Ha már most az (A, α) tartományt valamely $F(z) = 0$ egyenlet értelmezi a nélkül, hogy oly módszerek állanának rendelkezésünkre, a melyek $F(z)$ irreducibilis tényezőit szolgáltatják, akkor mégis képesek vagyunk az (A, α) tartományból származó formákat tisztán algebrai módszerek segítségével megvizsgálni, mint az a következő meggondolásból kitünik.

* Az ennek megfelelőleg bevezetendő hyperorthoid tartományok azonban *nem* a fennebb részletezettek, a reducibilis $F(z) = 0$ egyenletnek megfelelők. (L. a jegyzetet az V. fej. 8. §-ához.)

A míg a fellépő formák együtthatói között a zérus egy osztója sem fordul elő, az (A, α)-ból származó formatartományban a számolás szabályai ugyanazok maradnak, mint az orthoid tartomány esetében. Vajjon valamely γ mennyiség a zérus osztója-e, vagy sem, azt az annak megfelelő $G(z)$ forma és $F(z)$ legnagyobb közös osztója dönti el. Mihelyt ily legnagyobb közös osztó fellép, a mely az æquivalentia értelmében 1-től különböző, evvel meg van adva $F(z)$ egyik felbontása és $F(z)$-ről annak osztójára fogunk áttérni.

Az összes eredmények tehát, a melyeket a következőkben valamely irreducibilis $F(z) = 0$ egyenletre vonatkozólag levezetünk, érvényesek maradnak e feltevés nélkül is, hacsak szem előtt tartjuk azt a megszorítást, hogy, mihelyt a számolásban szereplő mennyiségek közt a zérus valamely osztója fellép, azonnal elvégezzük az $F(z)$-nek evvel megadott felbontását.

A Galois-féle tartomány.

10. §. Most ismét feltételezzük, hogy az (A)-ból származó tartomány jól értelmezett; azaz, hogy van oly módszerünk, a melynek segítségével minden e tartományból származó forma véges számú lépésben irreducibilis tényezőkre bontható. A további vizsgálatok tehát minden esetre érvényesek raczionális formák esetében, továbbá mindazokra az orthoid formatartományokra, a melyekben utólagosan a felbontás ily módszerét megállapíthatjuk.

Most oly bővített tartományt akarunk szerkeszteni, hogy a tetszés szerint megadott — irreducibilis vagy reducibilis —

$$F(z) = z^n + A_1 z^{n-1} + \cdots + A_n$$

forma e bővített tartományban mint lineáris formák szorzata legyen előállítható

E czélból a

$$P(z) = (z-x_1)(z-x_2)\ldots(z-x_n) =$$
$$= z^n - \mathfrak{f}_1 z^{n-1} + \mathfrak{f}_2 z^{n-2} - \cdots + (-1)^n \mathfrak{f}_n$$

formából indulunk ki. Alkossuk azután az x, $u_1, \ldots, u_n$ új határozatlanok segítségével a

$$\prod_{(i)} (x - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n}) = x^{n!} + \cdots$$

kifejezést, a hol a szorzás jele az $1, 2, \ldots, n$ számok összes permutáczióira vonatkozik, a melyek közül az egyik $i_1, \ldots, i_n$ legyen. Minthogy e szorzat azután az $x_1, \ldots, x_n$ határozatlanok symmetrikus formája, az a

$$\Pi(x; u_1, \ldots, u_n; \mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_n)$$

alakban is írható, a hol tehát Π-t valamely forma jelképe gyanánt használjuk.

Alkossuk azután a lineáris egyenleteknek következő n rendszerét:

$$x_{i_r} = \sum_{h=0}^{n!-1} X_h^{(r)} (u_1 x_{i_1} + \cdots + u_n x_{i_n})^h \quad (r=1,\ldots,n) \qquad (\Sigma^{(r)})$$
$$(i_1, \ldots, i_n = 1, 2, \ldots, n;\ i_k \neq i_l),$$

a melyekben $X_0^{(r)}, \ldots, X_{n!-1}^{(r)}$ legyenek az ismeretlenek úgy, hogy minden egyes $(\Sigma^{(r)})$ rendszerben úgy az ismeretlenek, mint az egyenletek száma $n!$

Ha az ismeretlenek együtthatóiból alkotott determinánst ϑ-val jelöljük, akkor a III. fej. 25. §-a szerint $\theta = \vartheta^2$ épen a Π forma discriminánsa, a mely csak e két esetben: $n=2$ vagy 3 negativ előjellel veendő. Tehát

$$\theta = \theta(u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

az u-k és az $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ elemi symmetrikus formák meghatározott formája és a mint az egyenletrendszer szerkezetéből rögtön kivehető,

$$\theta X_h^{(r)} = S_h^{(r)}(u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

és $S_h^{(r)}$ az $x_1, \ldots, x_n$ határozatlanoknak symmetrikus formája, mely tehát mint $u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n$ formája állítható elő.

Θ pontosabb alakja könnyen kipuhatolható; Θ az előjelt mellőzve az összes

$$(u_1(x_{i_1}-x_{j_1})+u_2(x_{i_2}-x_{j_2})+\cdots+u_n(x_{i_n}-x_{j_n}))^2$$

tényezők szorzata, a hol $i_1, \ldots, i_n$ és $j_1, \ldots, j_n$ az összes értékrendszereket felveszik, a melyeket az $1, 2, \ldots, n$ számok permutációi szolgáltatnak, de $i_1, \ldots, i_n$ és $j_1, \ldots, j_n$ mindig különböző ilyen értékrendszerek.

Ha Θ-t az $U_0, U_1, \ldots, U_l$ hatványszorzatok szerint rendezzük, akkor (a II. fej. 10. §-a szerint) minden egyes együttható $x_1, \ldots, x_n$ symmetrikus formája; ha pedig Θ-t mint az u-k formáját a lexicographikus elv (II. fej. 3. §.) szerint rendezzük és az U_l-t tartalmazó tag a legmagasabb, könnyen megmutathatjuk, hogy U_l együtthatója az előjel mellőzésével

$$[x_1^{n-1}]^2=\prod_{r,s}(x_r-x_s)^2=\Delta \qquad \left(\begin{smallmatrix} r,s=1,\ldots,n \\ r<s \end{smallmatrix}\right)$$

valamely hatványa. Ez az együttható ugyanis $(x_r-x_s)^2$ alakú tényezők szorzata és egyszersmind az x-ek symmetrikus formája. Az x_r-x_s tényező e szerint páros, például a $2k$ kitevővel ellátva lép fel. Ha azonban ez az együttható mint a határozatlanok symmetrikus formája osztható $(x_r-x_s)^{2k}$-val, oszthatónak kell lennie $(x_{r'}-x_{s'})^{2k}$-val is és viszont; a $2k$ kitevő tehát minden egyes x_r-x_s tényezőre nézve ugyanaz és az együttható maga lesz $[x_1^{n-1}]^{2k}$, a melyhez csak az $n=2$ és 3 esetekben hozzácsatolandó a negativ előjel.

E szerint tehát

$$\Theta=\pm\Delta^k U_l+\cdots$$

Helyettesítsük már most az $X_h^{(r)}$ együtthatók így meghatározott értékeit a $(\Sigma^{(r)})$ azon egyenletébe, hol $i_r=r$; akkor lesz

$$\Theta x_r = \sum_{h=0}^{n!-1} S_h^{(r)} (u_1 x_1 + \cdots + u_n x_n)^h,$$

vagy pedig

$$\Theta x_r = \varphi^{(r)}(u_1 x_1 + \cdots + u_n x_n; u_1, \ldots, u_n; \mathfrak{f}_1, \ldots, \mathfrak{f}_n),$$

a hol a $\varphi^{(r)}$ symbolumok az $u_1 x_1 + \cdots + u_n x_n$, $u_1, \ldots, u_n$, $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ mennyiségek teljesen meghatározott formáit jelentik. A

$$\Theta x_r = \varphi^{(r)}(x, u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

egyenletnek tehát (a melyben x az ismeretlen) gyöke $z = u_1 x_1 + \cdots + u_n x_n$, a mely tény a III. fej. 19. §-a szerint a

$$\Theta x_r \equiv \varphi^{(r)}(x, u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n) (\text{mod. } x - u_1 x_1 - \cdots - x_n u_n)$$

congruentiával is kifejezhető, a hol azután rendre $r = 1, \ldots, n$ tehető. Így tehát egyszersmind

$$\Theta^n P(z) = (\Theta z - \Theta x_1) \ldots (\Theta z - \Theta x_n)$$

és

$$\Theta^n P(z) \equiv (\Theta z - \varphi_1) \ldots (\Theta z - \varphi_n) (\text{mod. } x - u_1 x_1 - \cdots - u_n x_n),$$

a hol $\varphi^{(k)}(x, u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ helyébe röviden φ_k-t írtuk. A

$$\Theta^n P(z) - (\Theta z - \varphi_1) \ldots (\Theta z - \varphi_n)$$

forma tehát egyrészt az $x_1, \ldots, x_n$ határozatlanoknak symmetrikus formája, másrészt pedig osztható $x - u_1 x_1 - \cdots - u_n x_n$-nel. Ezért osztható $x - u_1 x_{i_1} - \cdots - u_n x_{i_n}$-nel is, a hol $i_1, \ldots, i_n$ az $1, \ldots, n$ számok bármely permutációja. Ámde

$$x - u_1 x_{i_1} - \cdots - u_n x_{i_n} \quad \text{és} \quad x - u_1 x_{j_1} - \cdots - u_n x_{j_n}$$

mint lineáris formák egyszersmind törzsformák is és ha $i_1, \ldots, i_n$ és $j_1, \ldots, j_n$ két különböző permutációt jelentenek, nem æquivalensek egymással. Ha ugyanis æquivalensek volnának, akkor, minthogy x együtthatója mind a kettőben 1, szükséges volna, hogy legyen $x_{i_1} = x_{j_1}$ stb.

Ama forma tehát a $z - u_1 x_{i_1} - \cdots - u_n x_{i_n}$ formák szorzatával, azaz $\Pi(x; u_1, \ldots, u_n; \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$-nel osztható és így azonosan lesz

$\Theta^n P(z) = (\Theta z - \varphi_1) \ldots (\Theta z - \varphi_n) + M\Pi(x, u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$.
Ha itt az $\mathfrak{f}$-ek hatványszorzatai szerint rendezünk, akkor GAUSS elve szerint minden egyes együtthatónak külön el kell tünnie és az identitás ezért ilyen marad akkor is, ha benne

$$\mathfrak{f}_i = (-1)^i A_i$$

tétetik. $P(z)$-ből ekkor az $F(z)$ forma származik; Θ továbbá az (A) tartományból származó meghatározott formába megy át, a mely részletesen kiírva:

$$T = \pm D^k U_l + \cdots,$$

a hol D az $F(z)$ discriminánsát jelenti. Ép úgy $\varphi_1, \ldots, \varphi_n$, M és Π az $x, u_1, \ldots, u_n$ határozatlanoknak az (A) tartományból származó meghatározott formáiba mennek át, a melyek jelölésére $f_1^{(u)}, \ldots, f_n^{(u)}, M^{(u)}, G^{(u)}$ szolgáljon és így végre nyerjük, hogy

$$T^n F(z) = \prod_{i=1}^{n} (Tz - f_i^{(u)}(x, u_1, \ldots, u_n)) + M^{(u)} G^{(u)}(x, u_1, \ldots, u_n), \quad (G^{(u)})$$

a hol

$$G^{(u)} = x^{n!} + \cdots$$

Legyen már most $F(z)$ discriminánsa, azaz a D mennyiség a 0-tól különböző, akkor akárhányféleképen határozhatjuk meg az u-k oly értékrendszereit, például csupán csak raczionális és egész számokból állókat is, a melyekre nézve T a 0-tól különböző érték. Legyen ez az érték t és az u-k amaz értékeinek behelyettesítése folytán $f_i^{(u)}$, $M^{(u)}$, $G^{(u)}$ menjen át f_i, M és $\bar{G}$-be. Akkor végre:

$$F(z) = \prod_{i=1}^{n} \left(z - \frac{1}{t} f_i(x)\right) + \frac{M}{t^n} \bar{G}(x). \qquad (G)$$

Legyen már most $G(x)$ a $\bar{G}(x)$ valamely irreducibilis tényezője. Ha az (A) tartományt azután $G(x) = 0$ egyik α gyökének adjunctiójával (A, α)-vá bővítjük, akkor $\xi_i = \frac{1}{t} f_i(\alpha)$ e tartománynak egy bizonyos meghatározott

mennyisége lesz és (G) átmegy a következőbe:

$$F(z) = \prod_{i=1}^{n}(z-\xi_i),$$

azaz az $F(z)$ formát evvel csakugyan lineáris tényezőkre bontottuk; az $F(z) = 0$ egyenlet összes gyökei a $\xi_1, \ldots, \xi_n$ mennyiségek, a melyek mind egymástól különbözők; mert különben az $F(z)$ formának volna többszörös valódi osztója; pedig föltettük, hogy Dscr. $F(z)$ a 0-tól különböző.

11. §. Az előbbi §. fejtegetései a következő tételben foglalhatók össze:

Legyen

$$F(z) = z^n + A_1 z^{n-1} + \cdots + A_n$$

és Dscr. $F(z)$ a 0-tól különböző. Alkossuk az $x_1, \ldots, x_n$-ben symmetrikus

$$\prod_{(i)}(x - u_1 x_{i_1} - \cdots - u_n x_{i_n})$$

formát, számítsuk ezt át a

$$\Pi(x; u_1, \ldots, u_n; \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

alakra és tegyük ebbe: $\mathfrak{f}_i = (-1)^i A_i$. Ekkor Π discriminánsa az u-k oly formája lesz, a mely nem tünik el. Igy tehát az u-k oly (többiek közt raczionális és egész) értékrendszereit is meghatározhatjuk, a melyekre nézve Dscr. Π a 0-tól különböző értéket vesz fel. Ha Π-be ily értékrendszert helyettesítünk, bizonyos $\bar{G}(x)$ formát nyerünk. Ha azután $G(x)$ a $\bar{G}(x)$ egyik irreducibilis tényezője, akkor a $G(x) = 0$ egyik α gyökének adjunctiója révén (A)*-ból oly orthoid* (A, α) *tartomány származik, a melyben az n-edfokú $F(z) = 0$ egyenletnek pontosan n egymástól különböző $\xi_1, \ldots, \xi_n$ gyöke van, a melyeket a müveletek előbb megállapított véges sora véglegesen meghatároz; $F(z)$ pedig elő van állítva mint lineáris tényezők szorzata:*

$$F(z) = (z-\xi_1)(z-\xi_2)\ldots(z-\xi_n).$$

Itt — mint azt még egyszer ki akarjuk emelni — *nem* tételeztük fel, hogy $F(z)$ irreducibilis.

További fontos megjegyzés a következő:

Az így nyert (A, a) *tartomány a «legkisebb» orthoid tartomány, a melyben* $F(z)$ *mint lineáris tényezők szorzata előállítható. Ennek az az értelme, hogy minden más,* (A) *bővítéséből származó tartomány, a melyben* $F(z)$*-nek az említett tulajdonsága megvan, az* (A, α) *tartomány összes mennyiségeit tartalmazza.*

Ha ugyanis $\xi_1, \ldots, \xi_n$ az $F(z) = 0$ gyökei a feltételezett bővített tartományban, $u_1, \ldots, u_n$ továbbá egy a feltételeknek megfelelő értékrendszer, akkor valamelyik $u_1 \xi_{i_1} + \cdots + u_n \xi_{i_n}$ a tartomány oly mennyisége, a mely nem különbözik α-tól; a bővített tartomány tehát tartalmazza (A, α) összes mennyiségeit.

Az így értelmezett $G(x) = 0$ egyenlet az $F(z) = 0$ egyenlet *Galois-féle resolvense** és ennek megvan az a jellemző tulajdonsága, hogy, ha α egyik gyöke, $F(z) = 0$ bármely ξ_i gyökére nézve lesz

$$\xi_i = A_{i0} + A_{i1} \alpha + \cdots + A_{in-1} \alpha^{n-1},$$

minthogy ξ_i az (A, α) tartományhoz tartozik és e tartomány minden mennyisége ebben az alakban írható.

Minthogy az $F(z) = 0$ egyenletnek az (A, α) tartományban n különböző gyöke van és így tehát $F(z)$, ha a 10. §-ban használt $x_1, \ldots, x_n$ jelek helyébe a $\xi_1, \ldots, \xi_n$ jeleket teszszük, a $P(z)$ alakban írható, az ott előadott fejtegetések most $F(z)$-re is érvényesek és így az $u_1 \xi_{i_1} + \cdots + u_n \xi_{i_n}$ meny-

* GALOIS, Mémoire sur les conditions de la résolubilité des équations par radicaux. «Oeuvres» Paris, 1897. 33. lap. — «Abhandlungen über die algebraische Auflösung der Gleichungen von ABEL und GALOIS» Deutsch herausgegeben von H. MASER, Berlin 1889.

nyiségek mindannyian egymástól különbözők és a $\bar{G}(x)=0$ egyenlet gyökei lesznek. Ennek az egyenletnek, a melynek foka $n!$, ugyanannyi különböző gyöke van, a melyek mind az (A,α) tartományhoz tartoznak. Ugyanaz állítható tehát $G(x)=0$-ról, valamint még akkor is, ha $G(x)$ helyett $\bar{G}(x)$ bármely más irreducibilis tényezőjét választjuk.

A Galois-féle resolvensnek tehát minden olyan tartományban, a melyben egyáltalában vannak gyökei, annyi különböző gyöke van, mint a hány egység van a fokszámban.

Lényeges körülmény még az is, hogy *az e §. elején előadott tételben szereplő* $u_1, \ldots, u_n$ *mennyiségeket meghagyhatjuk határozatlanoknak.* Ha ugyanis a 10. §. $(G^{(u)})$ identitásában ezt írjuk: $x=u_1\xi_{i_1}+\cdots+u_n\xi_{i_n}$, akkor $G^{(u)}(x,u_1,\ldots,u_n)$ eltünik és lesz

$$F(z)=\prod_{i=1}^{n}\left(z-\frac{1}{T}f_i^{(u)}(u_1\xi_{i_1}+\cdots+u_n\xi_{i_n})\right),$$

a hol T a 0-tól különböző forma. Akkor azonban, minthogy a $z-\xi_i$-k az $F(z)$ összes lineáris tényezői, az $\frac{f_i^{(u)}}{T}$ mennyiségeknek a sorrendtől eltekintve a $\xi_1, \ldots, \xi_n$ mennyiségekkel meg kell egyezniök és így az $\frac{f_i^{(u)}}{T}$-k kiszámításánál az $u_1, \ldots, u_n$ határozatlanok maguktól kiesnek.

12. §. A $\bar{G}(x)=0$ egyenletnek, a melynek foka $n!$, az (A,α) tartományban a következő $n!$ gyöke van: $u_1\xi_{i_1}+\cdots+u_n\xi_{i_n}$, a melyek mind egymástól különbözők. A $\bar{G}(x)$ forma tehát ebben a tartományban lineáris és egymással nem æquivalens formák szorzata; többszörös osztója e szerint nincsen és discriminánsa a 0-tól különböző.

Ha már mostan az (A) tartományra nézve

$$\bar{G}(x)=G(x)H(x)\ldots,$$

a hol $G, H, \ldots$ irreducibilis formákat jelentenek, akkor ezeknek is az æquivalentia értelmében különbözőknek kell len-

niök, mert a discrimáns most ugyanaz a mennyiség mint előbb, tehát ismét a 0-tól különböző és így többszörös osztó most sem lehetséges.

A $G(x) = 0, H(x) = 0, \ldots$ egyenletek egyaránt az adott $F(z) = 0$ egyenlet GALOIS-féle resolvenseinek vehetők. Ha $\alpha, \beta, \ldots$ rendre egy-egy gyökük, az (A, α) tartomány tartalmazza β-t is és ép úgy az (A, β) tartomány ismét α-t. Az (A, α) és (A, β) tartományok tehát egyáltalában nem különböznek egymástól. Ez különben már abból a tényből is következik, hogy úgy (A, α), mint (A, β) a legkisebb orthoid tartomány, a mely (A) bővítéséből származik és a melyben az $F(z) = 0$ egyenletnek n gyöke van. Ebből még könnyen a következő tétel adódik ki:

$\bar{G}(x)$-nek irreducibilis tényezői az (A) *tartományban egyenlő fokúak.*

Legyen $G(x)$ foka k, $H(x)$-é l. Minthogy β és β minden hatványa is az (A, α) tartományhoz tartozik, lesz

$$\beta^r = A_{r0} + A_{r1}\alpha + \cdots + A_{r,k-1}\alpha^{k-1}; \qquad (r=0,1,\ldots,k)$$

továbbá meghatározhatók az (A) tartománynak oly $C_0, \ldots, C_k$ mennyiségei, hogy ezek ne tünjenek el mind és a

$$\sum_{r=0}^{k} C_r A_{rs} = 0 \qquad (s=0,\ldots,k-1)$$

egyenleteket kielégítsék. Minthogy akkor

$$C_0 + C_1\beta + \cdots + C_k\beta^k = 0,$$

azért β a $H(z) = 0$ és

$$C(z) = C_0 + C_1 z + \cdots + C_k z^k = 0$$

egyenleteknek közös gyöke, $z-\beta$ tehát a $H(z)$ és $C(z)$ közös osztója és így még Res. $(H(z), C(z)) = 0$. Ha már most $H(z)$ foka nagyobb volna k-nál, $H(z)$ a feltevés ellenére (A)-ban reducibilis volna. E szerint $l \leqq k$ és épúgy bebizonyítható, hogy $k \leqq l$; tehát valóban $k = l$.

A GALOIS-féle resolvens foka *az* $F(z) = 0$ *egyenlet rendszáma az* (A) *tartományban,* a mely e tartományra nézve meghatározott pozitiv egész szám.

13. §. Az eddig kizárt eset, hogy *az* $F(z) = 0$ *egyenlet discriminánsa* eltünik,* most már könnyen beleilleszthető eddigi vizsgálatainkba.

$F(z)$ felbontása irreducibilis tényezőkre minden esetre ily eredményhez vezet:

$$F = P_1^{a_1} \dots P_r^{a_r},$$

a hol $P_1, \dots, P_r$ irreducibilis formákat jelentenek. Ha a z szerint vett deriváltat vonással jelöljük, lesz

$$F' = \sum_{i=1}^{r} a_i \frac{F}{P_i}$$

és így

$$(F(z), F'(z)) \sim D(z) = P_1^{a_1 - 1} \dots P_r^{a_r - 1};$$

tehát

$$\frac{F(z)}{D(z)} = P_1 \dots P_r$$

olyan forma, a melynek discriminánsa nem tünik el. Most már e formának megfelelőleg meghatározhatjuk a GALOIS-féle tartományt, a melyben $\frac{F(z)}{D(z)}$ és így $P_1, \dots, P_r$ is lineáris formák szorzatára bomlik, és ugyanez történik e tartományban F-fel is.

Egész általánosan tehát *az* (A) *tartományra vonatkozólag az* $F(z) = 0$ *egyenlet Galois-féle tartományának azt a bővített* (A, α) *tartományt tekintheljük, a mely származik, ha az*

$$\frac{F(z)}{(F(z), F'(z))} = 0$$

* «Az $F(z) = 0$ egyenlet discriminánsa» — mint az magától értetődik — az $F(z)$ forma discriminánsa.

egyenlethez tartozó Galois-féle resolvens egyik α gyökét adjungáljuk. Ezt az egyenletet általánosságban is az $F(z)=0$ egyenlet Galois-féle resolvensének fogjuk nevezni.

E tartományban azután lesz

$$F(z) = (z-\xi_1)^{k_1} \ldots (z-\xi_s)^{k_s},$$

a hol ξ_i-t az $F(z) = 0$ egyenlet k_i-szeres gyökének mondjuk. Magától értetődik, hogy többszörös gyökök akkor és csak akkor vannak, ha Dscr. $F(z)$ eltünik.

A genus-tartományok.

14. §. Legyen most már (A) valamely meghatározott és jól értelmezett orthoid tartomány és $F(z) = 0$ oly egyenlet, a melynek együtthatói e tartományhoz tartoznak, $G(x)=0$ pedig ennek az egyenletnek Galois-féle resolvense. A $G(x) = 0$ egyenlet egyik α gyökének adjunctiójával kibővített (A, α) tartományban $F(z)$ oly lineáris tényezőkre bomlik, a melyek a megelőzők szerint adottaknak tekinthetők. Az $F(z) = 0$ egyenletnek azután n különböző gyöke lesz: $\xi_1, \ldots, \xi_n$. Ha $F(z)$ discriminánsa a 0-tól különböző, n egyszersmind az $F(z) = 0$ egyenlet foka; az ellenkező nem különös jelentőségű esetben azonban, a mely a következőbe belé van foglalva, e fokszám n-nél nagyobb lesz.

Ha már most

$$f(\xi_1, \ldots, \xi_k)$$

a ξ mennyiségek oly formája, a melynek együtthatói az (A) tartományhoz tartoznak, akkor

$$\prod_{(i)} (y - f(\xi_{i_1}, \ldots, \xi_{i_k})),$$

a hol a szorzás az $1, \ldots, n$ számok összes $i_1, \ldots, i_n$ permutációira kiterjesztendő, a $\xi_1, \ldots, \xi_n$ mennyiségek symmetrikus formája és így y oly formája lesz, a melynek együtt-

hatói az (A) tartományhoz tartoznak. E forma felbomlik irreducibilis tényezőkre, és ezek között minden esetre van egy olyan, a mely 0-sal egyenlővé téve oly egyenletet szolgáltat, a melynek az (A, α) tartományban egyik gyöke $f(\xi_1, \ldots, \xi_k)$. Legyen az $\varphi(y)=0$. Ugyanabban a tartományban $\varphi(y)=0$ többi gyökeinek alakja minden esetre $f(\xi_{r_1}, \ldots, \xi_{r_k})$ és számuk megegyezik $\varphi(y)$ fokával. Ha $\varphi(y)=0$ gyökeit röviden $\eta_1, \eta_2, \ldots, \eta_m$-mel jelöljük, akkor, ha az (A) tartományt $\varphi(y)=0$ egyik η_i gyökének adjunctiójával bővítjük, a 7. §. fejtegetései szerint bizonyos meghatározott orthoid (A, η_i) tartományt nyerünk, a mely egyszerűen az összes

$$A_0 + A_1 \eta_i + \cdots + A_{m-1} \eta_i^{m-1}$$

alakú mennyiségekből áll. KRONECKER terminologiája szerint* (A, η_i)-t *az* (A)*-ból származó genus-tartománynak* (A)-t pedig (A, η_i) *törzstartományának* nevezzük.

Az (A, η_i) $(i=1, \ldots, m)$ tartományok *conjugált genus-tartományok;* az $\eta_1, \ldots, \eta_m$ mennyiségek — mint ugyanannak az irreducibilis egyenletnek gyökei — valamint általánosságban az $A_0 + A_1 \eta_i + \cdots + A_{m-1} \eta_i^{m-1}$, $(i=1, \ldots, m)$ számra nézve m mennyiség *conjugált mennyiség.* E kifejezés: «conjugált» természetesen csak (A)-ra és a $\varphi(y)=0$ egyenletre vonatkozólag értendő, mert valamely bővített tartományban a $\varphi(y)=0$ egyenlet esetleg már nem irreducibilis többé és az azután különböző tényezőknek megfelelő gyökei sem conjugáltak többé. Mint különös esetet foglalja ez magában a conjugált (A, ξ_i) tartományokat és az $F(z)=0$ egyenlet conjugált gyökeit, ha f-nek ξ_i-t választottuk.

Galois-féle genus-tartomány az olyan, a melynek «nin-

* Festschrift 2. §.

csenek conjugáltjai», azaz, a melyre nézve a conjugáltak: $(A, \eta_1), \ldots, (A, \eta_m)$ *egybeesnek.* Ez az eset, mint azt előbb (10., 11. §.) épen bebizonyítottuk, valóban mindig beáll akkor, ha $y = u_1 \xi_{i_1} + \cdots + u_n \xi_{i_n}$, azaz ha a $\varphi(y) = 0$ egyenlet a Galois-féle resolvens. Hogy viszont a conjugáltak egybeesnek, azt jelenti, hogy a $\varphi(y) = 0$ egyenlet egyik gyökének adjunctiója után a bővített tartomány tartalmazza a többi gyököket, $\eta_2, \ldots, \eta_m$-et is. A «legkisebb» tartomány tehát, a melyben a $\varphi(y) = 0$ egyenletnek egy gyöke van, egybeesik avval a «legkisebb» tartománynyal, a melyben m gyöke van, a Galois-féle tartománynyal. Ama tartomány tehát «Galois-féle tartomány».

Az (A, η_i) *tartomány minden mennyisége kielégít oly az* (A) *tartományra vonatkozólag irreducibilis egyenletet, a melynek foka a* $\varphi(y) = 0$ *egyenlet fokának, m-nek osztója.* Ha röviden

$$g(\eta_i) = A_0 + A_1 \eta_i + \cdots + A_{m-1} \eta_i^{m-1},$$

akkor e mennyiség minden esetre kielégíti a

$$H(z) = \prod_{i=1}^{m} (z - g(\eta_i)) = 0$$

egyenletet, a hol a bal oldalon álló szorzat az η_i-kben symmetrikus; az egyenlet tehát minden esetre a

$$z^m + C_0 z^{m-1} + \cdots = 0$$

alakot veszi fel és együtthatói az (A) törzstartományhoz tartoznak.

Ha ez az egyenlet irreducibilis, a felállított tétel helyes. Az ellenkező esetben legyen

$$\psi(z) = z^k + C_0' z^{k-1} + \cdots + C_k'$$

a bal oldalon álló forma egyik irreducibilis tényezője, a melynek gyöke pl. $g(\eta_i)$. De akkor η_i a

$$\psi(g(y)) = 0$$

és $\varphi(y) = 0$ egyenletek közös gyöke. Így tehát

$$\text{Res.}\left(\psi(g(y)), \varphi(y)\right) = 0$$

és minthogy $\varphi(y)$ irreducibilis, szükségképen

$$\psi(g(y)) = \varphi(y)\varphi_1(y),$$

azaz a $\psi(g(y)) = 0$ egyenletnek az összes $\eta_1, \ldots, \eta_m$ értékek, a $\psi(z) = 0$ egyenletnek az összes $g(\eta_i)$ értékek fognak mint gyökök megfelelni. Minthogy ez az egyenlet irreducibilis, $\psi(z) = 0$ gyökei a $g(\eta_i)$ összes különböző értékei, a melyek — mint az magától értetődik — mint egyszerű gyökök lépnek fel. Ugyanez érvényes $H(z)$ minden irreducibilis tényezőjére; ezeknek foka tehát egyenlő és ha ez k, ezek szerint lesz $m = kl$, a hol l a $H(z)$ irreducibilis tényezőinek számát jelenti és $H(z) = (\psi(z))^l$. Evvel most már a felállított tétel be van bizonyítva.

15. §. *Az* (A, η_i) *tartománynak valamely* $g(\eta_i)$ *mennyisége k-adrendű, ha kielégít oly az* (A)*-ban irreducibilis egyenletet, a melynek foka k. Az előbbiek szerint k itt mindig osztója m-nek, ha m az* η_i *mennyiség rendszáma.*

Conjugált mennyiségek természetesen egyenlő rendűek.

Ha az η_i *mennyiség m-edrendű, az* (A, η_i) *genus-tartományt is m-edrendűnek fogjuk nevezni.* Ez azonban alacsonyabb rendű mennyiségeket is tartalmaz és ezek közt minden esetre az elsőrendű mennyiségeket is, a melyek már az (A) törzstartományhoz tartoznak.

Az összes m-edrendű mennyiségek, a melyek az m-edrendű genus-tartományban benfoglaltatnak, összességükben az (A) törzstartományra vonatkozólag algebrai mennyiségeknek egy meghatározott *genusát* alkotják, a melyet ismét *m-edrendűnek* nevezünk.

E szerint az $F(z) = 0$ egyenlet $\xi_1, \ldots, \xi_k$ gyökeinek minden formája meghatároz egy meghatározott genus-tarto-

mányt és meghatározza az (A) törzstartományra vonatkozólag algebrai mennyiségek egy meghatározott genusát. A genus-tartomány tartalmazza a genus összes mennyiségeit. A genus-tartomány tartalmaz azonban más «alacsonyabb» genusokat is; még pedig oly módon, hogy ha tartalmaz valamely k-adrendű γ mennyiséget, akkor tartalmazza egyszersmind az evvel definiált genus összes mennyiségeit is. Ezek ugyanis mind $A_0 + A_1\gamma + \cdots + A_{k-1}\gamma^{k-1}$ alakúak, a hol a feltevés szerint γ hasonló módon állítható elő η_i-ből.

A meghatározás e módjai kiterjeszthetők «*az* $F(z) = 0$ *egyenlet raczionális függvényeire*» is, azaz az

$$\frac{f_1(\xi_1, \ldots, \xi_k)}{f_2(\xi_1, \ldots, \xi_k)},$$

mennyiségekre, a hol $f_2(\xi_1, \ldots, \xi_k)$ a 0-tól különböző. Ha ugyanis a számlálóban és nevezőben $f_2(\xi_1, \ldots, \xi_k)$ conjugált mennyiségeivel szorzunk és az $f_2(\xi_1, \ldots, \xi_k)$-t meghatározó egyenlet

$$z^k + C_1 z^{k-1} + \cdots + C_k = 0,$$

az új nevező ennek az egyenletnek C_k együtthatója lesz, a mely nem lehet 0, mert különben az egyenlet reducibilis volna. Evvel tehát ama kifejezést közvetlenül az $f(\xi_1, \ldots, \xi_k)$ alakra vezettük vissza.

Minden m-edrendű γ *mennyiség, a melyet az m-edrendű* (A, η_i) *genus-tartomány tartalmaz, ezt a genus-tartományt és az ebben foglalt m-edrendű genust egészen azonos módon határozza meg.*

Ez a tétel így is fogalmazható:

Ha γ *és* η_i *m-edrendűek és* γ *benne van* (A, η_i)*-ben, akkor az* (A, γ) *és* (A, η_i) *genus-tartományok ugyanazokat a mennyiségeket tartalmazzák.*

A feltevés szerint γ minden hatványa is benne van

(A, η_i)-ben úgy, hogy

$$\gamma^r = A_{r0} + A_{r1}\eta_i + \cdots + A_{r,m-1}\eta_i^{m-1}; \quad (r=0,1,\ldots,m-1)$$

az $|A_{rs}|$ determináns pedig nem tünhetik el, mert $|A_{rs}| = 0$ azt mutatná, hogy van a mennyiségeknek oly $C_r (r=0,\ldots,m-1)$ rendszere, a melynek elemei nem mind egyenlők 0-sal és a melyek kielégítik a

$$\sum_{r=0}^{m-1} C_r A_{rs} = 0 \qquad (s=0,\ldots,m-1)$$

egyenleteket. Akkor azonban egyszersmind volna

$$C_0 + C_1\gamma + \cdots + C_{m-1}\gamma^{m-1} = 0$$

és γ nem volna m-edrendű mennyiség, Ámde, ha $|A_{rs}|$ nem 0, akkor a γ^r-re vonatkozó egyenletekből az is következik, hogy

$$\eta_i = B_0 + B_1\gamma + \cdots + B_{m-1}\gamma^{m-1},$$

azaz, hogy η_i és evvel együtt az (A, η_i) genus-tartomány minden mennyisége benne van (A, γ)-ban.

Végül még közvetetlenül azt is látjuk, hogy ha α benne van az (A, η_i) genus-tartományban, akkor (A, η_i) tartalmazza α genusának és az (A, α) genus-tartomány összes mennyiségeit.

Az α *genusa,* ha α k-adrendű, az egyetlen k-adrendű genus, a melyet az (A, α) genus-tartomány magában foglal.

Az α genusa β *genusa alá van foglalva,* ha összes mennyiségei az (A, β) genus tartomány mennyiségei.

Genus-tartományok, a melyeknek törzstartományai is már genus-tartományok.

16. §. Legyen ismét (A) az az orthoid tartomány, a melyből kiindulunk, $F(z)$ valamely az (A) tartományból származó irreducibilis forma és $\xi_1, \ldots, \xi_n$ legyenek az $F(z) = 0$ egyenlet gyökei a megfelelőleg bővített tartományban. Akkor az (A, ξ_i) genus-tartomány újból oly orthoid tartomány, a mely az eddig kifejtett fogalomalkotás kiinduló pontjául szolgálhat úgy, hogy (A, ξ_i)-nek most (A) eddigi szerepe jut. Ez oly genus-tartományok alkotására vezet, a melyeknek törzstartománya is már genus-tartomány és így, ha az eddig megvizsgált «első rangúaktól» különbözők volnának, «magasabb rangú» genus-tartományokat alkotnának. Ki fog tünni azonban az a fontos eredmény, hogy *az* (A) *törzstartományból származó genus-tartományok magukban már is zárt összességet alkotnak*, azaz, ha bármely ilyen genus-tartományból, mint törzstartományból indulunk ki, az így származó «magasabb rangú» genus-tartomány ismét csak valamely közvetetlenül az (A)-ból származó genus-tartomány lesz.

Mielőtt azonban a részletekre áttérnénk, meg kell mutatnunk, hogy a fogalomalkotás, a mely valamely az (A, ξ_i)-ből származó genus-tartományhoz felemelkedik, a 14. és 15. §. fejtegetéseibe teljesen beleilleszkedik. Ez valóban úgy van, ha be tudjuk bizonyítani a következő tételt:

(A)*-val együtt az* (A, ξ_i) *genus-tartomány is jól értelmezett orthoid tartomány.*

A 3. §-ban történt megállapodások szerint ez alatt részletesen fogalmazva a következőt kell értenünk. Avval a módszerrel együtt, a melylyel képesek vagyunk, valamely az (A)-ból származó forma irreducibilis tényezőit véges számú lépésben meghatározni, adva van egyszersmind oly módszer

is, a melylyel ugyanezt a problémát bármely az (A, ξ_i) genus-tartományból származó formára vonatkozólag megoldhatjuk. E módszert már most részletesen akarjuk kifejteni *.

Erre mindenek előtt a következő előleges megjegyzések szolgálnak:

Legyen adva a

$$\Phi^{(i)}(x) = x^n + \alpha_1^{(i)} x^{n-1} + \cdots + \alpha_n^{(i)}$$

forma, melyet mindig már az egyik, pl. x határozatlanra nézve szabályosnak tételezhetünk föl és a melyben e szerint az $\alpha_r^{(i)}$-ek a többi határozatlannak az (A, ξ_i) genus-tartományból származó formái, vagyis részletesen

$$\alpha_r^{(i)} = A_{r0} + A_{r1}\xi_i + \cdots + A_{r,m-1}\xi_i^{m-1},$$

hol e szerint az A_{rs}-ek ismét az (A) tartományból származó formák. Most már $\Phi^{(i)}(x)$ oly tényezőkre bontandó, a melyek az (A, ξ_i) genus-tartományban irreducibilisek. A $\Phi^{(i)}, \alpha_r^{(i)}$ jelölések azért szükségesek, mert a $\Phi^{(1)}, \ldots, \Phi^{(m)}$ «conjugált formákat» ** egyidőben kell megvizsgálnunk.

Hogy ily

$$\Phi^{(i)}(x) = P_1^{(i)}(x) \ldots P_k^{(i)}(x) \qquad (a)$$

felbontás van és hogy e felbontás, ha minden egyes $P_l^{(i)}$ irreducibilis tényezőben x legmagasabb hatványának együtthatója 1, teljesen egyértelmű, azt e fejezet 3. §-ában már kimutattuk; itt tehát már csak magát e felbontást kell meghatároznunk. Világos továbbá az is, hogy evvel együtt ama felbontás mindjárt a conjugált genus-tartományok conjugált formáira nézve is megvan; mert hiszen ξ_i-re nézve csak az a feltevés lép be, hogy e mennyiség az (A)-ban irredu-

* Ezt legelőször KRONECKER tette a «Festschrift» 4. §-ában. L. egyszersmind MOLK idézett értekezését (Acta math. VI. k.).

** *Conjugált formák* az olyanok, a melyek megfelelő módon conjugált együttható-sorokból épülnek föl.

cibilis $F(z) = 0$ egyenlet gyöke úgy, hogy az eredmények $i=1, \ldots, m$ esetében egyaránt érvényesek.

Ha azt írjuk, hogy $x=u\xi_i+v$, a hol u és v új határozatlanok, akkor egyszersmind lesz

$$\Phi^{(i)}(u\xi_i+v) = P_1^{(i)}(u\xi_i+v)\ldots P_k^{(i)}(u\xi_i+v); \qquad (b_1)$$

és viszont $\Phi^{(i)}(u\xi_i+v)$ valamely

$$\Phi^{(i)}(u\xi_i+v) = Q_1^{(i)}(u, v)\ldots Q_l^{(i)}(u, v) \qquad (b_2)$$

felbontásából, ha ismét azt írjuk, hogy $u\xi_i+v=x$, származik

$$\Phi^{(i)}(x) = Q_1^{(i)}(u, x-\xi_i u)\ldots Q_l^{(i)}(u, x-\xi_i u),$$

a miből ismét $\Phi^{(i)}(x)$ felbontására is lehet következtetni; mert ez a forma semmi esetre sem osztható oly formával, a mely az u határozatlant tartalmazza; az u határozatlannak tehát $Q_t^{(i)}(u, x-\xi_i u)$-ból magától kell kiesnie.

$\Phi^{(i)}(x)$-nek (a) és $\Phi^{(i)}(u\xi_i+v)$-nek (b_1) és (b_2) felbontásaiban végre a $P_t^{(i)}(x)$ és $P_t^{(i)}(u\xi_i+v)$ tényezőknek egyidőben irreducibiliseknek kell lenniök; mert az egyik forma bármely valódi felbontásából az épen mondottak szerint a másik forma ép oly felbontására következtethetünk.

17. §. Vizsgálatainkat már most az $F(z) = 0$ egyenlet meghatározta Galois-féle tartományban folytatjuk, a mely az összes $\xi_1, \ldots, \xi_m$ mennyiségeket tartalmazza. Akkor azonban *két*

$$\Phi^{(i)}(u\xi_i+v) \qquad (i=1, \ldots, m)$$

formára nézve a legnagyobb közös osztó ~ 1. (Épen azért, hogy a problémának ezt az egyszerűsítését elérjük, kell általánosságban az $x = u\xi_i + v$ transformatiót alkalmaznunk) Ha ugyanis részletesen írva

$$\Phi^{(i)}(u\xi_i+v) = (u\xi_i+v)^n + \alpha_1^{(i)}(u\xi_i+v)^{n-1} + \cdots + \alpha_n^{(i)},$$
$$\Phi^{(j)}(u\xi_j+v) = (u\xi_j+v)^n + \alpha_1^{(j)}(u\xi_j+v)^{n-1} + \cdots + \alpha_n^{(j)}$$

és $u\xi_i+v=w$, akkor ezekből következik, hogy

$$u\xi_j + v = w + u(\xi_j - \xi_i)$$

és

$$\Phi^{(i)}(w) = w^n + \alpha_1^{(i)} w^{n-1} + \cdots + \alpha_n^{(i)},$$

$$\Phi^{(j)}\big(w+u(\xi_j-\xi_i)\big) = (w+u(\xi_j-\xi_i))^n + \alpha_1^{(j)}\big(w+u(\xi_j-\xi_i)\big)^{n-1} + \cdots + \alpha_n^{(j)}.$$

E transformált formák legnagyobb közös osztója akkor és csak akkor lesz 1, ha az eredeti formák legnagyobb közös osztója is az. Hogy azonban e transformált formákra nézve valóban

$$\big(\Phi^{(i)}(w), \Phi^{(j)}\big(w+u(\xi_j-\xi_i)\big)\big) \sim 1,$$

abból a megjegyzésből világos, hogy e legnagyobb közös osztó, mint $\Phi^{(i)}(w)$ osztója csak oly forma lehet, mely az u határozatlant nem tartalmazza, és így, ha $\Phi^{(j)}\big(w+u(\xi_j-\xi_i)\big)$-t az u hatványai szerint rendezzük, szükséges, hogy az u minden egyes hatványa mellett fellépő együtthatónak, tehát az u^n mellett fellépő együtthatónak, a

$$(\xi_j - \xi_i)^n$$

mennyiségnek is osztója legyen. Minthogy e mennyiség azonban a 0-tól különböző és a határozatlanokat egyáltalában nem tartalmazza, a feltételezett legnagyobb közös osztónak 1-gyel æquivalensnek kell lennie.

Feltételezhetjük továbbá még azt is, hogy Dscr. $\Phi^{(i)}(x)$ a 0-tól különböző, azaz hogy $\Phi^{(i)}(x)$-*nek nincsen többszörös osztója*. Különben ismeretes volna $\Phi^{(i)}$ valamely $\Phi^{(i)}=\Phi_1^{(i)}\Phi_2^{(i)}$ felbontása és további vizsgálatainkat e felbontás tényezőin folytathatnók.

Akkor végre

$$\prod_{i=1}^{m} \Phi^{(i)}(u\xi_i+v) = G(u,v)$$

az u, v és a többi x határozatlanoknak az (A) tartományból származó oly formája, a melynek többszörös osztója nincsen; mert bármely ily irreducibilis többszörös osztó vagy

a $\Phi^{(i)}$ forma többszörös osztója, vagy pedig a $\Phi^{(i)}$ és $\Phi^{(j)}$ formák közös osztója volna, pedig e két eset közül egyik sem állhat be.

Ha már most a $G(u, v)$ formát, a mely a jól értelmezett (A) tartományból származik, e tartományban irreducibilis tényezőire bontjuk:

$$G(u, v) = G_1(u, v)\, G_2(u, v) \ldots G_s(u, v),$$

akkor *az* (A, ξ_i) *tartományban*

$$\left(\Phi^{(i)}(u\xi_i + v),\ G_r(u, v)\right) \sim Q_r^{(i)}(u, v)$$

$\Phi^{(i)}$ *egyik irreducibilis valódi osztója lesz.* Először ugyanis nem lehet, hogy $Q_1^{(i)} \sim 1$, mert különben egyszersmind volna

$$\left(\Phi^{(i)}(u\xi_i + v),\ G_r(u, v)\right) \sim 1 \qquad (i = 1, \ldots, m)$$

és e szerint

$$(G, G_r) \sim 1,$$

míg G_r a G forma 1-től különböző osztója.

De az sem lehet, hogy

$$Q_r^{(i)} = Q_{r1}^{(i)}\, Q_{r2}^{(i)}$$

legyen, vagyis hogy ez két valódi osztó szorzata; mert $Q_r^{(i)}$ ha $i = 1, \ldots, m$, mindig $\Phi^{(i)}(u\xi_i + v)$ osztója és minthogy $(\Phi^{(i)}, \Phi^{(j)}) \sim 1$, szükséges, hogy egyszersmind $(Q_r^{(i)}, Q_r^{(j)}) \sim 1$ legyen. Minthogy azonban $i = 1, \ldots, m$-re nézve G_r osztható $Q_r^{(i)}$-rel, G_r-nek oszthatónak kell lennie $\prod_{i=1}^{m} Q_r^{(i)}$-rel. E szerint tehát

$$G_r = \prod_{i=1}^{m} Q_{r1}^{(i)} \prod_{i=1}^{m} Q_{r2}^{(i)}$$

két az (A)-ból származó igazi forma szorzata volna; mert $Q_{r1}^{(i)}$-gyel együtt e formák szorzata is tartalmazza a határozatlanokat.

Ezen eljárást az összes $G_1(u, v), \ldots G_s(u, v)$ formákra alkalmazva, megkapjuk $\Phi^{(i)}(u, v)$ valamennyi irreducibilis osztóját. Minden ilyen ugyanis a $G_1, \ldots, G_s$ formák valamelyikében mint osztó bennfoglaltatik.

A leírt módon talált irreducibilis $Q_r^{(i)}(u, v)\,(r=1, \ldots, s)$ osztók mind különbözők is; különben fejtegetéseink ellenére G_r és $G_{r'}$-nek közös és így G-nek többszörös osztója volna.

E szerint $\Phi^{(i)}$ minden irreducibilis osztója csak a G_r formák egyikében van benne; tehát lesz:

$$\Phi^{(i)}(u\xi_i+v) = Q_1^{(i)}(u, v) \ldots Q_s^{(i)}(u, v)$$

és végre, ha ismét azt írjuk, hogy $u\xi_i+v=x$, lesz

$$\Phi^{(i)}(x) = P_1^{(i)}(x) \ldots P_s^{(i)}(x);$$

mert, ha a jobb oldalon álló formákban v helyébe $x-u\xi_i$-t teszszük, u-nak magától ki kell esnie.

Oly $\Phi^{(i)}(x)$ formát tehát, a melynek discriminánsa a 0-tól különböző, az (A, ξ_i) genus-tartományra vonatkozólag a következő szabály szerint bonthatjuk fel tényezőkre:

Alkossuk a $\prod_{i=1}^{m} \Phi^{(i)}(u\xi_i+v) = G(u, v)$ formát, a melynek együtthatói az (A) tartományhoz tartoznak és bontsuk fel G-t az (A)-ra vonatkozólag érvényes módszerek szerint:

$$G = G_1 G_2 \ldots G_s.$$

Ha már most

$$\left(\Phi^{(i)}(u\xi_i+v), G_r(u, v)\right) \sim Q_r^{(i)}(u, v),$$

akkor lesz

$$\Phi^{(i)}(u\xi_i+v) \sim Q_1^{(i)}(u, v) \ldots Q_s^{(i)}(u, v)$$

és ha ismét azt írjuk, hogy $u\xi_i+v=x$, a keresett felbontás lesz:

$$\Phi^{(i)}(x) \sim Q_1^{(i)}(u, x-u\xi_i) \ldots Q_s^{(i)}(u, x-u\xi_i) \sim P_1^{(i)}(x) \ldots P_s^{(i)}(x).$$

18. §. A most kifejtett módszer, mely az (A, ξ_i) genus-tartományból származó $\Phi^{(i)}$ forma fölbontását adja irreducibilis tényezőkre, a formában föllépő határozatlanok számától elvileg teljesen független, a mint ez a módszer előadá-

sából világos. Még sem fölösleges annak fölemlítése, hogy mihelyt a forma egy határozatlannál többet tartalmaz, a II. fej. 4-ik §-a szerint $\Phi^{(i)}$-ről áttérhetünk a csak egy határozatlant tartalmazó $\varphi^{(i)}$-re. Ekkor $\varphi^{(i)}$-nek véges számban lévő osztói megadják $\Phi^{(i)}$ összes osztóit, tehát egyszersmind e forma fölbontását irreducibilis osztókra.

Az egy és a több határozatlant tartalmazó formák közt van azonban más fajta elvi különbség, mely még itt kifejtendő.

Valamely (A)-ból származó irreducibilis forma természetesen reducibilis lehet, vagy irreducibilis maradhat, ha más-más az (A)-ból származó (A, ξ_i) genus-tartományba megyünk át. Ha azonban a forma csak egy határozatlant tartalmaz, a megfelelő Galois-féle tartomány olyan, hogy benne ama forma minden esetre lineáris tényezőkre bomlik.

Az (A)-ból származó formát *föltétlenül irreducibilisnek* mondjuk, ha minden (A)-ból származó genus-tartományban irreducibilis marad.

Egy határozatlannak elsőnél magasabb fokú formái tehát sohasem föltétlenül irreducibilisek. Lineáris valódi formák pedig mindig föltétlenül irreducibilisek.

Ha most már valamely több határozatlant tartalmazó $\Phi^{(i)}$ forma reducibilis, akkor ugyanez áll a megfelelő, egy határozatlant tartalmazó $\varphi^{(i)}$-re nézve is; azaz a fölbontás már is a $\varphi^{(i)}=0$ egyenletnek megfelelő Galois-féle tartományban eszközölhető. Mert ekkor az irreducibilis tényezőknek szükségképen a $\varphi^{(i)}$ oly tényezői felelnek meg, melyekben a határozatlanoknak kitevői mint «magassági számok» lehetségesek.

Ha $\Phi^{(i)}$ e szerint reducibilis, fölbontása már egy bizonyos, előre meghatározott genus-tartományban eszközölhető.

Előfordulhat azonban, hogy $\varphi^{(i)}$-nek egy tényezője sem

felel meg az említett föltételnek, és ekkor $\Phi^{(i)}$ ama Galois-féle tartományban irreducibilis marad. Ekkor tehát $\Phi^{(i)}$ föltétlenül irreducibilis. Ez az eset csakugyan bárhányad fokú formáknál bekövetkezhetik, mihelyt a határozatlanok száma egynél nagyobb. Legyen pl. $F(x_1, \ldots, x_{m-1})$ valamely tetszés szerinti forma ; akkor

$$F(x_1, \ldots, x_{m-1}) + x_m$$

ilyenféle forma lesz. Minthogy ugyanis x_m-ben első fokú, mihelyt egyáltalában fölbontható, kell, hogy oly valódi osztója legyen, mely x_m-et nem tartalmazza. De ez a valódi osztó osztaná ismét x_m együtthatóját, az egységet, azaz a föltevés ellenére nem valódi osztó. Evvel a következő tételhez jutottunk :

Az (A)*-ból származó formák tartományában vannak bárhányad dimensiójú föltétlenül irreducibilis formák, melyek azonban legalább két határozatlant tartalmaznak.*

Vajjon $\Phi^{(i)}$ föltétlenül irreducibilis-e, vagy sem, azt eldöntjük az által, hogy a $\varphi^{(i)}=0$ egyenletnek megfelelő Galois-féle tartományban vizsgáljuk. $\Phi^{(i)}$ *akkor és csak akkor föltétlenül irreducibilis, ha a* $\varphi^{(i)}=0$ *értelmezte Galois-féle tartományban irreducibilis.*

19. §. Ha már most (A, ξ_i) az (A)-ban irreducibilis $F(z) = 0$ egyenlet bármely gyökével értelmezett genus-tartomány és $G_i(z) = 0$ ismét valamely az (A, ξ_i)-ben irreducibilis n-edfokú egyenlet, ennek egyik gyöke pedig η_{ij}, akkor (A, ξ_i, η_{ij}) oly genus-tartomány lesz, a melynek törzstartománya (A, ξ_i). E genus-tartomány áll az összes

$$\sum_{r=0}^{n-1} \alpha_r^{(i)} \eta_{ij}^r$$

mennyiségekből, vagy pedig, ha bevezetjük $\alpha_r^{(i)}$ részletes alakját, az összes

$$g(\xi_i, \eta_{ij}) = \sum_{s=0}^{m-1} \sum_{r=0}^{n-1} A_{rs} \xi_i^s \eta_{ij}^r$$

mennyiségekből.

Ha két új határozatlan, u és v bevezetésével az

$$u\xi_i + v\eta_{ij} \qquad (i=1, \ldots, m;\ j=1, \ldots, n)$$

formákat * alkotjuk, azt látjuk, hogy két ily forma, $u\xi_i+v\eta_{ij}$ és $u\xi_{i'}+v\eta_{i'j'}$ akkor és csak akkor lehet egyenlő, ha $i=i'$ és $j=j'$. Így tehát (a II. fej. 17. §-a szerint) két az (A) tartományhoz tartozó mennyiséget, egyebek közt két racionális és egész számot k-t és l-t úgy határozhatunk meg, hogy

$$\gamma_{ij} = k\xi_i + l\eta_{ij} \qquad (i=1, \ldots, m;\ j=1, \ldots, n)$$

mn különböző mennyiséget jelent. Ezek e szerint a

$$H(z) = \prod_{i=1}^{m} \prod_{j=1}^{n} (z-\gamma_{ij}) = 0$$

egyenletet fogják kielégíteni, a hol $H(z)$ bizonyos az (A) tartományból származó forma. $\prod_{j=1}^{n} (z-\gamma_{ij})$ ugyanis symmetrikus $\eta_{i1}, \ldots, \eta_{in}$-re nézve és így tehát az (A, ξ_i) tartomány formája; $H(z)$ pedig e szerint symmetrikus $\xi_1, \ldots, \xi_m$-re vonatkozólag.

Az (A, ξ_i, η_{ij}) tartománynak bármely $g(\xi_i, \eta_{ij})$ mennyisége tehát a

$$g(\xi_i, \eta_{ij}) = C_0 + C_1 \gamma_{ij} + \cdots + C_{mn-1} \gamma_{ij}^{mn-1} \qquad (g)$$

alakra hozható, a hol a C mennyiségek az (A) tartományhoz tartoznak. (g) ugyanis, ha $i=1, \ldots, m$; $j=1, \ldots, n$ oly egyenletrendszert képvisel, a melyből a C «ismeretlenek» mint az (A) tartomány mennyiségei adódnak ki. Minden esetre

$$\Delta C_s = \Delta_s,$$

a hol az összes $\Delta, \Delta_1, \ldots, \Delta_{mn-1}$ determinánsok a következő

* A további kifejtés e szerint az $F(z)\,G_1(z) \ldots G_m(z)=0$ egyenlet Galois-féle tartományában megy végbe.

alakúak:

$$|g_h(\xi_i, \eta_{ij})| \qquad \left(\begin{smallmatrix} h=1,\ldots,mn \\ i=1,\ldots,m;\ j=1,\ldots,n \end{smallmatrix}\right)$$

és minden esetre azt írhatjuk, hogy

$$g_h(\xi_i, \eta_{ij}) = \sum_{s=0}^{m-1} \sum_{r=0}^{n-1} A_{rs}^{(h)} \xi_i^s \eta_{ij}^r.$$

Δ itt a 0-tól különböző, mert Δ^2 a $H(z)$ discriminánsa és $H(z) = 0$ oly mn-edfokú egyenlet, a melynek mn különböző gyöke van.

$g_h(\xi_i, \eta_{ij})$ amaz előállítása után a determinánsok szorzás-tétele szerint lesz

$$|g_h(\xi_i, \eta_{ij})| = |A_{rs}^{(h)}| \, |\xi_i^s \eta_{ij}^r|$$

és $|\xi_i^s \eta_{ij}^r|$ nem 0, mert különben Δ is egyenlő volna 0-sal*. A $|\xi_i^s \eta_{ij}^r|$ elhagyása után tehát valóban lesz

$$KC_s = K_s,$$

a hol K, $K_1, \ldots, K_{mn-1}$ az (A) tartomány mennyiségeiből összeállított determinánsok és K a 0-tól különböző.

Evvel azonban be van bizonyítva, hogy *az* (A, ξ_i, η_{ij}) *genus-tartomány azonos az* (A, γ_{ij}) *genus-tartománynyal,* a mely utóbbi az (A) tartományból a $H(z) = 0$ egyenlet egyik gyökének adjunctiója révén származik. A (g) szerint ugyanis minden $g(\xi_i, \eta_j)$ mennyiség benne van (A, γ_{ij})-ben és viszont az utóbbi tartomány minden mennyisége benne van (A, ξ_i, η_{ij})-ben; mert ez az eset fennáll γ_{ij}-re nézve.

Az (A) törzstartományból származó genus-tartományok összessége tehát, a mennyiben már nem bővíthető oly egyenletek gyökeinek adjunctiójával, a melyeknek együtthatói valamely ilyen genus-tartományba tartoznak, *a mennyiségek önmagában zárt országát alkotják.*

* A $|\xi_i^s \eta_{ij}^r|$ determináns a II. fej. 12. §-ában használt módszerrel közvetetlenül kiszámítható.

A mennyiségeknek legegyszerűbb ilyen országa *az algebrai számok országa,* a mennyiben minden egyenlet, a melynek együtthatói algebrai számok az épen bebizonyítottak szerint ismét csak a szó közönséges értelmében vett (e fejezet 7. §-ában értelmezett) algebrai számokat értelmez. Ép úgy származik az *n határozatlan algebrai függvényeinek országa.*

Így tehát mondhatjuk, hogy csak «első rangú» algebrai mennyiségek (számok és függvények) vannak, ha ezt a *feleslegessé* vált elnevezést a 16. §. bevezető szavainak értelmében még ez egyszer alkalmazzuk.

Ama $H(z) = 0$ egyenlet, a mely az illető algebrai mennyiséget egyenesen mint az (A) tartományból származó mennyiséget értelmezi, az adott utasítás szerint közvetetlenül fölállítható.

Raczionális tartományok.

20. §. Legyenek

$$\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_\mu$$

valamely meghatározott holoid vagy orthoid tartomány bármely mennyiségei. Akkor $\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu$ raczionális és egész formáinak összesége — mint azt közvetetlenül látni — (valódi vagy nem valódi) holoid tartományt alkot.

Az «$\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu$ raczionális függvényeinek» összessége, azaz a két ily raczionális és egész formából alkotott hányadosok összessége, a hol csupán csak a 0 mint nevező kizárandó, az I. fej. 4. §-a szerint orthoid tartomány, a melyet Kronecker-rel az $\mathfrak{R}$ mennyiségek raczionális tartományának nevezünk és az

$$(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$$

jellel jelölünk.

Ekkor természetesen a $\sum k_g \mathfrak{R}_1^{a_1} \mathfrak{R}_2^{a_2} \ldots$ mennyiségeket

az eredetileg adott orthoid tartomány mennyiségeinek kell tekintenünk és nincsen kizárva az sem, hogy két ily mennyiség egyenlő a nélkül, hogy megfelelő együtthatóik egyenlők. Ez természetesen nem akadálya az adott megállapodásoknak; de jó lesz arra figyelnünk, hogy a nevezőkből kizárt $\sum_g k_g \mathfrak{R}_1^{a_1} \mathfrak{R}_2^{a_2} \ldots$ kifejezések azok, a melyek mint az eredeti tartomány mennyiségei 0-sal egyenlők.

Ha csak egy $\mathfrak{R}$ mennyiség van és ez 1-gyel egyenlő, akkor az így értelmezett raczionális tartomány a raczionális számok tartománya, *az absolut raczionális tartomány*, az (1).

Ha az $\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu$ mennyiségek mind határozatlanok, $\mathfrak{R}_i = x_i$, akkor nyerjük az $[[1], x_1, \ldots, x_\mu]$ holoid forma-tartomány mellérendelt orthoid tartományát, a melyet *a μ határozatlant tartalmazó természetes raczionális tartománynak nevezünk és jelképben röviden így jelölünk:*

$$(x_1, x_2, \ldots, x_\mu).$$

E megállapítások után bebizonyíthatjuk KRONECKER következő alapvető tételét:

Mindaddig, míg csak az algebrai mennyiségek elméletében megvizsgált tulajdonságok jönnek tekintetbe, azaz míg a kérdéstételben csak az eredeti holoid vagy orthoid tartománynak megfelelőleg értelmezett kapcsolatok fordulnak elő, *minden raczionális tartomány azonos bizonyos genus-tartománynyal, a mely valamely természetes raczionális tartományból származik.*

Ennek bizonyítására vizsgáljuk meg először az $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$-ben minden esetre bennfoglalt $(\mathfrak{R}_1)$ raczionális tartományt. Akkor két eset lehetséges. Az $\mathfrak{R}_1$ raczionális és egész formáiként értelmezett

$$\sum_{i=1}^{n} c_i \mathfrak{R}_1^i \qquad (n = 0, 1, \ldots)$$

mennyiségek, vagy mindannyian a 0-tól különbözők, hacsak

az összes c_i együtthatók nem mind egyenlők 0-sal; vagy pedig van köztük oly mennyiség, a mely 0-sal egyenlő a nélkül, hogy az összes együtthatók eltünnének.

Az első esetben $(\Re_1)$ minden tulajdonságában megegyezik az (x_1) természetes raczionális tartománynyal és $\Re_1$ egyszerűen határozatlan jelének tekinthető.

A második esetben bizonyos meghatározott n-re és bizonyos meghatározott raczionális és egész $c_0, \ldots, c_n$ értékrendszerre nézve

$$\sum_{i=1}^{n} c_i \Re_1^i = 0.$$

Ha a bal oldalon álló formát, mint az $\Re_1$ határozatlan formáját irreducibilis tényezőire bontjuk, ezek közül az egyiknek 0-sal kell egyenlőnek lennie; azaz $\Re_1$ algebrai szám és $(\Re_1)$ az absolut raczionális tartományból származó egyik genus-tartomány.

Ámde, minthogy a természetes raczionális tartomány is úgy fogható fel mint a belőle származó *elsőrendű genus-tartomány*, evvel a tétel *egy* $\Re_1$ *mennyiség* esetére be van bizonyítva.

Az általános eset bebizonyítása könnyen végezhető a teljes inductio segítségével. Általánosságban feltételezhetjük, hogy az $(\Re_1, \ldots, \Re_{\mu-1})$ raczionális tartomány oly genus-tartomány, a mely valamely természetes raczionális tartományból származik. E szerint $(\Re_1, \ldots, \Re_{\mu-1})$ egyszersmind orthoid tartomány is.

Most ismét csak az a két eset lehetséges, hogy a

$$\sum_{i=1}^{n} \varrho_i \Re_\mu^i \qquad (n=0, 1, \ldots)$$

formák, a melyekben a ϱ_i-k az $(\Re_1, \ldots, \Re_{m-1})$ raczionális tartományba tartozó mennyiségek vagy mindannyian a 0-tól különbözők, ha az összes ϱ_i mennyiségek nem mind zérusok, vagy pedig bizonyos meghatározott n-re és bizonyos meghatározott $\varrho_0, \ldots, \varrho_n$ értékrendszerre nézve

$$\sum_{i=1}^{n} \varrho_i \mathfrak{R}_\mu^i = 0.$$

Az első esetben $\mathfrak{R}_\mu$ minden itt tekintetbe jövő kapcsolatra nézve nem más, mint új határozatlan és $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ ismét oly genus-tartomány, a melynek törzstartománya egyszerűen az $\mathfrak{R}_\mu$ határozatlannal bővült. Az ugyanis, hogy annak az egyenletnek együtthatói, a mely a genust meghatározza, nem tartalmazzák az $\mathfrak{R}_\mu$ határozatlant, csak oly speciális körülmény, a mely a genus-tartomány értelmezésén lényegében nem változtat.

A második esetben $\mathfrak{R}_\mu$ ismét oly irreducibilis egyenlet gyöke, a melynek együtthatói az $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{\mu-1})$ genus-tartományhoz tartoznak, a mely maga valamely természetes raczionális tartományból származik; $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ tehát oly genus-tartomány, a melynek törzstartománya $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$. Akkor azonban a 19. §-ban bebizonyított tétel szerint $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ valóban oly genus-tartomány, a mely valamely természetes raczionális tartományból származik.

A mennyiben az $\mathfrak{R}$ mennyiségeket «algebrai» tulajdonságaik értelmezik, ez csak úgy lehetséges, hogy megadjuk azokat az egyenleteket, a melyeket az $\mathfrak{R}$ mennyiségek kielégítenek; még pedig úgy, hogy az $\mathfrak{R}_i$-t meghatározó egyenlet együtthatói az $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{i-1})$ raczionális tartományba tartoznak. A két eset megkülönböztetése, valamint annak a $\mathfrak{G}$ genus-tartománynak felállítása, a mely arithmetikai és algebrai kérdésekben az adott raczionális tartománynyal azonosnak tekinthető, ekkor magától adódik ki.

21. §. Az evvel elért, az algebrai mennyiségek elméletére nézve nagy jelentőségű eredményt először KRONECKERnek a «Festschrift»-ből* vett következő szavaival akarjuk jellemezni:

* A 3. §. elején.

«Az $\Re_1, \Re_2, \Re_3, \ldots$ mennyiségek, azaz a raczionális tartomány elemeinek választása magában semmi megszorításnak sincsen alávetve, de azért az algebrai mennyiségek elméletére nézve annak nincsen semmi értelme, hogy az elemek közé transcendens számokat, vagy pedig változók transcendens függvényeit is felvegyük; mert ez eredmények változatlanok maradnak, ha az ily transcendensek helyébe új független változókat teszünk. Ha ugyanis az $\Re_1, \Re_2, \Re_3, \ldots$ algebrai függvényeinek elméletébe tartozó eredményeket arra az esetre már kifejtettük, a midőn a transcendens $\Re$-eket független változókkal helyettesítettük, akkor ezen eredmények természetük és eredetük szerint az $\Re$ mennyiségeknek csak oly specialisatiója esetén változhatnak vagy módosulhatnak, a melynél ezen elemek algebrai vonatkozásai lépnek be.»

Ebből azután — az épen bebizonyított tétel szerint — ismét KRONECKER-nek az idézett helyen előforduló szavait használva, továbbá következik:

«E szerint végre oly raczionális tartományok felvételére szorítkozhatunk, a melyeknek elemei bizonyos számú változó vagy határozatlan mennyiségek, a melyekhez ezeknek még legfölebb *egy* algebrai függvénye csatlakozik. Oly $\Re$ mennyiségek hozzácsatolását, a melyek a raczionális-tartományt az algebrai meggondolásokra vonatkozólag lényegesen módosítják, GALOIS óta az adjunctio műszóval fejezzük ki. A legáltalánosabb feltevés tehát úgy fogalmazható, hogy az $\Re$ mennyiségek helyébe bizonyos számú változó teendő és ezekhez legfölebb még *egy* algebrai függvény adjungálandó. Ez magában foglalja azt az esetet is, a melyben az $\Re$ mennyiségek általában hiányzanak.»

Evvel tehát az algebrai mennyiségek elméletét az $[[1], x_1, \ldots x_m]$*-re vonatkozólag algebrai mennyiségek, azaz*

az absolut algebrai mennyiségek elméletére vezettük vissza (l. e fej. 7. §-át).

Hogy e reductio miképen alakul különösen valamely

$$F(z) = 0$$

egyenlet értelmezte mennyiségre vonatkozólag, az most még részletesebben kifejtendő.

Az F forma együtthatói minden esetre valamely meghatározott raczionális tartományhoz tartoznak, a melynek elemei gyanánt a legrosszabb esetben magukat azokat az együtthatókat tekinthetjük. E raczionális tartomány oly genus-tartomány, melynek értelmezését bizonyos

$$G(x, \mathfrak{R}_1, \mathfrak{R}_2, \ldots) = 0$$

egyenlet szolgáltatja, a hol már most $\mathfrak{R}_1, \mathfrak{R}_2, \ldots$ határozatlanokat jelentenek, a melyek a $G=0$ egyenlet együtthatóiba belépnek. Ha már most a $G=0$ egyenletnek megfelelő Galois-féle tartományt képezzük, a melyben az egyenlet gyökei $\gamma_1, \ldots, \gamma_n$ legyenek, akkor az $F=0$ egyenlet együtthatói mint $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \gamma_i$ raczionális és egész formái írhatók. Legyen az így felírt egyenlet $F_i(z) = 0$, akkor minden gyöke egyszersmind gyöke lesz a

$$\prod_{i=1}^{n} F_i(z) = 0$$

egyenletnek is és így tehát értelmezését oly egyenletből is nyeri, a melynek együtthatói a természetes $(\mathfrak{R}_1, \mathfrak{R}_2, \ldots)$ raczionális tartományhoz tartoznak.

E fejtegetés a III. fej. 20. §-a szerint közvetlenül oly mennyiségekre is átvihető, a melyek mint bármely egyenletrendszer gyökei vannak értelmezve; ezt azonban későbbi helynek tartjuk fenn (V. fej. 7. §), a hol az ú. n. eliminációproblémák belső összefüggésük szerint lesznek tárgyalandók.

Ha valamely orthoid tartomány mennyiségeit nem algebrai módszerek, hanem más fogalomalkotások határozzák

meg, így pl. ha az analizis ú. n. határértékeivel van dolgunk, akkor az a kérdés, vajjon az ilyen határérték algebrai mennyiség-e, természetesen teljesen az algebrai módszerek keretén kívül áll. Az oly mennyiséget, a mely nem algebrai, *transcendensnek* nevezzük. E kérdéstétel a mathematika legnehezebb problémáira vezet; így pl. csak a legújabb időben állapította meg HERMITE (1873.) az e és LINDEMANN (1882.) a π transcendens jellemét.

Ha valamely szám transcendens jellemét úgy, mint e esetében már kimutattuk, akkor avval bármely egyenletrendszerben teljesen ép úgy kell elbánnunk, mint ha határozatlan volna; ha azonban valamely egyenletrendszerben e és π fordulnának elő, még mindig fenmarad az a kérdés, vajjon π és e nem állanak-e egymással «algebrai kapcsolatban», azaz nem áll-e fenn talán oly $\sum_{r=0}^{m} \sum_{s=0}^{n} k_{rs} e^r \pi^s = 0$ egyenlet, a melynek együtthatói egész számok?

22. §. Ha $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ valamely raczionális tartomány, akkor összes mennyiségei az

$$r_0 \omega_0 + r_1 \omega_1 + \cdots + r_{n-1} \omega_{n-1}$$

alakra hozhatók, a hol az r_i-k bizonyos $(x_1, \ldots, x_m)$ természetes raczionális tartományhoz tartoznak. Erre $x_1, \ldots, x_m$ gyanánt csak azokat az $\mathfrak{R}$ mennyiségeket kell választanunk, a melyek határozatlanoknak megmaradnak, ha a raczionális tartományt mint genus-tartományt fogjuk fel, ω_i helyébe pedig γ^i-t kell tennünk, ha γ annak az n-edfokú irreducibilis

$$F(z; x_1, \ldots, x_m) = 0$$

egyenletnek gyöke, a mely ama genus-tartományt értelmezi.

Hogy ily $\omega_0, \omega_1, \ldots, \omega_{n-1}$ értékrendszer végtelen sokféle módon választható, az közvetlenül belátható. Így pl. ha

$$\omega_h = \sum_{k=0}^{n-1} r_{hk} \gamma^k, \qquad (h=0, 1, \ldots, n-1),$$

ω_h $(h=0, \ldots, n-1)$ mindig ilyen értékrendszer lesz, ha az r_{hk}

mennyiségek a természetes $(x_1, \ldots, x_m)$ raczionális-tartományhoz tartoznak és $|r_{hk}|$ determinánsuk a 0-tól különböző.

Ez az előállítás, a melyet a következőkben folyton használunk, különösen azért fontos, mert a raczionális tartományra nézve jellemző, t. i. megengedi a következő megfordítást:

Ha valamely orthoid tartomány összes mennyiségei az

$$r_0\omega_0 + \cdots + r_{n-1}\omega_{n-1}$$

alakban állíthatók elő, a hol az r-ek valamely természetes raczionális tartományhoz tartoznak, akkor amaz orthoid tartomány raczionális tartomány.

Ha ω ugyanis az orthoid tartomány bármely mennyisége, akkor a feltevés szerint

$$\omega\omega_h = \sum_{k=0}^{n-1} r_{hk}\omega_k \qquad (h=0, \ldots, n-1)$$

oly egyenletrendszer, a mely a

$$\sum_{k=0}^{n-1}(r_{hk} - \delta_{hk}\omega)\omega_k = 0 \qquad (h=0, \ldots, n-1)$$

alakban is írható, a hol úgy, mint előbbi esetekben $\delta_{hh}=1$ és $\delta_{hk}=0, (h\neq k)$. Minthogy az orthoid tartomány az 1-et is tartalmazza és így az ω_k mennyiségek nem tünhetnek el mind, szükséges, hogy az

$$|r_{hk} - \delta_{hk}\omega|$$

determináns egyenlő legyen 0-sal, azaz az ω mennyiség kielégítse az

$$|r_{hk} - \delta_{hk}\omega| = 0$$

egyenletet, a melynek együtthatói a természetes $(x_1, \ldots x_m)$ raczionális tartományhoz tartoznak. Ez így van minden egyes $\omega_0, \omega_1, \ldots, \omega_{n-1}$ mennyiségre is. Amaz orthoid tartomány tehát az $(x_1, \ldots, x_m, \omega_0, \ldots, \omega_{n-1})$ raczionális tartománynyal azonos.

Ebből egyszersmind kiadódik az $\omega_0, \ldots, \omega_{n-1}$ elemek

szükséges legkisebb száma. Mert, ha a raczionális tartomány, mint a természetes $(x_1, \ldots, x_m)$ *raczionális tartományból származó genus-tartomány s-edrendü, akkor van oly* $\omega_i = \gamma^i$ $(i = 0, 1, \ldots, s-1)$ *rendszer, a mely már a követelményeknek megfelel; de egyetlen olyan a követelményeknek megfelelő rendszer sem lehetséges, mely ennél kevesebb elemet tartalmazna.*

E tétel első része e § bevezető szavai alapján közvetetlenül belátható. Ha azonban volna oly megfelelő $\omega_0', \ldots, \omega_{r-1}'$ rendszer, a hol $r<s$, a tartomány minden egyes mennyiségének oly r-edfokú egyenletet kellene kielégítenie, a melynek együtthatói $(x_1, \ldots, x_m)$-hez tartoznak; míg γ a tartomány oly mennyisége, a mely bizonyos irreducibilis s-edfokú egyenletet kielégít $(s>r)$ és így nem elégíthet ki hasonló r-edfokú egyenletet.

Az $\omega_0, \omega_1, \ldots, \omega_{k-1}$ *elemek szükséges legkisebb száma tehát egyszerüen a raczionális tartomány rendszáma, ha azt valamely természetes raczionális tartományból származó genus-tartománynak tekintjük.*

Minden oly $\omega_0, \omega_1, \ldots$ értékrendszer, a melyben az elemek száma a legkisebbre van visszavezetve, *a raczionális tartomány basisa**. Evvel a «raczionális tartomány» elnevezés új, mélyebbreható jelentést nyer. Most ugyanis annak mennyiségeit — a szó absolut értelmében vett — raczionális mennyiségek $(r_0, r_1, \ldots, r_{n-1})$ complexusaiként értelmezhetjük és ezeknek összefoglalása orthoid tartománynyá oly kapcsolatok segítségével történik, a melyek kizárólag e complexusokra vonatkoznak, habár az $r_0\omega_0 + \cdots + r_{n-1}\omega_{n-1}$ írásmódhoz rövidebben és kényelmesebben csatlakoznak. És ezután *az algebrai mennyiségek elmélete elvileg nem más*

* Dirichlet-Dedekind, Zahlentheorie, IV. kiad. 468. l.

mint valamely természetes raczionális tartományból származó mennyiségek complexusainak elmélete.

A mondottakkal szemben még meg kell jegyeznünk, hogy az algebrai mennyiségeknek raczionális tartományokban való összefoglalásának határt szab az a körülmény, hogy a mennyiségek ama complexusai bizonyos meghatározott, ha még oly nagy, de véges számú elemből állanak. *Igy az algebrai számok összessége alkot ugyan orthoid tartományt, de többé nem raczionális tartományt.* Ha az ilyen volna, akkor e raczionális tartománynak, mint genus-tartománynak rendszáma bizonyos meghatározott szám, n volna és minden algebrai szám kielégítene oly egyenletet, a melynek együtthatói raczionális és egész számok és foka n valamely osztója. Ámde vannak algebrai számok, a melyeket (e fej. 4. §-a szerint) bármily magas N-edfokú irreducibilis egyenletek értelmeznek, a mivel állításunk be van bizonyítva.

E szerint az orthoid tartomány fogalma sokkal bővebb, mint a raczionális tartományé. Azt még oly fogalomalkotások *sem* merítik ki, mint a milyen az algebrai számok, vagy pedig az algebrai függvények országa. Az analizisben tárgyalt valós számok összessége vagy a complex számoké is orthoid tartomány.

Itt helyén lesz, hogy megemlítsük még a DEDEKIND-től származó «test» elnevezést is, a melyet gyakran, bár helytelenül a KRONECKER-féle raczionális tartománynyal egyenlő értelműnek tekintenek.

DEDEKIND definicziója szerint* «a valós vagy complex a számok valamely A rendszerét testnek nevezzük, ha az a számok közül bármely kettőnek összege, különbsége, szorzata és hányadosa is ugyanazon A rendszerhez tartozik».

* Az i. h. 452. l.

Eltekintve a DEDEKIND részéről magától értetődőnek tekintett vonatkozástól az összeadás és szorzás valamely «közönséges» törvényére, a «test» definicziója, noha bizonyos módszertani különbségekkel, lényegében ugyanaz, mint az orthoid tartományé. Hogy mégis ezt az utóbbi, bár új kifejezést kellett választanom, szükséges következménye volt annak az elmélet rendszeres felépítésénél elkerülhetetlen körülménynek, hogy a holoid és orthoid tartomány kezdettől fogva elvileg egymással szembe állítandó és hogy e párhuzamos elnevezésből legvilágosabban tünik ki, hogy miként vettük belé definicziójukba a raczionális egész, ill. a raczionális számok tartományának lényeges tulajdonságait. Ezen kívül még tekintettel kellett lennünk az összhangzásra a további következetes KRONECKER-féle terminologiával.

Galois elve.

23. §. Legyen $F(z) = 0$ oly n-edfokú egyenlet, a melynek együtthatói valamely tetszés szerinti raczionális tartományhoz tartoznak és a melynek discriminánsa a 0-tól különböző. Gyökei a megfelelő adjunctio révén származott GALOIS-féle tartományban legyenek $\xi_1, \ldots, \xi_n$, a feltevés szerint e tartomány n különböző mennyisége.

Ha az $1, \ldots, n$ számok összes $i_1, \ldots, i_n$ permutáczióira kiterjesztett

$$\prod_{(i)} (x - u_1 \xi_{i_1} - u_2 \xi_{i_2} - \cdots - u_n \xi_{i_n})$$

szorzatot alkotjuk, ez a $\xi_1, \ldots, \xi_n$ mennyiségek symmetrikus formája, tehát az $x, u_1, \ldots, u_n$ határozatlanoknak oly formája lesz, a melynek együtthatói az adott raczionális tartományhoz tartoznak. Mint ilyen, irreducibilis tényezőire felbontva, legyen az:

$$G(x; u_1, \ldots, u_n) = G_1(x; u_1, \ldots, u_n) G_2(x; u_1, \ldots, u_n) \ldots$$

A puszta megtekintés mutatja, hogy az $1, \ldots, n$ számok összes $j_1, \ldots, j_n$ permutációira kiterjesztett

$$\prod_{(j)} (x - u_{j_1}\xi_1 - u_{j_2}\xi_2 - \cdots - u_{j_n}\xi_n)$$

szorzat az előbbivel azonos; hogy tehát $G(x; u_1, \ldots, u_n)$ az $u_1, \ldots, u_n$ határozatlanoknak is symmetrikus formája. De akkor egyszersmind lesz

$$G(x; u_{r_1}, \ldots, u_{r_n}) = G_1(x; u_{r_1}, \ldots, u_{r_n})\, G_2(x; u_{r_1}, \ldots, u_{r_n}) \cdots =$$
$$= G(x; u_{s_1}, \ldots, u_{s_n}) = G_1(x; u_{s_1}, \ldots, u_{s_n})\, G_2(x; u_{s_1}, \ldots, u_{s_n}) \cdots$$

és a jobb oldalon álló szorzatok újból szolgáltatják a felbontást irreducibilis tényezőkre, minthogy azok a $G_1(x; u_1, \ldots, u_n), \ldots$ tényezőktől csakis a határozatlanok elnevezésében különböznek. A $G_1, G_2, \ldots$ tényezők dimensiója különben a 12. §. szerint egyenlő.

Legyenek

$$x - u_{r_1}\xi_1 - u_{r_2}\xi_2 - \cdots - u_{r_n}\xi_n$$
$$x - u_{s_1}\xi_1 - u_{s_2}\xi_2 - \cdots - u_{s_n}\xi_n$$
$$\ldots\ldots\ldots\ldots$$

bármely oly lineáris tényezők, a melyek ugyanahhoz, az eredeti raczionális tartományban irreducibilis tényezőhöz, pl. G_1-hez tartoznak. (A határeset, a melyben e tényezők mindegyikének dimensiója 1, később könnyen lesz elintézhető.) Akkor szükségképen lesz

$$G_1(x; u_{r_1}, \ldots, u_{r_n}) = G_1(x; u_{s_1}, \ldots, u_{s_n}) = \cdots, \qquad (1)$$

mert kettő-kettőnek resultánsa zérus, míg e formák maguk irreducibilisek és (x-ben) legmagasabb tagjaik megegyezők.

Ha tehát G_1 dimensiója pl. k, akkor az $u_1, \ldots, u_n$ mennyiségeknek oly k permutációja van:

$$\begin{matrix} u_{r_1}, \ldots, u_{r_n} \\ u_{s_1}, \ldots, u_{s_n} \\ \ldots\ldots \end{matrix} \qquad (P)$$

«a melyekre nézve a G_1 forma változatlan marad». Így akarjuk ugyanis az (1)-ben részletesen definiált tulajdonságot röviden kifejezni. Ha az $F(u_1, \ldots, u_n)$ formában $u_{r_1}, \ldots, u_{r_n}$ helyébe rendre $u_{s_1}, \ldots, u_{s_n}$-t teszszük, ez meghatározott és az F formán könnyen elvégezhető «művelet», a melyet *substitutiónak* fogunk nevezni; jelölésére szolgáljon:

$$S_{rs} = \begin{pmatrix} u_{r_1}, \ldots, u_{r_n} \\ u_{s_1}, \ldots, u_{s_n} \end{pmatrix}.$$

Ha az S_{rs} substitutiót elvégezzük az F formán, az eredmény új forma, a melyet röviden $S_{rs}F$-fel jelölünk. Ha már most

$$S_{st} = \begin{pmatrix} u_{s_1}, \ldots, u_{s_n} \\ u_{t_1}, \ldots, u_{t_n} \end{pmatrix}$$

valamely második substitutio, akkor a kettőt egymásután is végezhetjük, azaz az $S_{rs}F$ formán ismét az S_{st} substitutiót végezhetjük; világos, hogy a változást, a melyet ez okozott F-ben, egyszerre is előidézhető az

$$S_{rt} = \begin{pmatrix} u_{r_1}, \ldots, u_{r_n} \\ u_{t_1}, \ldots, u_{t_n} \end{pmatrix}$$

substitutióval. Ennek megfelelőleg írjuk, hogy

$$S_{rt} = S_{st} S_{rs},$$

a hol a jobb oldalon álló substitutiókat abban a sorrendben kell elvégeznünk, a mint azok jobbról bal felé egymásra következnek. E symbolikus egyenlet jelentése egyszerűen az, hogy bármely $F(u_1, \ldots, u_n)$ forma esetében lesz

$$S_{rt} F = S_{st}(S_{rs} F).$$

Itt $S_{st} S_{rs}$-et *az* S_{st} és S_{rs} *substitutiók egymásutánjának* vagy pedig *szorzatának* is nevezzük. Ha azonban ezt az általánosan szokásos «szorzat» elnevezést használjuk, arra kell ügyelnünk, hogy a tényezők sorrendje általánosságban *nem* változtatható.

A G_1 forma ama tulajdonságát e szerint így is fejezhetjük ki, hogy *az nem változik egyetlen oly substitutióra*

nézve sem, a mely úgy származik, ha a substitutiók jelölésére bevezetett symbolumban első és második sorként a (P) permutációk közül bármely kettőt alkalmazunk. *E substitutiók csoportot alkotnak,* a mely kifejezéssel röviden a substitutiók e sorozatának azt a tulajdonságát akarjuk jellemezni, hogy *közülük bármely kettőnek szorzata ismét benne van a sorozatban.* E tulajdonság fennállása kitünik abból a megjegyzésből, hogy ily szorzat minden esetre oly substitutiót szolgáltat, a mely G_1-et nem változtatja, míg másrészt minden substitutiónak, a mely G_1-et nem változtatja, a sorozatban benne kell lennie. Ennek az utóbbi állításnak helyessége is igen könnyen kimutatható, mert arra, hogy bizonyos substitutio alkalmazása mellett G_1 változatlan maradjon, szükséges, hogy ennek minden $x - u_{r_1}\xi_1 - \cdots - u_{r_n}\xi_n$ lineáris tényezője valamely más lineáris tényezőjébe, például $x - u_{s_1}\xi_1 - \cdots - u_{s_n}\xi_n$-be menjen át, úgy hogy ama substitutiónak S_{rs} alakúnak kell lennie.

Ennek megfelelőleg azt is mondjuk, hogy a (P) permutációk csoportot alkotnak.

Ez a fejtegetés tehát *az adott raczionális tartományból származó oly formához vezet, a mely az S_{rs} substitutiók csoportjára nézve, még pedig csakis e substitutiókra nézve marad változatlan.*

Most már G_1-be x helyébe az eredeti raczionális tartományhoz tartozó akárhány mennyiséget, sőt raczionális és egész a számokat is helyettesíthetünk úgy, hogy a *speciális*

$$G_1(a; u_1, \ldots, u_n) = \Gamma_1(u_1, \ldots, u_n)$$

forma pontosan ugyanazt a tulajdonságot mutatja. Hogy Γ_1 valamely substitutióra nézve nem változik, ha G_1 így viselkedik, az közvetetlenül világos. Ha azonban valamely S_{rs} substitutióra nézve volna

$$S_{rs}\Gamma_1 = \Gamma_1$$

a nélkül, hogy

$$S_{rs} G_1 = G_1,$$

akkor $S_{rs} G_1 - G_1$ az u-k oly formája, a melynek együtthatói abban a felfogásban, hogy x egész függvényei, nem tünnek el mind. Minthogy a substitutiók száma meghatározott és véges, x számára meghatározhatunk oly a értékeket, hogy $S_{rs} \Gamma_1 - \Gamma_1$ csak akkor legyen különböző a 0-tól, ha ez az eset $S_{rs} G_1 - G_1$-re nézve is fennáll. Evvel azonban állításunk be van bizonyítva.

24. §. A Γ_1 minden lineáris tényezője,

$$L = a - u_{t_1} \xi_1 - u_{t_2} \xi_2 - \cdots - u_{t_n} \xi_n$$

egyszersmind az

$$a - u_{r_1} \xi_{\varrho_1} - u_{r_2} \xi_{\varrho_2} - \cdots - u_{r_n} \xi_{\varrho_n},$$

vagy

$$a - u_{s_1} \xi_{\sigma_1} - u_{s_2} \xi_{\sigma_2} - \cdots - u_{s_n} \xi_{\sigma_n},$$

két alak bármelyikében írható és az u határozatlanokon elvégzett S_{rs} substitutio szolgáltatja, hogy

$$S_{rs} L = a - u_{s_1} \xi_{\varrho_1} - u_{s_2} \xi_{\varrho_2} - \cdots - u_{s_n} \xi_{\varrho_n}.$$

A ξ mennyiségeken elvégzendő substitutiókat hasonló módon jelölhetjük. Legyen

$$\Sigma_{\varrho\sigma} = \begin{pmatrix} \xi_{\varrho_1}, \xi_{\varrho_2}, \ldots, \xi_{\varrho_n} \\ \xi_{\sigma_1}, \xi_{\sigma_2}, \ldots, \xi_{\sigma_n} \end{pmatrix},$$

akkor ép úgy lesz

$$\Sigma_{\sigma\varrho} = \begin{pmatrix} \xi_{\sigma_1}, \xi_{\sigma_2}, \ldots, \xi_{\sigma_n} \\ \xi_{\varrho_1}, \xi_{\varrho_2}, \ldots, \xi_{\varrho_n} \end{pmatrix}$$

és $\Sigma_{\sigma\varrho} \Sigma_{\varrho\sigma}$ — mint az szembeötlő — az ú. n. azonos *(identikus) substitutio* lesz, azaz olyan, mely minden elemet meghagy a maga helyén. A két *(invers)* substitutio e magatartását czélszerűen a

$$\Sigma_{\sigma\varrho} \Sigma_{\varrho\sigma} = 1$$

symbolikus egyenlettel jellemezzük. E jelölést használva, lesz

$$\Sigma_{\varrho\sigma} S_{rs} L = L,$$

vagy ha mind a két oldalon a $\Sigma_{\sigma\varrho}$ substitutiót alkalmazzuk,

$$S_{rs} L = \Sigma_{\sigma\varrho} L.$$

Azokat a változásokat tehát, a melyeket Γ_1-ben az u-k substitutióival előidéztünk, előidézhetjük a ξ-k substitutióival is és viszont, még pedig e substitutiók kölcsönösen egyértelmű módon határozzák meg egymást. Két S substitutio szorzatának megfelel a megfelelő Σ-k szorzata és az S-ek csoportjának a Σ-k csoportja.

A Γ_1 forma tehát változatlan marad az összes $\Sigma_{\varrho\sigma}, \ldots$ substitutiókra és csak ezekre nézve. E substitutiók csoportot alkotnak és számuk ugyanaz, mint az S_{rs}-eké.

Valamely csoport rendszáma az abban foglalt substitutiók száma, a melybe az «azonos» substitutiót is mindig belé kell számítanunk.

Az S_{rs} valamint a $\Sigma_{\sigma\varrho}$ substitutiók csoportjának rendszáma k és k egyszerűen G_1-nek dimensiója, vagy pedig a (P) permutáczióinak száma. Mert van egy oly substitutio, a mely az egyik meghatározott lineáris tényezőt átvezeti valamely tetszés szerinti másodikba és ilyen csak egy van, a substitutio evvel teljesen meg lévén határozva. A csoportban tehát ép annyi substitutio van, mint a hány permutáczió (P)-ben.

Végül, ha most Γ_1-et, hogy benne a ξ-k fellépését jelezzük, így írjuk: $\Gamma_1(u_1, \ldots, u_n, \xi_1, \ldots, \xi_n)$, akkor az $u_1, \ldots, u_n$ mennyiségek helyébe ismét a raczionális tartományhoz tartozó mennyiségeket, sőt raczionális és egész számokat is helyettesíthetünk úgy, hogy $\Gamma_1(a_1, \ldots, a_n, \xi_1, \ldots, \xi_n)$ a $\Sigma_{\sigma\varrho}$ substitutiókra nézve és csak ezekre nézve ne változzék. Ez pontosan ugyanazokkal a szavakkal bizonyítható be, mint az előbbi §. végén foglalt állítás.

Bármely egyenletnek tehát, a melynek együtthatói va-

lamely meghatározott raczionális tartományhoz tartoznak, a leírt módon megfelel az oly substitutiók bizonyos meghatározott «charakteristikus csoportja», a melyeknek elemeiként az u határozatlanok, vagy pedig az egyenlet gyökei, a ξ-k szerepelnek; továbbá van módszerünk az u határozatlanok, valamint a ξ gyökök oly meghatározott formáinak alkotására, melyeknek együtthatói az eredeti raczionális tartományhoz tartoznak és a melyek a charakteristikus csoporthoz tartozó substitutiókra és csak e substitutiókra nézve változatlanok maradnak.

Az így kimondott tétel az algebrai egyenletek elméletének *Galois-féle elve**, a mely legelőször vezetett az ebben az elméletben fellépő problémák és módszerek teljes fölismeréséhez. A tételnek az a fogalmazása, a mely a ξ gyökökre vonatkozik, az eredeti, és még Galois-tól származik; az a fogalmazás, a melyben csak az *u* határozatlanok lépnek fel, a mi a tételt teljesen a raczionális tartományokból származó formák elméletébe vonja be, Kronecker-től ered.

25. §. A substitutiók ama $\Sigma_{\varrho\sigma}$ csoportját, a melyről a Galois-féle elv szól, a következő tény teszi alapvető jelentőségűvé:

Ha φ bizonyos határozatlanoknak és a $\xi_1, \ldots, \xi_n$ gyököknek valamely az adott raczionális tartományból származó formája, azaz valamely ily alakú mennyiség:

$$\varphi = \sum_{(k)} c_k \xi_1^{k_1} \xi_2^{k_2} \ldots \xi_n^{k_n},$$

a hol a c_k-k a raczionális tartományból származó formák, akkor a φ mennyiség akkor és csak akkor lesz a raczionális tartományból származó forma, ha a $\Sigma_{\varrho\sigma}$ substitutio-csoportra nézve változatlan marad.

* Kronecker, Festschrift § 4.

Ha e fej. 11. §-a értelmében alkotjuk az $F(z) = 0$ egyenlet Galois-féle resolvensét úgy, hogy az u-kat határozatlanoknak hagyjuk meg, és azt az irreducibilis tényezőt választjuk, a mely az $x - u_1 \xi_{\varrho_1} - \cdots - u_n \xi_{\varrho_n}$ lineáris tényezőt tartalmazza, akkor az a forma, a mely ennek az egyenletnek bal oldalán áll, lesz

$$G_1(x, u_1, \ldots, u_n) = \Pi(x - u_1 \xi_{i_1} - \cdots - u_n \xi_{i_n}),$$

a hol a szorzás kiterjesztendő mindazokra a permutációkra, a melyek $\varrho_1, \ldots, \varrho_n$-ből a $\Sigma_{\varrho\sigma}$ substitutiók csoportjának alkalmazása révén származnak. Itt G_1 *csak* e csoport substitutióira nézve marad változatlan; mert minden más substitutio behoz legalább is egy oly lineáris tényezőt, a melyet G valamely más irreducibilis tényezője tartalmaz.

Ha már most φ a $\Sigma_{\varrho\sigma}$ substitutiók csoportjára nézve változatlan, tehát

$$\varphi(\xi_{\varrho_1}, \ldots, \xi_{\varrho_n}) = \varphi(\xi_{\sigma_1}, \ldots, \xi_{\sigma_n}) = \cdots,$$

akkor a 10. §. szerint minden esetre $\xi_{\varrho_1}, \ldots, \xi_{\varrho_n}$ és így φ is azonosan a

$$\Theta^l \varphi(\xi_{\varrho_1}, \ldots, \xi_{\varrho_n}) = H(u_1 \xi_{\varrho_1} + \cdots + u_n \xi_{\varrho_n}) \qquad (\varphi)$$

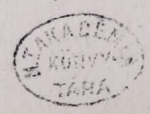
alakban állítható elő, a hol úgy, mint az idézett helyen

$$\Theta = \pm \Delta^k U_t + \cdots$$

és $\Delta = \mathrm{Dscr.}\ F$, míg $H(z)$ a $z, u_1, \ldots, u_n$-nek az adott raczionális tartományból származó bizonyos formája. Amaz identitás származása szerint azonban érvényes marad, ha $\varrho_1, \ldots, \varrho_n$ helyébe bármely más permutációt teszünk. Ha tehát az összeadást a csoport összes permutációira kiterjesztjük, akkor, minthogy a feltevés szerint φ változatlan marad, lesz

$$k\Theta^l \varphi = \sum_{(\varrho)} H(u_1 \xi_{\varrho_1} + \cdots + u_n \xi_{\varrho_n}).$$

A jobb oldalon álló összeg azonban a Galois-féle resolvens gyökeiben symmetrikus és így tehát a raczionális tartomány-



ból származó forma. Ha tehát φ a $z, u_1, \ldots, u_n$ határozatlanokat nem tartalmazza, φ-t az U_t-k együtthatóinak összehasonlitása révén mint a raczionális tartomány mennyiségét nyerjük. Ha ellenben φ e határozatlanok, vagy más határozatlanok formája, abban minden egyes hatványszorzat együtthatójának a $\Sigma_{\varrho\sigma}$ substitutiókra nézve változatlannak kell maradnia és φ akkor is a határozatlanoknak a raczionális tartományból származó formája lesz.

Ha viszont φ a raczionális tartományhoz tartozó forma, akkor a (φ) identitás miatt

$$\theta^l \varphi = H(z)$$

oly egyenlet, a melyet az irreducibilis Galois-féle resolvens $u_1 \xi_{\varrho_1} + \cdots + u_n \xi_{\varrho_n}$ gyöke kielégít. Azt tehát ennek minden más gyöke is ki fogja elégíteni és azonosan lesz

$$\theta^l \varphi = H(u_1 \xi_{\varrho_1} + \cdots + u_n \xi_{\varrho_n}) = H(u_1 \xi_{\sigma_1} + \cdots + u_n \xi_{\sigma_n}) = \cdots;$$

φ tehát a $\Sigma_{\varrho\sigma}$ substitutiók csoportjára nézve változatlan marad, a mivel a kimondott tétel be van bizonyítva. Abban a határesetben, a melyben a Galois-féle resolvens elsőfokú, a $\Sigma_{\varrho\sigma}$ substitutiók csoportja az egyetlen azonos substitutióból áll és az $F(z) = 0$ egyenlet minden gyöke, valamint minden φ forma az adott raczionális tartományból származik.

A most bebizonyított tétel közvetetlen folyománya, hogy *egy és csak egy ily charakteristikus csoport van.* Képezésénél tehát a Galois-féle resolvens bármely irreducibilis tényezőjéből indulhatunk ki.

26. §. *Általános n-edfokú egyenletnek* nevezzük az

$$F(z) = z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

egyenletet, ha az összes a együtthatók egymástól független határozatlanok és az F forma tehát az $(a_1, \ldots, a_n)$ raczionális tartományból származik.

Az általános n-edfokú egyenlet charakteristiksu csoportja a legáltalánosabb, a melyet a $\xi_1, \ldots \xi_n$ *gyökökből alkothatunk,* azaz tartalmazza az összes substitutiókat, a melyekkel $\xi_1, \ldots, \xi_n$-t bármely más permutációba vezethetjük át, úgy hogy rendszáma $n!$

Hogy ezt bebizonyítsuk, csak meg kell mutatnunk, hogy, ha φ a $\xi_1, \ldots, \xi_n$ mennyiségeknek az $(a_1, \ldots, a_n)$ raczionális tartományból származó formája a nélkül, hogy a ξ gyökökben symmetrikus volna, akkor φ nem lehet a raczionális tartományból származó forma. Az ellenkező állítást az

$$A\varphi - B = 0$$

alakban írhatnók, a hol A és B az $a_1, \ldots, a_n$ és az esetleg φ-ben előforduló határozatlanok raczionális és egész formái.

Ha $A\varphi - B$-ben $a_1, \ldots, a_n$ helyébe $\xi_1, \ldots, \xi_n$ elemi symmetrikus formáit teszszük, akkor $A\varphi - B$ a ξ-k oly formájába megy át, a mely — a mennyiben ezeket határozatlanoknak fogjuk fel — nem lesz 0, mert B symmetrikus formájuk, míg $A\varphi$-re a feltevés szerint ez nem áll. Ugyanaz megtartja érvényességét, ha $\xi_1, \ldots, \xi_n$ helyébe e mennyiségek bármely más permutációját teszszük. Ha a φ-ből így származó formákat $\varphi_1, \varphi_2, \ldots$-nek írjuk, akkor

$$\Pi(A\varphi_i - B)$$

sem fog eltünni, ha e szorzatot mint a ξ_i-k formáját fogjuk fel és akkor sem, ha a ξ_i-k helyébe bevezetjük az a_i-ket, a mi teljességben történhetik, mert ama szorzat — mint az közvetetlenül szembeötlő — a ξ_i-kben symmetrikus. Másrészt azonban az $A\varphi_1 - B = 0$ feltevés értelmében ama szorzatnak zérussal egyenlőnek kell lennie. Igy tehát bizonyos

$$\sum_{(g)} k_g A_g = 0$$

egyenlethez jutnánk, a melyben a k_g-k egész számokat és az A_g-k az a_i-k hatványszorzatait jelentik. Ez pedig ellenkezik

ama föltevéssel, hogy az a-k egymástól független határozatlanok.

Az eddig kifejtett alaptételeken épül fel azután az algebrai egyenleteknek nagy fontosságú GALOIS-féle elmélete. Itt csak azt akartuk megmutatni, hogy az mikép lép vonatkozásba az algebrai mennyiségek általános elméletével; a fontos specziális problémák részletezése, a melyeket abban fejtegetnek, e tárgyalás tervén kívül áll *.

Gauss alaptétele.

27. §. E fejezet függelékeképen még ki kell fejtenünk, hogy az algebrai mennyiségek elmélete miképen lép vonatkozásba az «algebra ú. n. alaptételével». Ezt a vonatkozást bizonyos identitás közvetíti, a melyet GAUSS egyik híres értekezésében állított fel **.

Legyen $F(z) = 0$ oly n-edfokú egyenlet, a melynek együtthatói valamely tetszés szerint adott orthoid tartományhoz tartoznak, discriminánsa pedig legyen a 0-tól különböző. Ha a megfelelő GALOIS-féle tartományt alkotjuk, az egyenletnek ebben n különböző gyöke lesz, a melyeket $\xi_1, \ldots, \xi_n$-nel fogunk jelölni. Akkor

* Annál is inkább, mert erre az elméletre a kiváló tankönyvek egész sora áll rendelkezésre és a KRONECKER-féle előadások is, a melyek kiadása legközelebb várható, részletesen foglalkoznak ezen elmélettel. Még meg kell említenünk KLEIN FÉLIX «Vorlesungen über das Ikosæder» és «Vorlesungen über die Theorie der elliptischen Modulfunctionen» cz. műveit, a melyek különösen az algebrai problémáknak más mathematikai disciplinákra való vonatkozásait hangsulyozzák és igen elegáns alakban tárgyalják.

** Demonstratio nova altera etc. Werke III. köt. GAUSS-nak ez az értekezése volt a legelső és classikus minta az algebrai mennyiségek elméletének következetes kifejtésére.

$$u(\xi_i + \xi_j) + v\xi_i\xi_j$$

az u és v oly formája lesz, a mely a ξ-k felcserélése révén — a mint az közvetetlenül szembeötlő — felvesz $\frac{n(n-1)}{2}$ értéket, a melyek az $1, \ldots, n$ számokból alkotható ugyanannyi (i, j) combinatiónak felelnek meg. Ezek az értékek is mind különbözők, mert csak akkor lehet, hogy

$$u(\xi_i+\xi_j) + v\xi_i\xi_j = u(\xi_{i'}+\xi_{j'}) + v\xi_{i'}\xi_{j'},$$

ha

$$\xi_i + \xi_j = \xi_{i'} + \xi_{j'},\ \xi_i\xi_j = \xi_{i'}\xi_{j'}$$

és így egyszersmind

$$(z-\xi_i)(z-\xi_j) = (z-\xi_{i'})(z-\xi_{j'}).$$

Erre pedig szükséges, hogy az (i, j) számpár megegyezzék az (i', j') számpárral, a mit épen kizártunk.

Az összes (i, j) combinatiókra kiterjesztett

$$\prod_{(i,j)} (x - u(\xi_i + \xi_j) + v\xi_i\xi_j)$$

szorzat tehát a ξ-k symmetrikus formája és így az x, u és v határozatlanoknak az adott orthoid tartományból származó formája, a melyet $G(x, u, v)$-vel fogunk jelölni. Az $\frac{n(n-1)}{2}$-edfokú

$$G(x, u, v) = 0$$

egyenletnek tehát $\frac{n(n-1)}{2}$ gyöke van; ezek az $u(\xi_i + \xi_j) + v\xi_i\xi_j$ mennyiségek, a melyek mind egymástól különbözők és u és v helyébe tehetünk raczionális és egész számokat is a nélkül, hogy ezek a viszonyok megváltoznának. G-nek x-re vonatkozó discriminánsa ugyanis az u és v határozatlanoknak a 0-tól különböző formája; így tehát u és v gyanánt csak oly egész számokat kell választanunk, a melyekre nézve e formából valamely a 0-tól különböző mennyiség származik.

Legyen már most a és b két ily módon választott szám és rövidség kedvéért

$$\eta_{ij} = a(\xi_i + \xi_j) + b\xi_i\xi_j;$$

σ_{ij} továbbá legyen ξ_i és ξ_j oly az orthoid tartományból származó formája, a mely e két mennyiségre vonatkozólag symmetrikus.

Akkor a

$$\sigma_{ij} = \sum_{r=0}^{\frac{n(n-1)}{2}-1} \alpha_r \eta_{ij}^r \qquad (\sigma)$$

$$(i,j=1,\ldots,n;\ i<j)$$

egyenletrendszerből az α_r mennyiségekre vonatkozólag kiadódik, hogy

$$\Delta^2 \alpha_r = \Delta\Delta_r,$$

a hol Δ az $|\eta_{ij}^r|$ determinánst jelenti és nem tünik el, mert Δ^2 a $G(x;a,b)$ forma discriminánsa. Továbbá látjuk, hogy Δ és Δ_r, ha $\xi_1,\ldots,\xi_n$-t felcseréljük $\xi_{i_1},\ldots,\xi_{i_n}$-nel, csak annyiban változnak, hogy azokban bizonyos sorok helyet cserélnek; még pedig Δ-ban és Δ_r-ben a sorok e helycseréje ugyanaz. $\Delta\Delta_r$ tehát, épúgy mint Δ a ξ-k symmetrikus formája és így az eredeti orthoid tartomány mennyisége. Ugyanez áll az $\alpha_0, \alpha_1, \ldots$ mennyiségek sorozatára.

Ha már most $F(z)$-t mint a következő két tényező szorzatát írjuk;

$$(z-\xi_i)(z-\xi_j) = z^2 + \sigma_1' z + \sigma_2'$$

és

$$\prod_{(r)} (z-\xi_r) = z^{n-2} + \sigma_1'' z^{n-3} + \cdots + \sigma_{n-2}'',$$

a hol r átfutja az 1-től n-ig terjedő számok sorát az i és j kizárásával, akkor $\sigma_1' = -(\xi_i+\xi_j)$, $\sigma_2' = \xi_i\xi_j$ — mint közvetetlenül látni — de $\sigma_1'', \ldots, \sigma_{n-2}''$ is oly mennyiségek, a melyek a σ_{ij}-ben feltételezett tulajdonságokat mutatják. Az utóbbiakra nézve ugyanis a redukált formákra vonatkozó tételek, különösen a II. fej. 14. §-a alapján világos, hogy a

$$\Sigma\gamma_{rs}\xi_i^r\xi_j^s \qquad (r=0,\ldots,n-1,\ s=0,\ldots,n-2)$$

alakban és minthogy nem változnak, ha ξ_i-t ξ_j-vel felcseréljük, az

$$\frac{1}{2}\Sigma\gamma_{rs}(\xi_i^r\xi_j^s+\xi_i^s\xi_j^r)$$

alakban is írhatók. Akkor a (σ)-ban adott meghatározást alkalmazva, lesz

$$\sigma_1'=\varphi_1(\eta_{ij}),\quad \sigma_2'=\varphi_2(\eta_{ij}),$$
$$\sigma_k''=\psi_k(\eta_{ij}),\qquad (k=0,\ldots,n-2)$$

a hol a φ és ψ formák együtthatói az eredeti orthoid tartományhoz tartoznak.

Ha tehát η_{ij} az $a(\xi_i+\xi_j)+b\xi_i\xi_j$ mennyiségek bármelyikét jelenti, lesz

$$F(z)=(z^2+\varphi_1(\eta_{ij})z+\varphi_2(\eta_{ij}))(z^{n-2}+\psi_1(\eta_{ij})z^{n-3}+\cdots+\psi_{n-2}(\eta_{ij})).$$

E szerint

$$F(z)-(z^2+\varphi_1(x)z+\varphi_2(x))(z^{n-2}+\psi_1(x)z^{n-3}+\cdots+\psi_{n-2}(x))$$

osztható az $x-a(\xi_i+\xi_j)-b\xi_i\xi_j$ formák mindegyikével és minthogy ezek az æquivalentia értelmében különböző lineáris formák, osztható szorzatukkal, azaz $G(x;a,b)$-vel is. Evvel eljutottunk Gauss identitásához:

$$F(z)=(z^2+\varphi_1(x)z+\varphi_2(x))(z^{n-2}+\cdots+\psi_{n-2}(x))+G(x)H(x),\quad (G)$$

a hol $G(x)$ foka $\frac{n(n-1)}{2}$ és együtthatói ép úgy, mint a $H(x)$-éi az eredeti orthoid tartományhoz tartozó oly mennyiségek, a melyek raczionális műveletek segítségével teljesen meghatározhatók.

28. §. Az «algebra alaptétele» a következő: *Minden $F(z)$ egész függvénynek megfelelőleg, a melynek együtthatói bármely valós vagy complex számok és a melynek foka $n\geqq 1$, meghatározhatunk oly complex számot, ζ-t, a melyre nézve $F(\zeta)=0$.*

E tétel — mint azt tartalma mutatja — az analitikai

függvények elméletébe tartozik; bebizonyítása azonban az épen levezetett identitás felhasználásával nemcsak különösen egyszerűvé válik, hanem egyszersmind a legpontosabban jellemzi az $F(z) = 0$ egyenlet megoldásában fellépő számokat is és a bebizonyításban fellépő függvényelméleti elemet a minimumra redukálja.

A complex számok összessége orthoid tartományt alkot; a (G) identitás tehát alkalmazható.

Az alaptétel továbbá másodfokú egyenletekre minden esetre érvényes; ebben az esetben a gyököket bizonyos, már az elemekben megvizsgált határértékek, az ú. n. quadratikus irraczionálitások szolgáltatják.

A függvényelmélet alapvető folytonossági vizsgálatai továbbá az alaptétel következő specziális esetére vezetnek: Minden egyenletnek, a melynek együtthatói valósak és foka páratlan szám, van egy valós gyöke.

Oly egyenletekre azután, a melyeknek együtthatói valósak, az alaptétel általános érvényességét a következő teljes inductio segítségével mutatjuk ki:

Feltételezzük, hogy a tétel érvényes oly egyenletekre, a melyek fokszáma osztható ugyan 2^{k-1}-vel, de nem 2^k-val és bebizonyítjuk azután, hogy oly egyenletekre is érvényes, a melyek fokszáma osztható 2^k-val, de nem 2^{k+1}-vel.

Legyen $F(z) = 0$ oly egyenlet, a melynek fokszáma az épen kimondott tulajdonságot mutatja. Akkor, ha $n = 2^k h$, a hol h páratlan szám, $G(x)$ foka,

$$\frac{n(n-1)}{2} = \frac{2^k h(2^k h-1)}{2}$$

osztható lesz ugyan 2^{k-1}-vel, de nem 2^k-val. A $G(x) = 0$ egyenletnek tehát van egy gyöke, ξ. Ha a (G) identitásba $x=\xi$-t írjuk, akkor lesz $G(\xi) = 0$,

$$F(z) = (z^2+\varphi_1(\xi)z+\varphi_2(\xi))(z^{n-2}+\psi_1(\xi)z^{n-3}+\cdots+\psi_{n-1}(\xi))$$

és a

$$z^2 + \varphi_1(\xi)\, z + \varphi_2(\xi) = 0$$

másodfokú egyenlet ζ gyökére nézve egyszersmind lesz $F(\zeta) = 0$.

Egész elemi meggondolással intézhetjük el most végre a complex együtthatók esetét is. Akkor írhatjuk, hogy

$$F(z) = F_1(z) + \sqrt{-1}\, F_2(z),$$

a hol $F_1(z)$ és $F_2(z)$ együtthatói valósak. Ugyancsak valósak

$$\left(F_1(z) + \sqrt{-1}\, F_2(z)\right)\left(F_1(z) - \sqrt{-1}\, F_2(z)\right) = 0$$

egyenlet együtthatói; ennek tehát van egy $\zeta = \alpha + \beta\sqrt{-1}$ gyöke. Ha már most $F(\alpha+\beta\sqrt{-1})$ a 0-tól különböző lenne, szükséges, hogy legyen

$$F_1(\alpha+\beta\sqrt{-1}) - \sqrt{-1}\, F_2(\alpha+\beta\sqrt{-1}) = 0$$

de ha ez így van, 0 marad akkor is, ha $\sqrt{-1}$ helyébe $-\sqrt{-1}$-et teszszük. Azaz, akkor $F(\alpha-\beta\sqrt{-1})=0$. Az $\alpha \pm \beta\sqrt{-1}$ két complex szám közül az egyik tehát minden esetre az $F(z) = 0$ egyenlet gyöke.

ÖTÖDIK FEJEZET.

AZ ELIMINÁCZIÓ ÁLTALÁNOS ELMÉLETE.

Az alap-probléma.

1. §. A holoid [A] tartomány fogalmilag teljesen megadja a mellérendelt orthoid tartományt, (A)-t és evvel együtt az (A)-ra vonatkozólag algebrai mennyiségek országát. Ezt az utóbbi tartományt, a melyről a IV. fejezet értelmében tudjuk, hogy ismét orthoid tartomány, röviden az $\{A\}$ jelképpel jelöljük. Valamely x mennyiség az $\{A\}$ tartományban «*korlátlanúl változó*», ha megállapítása nincs más feltételhez kötve, mint ahhoz, hogy egyenlő legyen az $\{A\}$ tartomány valamely mennyiségével. Ha [A] a complex számok összessége, akkor x korlátlan változó volta egyszerűen azt jelenti, hogy x az analitikai függvények elméletének értelmében szabadon változik.

Ha a következőkben már egyszer mindenkorra megállapítottuk az alapúl felvett [A] tartományt, akkor, ha valamely mennyiségről ki kell majd jelentenünk, hogy az korlátlanúl változó, rövidség kedvéért azt a meghatározást, hogy «az $\{A\}$-ban», mint magától értetődőt, elhagyjuk.

Az eliminácziò elméletének alap-problémáját ezek után a következő módon fogalmazhatjuk:

Legyenek $F_j(z_1, z_2, \ldots, z_m)$, $(j=1, \ldots, k)$ bármely az orthoid (A) tartományból származó a zérustól különböző formák; akkor az

$$F_j(x_1, x_2, \ldots, x_m) = 0 \qquad (j=1, 2, \ldots, k)$$

egyenletrendszer az $\{A\}$ tartományban eredetileg korlátlan változóknak gondolt $x_1, \ldots, x_m$ mennyiségek változó voltának (variabilitásának) minden esetre korlátot szab, mert hiszen $x_1, \ldots, x_m$ helyébe már oly egész számokat is tehetünk, a melyekre nézve F_j a 0-tól különböző. *Az eliminácziò elméletének első és alapvető feladata most már az, hogy teljesen és lehetőleg egyszerűen leírjuk a korlátozást, a melyet valamely egyenletrendszer az $x_1, \ldots, x_m$ mennyiségek változó voltában létesít.* Egy ismeretlen, x_1 esetére a megfelelő problémát teljesen megoldottnak tekinthetjük; mert hisz ekkor x_1 változása véges számú, (A)-ra vonatkozólag algebrai mennyiségre szorítkozik, a melyeknek előállítása a IV. fejezetben már megtörtént.

Hogy azonban a változás e megszorítása egyenletrendszerek esetében egészen másképen alakúlhat, már elejétől fogva kitünik abból a körülményből, hogy a legelemibb módon oly egyenletrendszereket is alkothatunk, a melyeknek végtelen sok gyökrendszer felel meg.

Vizsgálatainknak egyik elvileg fontos eredményét már itt fölemlítjük, hogy t. i. a megfelelő problémát az egy ismeretlent tartalmazó egyenlet esetére megoldottnak* véve, a további kifejtés kizárólag csak «*raczionális művelet*»-ek bizonyos meghatározott sorozatát követeli; ez alatt értve a négy alapművelet alkalmazását az (A) tartomány mennyiségeire és az (A) tartományból származó formák legnagyobb közös osztójának meghatározását.

* Nem kell épen az algebrai mennyiségek elméletének felfogásában történő megoldásra gondolnunk; történhetik ez úgy is, a hogy a függvények elmélete követeli, a hol az egy ismeretlent tartalmazó egyenlet gyökei, mint határértékek, illetőleg mint algebrai függvények lépnek fel.

Az F_j formák az együtthatóknak csak véges sorozatát tartalmazzák, és magától értetődik, hogy (A) helyett minden oly orthoid tartomány is választható, mely az együtthatókként szereplő mennyiségeket tartalmazza, így pl. minden oly (A′) tartomány, a mely tartalmazza az (A) tartomány összes mennyiségeit. Evvel szemben a «legkisebb» tartomány, a melyből a vizsgálat kiindulhat, az a raczionális tartomány, a melyet az F_j formák együtthatói teljesen meghatároznak és minden (A′) tartomány, a mely (A) helyébe léphet, «tartalmazza» ezt a raczionális tartományt.

Az így alapúl felvett (A) tartomány határozatlanokat is tartalmazhat, a melyeket azonban a vizsgálat folyamában ilyeneknek meg kell hagynunk; azaz fogalmi meghatározásuk értelmében nincsen megengedve, hogy változó voltuk korlátozásáról beszéljünk. Ez semmiképen sem szorítja meg a vizsgálat általánosságát; csakhogy ugyanannak az $F_j(x_1, x_2, \ldots, x_m)=0$ egyenletrendszernek különböző eliminácziò-problémák felelhetnek meg a szerint, hogy az x-ek közül melyeket tekintünk határozatlanoknak és melyeket ismeretleneknek*.

* Így pl. a

$$zx + y = 2,$$
$$x + y = 1$$

egyenletrendszernek, ha x-et és y-t ismeretleneknek, z-t pedig határozatlannak veszszük, csak ez az *egy* megoldása lesz:

$$x = \frac{1}{z-1}, \quad y = \frac{z-2}{z-1};$$

míg ha x-et, y-t és z-t egyformán ismeretleneknek tekintjük, ugyanannak a rendszernek végtelen sok megoldás felel meg, a melyekben x, y és z változását oly módon korlátoztuk, hogy x felvehet minden értéket a 0 kizárásával, y minden értéket az 1 kizárásával és ép úgy z is minden értéket az 1 kizárásával; továbbá mihelyt egyik ismeretlen értékét e feltételeknek megfelelőleg választottuk, evvel a másik kettő teljesen meg van határozva.

Kronecker eliminácz ió-módszere.

2. §. A felállított problémát teljesen megoldja egy KRONECKER-től* származó módszer, melyet azonban a szerző az idézett helyen épen csak a legrövidebben jelzett. Minthogy a probléma lényegében már az F_j formarendszer resolvens formájának felállításával és az ehhez csatlakozó fejtegetésekkel (III. fej. 18–21. §.) meg van oldva, itt a dolog csak a legnagyobb közös osztó képezésénél előfordúló kivételes eset (III. fej. 20. §.) elkerülésén fordúl meg, hogy így egyszerű és általános előállításhoz jussunk. Ez megtörténik, ha az új u_j és u'_j határozatlanok segítségével KRONECKER eliminácz ió-elve szerint nem csupán csak az F_j formákat foglaljuk össze $\sum_{j=1}^{k} F_j u_j$-ben és $\sum_{j=1}^{k} F_j u'_j$-ben, hanem *ép úgy összefoglaljuk a* $t_1, \ldots, t_m$ *határozatlanok segítségével az* $x_1, \ldots, x_m$ *határozatlanokat is (melyek hiszen szintén formák)* $\sum_{i=1}^{m} t_i x_i$*-ben; ez az eljárás a számolásra alkalmas módon úgy fogalmazható, hogy az* x_m *határozatlan helyébe az*

$$x = t_1 x_1 + t_2 x_2 + \cdots + t_m x_m$$

lineáris transformatio segítségével bevezetjük az x határozatlant.

Hogy a tárgyalást lényegtelen esetleges körülményektől megszabadítsuk, czélszerű még az adott forma- ill. egyenletrendszert előbb bizonyos lineáris transformatiónak alávetni, a melynek együtthatóit minden egyes esetben könnyen meghatározhatjuk.

Ha ugyanis az eredetileg adott egyenletrendszer:

$$G_j(z_1, z_2, \ldots, z_m) = 0, \qquad (j=1, \ldots, k)$$

* Festschrift. 10. §. Az ott kifejezett szándék, hogy az eliminácz ió elméletét későbbi értekezésekben részletesebben tárgyalja, fájdalom, nem valósúlt meg.

és erre a

$$z_i = v_{i1}x_1 + v_{i2}x_2 + \cdots + v_{im}x_m \qquad (i=1,\ldots,m) \qquad (T)$$

lineáris transformatiót alkalmazzuk, a hol a transformatio együtthatóinak kellő meghatározását még későbbre tartjuk fenn, akkor a «transformált» egyenletrendszer:

$$F_j(x_1,\ldots,x_m) = 0, \qquad (j=1,\ldots,k)$$

a melynek együtthatói egyelőre mint a v-k formái értendők.

Ha már most evvel a rendszerrel a III. fej. 18. §-ában előadott utasítás szerint bánunk el, akkor az ott fellépő $F_{j_h}^{(h)}$, $D^{(h)}$ formák, míg *az együtthatókban fellépő v mennyiségeket határozatlanoknak tekintjük*, $x_{h+1},\ldots,x_m$-re nézve mindannyian szabályosak lesznek. Ha ez e formák közül legelőször pl. φ-re nem állana be, úgy hogy e φ forma N-ed dimensiójú volna, de nem volna szabályos, akkor φ okvetetlenül valamely $F_{j_h}^{(h)}$ forma. Ha ugyanis valamely h-ra nézve az $F_{j_h}^{(h)}$ formák mindannyian szabályosak, akkor legnagyobb közös osztójuk, $D^{(h)}$ szintén szabályos. Ha pedig φ valamely $F_{j_h}^{(h)}$, akkor az F_j-kre az $x_{h+1},\ldots,x_m$ oly meghatározott lineáris (T_1) transformatióját alkalmazhatnók, hogy ez a φ most is N-ed dimensiójú forma marad és szabályossá válik, míg a megelőző formák megtartják dimensiójukat és szabályos voltukat. A (T) és (T_1) transformatiók egymásutánja tehát oly transformatióra vezetne, a melynek alkalmazása után φ-ben x_i^N, $(i=h+1,\ldots,m)$ együtthatója a 0-tól különböző, míg a feltevés szerint az egyik ilyen együttható a v-k minden értékrendszere mellett 0-sal egyenlő. E feltevés tehát nem állhat meg és így *az F_j formarendszerből származó $F_{j_h}^{(h)}$, $D^{(h)}$ formák mindannyian $x_{h+1},\ldots,x_m$-re nézve szabályosak.*

Ha már most az F_j formarendszerre a további

$$x = t_1x_1 + t_2x_2 + \cdots + t_mx_m \qquad (T')$$

lineáris transformatiót alkalmazzuk, a hol $x_1,\ldots,x_{m-1}$ meg-

maradnak és csak x_m helyébe lép x, akkor a (T) és (T') transformatiók egymásutánja egyenlő értékű a

$$z_i=\left(v_{i1}-v_{im}\frac{t_1}{t_m}\right)x_1+\left(v_{i2}-v_{im}\frac{t_2}{t_m}\right)x_2+\cdots+v_{im}\frac{1}{t_m}x \quad (T'')$$
$$(i=1,\ldots,m)$$

transformatióval. A (T') transformatio révén az $F_j=0$ egyenletrendszerből származó egyenletrendszerben, a melynek jelölésére

$$f_j=0 \qquad (j=1,\ldots,k)$$

szolgáljon, az együtthatókat a t határozatlanok formáinak tekintjük; mert e végből csak t_m bizonyos hatványával kell szoroznunk, a mi az æquivalentia-meghatározás értelmében meg van engedve *.

Ha már mostan az f_j rendszer resolvens formájának taglalásában fellépő formák

$$D_t^{(h)} \quad \text{és} \quad f_{j_h}^{(h)},$$

a hol t_m-nek nevezőkként fellépő hatványait, a melyeknek a további tárgyalásra nincsen befolyásuk, ismét mellőzzük, ezek újból $x_{h+1},\ldots,x_{m-1}$, *x-re nézve* szabályosak. Ugyanis $D_t^{(h)}$ és $f_{j_h}^{(h)}$ a $D^{(h)}$ és $F_{j_h}^{(h)}$-ból úgy keletkezik, hogy a v-k helyébe annak a lineáris transformatiónak együtthatóit

* A resolvens forma elméletének értelmében a megvizsgálandó formákat az x határozatlanok formáinak kell tekintenünk; együtthatóik az $[(A), t_1,\ldots,t_m]$ formatartomány mellérendelt orthoid tartományához tartoznak; ez maga pedig teljes holoid tartomány. Minthogy azonban ezeket a formákat az $[(A), t_1,\ldots,t_m]$ æquivalentia-tartományra vonatkozólag kell megvizsgálnunk, és æquivalens formák egymást feltétlenül helyettesíthetik, a nevezőket mindig eltávolíthatjuk és végre a formákból, a melyeknek együtthatói már most az $[(A), t_1,\ldots,t_m]$ teljes holoid tartományból valók, eltávolíthatjuk az együtthatók legnagyobb közös osztóját; azaz *a fellépő formák mindig az* $x_1,\ldots,x_{m-1}$ *és* x *határozatlanok primitiv formáinak tekinthetők.*

teszszük, melyre a T és T' egymásutánja vezet, azután pedig t_m bizonyos hatványával szorzunk. Az ekként nyert formák szabályos vagy nem szabályos volta fölött döntő tagok együtthatói pedig a v és t határozatlanoknak az (A) tartományból származó oly formái, a melyek nem egyenlők azonosan a zérussal; mert ez az eset akkor sem áll be, ha $t_1=\cdots=t_{m-1}=0$, $t_m=1$, a mikor tulajdonképen az előbbi formákra térünk vissza. Meghatározhatunk tehát olyan

$$v_{ij}=a_{ij}$$

értékrendszereket, (a melyek még raczionális és egész számokból is állhatnak), a melyekre nézve az együtthatók a t határozatlanoknak a zérustól különböző formáiba mennek át és az $|a_{ij}|$ determináns sem egyenlő zérussal. Evvel a következő eredményre jutottunk:

Az eredeti $G_j=0$ *egyenletrendszerből bizonyos meghatározott lineáris transformatio alkalmazása révén (a melynek determinánsa nem egyenlő a zérussal) nyerjük az* $F_j=0$ *egyenletrendszert, a mely oly szerkezetü, hogy akkor, midőn azt a további*

$$x=t_1 x_1+\cdots+t_m x_m$$

transformatióval az $f_j=0$ *rendszerbe vezetjük át, az ennek megfelelő* $D_t^{(h)}$ *és* $f_{j_h}^{(h)}$ *formák mindannyian* $x_{h+1},\ldots,x_{m-1}$ *és* x*-re nézve szabályosak.*

E mellett a t-k határozatlanoknak tekintendők; de e tétel megtartja érvényességét még akkor is, ha a t-k helyébe oly értékrendszereket teszünk, a melyekre nézve a t-knek amaz általánosságban a 0-tól különböző formái a 0-tól különböző értékeket vesznek fel.

3. §. A $G_j=0$ és $F_j=0$ rendszerek taglalása két teljesen azonos probléma, mert az azokból származó értékrendszerek egymásnak lineáris és egyértelmű módon felelnek meg. (Geometriai felfogásban az így meghatározott lineáris trans-

formatio egyszerű koordináta-transformatio.) Az eredeti rendszer helyett tehát «az esetleges körülményektől megszabadított» $F_j=0$ rendszert és az evvel az

$$x=t_1 x_1+\cdots+t_m x_m$$

transformatio kapcsán összefüggő $f_j=0$ rendszert vizsgálhatjuk meg, a melyben — mint már említettük — az együtthatók a t határozatlanok formáinak tekintendők, a mi csak a t_m nevezőkként szereplő hatványainak feltétlenül megengedett eltávolítását kívánja meg.

Az $F_j=0$ és $f_j=0$ egyenletrendszereknek megfelelő értékrendszerek kölcsönösen meghatározzák egymást. A további tárgyalás áttekinthetősége szempontjából kényelmes lesz, ha ezt pontosabban fogalmazzuk.

Minden olyan $\xi_1, \xi_2, \ldots, \xi_m$ értékrendszer, a mely kielégíti az $F_j=0$ egyenletrendszert, olyan

$$\xi_1, \xi_2, \ldots, \xi_m, \ \xi=\sum_{i=1}^{m} t_i \xi_i$$

értékrendszert szolgáltat, a mely kielégíti az

$$F_j=0, \ x=t_1 x_1+\cdots+t_m x_m$$

egyenletrendszert. Továbbá, ha ez úgy van,

$$\xi_1, \ldots, \xi_{m-1}, \ \xi=\sum_{i=1}^{m} t_i \xi_i$$

kielégíti az $f_j=0$ egyenleteket.

Viszont, ha

$$\xi_m=\frac{1}{t_m}(\xi-t_1 \xi_1-\cdots-t_{m-1}\xi_{m-1}),$$

akkor minden

$$\xi_1, \xi_2, \ldots, \xi_{m-1}, \xi$$

értékrendszer, a mely kielégíti az

$$f_j=0 \qquad (j=1, \ldots, k)$$

egyenletrendszert, olyan

$$\xi_1, \ldots, \xi_m, \xi$$

értékrendszert szolgáltat, a mely kielégíti az

$$F_j=0, \quad x=t_1 x_1+\cdots+t_m x_m$$

egyenleteket és mivel az F_j formák az x határozatlant egyáltalában nem tartalmazzák, azért végre a

$$\xi_1, \xi_2, \ldots, \xi_m, \quad \xi_\tau=\sum_{i=1}^{m} \tau_i \xi_i$$

értékrendszer kielégíti az

$$F_j=0, \quad x=\tau_1 x_1+\cdots+\tau_m x_m$$

egyenletrendszert, a hol $\tau_1, \ldots, \tau_m$ új határozatlanokat jelentenek.

4. §. Legyenek most ismét $D_t^{(h)}$ és $f_{j_h}^{(h)}$ ama formák, a melyek az f_j rendszer resolvens formájának alkotásában és taglalásában szerepelnek. Akkor a

$$\Phi_t=D_t D_t^{(1)} \ldots D_t^{(m-1)}=0$$

egyenlet *az* $F_j=0$ *egyenletrendszer összresolvense,* abban az értelemben, hogy ez az egyenlet az $F_j=0$ rendszer összes gyökrendszereit teljesen és egyszerű módon jellemzi. Az e fej. 2-ik §-ához tartozó jegyzet szerint D_t, $D_t^{(1)}$, ... és így Φ_t is az $x, x_1, \ldots, x_{m-1}$ határozatlanoknak oly primitiv formája, a melynek együtthatói az $[(A), t_1, \ldots, t_m]$ formatartományhoz tartoznak. E mellett $D_t^{(h)}$, vagy részletesen írva

$$D_t^{(h)}=D_t^{(h)}(x; x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m)$$

az $x; x_{h+1}, \ldots, x_{m-1}$ határozatlanoknak oly szabályos formája, a melynek dimensiója 0 is lehet; ebben az esetben azonban megállapodásaink értelmében 1-gyel egyenlőnek veendő.

Ha $\Phi_t=\Psi_t X_t$, akkor a $\Psi_t=0$ egyenletet az $F_j=0$ egyenletrendszer *részlet-resolvensének,* jelesen a $D_t^{(h)}=0$ egyen-

letet pedig az $F_j=0$ rendszer *teljes* $h+1$*-edfokozatú (részlet-) resolvensének* nevezzük. Ily resolvens «nincsen», ha $D_t^{(h)}$ 1-gyel egyenlö.

A III. fej. 18. §-ának $(\overline{R})$ congruentiái közül bármelyik most ily alakú:

$$D_t D_t^{(1)} \ldots D_t^{(m-1)} C \equiv 0 \,(\text{mod. } f_1, \ldots, f_k), \qquad (C)$$

a hol C az $[(A), t_1, \ldots, t_m]$ formatartományhoz tartozik és a 0-tól különböző. Minthogy továbbá az értelmezés szerint $x=t_1 x_1+\cdots+t_m x_m$-re nézve $f_j=t_m^{a_j} F_j$, azért $f_j-t_m^{a_j} F_j$, mint az x-ek formája, osztható $x-t_1 x_1-\cdots-t_m x_m$-mel és így a (C) congruentia ezt az új alakot nyeri:

$$D_t D_t^{(1)} \ldots D_t^{(m-1)} C \equiv 0 \,(\text{mod. } F_1, \ldots, F_k, x-\sum_{i=1}^{m} t_i x_i).$$

Ha már most $x_1=\xi_1, \ldots, x_m=\xi_m$ az $F_j=0$ rendszer bármely gyökrendszere és $x=\xi=\sum_{i=1}^{m} t_i \xi_i$, akkor a $D_t^{(h)}$ tényezők valamelyikének a zérussal kell egyenlőnek lennie; mert C az x-ektől független és a 0-tól különböző mennyiség.

Ha pedig viszont $x_{h+1}=\xi_{h+1}, \ldots, x_{m-1}=\xi_{m-1}$, $x=\xi$ olyan értékrendszer, a melyre nézve $D_t^{(h)}$ a zérussal egyenlő, akkor a III. fejezetben (különösen annak 20. §-ában) előadott, már többször idézett fejtegetések szerint mindig van véges számú, de legalább is egy olyan $\xi_1, \ldots, \xi_h$ értékrendszer, a melyre nézve minden egyes f_j zérus lesz, és így

$$\xi_1, \xi_2, \ldots, \xi_{m-1}, \xi_m = \frac{1}{t_m}(\xi - t_1 \xi_1 - \cdots - t_{m-1} \xi_{m-1})$$

az előbbiek szerint az $F_j=0$ egyenletek gyökrendszere.

Most már a következő, az eliminácziö elméletében alapvető tételre térhetünk át:

Ha $D_t^{(h)}(x; x_{h+1}, \ldots, x_{m-1}, t_1, \ldots, t_m)$*-ben az* $x_{h+1}, \ldots, x_{m-1}$ *határozatlanok helyébe tetszés szerinti* $\xi_{h+1}, \ldots, \xi_{m-1}$ *mennyiségeket helyettesítünk, akkor*

$$D_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$$

az $x; t_1, \ldots, t_m$ *határozatlanoknak homogén formája lesz és ha ez az* 1*-től különböző, akkor mint ugyanezen határozatlanok lineáris formáinak szorzata állítható elő.*

A $D_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$ együtthatói az (A) tartomány mennyiségeiből és a $\xi_{h+1}, \ldots, \xi_{m-1}$ mennyiségekből összeadás és szorzás segítségével vannak összeállítva. Így tehát bizonyos (R) raczionális tartományt határoznak meg és valamely ebből származó genus-tartomány lesz az, a melyben ama felbontás végbe megy.

A tétel bebizonyítására bevezetjük a további, tetszés szerint választott $\xi_1, \ldots, \xi_h$ mennyiségeket; a helyettesítési eredményt pedig, a mely származik, ha $D_t^{(h)}$-ben és Φ_t-ben $x_1, \ldots, x_{m-1}$ helyébe a $\xi_1, \ldots, \xi_{m-1}$ értékeket helyettesítjük, $\bar{D}_t^{(h)}$-val ill. $\bar{\Phi}_t$-vel jelöljük. Ezeknek az utóbbi formáknak (a melyek az $x, t_1, \ldots, t_m$ határozatlanokat tartalmazzák) lehetnek többszörös osztóik; hogy ezeket eltávolítsuk, képezzük $\bar{D}_t^{(h)}$ és $\frac{\partial}{\partial x} \bar{D}_t^{(h)}$ ill. $\bar{\Phi}_t$ és $\frac{\partial}{\partial x} \bar{\Phi}_t$ legnagyobb közös osztóját és távolítsuk azt el $\bar{D}_t^{(h)}$-ből, ill. $\bar{\Phi}_t$-ből. Legyenek még $\bar{E}_t^{(h)}$ és $\bar{\Psi}_t$ a $\bar{D}_t^{(h)}$, ill. $\bar{\Phi}_t$ egyszerű osztóinak szorzatai, akkor minden esetre:

$$\bar{\Psi}_t = \bar{E}_t^{(h)} \bar{X}_t^{(h)}.$$

Az

$$\bar{E}_{t'}^{(h)} = 0$$

egyenletből, a hol a $t_1', \ldots, t_m'$ sorozat a $t_1, \ldots, t_m$ határozatlanokkal egyenlőjogú új határozatlanoknak sorozatát jelenti, x, mint ismeretlen számára bizonyos az $((R), t_1', \ldots, t_m')$ tartományból származó genus-tartományhoz tartozó mennyiségeket nyerünk. Legyen azok közül az egyik ξ'. Erre nézve minden esetre egyszersmind $\bar{D}_{t'}^{(h)} = 0$ és így tehát a III. fej. 20. §-ában jellemzett algorithmus a mennyiségeknek legalább is egy oly

$$\xi', \xi_1', \ldots, \xi_h'$$

rendszerére vezet, hogy

$$\xi', \xi_1', \ldots, \xi_h', \xi_{h+1}, \ldots, \xi_{m-1}$$

az $[f_j]_{t'}=0$ egyenletrendszert* kielégíti. Ha ezekhez a mennyiségekhez még hozzácsatoljuk a

$$\xi'=\sum_{r=1}^{h} \xi_r' t_r' + \sum_{s=h+1}^{m-1} \xi_s t_s' + \xi_m' t_m' \qquad (\xi')$$

értelmezte ξ_m' mennyiséget, akkor a

$$\xi', \xi_1', \ldots, \xi_h', \xi_{h+1}, \ldots, \xi_{m-1}, \xi_m'$$

értékrendszer kielégíti az

$$[f_j]_{t'}=0, \quad x=t_1' x_1+\cdots+t_m' x_m$$

egyenletrendszert és így tehát egyszersmind az

$$F_j=0, \quad x=t_1' x_1+\cdots+t_m' x_m$$

egyenletrendszert is.

Minthogy azonban az F_j formák az x határozatlant nem is tartalmazzák, a

$$\xi_1', \ldots, \xi_h', \xi_{h+1}, \ldots, \xi_{m-1}, \xi_m'$$

mennyiség-rendszer és

$$\xi_t=\sum_{r=1}^{h} \xi_r' t_r + \sum_{s=h+1}^{m-1} \xi_s t_s + \xi_m' t_m,$$

a hol $t_1, \ldots, t_m$ az először használt határozatlanokat jelentik, kielégíti az

$$F_j=0, \quad x=t_1 x_1+\cdots+t_m x_m$$

rendszert és végül az $f_j=0$ egyenleteket is. E mennyiségek helyettesítésénél a $\bar{\Phi}_t$ és $\bar{\Psi}_t$ zérus lesz, és így tehát végre ugyancsak $\bar{E}_t^{(h)}$ *vagy* $\bar{X}_t^{(h)}$. E mellett a $\bar{\Phi}_t$ stb. mennyiségek a $\bar{\Phi}_{t'}$ stb. mennyiségektől csakis a t határozatlanok jelölésében különböznek.

* Itt $[f_j]_{t'}$ azt a formát jelenti, mely f_j-ből keletkezik, ha a $t_1, \ldots, t_m$ helyébe a $t_1', \ldots, t_m'$-et teszszük.

Ha a

$$\bar{X}_t^{(h)} = 0$$

egyenletben x-et tekintjük ismeretlennek, akkor

$$\xi_t = \sum_{r=1}^{h} \xi_r' t_r + \sum_{s=h+1}^{m-1} \xi_s t_s + \xi_m' t_m$$

nem lehet annak gyöke; különben, minthogy a t-k épen határozatlanok,

$$\xi' = \sum_{r=1}^{h} \xi_r' t_r' + \sum_{s=h+1}^{m-1} \xi_s t_s' + \xi_m' t_m'$$

a $\bar{X}_{t'}^{(h)} = 0$ egyenletnek megfelelő gyöke volna, a mely a ξ_m' értelmezése szerint a $\bar{E}_{t'}^{(h)} = 0$ egyenletet is kielégíti; pedig képezésüknek megfelelőleg $\bar{E}_{t'}^{(h)}$-nek és $\bar{X}_{t'}^{(h)}$-nek nincsen az 1-től különböző közös osztója.

Ezek szerint

$$L_1 = x - \sum_{r=1}^{h} \xi_r' t_r - \sum_{s=h+1}^{m-1} \xi_s t_s - \xi_m' t_m$$

$\bar{E}_t^{(h)}$-nek és $\bar{D}_t^{(h)}$-nek is lineáris osztója.

Ha az így meghatározott osztót $\bar{E}_t^{(h)}$-ből eltávolítjuk és $\bar{X}_t^{(h)}$-hez csatoljuk, az épen befejezett következtetést pontosan ismételhetjük és akkor az előre kimondott tételnek megfelelőleg

$$\bar{E}_t^{(h)} = T_1' L_1 \dots L_{\nu_h},$$

a hol

$$L_k = x - \sum_{r=1}^{h} \xi_r^{(k)} t_r - \sum_{s=h+1}^{m-1} \xi_s t_s - \xi_m^{(k)} t_m \qquad (k=1, \dots, \nu_h)$$

és ν_h az $\bar{E}_t^{(h)}$-nek x-re vonatkozó foka; végre pedig

$$\bar{D}_t^{(h)} = T_h L_1^{c_{h1}} \dots L_{\nu_h}^{c_{h\nu_h}},$$

a hol a $c_{h\nu_h}$-k pozitiv egész számokat jelentenek.

E mellett még ki kell mutatnunk, hogy T_h az (A) tartomány mennyisége és így tehát 1-gyel egyenlőnek is vehető. T_h ugyanis x legmagasabb hatványának együtthatója $\bar{D}_t^{(h)}$-ben.

Minthogy azonban $D_t^{(h)}$ az x-re nézve szabályos forma, ez az együttható az $x_{h+1}, \ldots, x_{m-1}$ határozatlanok közül egyet sem tartalmaz. Ha tehát ezek helyett valamely $\xi_{h+1}, \ldots, \xi_{m-1}$ értékrendszert vezetünk be, T_h a t határozatlanoknak az (A) tartományból származó ugyanazon formája marad, mint előbb.

De a $\xi_{h+1}, \ldots, \xi_{m-1}$ mennyiségeket egyenesen határozatlanoknak is választhatjuk; azaz az $x_{h+1}, \ldots, x_{m-1}$ mennyiségeket meghagyhatjuk ilyeneknek. Ekkor következtetéseink magára $D_t^{(h)}$-re vonatkoznak; ha tehát T_h a t-knek igazi formája volna, akkor $D_t^{(h)}$ osztható volna T_h-val, azaz feltevésünk ellenére nem primitiv forma. T_h tehát valóban az (A) tartomány mennyisége és ~ 1-gyel, és így, ha $D_t^{(h)}$-t elosztjuk T-vel és a formának ezt az alakját veszszük alapúl, T végre 1-gyel egyenlőnek vehető.

Végre még igen egyszerű meggondolás mutatja, hogy *a lineáris tényezőkben fellépő* $\xi_1^{(k)}, \ldots, \xi_h^{(k)}, \xi_m^{(k)}$ *együtthatók már az* (R) *tartományra vonatkozólag algebrai mennyiségek,* azaz meghatározásuknál a t' határozatlanok csak látszólag szerepelnek.

Ezt pontosan kifejtendők, gondoljuk, hogy $\bar{D}_t^{(h)}$ felbontását elvégeztük úgy is, hogy a $t'_1, \ldots, t'_m$ határozatlanok helyébe az ezekkel egyenlőjogú határozatlanoknak egy harmadik új sorozatát is bevezetjük, a melyek jelölésére szolgáljanak $t''_1, \ldots, t''_m$. Ekkor teljesen úgy mint előbb nyerjük a $\bar{D}_t^{(h)}$ olyan felbontását lineáris tényezőkre:

$$\bar{D}_t^{(h)} = \Lambda_1^{a_{h1}} \Lambda_2^{a_{h2}} \ldots \Lambda_{\nu_h}^{a_{h\nu_h}},$$

a hol úgy mint előbb T-t már 1-nek veszszük és

$$\Lambda_k = x - \sum_{r=1}^{h} \eta_r^{(k)} t_r - \sum_{s=h+1}^{m-1} \xi_s t_s - \eta_m^{(k)} t_m.$$

Ebben az $\eta_i^{(k)}$-k csak abban különböznek a $\xi_i^{(k)}$-któl, hogy, míg az utóbbiak értelmezésénél a t' határozatlanokat használtuk, az előbbiekében a t'' határozatlanok szerepelnek.

Ily módon abban a genus-tartományban, a mely az összes

$$\xi_i^{(j)}, \eta_i^{(j)} \qquad (i=1, \ldots, h, m; j=1, \ldots, \nu_h)$$

mennyiségeket tartalmazza, adva van a $\bar{D}_t^{(h)}$ kétféle felbontása lineáris, tehát irreducibilis tényezőkre; minden Λ_j æquivalens tehát valamelyik L_k-val; minthogy pedig x együtthatója mind a kettőben az egység, ebből végre következik, hogy $L_k=\Lambda_j$; azaz

$$\xi_r^{(k)}=\eta_r^{(j)} \qquad (r=1, \ldots, h, m)$$

Ámde $\xi_r^{(k)}$ kielégít oly egyenletet, a melynek együtthatói a $t_1', \ldots, t_m'$ határozatlanoknak az (R) tartományból származó formái és ép úgy $\eta_r^{(j)}$ oly egyenletnek tesz eleget, a melynek együtthatói a $t_1'', \ldots, t_m''$ határozatlanoknak az (R) tartományból származó formái. Legyenek ezek az egyenletek $\varphi_1=0$ és $\varphi_2=0$, akkor, mert $\xi_r^{(k)}=\eta_r^{(j)}$, φ_1-nek és φ_2-nek lesz egy közös osztója, φ és $\xi_r^{(k)}=\eta_r^{(j)}$ már a $\varphi=0$ egyenletet is kielégíti. De φ-ben egy t' sem fordúlhat elő, valamint egy t'' sem; különben az első esetben nem lehetne φ_1-nek, a második esetben pedig φ_2-nek osztója.

A $\xi_r^{(k)}$ mennyiség tehát kielégít oly egyenletet, a melynek együtthatói az (R) tartományhoz tartoznak, és épen ezt kellett bebizonyítanunk.

Magától értetődik ezután, hogy $j=k$, $a_{h1}=c_{h1}$ stb.

Az $F_j=0$ rendszer megoldásainak összessége.

5. §. A megelőző fejtegetések megadják most már az összes segédeszközöket arra, hogy teljesen leírhassuk azt a korlátozást, melyet az

$$F_j=0 \qquad (j=1, \ldots, k)$$

egyenletrendszer az $x_1, \ldots, x_m$ ismeretlenek változó voltá-

nak szab. Itt már feltételezhetjük és feltételezzük is, hogy valamely kellően választott lineáris transformatio segítségével már megszabadítottuk az egyenletrendszert az előbb leírt értelemben vett «esetleges körülményektől». Az egyenletrendszer együtthatói tartozzanak az orthoid (A) tartományhoz és az ismeretlenek változó voltát vizsgáljuk meg az $\{A\}$ tartományban. E megállapodások csak a vizsgálat alapjait rögzítik meg a nélkül, hogy általánosságát megszorítanák.

Az

$$x_1=\xi_1, \ldots, x_m=\xi_m$$

gyökrendszerek összességét, a melyek az $F_j=0$ egyenleteket kielégítik, röviden *az egyenletrendszer tartalmának* nevezzük.

E szerint az $F_j=0$ egyenletrendszer tartalmát úgy nyerjük, hogy rendre képezzük az 1-től különböző $D_t^{(h)}$ formákat; ezután mindegyikben $x_{h+1}, \ldots, x_{m-1}$ helyébe a tetszés szerinti $\xi_{h+1}, \ldots, \xi_{m-1}$ mennyiségeket helyettesítjük és végre a III. fej. 20. §-a szerint meghatározzuk a $\xi_1, \ldots, \xi_h, \xi$ mennyiség-rendszereket, valamint a

$$\xi=\sum_{i=1}^{m} \xi_i t_i = \xi_t$$

kapcsán ξ_m-et is, mely ép úgy, mint $\xi_1, \ldots, \xi_h$, a t-ktől független.

Ekkor

$$D_t^{(h)}(\xi_t; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)=0,$$

azaz $x-\xi_t=x-\sum_{i=1}^{m} \xi_i t_i$ a $D_t^{(h)}$ lineáris tényezője. Ez az eredmény a következő módon is fogalmazható:

Minden a $h+1$-edfokozatú $D_t^{(h)}=0$ resolvensből származó $\xi_1, \ldots, \xi_m$ gyökrendszer kielégíti a

$$D_t^{(h)}(x_1 t_1+\cdots+x_m t_m; x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m)=0$$

egyenletet, a melyben $t_1, \ldots, t_m$ határozatlanoknak és az

$x_1, \ldots, x_m$ *ismeretlenek az* $\{A\}$*-ban változó mennyiségeknek tekintendők.*

E tétel megfordítása is érvényes:

Ha $x_1=\xi_1, \ldots, x_m=\xi_m$ *az adott értelemben az épen felírt egyenletnek egyik megoldása, akkor ez a megoldás az ismert módon származik* $D_t^{(h)}=0$*-ból, ha t. i. ebben*

$$x_{h+1}=\xi_{h+1}, \ldots, x_{m-1}=\xi_{m-1}$$

tételtik és a további $\xi_1, \ldots, \xi_h, \xi_m$ *mennyiségeket az egyenletek megfelelő lánczolatából meghatározzuk.*

A mennyiségek minden ily sorozatából ugyanis olyan $\xi_t=\sum_{i=1}^{m} \xi_i t_i$ származik, a melyre nézve az épen befejezett részletes fejtegetés értelmében

$$D_t^{(h)}(\xi_t; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)=0.$$

Magától értetődik, hogy *mind a két tétel* $D_t^{(h)}$ *minden osztójára nézve is érvényes; jelesen az egyszerűbb* $E_t^{(h)}$ *formára nézve,* a mely $D_t^{(h)}$-ből úgy származik, hogy eltávolítjuk belőle $D_t^{(h)}$ és $\frac{\partial}{\partial x} D_t^{(h)}$ legnagyobb közös osztóját. Az $E_t^{(h)}=0$ egyenletet *redukált resolvensnek* nevezzük. A $h+1$-edfokozatú resolvensnek megfelelő megoldásokat már az

$$E_t^{(h)}\left(\sum_{i=1}^{m} x_i t_i; x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m\right)=0$$

egyenletből nyerjük, a hol $D_t^{(h)}$ minden egyes tényezője csak mint egyszerű tényező lép fel. Ily módon azonban elvész a további vizsgálatban a megoldásnak egyik igen jellemző tulajdonsága, annak «sokszorosság»-a*; de azért mégis az

* KRONECKER eliminácziő-módszerének e munkában *először adott általánosabb alakja* annyiban meghaladja a «Festschrift» tárgyalásait, hogy a megoldásoknak ú. n. sokszorosságát *nem hanyagolja el;* csak szétválasztja — még pedig egész természetes módon — a két problémát, a melyek közül az egyik $F_i=0$ megoldásainak meghatározását

$F_j=0$ egyenletek tartalmát már az $E_t^{(h)}=0$ egyenletek is teljesen megadják.

Végre még erősen hangsúlyozandó, hogy az x-ek és a t-k jelentése miatt az

$$E_t^{(h)}\left(\sum_{i=1}^{m} x_i t_i;\ x_{h+1}, \ldots, x_{m-1};\ t_1, \ldots, t_m\right)=0$$

egyenlet és ép úgy a megfelelő $D_t^{(h)}=0$ *egyenlet is valójában bizonyos egyenletrendszer formális összefoglalása;* mert, ha a t-k hatványszorzatai szerint rendezünk, akkor minden egyes együtthatónak (mely az x-ek egész függvénye) különkülön egyenlőnek kell lennie zérussal.

Az $E_t^{(h)}=0$ egyenletnek ily módon megfelelő egyenletrendszert röviden majd E_h-val jelöljük.

6. §. *Evvel az* $F_j=0$ *egyenletek tartalmának jellemző szétbontásához jutottunk.* Minden egyes E_h rendszer tartalma benne van az $F_j=0$ rendszer tartalmában és a különböző

követeli, a másik pedig e megoldásoknak megfelelő bizonyos jellemző számot, a «sokszorosságot» (multiplicitást) állapítja meg. Az a rövid jelentés, a melyben a «Festschrift» e módszerről beszámol, csak az $E_t^{(h)}=0$, nálunk «redukált»-aknak nevezett resolvenseket ismeri.

De evvel egyidőben a $D_t^{(h)}$ lineáris tényezői mellett elöfordúló kitevőknek is megvan az egyenletrendszerre vonatkozó jelentésük. Ezek egyenesen alapját szolgáltatják annak az elméletnek, a mely az ily általánosságban tárgyalt egyenletrendszerek megoldásainak sokszorosságára vonatkozik. Ily értelemben e kérdést még nem vizsgálták részletesen.

A szó közönséges, sokkal szűkebb értelmében vett sokszorosság elméletét majd a VI. fej. 27. és 28. §-aiban tárgyaljuk.

Az itt tárgyalt általánosított elmélet főfontossága abban rejlik, hogy az f_j rendszer resolvens formája, Φ_t *mindig* $\equiv 0$ (mod. $F_1, \ldots, F_k$); a mi többiek közt lehetővé tette a VIII. és IX. fejezetben tárgyalt arithmetikai problémák teljes megoldását.

Az eredeti Kronecker-féle elmélettel foglalkoztak még Molk már előbb idézett értekezésében (Acta math. VI. köt.) és Netto (Vorl. über Algebra, II. köt. 127 l.).

E_h rendszerek tartalma teljesen kimeríti az $F_j=0$ rendszer tartalmát.

Az E_h rendszer tartalma «*az* $\{A\}$ *tartományból származó* $m-h-1$*-szeres sokaság*»; ennek minden «*elemét*» nyerjük és csak ilyeneket nyerünk, ha a $(\xi_1, \ldots, \xi_m)$ értékrendszerben a $\xi_{h+1}, \ldots, \xi_{m-1}$ mennyiségeket, a melyeknek száma $m-h-1$, tetszés szerint választjuk és a fenmaradó $\xi_1, \ldots, \xi_h, \xi_m$ mennyiségek helyébe véges számmal levő értékrendszereket teszünk. *Ezen értékrendszerek száma általánosságban egyenlő* μ_h*-val,* $E_t^{(h)}$*-nek* x*-re vonatkozó fokával és ennek megfelelőleg az így nyert sokaságot* μ_h*-adfokúnak nevezzük.*

Itt, a mennyiben $x_{h+1}, \ldots, x_{m-1}$ határozatlanok, $E_t^{(h)}$ a $D_t^{(h)}$ egyszerü tényezőinek szorzatát jelenti. E felfogásban $E_t^{(h)}$-nek x szerint vett discriminánsa az $x_{h+1}, \ldots, x_{m-1}$ határozatlanoknak 0-tól különböző formája és mindaddig, míg $\xi_{h+1}, \ldots, \xi_{m-1}$ a mennyiségek oly rendszere, a melynek behelyettesítése után e discrimináns nem tünik el, $E_t^{(h)}$-nek és $\bar{E}_t^{(h)}$-nek x-re vonatkozó foka ugyanaz. Ha azonban e discrimináns bizonyos $\xi_{h+1}, \ldots, \xi_{m-1}$ értékrendszerre nézve eltünik, akkor $E_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$ többszörös lineáris tényezőket tartalmaz, μ_h nagyobb ν_h-nál, $\bar{E}_t^{(h)}=0$ fokánál és az ilyen rendszernek megfelelő értékrendszerek száma, $\nu_h < \mu_h$.

Hogy az értékrendszerek számára vonatkozó tétel általános érvényességét fentartsuk, a megfelelő $\xi_1', \ldots, \xi_h', \xi_m'$ értékrendszert annyiszor számláljuk, mint a mennyi a megfelelő lineáris tényező kitevője $E_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$-ben. A sokaság így meghatározott elemét *többszörös (kettős) elemnek, vagy pedig singuláris elemnek* nevezzük. Azt is szokás mondani, hogy e singuláris elemben több egyszerű elem «összecsik»*.

* Félreértések elkerülése végett még egyszer kiemeljük, hogy

Ha $E_t^{(h)}$-nek x szerint vett discriminánsát $\Delta_t^{(h)}$-vel jelöljük, akkor a

$$\Delta_t^{(h)}(x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m)=0$$

egyenlet, a melyet ismét bizonyos egyenletrendszer formális összefoglalásának kell tekintenünk, azokat a $\xi_{h+1}, \ldots, \xi_{m-1}$ értékrendszereket értelmezi, a melyek singuláris elemekre vezetnek és közvetetlenül világos, hogy az

$$E_t^{(h)}=0, \quad \frac{\partial}{\partial x} E_t^{(h)}=0$$

egyenletekben formálisan összefoglalt egyenletrendszer az $E_t^{(h)}=0$ egyenlet értelmezte sokaság singuláris elemeit és csak ezeket értelmezi.

Az $\{A\}$-ból származó algebrai sokaság fogalmát természetszerűen *bővítjük,* ha ezen a néven azoknak a $\xi_1, \ldots, \xi_m$ értékrendszereknek összességét értjük, a melyek az $F_j=0$ egyenleteket kielégítik. A sokaság pontosabb megjelölését, mint «algebrai»-t, a továbbiakban mellőzzük; mert az itt előadott elmélet czéljainak megfelelőleg e könyvben más sokaságokról egyáltalában nem is lesz szó. Az alapúl felvett m-szeres sokaság, $(x_1, \ldots, x_m)$ is, a hol minden egyes x az $\{A\}$ bármely mennyiségével egyenlőnek vehető, ebben az értelemben algebrai sokaság, mert értelmezését a $0=0$ egyenletből nyeri, a mely az x-ek változásának nem szab korlátot.

Evvel ellentétben pl. az a feltétel, hogy az x-ek racziónális és egész számok legyenek, nem algebrai, hanem «transcendens» sokaságot értelmez*.

e fogalmak megalkotásánál az $E_t^{(h)}=0$ értelmezte sokaságból indulunk ki, a hol $E_t^{(h)}$-nek, mint az $x, x_{h+1}, \ldots, x_{m-1}$ határozatlanok formájának nincsenek többszörös tényezői.

* Magától értetődik, hogy e fogalomalkotások megtartják érvényességüket még akkor is, ha az adott $G_j(z_1, \ldots, z_m)=0$ egyenlet-

Ha tehát a $G_j=0$ egyenletrendszernek megfelelő

$$D_t^{(h_1)},\ D_t^{(h_2)},\ \ldots$$

formák az æquivalentia értelmében az 1-től különbözők, akkor az egyenletrendszer tartalma egy $m-h_1-1$-szeres sokaságból, egy $m-h_2-1$-szeres sokaságból stb. áll. Geometriai kifejezésmóddal élve a $G_j=0$ egyenletrendszer «az m-dimensiós térben bizonyos számú különböző kiterjedésű képződményt, «pontokat,» «vonalakat,» «felületeket,» háromszorosan kiterjedt képződményeket, stb. *egyidejüleg* értelmez.

rendszert a megelőző lineáris transformatio nélkül veszszük a vizsgálat alapjául. Az ekkor fellépő kivételes esetek onnan erednek, hogy az egyenletek alkotására felhasznált formák többé nem szabályosak. Ha már most $z_{h+1}, \ldots, z_{m-1}$ értékeiből folytatólag a $z_h, \ldots$ értékeket kell meghatároznunk, megeshetik, hogy $z_h, \ldots$ legmagasabb hatványának együtthatója eltünik és akkor a megfelelő értékrendszerek száma μ_h alászáll még akkor is, ha a többszörös elemeket megfelelőleg többszörösen számláljuk. Hogy ilyenkor is a μ_h szám állandóságát formailag föntartsuk, a sokaságnak ú. n. «végtelen» elemeit szokás bevezetni. Az összes együtthatók eltünése révén a $z_h, \ldots$ meghatározására szolgáló egyenlet továbbá azonossá is válhatik. Ezt az esetet egyszerűen megvilágítja annak a felületnek a példája, a mely az $x=a$, $y=b$ egyenest teljesen tartalmazza. Mindezek a kivételes esetek azonban csak akkor léphetnek fel, ha a $z_{h+1}, \ldots, z_{m-1}$ mennyiségek kielégítenek valamely $\varphi(z_{h+1}, \ldots, z_{m-1})=0$ algebrai egyenletet.

Az ily esetleges körülményeket elkerüljük azon kölcsönösen egyértelmű vonatkozás által, a melyet a

$$z_i = \sum_{j=1}^{m} a_{ij}\, x_j, \qquad |a_{ij}| \neq 0$$

lineáris transformatio a $(z_1, \ldots, z_m)$ és $(x_1, \ldots, x_m)$ sokaságok között megállapít. Geometriai felfogásban ekkor az első sokaságnak is minden elemét az $x_1, \ldots, x_m$ «koordináták» által gondoljuk adottnak, a mi közvetetlenül átvihető az abban foglalt $m-1$, $m-2, \ldots$-szeres sokaságokra.

Az egységes nomenclatura érdekében még a következőkben állapodunk meg:

Az $F_j=0$ egyenletrendszer értelmezte sokaságot $h+1$-*edfokozatúnak* (vagy $h+1$-*edrangúnak*) nevezzük, ha h a legkisebb egész szám, a melyre nézve $D_t^{(h)}$ az æquivalentia értelmében 1-től különböző (D_t-nek megfelelőleg $h=0$); ugyanezt az elnevezést kiterjesztjük az $F_j=0$ egyenletrendszerre, valamint az F_j formákból álló orthoid formarendszerre is*.

A $h+1$-edfokozatú $F_j=0$ rendszert és a hozzá tartozó sokaságot *tiszta* $h+1$-*edfokozatú rendszernek, ill. tiszta sokaságnak* nevezzük, ha $k>h$ esetében $D_t^{(k)}\sim 1$. Ellenkező esetben *vegyes* $h+1$-*edfokozatú rendszerrel*, ill. *vegyes sokasággal* van dolgunk.

Helyén lesz, ha ebben az értelemben még $m+1$-*edfokozatú* rendszerekről is beszélünk, a melyeknek aztán «nincsen tartalmuk». Az $F_j=0$ egyenletrendszernek ugyanis ebben az esetben egyetlen egy gyökrendszer sem felel meg.

Magától értetődik, hogy, hacsak $D_t^{(h)}$ nem ~ 1, a

$$D_t^{(h)}=0, \text{ vagy } E_t^{(h)}=0$$

egyenletekben összefoglalt egyenletrendszer $h+1$-edfokozatú, a mi e resolvens előbbi elnevezésével megegyezik.

A $h+1$-edfokozatú sokaság (varietas) rövid jelölésére a $V^{(h+1)}$-t használjuk.

* Ha a formák együtthatói valamely valódi holoid tartományhoz tartoznak és a probléma felállítása követeli, hogy csakis erre a tartományra szorítkozzunk, ha tehát a szó szűkebb értelmében vett arithmetikai kérdéseket kell tárgyalnunk; akkor az F_j formarendszer fokozatszámát nem értelmezhetjük többé úgy, hogy az $F_j=0$ egyenletrendszerével megegyezzék. Mihelyt «egyenletrendszer»-ről beszélünk, a holoid tartományt már is a mellérendelt orthoid tartománynyá bővítettük ki.

A $D_t^{(h)}=0$ értelmezte $V^{(h+1)}$ sokaság singuláris elemei — mint azt az értelmező egyenletek közvetetlenül mutatják — oly sokaságot szolgáltatnak, a melynek fokozatszáma legalább is $h+2$. E fokozatszám azonban nagyobb is lehet és egészen $m+1$-ig emelkedhetik; azaz vannak oly sokaságok is, a melyek singuláris elemet egyáltalában nem tartalmaznak. A lineáris egyenlet értelmezte $V^{(1)}$ sokaság triviális példáján kívül az analitikai geometria elemeiből ismerünk erre példát, a hol az «általános» másodfokú egyenlet (szét nem eső kúpszelet stb.) ilyen sokaságot értelmez.

7. §. Most az $F_j=0$ egyenletrendszer összresolvensére térünk vissza. Ez a következő:

$$\Phi_t=D_t\,D_t^{(1)}\ldots D_t^{(m-1)}=0,$$

a hol a bal oldalon álló resolvens forma az $x, x_1, \ldots, x_{m-1}$; $t_1, \ldots, t_m$ határozatlanoknak olyan formája, a melynek együtthatói az orthoid (A) tartományhoz tartoznak.

Mindenekelőtt közvetetlenül látni, hogy az így értelmezett $D_t^{(h)}$ és $D_t^{(k)}$ formáknak $(h+k)$ nincsen az 1-től különböző közös osztójuk. Ez tisztán formális alapon abból a körülményből következik, hogy $D_t^{(h)}$ és $D_t^{(k)}$, mint a bennök előfordúló x-ek formái szabályosak és primitivek.

$D_t^{(h)}$ felbontása irreducibilis tényezőkre tehát a következőt szolgáltatja:

$$D_t^{(h)}=P_{h1}^{c_{h1}}\ldots P_{h\mu_h}^{c_{h\mu_h}},$$

a hol az $=$ jelt tehetjük az $\sim$ jel helyébe, ha az összes tényezőkben x legmagasabb hatványának együtthatóját 1-nek veszszük. Ekkor a már használt jelöléssel élve:

$$E_t^{(h)}=P_{h1}\ldots P_{h\mu_h},$$

továbbá

$$\Phi_t=\prod_{h=0}^{m-1}\prod_{j_h=1}^{\mu_h}P_{hj_h}^{c_{hj_h}},$$

$$\Psi_t = \prod_{h=0}^{m-1} \prod_{j_h=1}^{\mu_h} P_{hj_h},$$

és

$$(P_{hj_h}, P_{kj_k}) \sim 1, \quad (h \neq k).$$

Akkor $P_{hj_h} = 0$ *az* (A)*-ra vonatkozólag irreducibilis* $h+1$*-edfokozatú részlet-resolvens* és az *egyenletrendszerről*, a mely $P_{hj_h} = 0$-ból származik, ha $x = \sum_{i=1}^{m} t_i x_i$-t helyettesítünk, valamint az így értelmezett *sokaságról* is azt mondjuk, hogy (A)*-ban irreducibilis.*

Ebben az esetben a következő *az irreducibilitásra vonatkozó tétel* érvényesül:

Ha a $h+1$*-edfokozatú* $V^{(h+1)}$ *sokaságot oly egyenletrendszer értelmezi, a melynek együtthatói* (A)*-hoz tartoznak, akkor a* $P_{hj_h} = 0$ *egyenlet értelmezte,* (A)*-ban irreducibilis sokaságnak vagy összes elemei benne vannak* $V^{(h+1)}$*-ben, vagy pedig a közös elemek oly sokaságot alkotnak, a melynek fokozatszáma nagyobb* $h+1$*-nél.*

$V^{(h+1)}$-t minden esetre oly egyenletrendszer értelmezi, a melynek összresolvense a következő alakú:

$$d_t^{(h)} \ldots d_t^{(m-1)} = 0;$$

$d_t^{(i)}$-nek $(i < h)$ ugyanis 1-gyel kell egyenlőnek lennie, mivel a $V^{(h+1)}$ sokaság fokozatszáma épen $h+1$. Ha már most $d_t^{(h)}$ osztható P_{hj_h}-val, beáll az első eset; vagy pedig ellenkezőleg

$$\text{Res.} \begin{pmatrix} d_t^{(h)}, & P_{hj_h} \\ x, & 1 \end{pmatrix} = g(x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m).$$

E mellett g a 0-tól különböző és a resultáns képezési törvényének megfelelőleg a $d_t^{(h)}$ és P_{hj_h} formák lineáris formája. Az $x = \sum_{i=1}^{m} t_i x_i$ helyettesítés után tehát a $d_t^{(h)} = 0$ és $P_{hj_h} = 0$ egyenletek értelmezte sokaságok minden közös elemére nézve

$$g(x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m) = 0.$$

Ekkor azonban a $d_t^{(h)}=0$, $P_{hj_h}=0$ értelmezte egyenletrendszer összresolvense nem tartalmazhat oly részlet-resolvenst, a melynek fokozata $h+1$, vagy ennél alacsonyabb; mert, ha volna ilyen resolvens, akkor oly megoldásnak is kellene lennie, a melyben $x_{h+1}, \ldots, x_{m-1}$ megmaradnak mint határozatlanok, a mi pedig a $g=0$ következtében ki van zárva.

A további közös elemeket azok a sokaságok tartalmazzák, a melyeket a $d_t^{(h+1)}=0, \ldots$ egyenletek szolgáltatnak és így minden esetre oly sokaságoknak részei, a melyeknek fokozatszámai magasabbak $h+1$-nél.

Ha m-edfokozatú sokasággal van dolgunk, azaz olyannal, a mely véges számú az $\{A\}$-hoz tartozó értékrendszerből áll, akkor $V^{(m)}$ vagy az összes a $P_{m-1, j_{m-1}}=0$ meghatározta értékrendszereket tartalmazza, vagy egyiküket sem; mert a $V^{(m+1)}$ sokaságnak nincsen tartalma. Ebben az esetben ugyanis g a t-knek el nem tünő formája és egyáltalában nem lehetséges, hogy $g=0$. Ez az utóbbi eset egyszersmind az egy ismeretlent tartalmazó egyenletek irreducibilis voltára vonatkozó tételt is tartalmazza, a melyet mint fontos speciális esetet még részletesebben kell kifejtenünk.

Valamely egy ismeretlent tartalmazó

$$F(z)=A_0 z^n+A_1 z^{n-1}+\cdots+A_n=0 \qquad (A_0 \neq 0)$$

egyenlet összresolvensét az előadott utasítás szerint úgy alkotjuk, hogy bevezetjük $x=zt$-t és azután t^n-nel szorzunk. Az összresolvens tehát

$$t^n F\left(\frac{x}{t}\right)=A_0 x^n+A_1 x^{n-1} t+\cdots+A_n t^n=0.$$

Ha ebben ismét $x=zt$-t teszszük, akkor belőle $t^n F(z)=0$ származik; egy egyetlen egyenlet esetében tehát az összresolvensre vonatkozó tételek — mint előre látható volt — tautologiára vezetnek. De nem így az egyenlet irreducibilis voltára vonatkozó tétel, a mely ebben az esetben, a hol

mint «sokaság» egy egyenlet összes gyökei szerepelnek, a következő alakot nyeri:

Ha $G(z)=0$ bármely oly egyenlet, a melynek együtthatói (A)*-hoz tartoznak, akkor ezt az* (A)*-ban irreducibilis $F(z)=0$ egyenlet gyökei vagy mindannyian kielégítik, vagy pedig e gyökök közül egy sem**. Az «$F(z)=0$ egyenlet gyökének» fogalma itt természetesen {A}-ra vonatkozik.

Magától értetődik, hogy a tétel alapjául felvehető minden oly orthoid tartomány, mely az egyenletrendszer együtthatóit tartalmazza; jelesen tehát minden oly ($\bar{A}$) tartomány, a mely tartalmazza az (A) tartomány összes mennyiségeit. Ebből azután az irreducibilitásra vonatkozó tétel új fogalmazása következik, a mely, ellentétben az egy ismeretlent tartalmazó egyenlet esetében fellépő viszonyokkal, a végtelen sok elemet tartalmazó sokaságokra nézve jellemző.

A Φ_l minden tényezőkre bontása — mint azt a IV. fej. 18. §-ából tudjuk — már bizonyos az (A)-ból származó (G) genus-tartományban végezhető. Ha ezt a genus-tartományt veszszük fel alapúl, P_{hj_h} föltétlenül irreducibilis forma lesz és $P_{hj_h}=0$ *föltétlenül irreducibilis* $h+1$*-edfokozatú sokaságot* értelmez, a melyre a következő tétel vonatkozik.

Valamely föltétlenül irreducibilis $h+1$*-edfokozatú sokaság vagy teljesen benne van bármely más* $V^{(h+1)}$ *algebrai*

* Magától értetődik, hogy ez az irreducibilitásra vonatkozó legegyszerűbb tétel az egyenletrendszerek esetében szükséges körülményes fejtegetések nélkül is nyerhető. Ha ugyanis $F(z)$ irreducibilis, akkor vagy $G(z)=F(z)\Phi(z)$ és így $F(z)=0$ minden gyöke kielégíti egyszersmind a $G(z)=0$ egyenletet is; vagy pedig $F(z)$ és $G(z)$ resultánsa, R a 0-tól különböző. De ekkor az

$$R = G_1(z)\,F(z) + F_1(z)\,G(z)$$

kapcsolat mutatja, hogy egyetlen α-ra nézve sem lehet $F(\alpha)$ és $G(\alpha$ egyidejűleg 0.

$h+1$-edfokozatú sokaságban, vagy pedig a kettőnek közös elemei oly sokaságot alkotnak, a melynek fokozatszáma nagyobb $h+1$-nél.

Ama $V^{(h+1)}$ sokaság értelmezésére oly egyenletrendszer szolgál, a melynek együtthatói bizonyos raczionális tartományhoz tartoznak. Ha ehhez a (G) genus-tartomány mennyiségeit adjungáljuk, oly orthoid tartományt nyerünk, a mely az irreducibilitásra vonatkozó előbb levezetett tételben (A) helyébe léphet; mivel pedig P_{hj_h} ebben a tartományban is irreducibilis, evvel közvetetlenül megvan az épen kimondott tétel.

A $h+1$-edfokozatú, azaz az $m-h-1$-szeres sokaságot geometriai felfogásban *$m-h-1$-szeresen kiterjedt képződménynek* is nevezzük; ennek megfelelőleg az utolsó tétel még a következő módon is fogalmazható:

Valamely föltétlenül irreducibilis, k-szorosan kiterjedt (algebrai) képződmény esetében annak valamely szintén k-szorosan kiterjedt részét nem lehet algebrai egyenletrendszerrel jellemezni, hacsak ez a «rész» nem meríti ki már az egész képződményt.

Az m-edfokozatú sokaságok esetében, a melyek «0-szorosan kiterjedtek», azaz geometriai kifejezéssel élve «véges számú pontból állanak», e tétel elveszti tartalmát. A föltétlenül irreducibilis m-edfokozatú sokaságot ugyanis oly $P_{m-1,j_{m-1}}=0$ egyenlet értelmezi, a hol $P_{m-1,j_{m-1}}$ a $D_t^{(m-1)}$ egyik osztója. De (G)-ben $D_t^{(m-1)}$ oly $x-\sum_{i=1}^{m}\xi_i t_i$-alakú lineáris tényezőkre bomlik, a melyekben a ξ_i mennyiségek a (G) tartományhoz tartoznak és e szerint $P_{m-1,j_{m-1}}=0$ egyetlen egy $\xi_1,\ldots,\xi_{m-1}$ értékrendszert, «egyetlen egy pontot» értelmez, és ekkor a tétel közvetetlenül belátható.

8. §. Ha az $F_j=0$ egyenletrendszernek megfelelnek olyan resolvensek is, a melyeknek fokozatszáma kisebb m-nél, ak-

kor végtelen sok gyökrendszer van és a rendszer tartalmát nem lehet ezeknek teljes felsorolásával leírni. Mindamellett ezt a tartalmat teljesen jellemezhetjük az algebrai mennyiségek véges sorozatával. Ez úgy történik, hogy a $D_t^{(h)}=0$ egyenlet értelmezte $h+1$-edfokozatú sokaság helyett belevonjuk a tárgyalásba azokat a véges számú «*$h+1$-edfokozatú főmegoldásokat*», *a melyekben az* $x_{h+1}, \ldots, x_{m-1}$ *mennyiségeket nem választjuk többé «tetszés szerint», hanem meghagyjuk ezeket határozatlanoknak.* A 4. §. szerint $D_t^{(h)}$, mint az $x, t_1, \ldots, t_m$ mennyiségek formája most is felbontható lineáris tényezőkre; csakhogy ezeknek együtthatói valamely az

$$((A), x_{h+1}, \ldots, x_{m-1})$$

tartományból származó genus-tartományhoz tartozó mennyiségek. E lineáris tényezők alakja a következő*:

$$x - \sum_{r=1}^{h} \xi_r' t_r - \sum_{s=h+1}^{m-1} x_s t_s - \xi_m' t_m,$$

a hol a t-k együtthatói az épen említett genus-tartományhoz tartozó mennyiségek, a melyek összességükben nem származhatnak oly formatartományból, a mely kevesebb határozatlant tartalmaz. A mennyiségeknek ez a rendszere, a melyet $h+1$-edfokozatú főmegoldásnak neveztünk, t. i. mindig tartalmazza magukat az $x_{h+1}, \ldots, x_{m-1}$ határozatlanokat.

A különböző $h+1$-edfokozatú főmegoldások számát $D_t^{(h)}$ különböző lineáris tényezőinek száma, azaz $E_t^{(h)}$ foka szolgáltatja, a melyet előbb μ_h-val jelöltünk.

Ha $D_t^{(h)}$-t az $x, t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1}$, mennyiségek

* Ebből következik — a mit a későbbi alkalmazás miatt már itt megjegyzünk — hogy az $x = \sum_{i=1}^{m} t_i x_i$ helyettesítés után $D_t^{(h)}$-ból a $t_{h+1}, \ldots, t_{m-1}$ határozatlanok teljesen kiesnek; mert kiesnek minden lineáris tényezőből és így $D_t^{(h)}$-ből is. $[D_t^{(h)}]_{x=\sum_{i=1}^{m} t_i x}$ tehát az x-eknek és $t_{h+1}, \ldots, t_{m-1}$ kizárásával a t-knek formája.

formájának tekintjük és P_{hj_h} ennek egyik föltétlenül irreducibilis osztója, akkor a P_{hj_h} lineáris osztóinak megfelelő főmegoldások *conjugált megoldások*, még pedig abban az értelemben, hogy az ezekből összeállított $\sum_{r=1}^{h} \xi'_r t_r + \sum_{s=h+1}^{m-1} x_s t_s + \xi'_m t_m$ lineáris formák conjugált mennyiségek. E formák száma szolgáltatja annak a legkisebb genus-tartománynak rendszámát, a melyben azok mindannyian benne vannak (IV. fej. 14—19. §.). E rendszám természetesen P_{hj_h} foka; még pedig ha ezt l-lel jelöljük, akkor az egyes ξ' mennyiségek az $x_{h+1}, \ldots, x_{m-1}$ határozatlanoknak oly algebrai függvényei, a melyeknek rendszáma l-nek osztója, míg ama lineáris formának rendszáma pontosan l, a mi az épen idézett helyen használt módszerek alapján könnyen belátható.

Határozatlanoknak algebrai függvényei ugyanabban a viszonyban vannak változók algebrai függvényeivel, mint a formák az egész függvényekkel.

A $h+1$-edfokozatú főmegoldásokkal egyidejűleg teljesen meg vannak adva a $D_t^{(h)}$ lineáris tényezői is és így elvileg meg van határozva a $D_t^{(h)}$-nek megfelelő sokaság is*.

Magától értetődik, hogy azoknak a lineáris tényezőknek, a melyek valamely föltétlenül irreducibilis $P_{hj_k}=0$ sokaságnak megfelelnek, $D_t^{(h)}$-ben ugyanaz a kitevőjük.

Az természetesen nincsen kizárva, hogy bizonyos gyökrendszerek egyidejűleg mint különböző sokaságok elemei szerepelhessenek; de akkor minden egyes sokaságban külön kell azokat számlálnunk.

Közvetlenül látni, hogy az m-edfokozatú főmegoldások az $\{A\}$-ba tartozó mennyiségek rendszerei.

* Hogy egyes esetekben a főmegoldások mily módon függnek össze a $D_t^{(h)}$ sokaság előállításával, a következő §-ban fejtegetjük majd részletesen.

Bármely egyenletrendszer tartalmát a főmegoldások sorozata, azaz bizonyos számú algebrai mennyiség teljesen szolgáltatja. De még akkor is, ha az egyes megoldások összességét tekintjük, bármely mennyiség, a mely e megoldásokban szerepel, oly algebrai mennyiség, a milyent már valamely egy ismeretlent tartalmazó egyenlet értelmez; csak azt a megszorítást kell fentartanunk, hogy, a mennyiben bizonyos számú ismeretlen «tetszés szerinti» mennyiségnek választható, az így választott értékek is algebrai mennyiségek legyenek. Míg tehát semmi a fogalomalkotástól idegen elem nem lép be, az egy ismeretlent tartalmazó egyenletek meghatározta algebrai mennyiségek országa oly önmagában zárt ország, a mely egyenletrendszerek hozzávételével sem bővíthető többé.

Az egy ismeretlent tartalmazó egyenletet az æquivalentia-meghatározás értelmében annak megoldásai és az egyes megoldások «sokszorossága» teljesen megadják.

Ha ugyanis $f(x)$ és $g(x)$ ugyanazokat a lineáris tényezőket tartalmazzák, ugyanazokkal a kitevőkkel ellátva, akkor az együtthatók raczionális tartományára, mint æquivalentia-tartományra vonatkozólag $f(x) \sim g(x)$.

Hogy egyenletrendszerek esetében a viszonyok nem mindig ilyenek, az már itt is kiemelendő. Vannak egyenletrendszerek, melyeknek összresolvense ugyanaz, de azért még sem pótolhatják egymást teljesen. Erre egyszerű példát szolgáltat a következő két rendszer:

$$(x_1+x_2)^2=0, \quad x_1-x_2=0 \qquad \text{(I)}$$

és

$$(x_1-x_2)^2=0, \quad x_1+x_2=0. \qquad \text{(II)}$$

Mind a kettőnek összresolvense $x^2=0$, azaz mind a kettőnek megoldása a kétszer számlálandó $(0, 0)$ gyökrendszer. Mindamellett még sem mindegy, vajjon az $x_1+x_2=0$ egyenlethez

az (I) rendszert, vagy pedig a (II) rendszert csatoljuk-e hozzá. A második esetben az összresolvens marad $x^2=0$; míg az első esetben $x=0$ *.

* E kivételes esetek fellépésének tulajdonképeni oka abban rejlik, hogy az $F_j=0$ egyenletek {A}-ból vett gyökrendszereinek összessége, azaz e rendszer «tartalma» nem elegendő annak jellemzésére; ez csak akkor áll be, ha a vizsgálat körébe végtelen kis mennyiségeket is bevonunk. Mint már (a IV. fej. 9. §-ában) megemlítettük, ezt megtehetjük a nélkül, hogy az arithmetikai és algebrai módszerek talaját elhagynók. Erre ugyan e könyvben nem terjeszkedünk ki; de fentartva magunknak a részletes kifejtést, mégis czélszerű, ha kapcsolatban a szövegben bemutatott példával a dolog lényegét e legegyszerűbb esetben jellemezzük.

Legyen (A) az alapúl felvett orthoid tartomány; $a_1, a_2, \ldots$, $b_1, b_2, \ldots$ legyenek annak bármely mennyiségei; δ pedig új jelkép, a melyet *elsőrendü végtelen kis mennyiségnek* nevezünk. Akkor az

$$a_1+b_1\delta, \quad a_2+b_2\delta, \ldots$$

«mennyiségek», a melyek az összeadás és szorzás következő törvényét követik:

$$(a_1+b_1\delta)+(a_2+b_2\delta)=a_1+a_2+(b_1+b_2)\delta,$$
$$(a_1+b_1\delta)(a_2+b_2\delta)=a_1a_2+(a_1b_2+a_2b_1)\delta,$$

hyperorthoid tartományt alkotnak; ezt az (A) tartományból származó *elsőrendü infinitesimalis tartománynak* nevezhetjük. (E mellett valójában csak a mennyiségeknek $(a_1, b_1), \ldots$ párjaival van dolgunk és az $a_1+b_1\delta$ irásmódot csak a kényelem kedvéért használjuk; δ egyszerűen a (0, 1) mennyiségpár jele).

Most már nem ugyanaz az (I) és (II) rendszerek tartalma. Az (I) rendszert kielégíti a mennyiségek minden $x_1=a\delta$, $x_2=a\delta$ rendszere, a (II) rendszert pedig a mennyiségek minden $x_1=a\delta$, $x_2=-a\delta$ rendszere, a hol a az (A) tartomány bármely mennyisége lehet. Úgy az (I), mint a (II) rendszert végtelen sok gyökrendszer elégíti ki, a mely mindannyi «végtelen közel» esik a (0, 0) megoldáshoz. Közös gyökrendszerük azonban csak az egyetlen (0, 0) gyökrendszer.

Tiszta sokaságok főelőállítása.

9. §. Valamely *tiszta* $h+1$-*edfokozatú* (algebrai) *sokaságot*, $V^{(h+1)}$-t, bármely módon legyen is megadva, a megelőzők szerint kellő lineáris transformatio után végül mindig bizonyos

$$\varphi(x; t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1})$$

forma jellemez; még pedig oly módon, hogy φ, ha $E_l^{(h)}=0$ valamely teljes $h+1$-edfokozatú redukált resolvens, az $E_l^{(h)}$ osztója és

$$[\varphi]_{x=\sum_{i=1}^{m} x_i t_i}=0$$

rövid összefoglalásban azt az egyenletrendszert jelenti, a melynek tartalma a $V^{(h+1)}$ sokaság összes elemeiből és csakis ezekből áll. Az a kifejezés ugyanis a t-k hatványszorzatai szerint rendezendő és azután minden egyes hatványszorzat együtthatója 0-sal egyenlővé teendő.

E szerint, ha $x_1, \ldots, x_m$ a $V^{(h+1)}$-nek egyik eleme, akkor $x = \Sigma x_i t_i$ tétetvén, φ mindig azonosan zérus és ugyanannak kell beállania $t_1, \ldots, t_m$ szerint vett deriváltjaira vonatkozólag is.

Ha továbbá bevezetjük a következő rövidítéseket:

$$\frac{\partial \varphi}{\partial x} = \varphi_0, \quad \frac{\partial \varphi}{\partial t_i} = \varphi_i,$$

és a szögletes zárójelt már az $x = \Sigma x_i t_i$ hozzátétel nélkül is e helyettesítés jelölésére használjuk, akkor egyszersmind

$$[\varphi_0] x_i + [\varphi_i] = 0.$$

Minthogy φ-nek nincsenek többszörös osztói, φ-nek x szerint vett discriminánsa a $t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1}$ mennyiségeknek a zérustól különböző formája és meghatározhatunk akárhány oly

$$t_i = a_i, \quad a_m \neq 0$$

értékrendszert, a melyre nézve

$$\varphi(x; a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1})$$

discriminánsa az $x_{h+1}, \ldots, x_{m-1}$ határozatlanoknak a 0-tól különböző formája. E discrimináns legyen $\Delta_a(x_{h+1}, \ldots, x_{m-1})$.

Akkor

$$\begin{aligned} [\varphi]_a &= \varphi(x, a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1}) = 0, \\ [\varphi_0]_a x_i + [\varphi_i]_a &= 0, \qquad (i=1, \ldots, h) \end{aligned} \tag{I}$$

a hol a $[\cdots]_a$ jelkép a $t_i = a_i$ helyettesítés elvégzésére utasít, *a $V^{(h+1)}$ sokaság $h+1$ egyenletből álló oly főelőállítását szolgáltatja, a melyben a $V^{(h+1)}$-ben foglalt és a $\Delta_a = 0$ egyenlet által megadott, legfölebb* $h+2$-edfokozatú sokaság kivételes helyzetet foglal el.*

Ha ugyanis $x_1, x_2, \ldots, x_m$ a $V^{(h+1)}$ sokaság bármely oly eleme, a melyre nézve Δ_a a 0-tól különböző, akkor, minthogy φ lineáris tényezőkre való felbontásának $t_i = a_i$-re nézve is meg kell maradnia, a $\varphi = 0$ egyenlet gyökei közt

$$x = \sum_{i=1}^{m} a_i x_i$$

is előfordúl, hacsak $x_{h+1}, \ldots, x_{m-1}$ a $V^{(h+1)}$ valamely elemének koordinátái. Minthogy pedig $\varphi = 0$-ra nézve $\left[\frac{\partial \varphi}{\partial x}\right]_a = [\varphi_0]_a$ nem 0, az (I) második sorában előfordúló egyenletekből $x_1, \ldots, x_h$ és végre az

$$x = \sum_{i=1}^{m} a_i x_i \quad \text{vagy} \quad [\varphi_0]_a x_m + [\varphi_m]_a = 0$$

egyenletből x_m is egyértelműleg kiadódik, az $x, x_{h+1}, \ldots, x_{m-1}$ mennyiségekkel kifejezve. Viszont pedig a $[\varphi]_a = 0$ egyenlet minden gyöke az $x = \Sigma a_i x_i$ alakban állítható elő, a hol $x_1, \ldots, x_m$ a $V^{(h+1)}$ egyik eleme. Ha tehát a $\Delta_a = 0$-ban foglalt elemeket kizárjuk, (I) minden megoldása $V^{(h+1)}$ egy elemét szolgáltatja és viszont.

* A «legfölebb» szó azért volt közbeiktatandó, mert meglehet, hogy Δ_a-ból az x-ek teljesen kiesnek; ekkor pedig a $\Delta_a = 0$ egyenletnek «nincs tartalma».

Tekintettel arra a kivételes helyzetre, a melyet a $\Delta_a=0$ elemei elfoglalnak, ama főelőállítást kétféle módon értelmezhetjük.

a) Az (I) egyenletek a $\Delta_a \neq 0$ feltétel hozzácsatolásával a $V^{(h+1)}$ sokaság oly főelőállítását szolgáltatják, a mely annak elemeit bizonyos kiváló, legfölebb $h+2$-edfokozatú $W^{(h+2)}$ sokaság kizárása után teljesen és kizárólagosan szolgáltatja. Ama kizárt kiváló sokaság két teljesen különböző jellemű részből alakúl. A $V^{(h+1)}$ sokaságnak lehet singuláris sokasága is (l. a 6. §. végét) és ekkor ez, minthogy erre nézve Δ_a épen az a-k bármely választása mellett zérus, minden esetre benne lesz $W^{(h+2)}$-ben. Ellenben minden más elemének föllépése az a-k választásától függ, vagyis geometriai kifejezésmóddal élve, minthogy $x = \Sigma a_i x_i$ koordináta-transformatiót jelent, a koordinátarendszer specziális választásának következménye. Mihelyt ugyanis

$$\varphi(x, t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1})$$

-nek x szerint vett discriminánsa nem azonosan egyenlő zérussal, meghatározhatunk oly $t_i = a_i$ értékrendszert is, a melyre nézve már Δ_a *nem* 0.

b) Az (I) egyenletek minden további megszorító feltétel nélkül szolgáltatják a $V^{(h+1)}$ sokaság összes elemeit, de ezeken kívül még $(x_1, \ldots, x_m)$ mindazon elemeit is, a melyekre nézve $\Delta_a(x_{h+1}, \ldots, x_{m-1})=0$, $x_1, \ldots, x_h$ tetszés szerint választott értékek, x a $[\varphi]_a=0$ egyenlet valamely többszörös gyöke, x_m pedig az $x = \Sigma a_i x_i$-ből határozandó meg. Az így jellemzett elemek, mint közvetetlenül látni, egy további másodfokozatú sokaságot alkotnak. Mindaddig ugyanis, míg $\Delta_a \neq 0$, a viszonyok ugyanazok, mint előbb; valamint akkor is, ha $\Delta_a=0$, de x nem többszörös gyöke a $[\varphi]_a=0$ egyenletnek. Ha ellenben $\Delta_a=0$ és x a $[\varphi]_a=0$ egyenlet többszörös gyöke, akkor egyszersmind $[\varphi_0]_a=0$. Az (I) egyenletek

tehát csak úgy elégíthetők ki, ha továbbá:

$$[\varphi_i]_a=0. \qquad (i=1,\ldots,h)$$

Minthogy azonban eredeti egyenletrendszerünket már kellő lineáris transformatióval átalakítottnak veszszük, mindig van a sokaságnak oly eleme, mely megfelel a most megállapított $x, x_{h+1}, \ldots, x_{m-1}$ értékeknek. Az ezen elemeknek megfelelő $x_1, \ldots, x_h$ értékek pedig szükségkép kielégítik az (I) második sorában álló egyenleteket; azaz $\Delta_a=0$ *és* $[\varphi_0]_a=0$-ból mindig következik, hogy

$$[\varphi_i]_a=0. \qquad (i=1,\ldots,h)$$

Így tehát (I)-ből csak az első sorban álló egyenlet marad hátra; tehát $(x_1, \ldots, x_m)$ szabad változását két egyenlet szorítja meg, a melyek közül az egyik x_{h+1}-et, a másik x_m-et határozza meg a többi x segítségével. Abban az esetben, midőn Δ_a az x_{h+1}-re nézve nem szabályos, ismét úgy mint előbb bizonyos lineáris transformatiót kell alkalmaznunk.

Hogy egyszerű példát is lássunk, legyenek valamely tiszta algebrai térgörbe főelőállítására x, x_1, x_2 már is a közönséges DESCARTES-féle koordináták; akkor az a főelőállítás, ha az a-k alatt is már speciális számokat értünk, a következő lesz:

$$\varphi(x, x_2)=0,$$
$$\varphi_0(x, x_2)\,x_1+\varphi_1(x, x_2)=0,$$

a hol φ_0 és φ egyidejűleg csak azokra az értékrendszerekre nézve egyenlők zérussal, a melyekre nézve egyszersmind a φ-knek x szerint vett discriminánsa és $\varphi_1(x, x_2)$ is zérus. Az algebrai térgörbe e főelőállításába tehát mint felesleges rész véges számú párhuzamos egyenes lép be.

10. §. Bizonyos esetekben azonban a főelőállítás mégis már az adott sokaság teljes és kizárólagos előállítását szolgáltatja; így történik ez pl. minden az $(x_1, \ldots, x_m)$-ben fog-

lalt első- és m-edfokozatú sokaság esetében. Erre vonatkozólag a következő tételek érvényesek:

A tiszta elsőfokozatú sokaságot mindig teljesen és kizárólagosan egy egyenlet tartalma adja meg.

Ugyanis a 9. §. következtetéseit ismételve, az (I) másodfajú egyenletei teljesen elmaradnak. Ugyanerre az eredményre abból is juthatni, hogy a 8. §. első jegyzete szerint D_t az $x=\sum_{i=1}^{m} t_i x_i$ substitutio alkalmazása folytán t_m homogén formájába megy át és így felveszi a $t_m^k \Phi$ alakot; ugyanaz érvényes tehát D_t minden osztójára nézve is és így a megfelelő elsőfokozatú sokaság teljes értelmezését a $\varphi=0$ egyenlet adja.

Továbbá:

Minden az $(x_1, \ldots, x_m)$-ből származó m-edfokozatú sokaságot, azaz a véges számmal levő

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk} \qquad (k=1, 2, \ldots, N)$$

értékrendszereket egy m egyenletből álló rendszer tartalma teljesen és kizárólagosan szolgáltatja.

Ama Δ_a-val jelölt discrimináns ugyanis most olyan a 0-tól különböző mennyiség, a mely egyetlen x-et sem tartalmaz; ebben az esetben tehát semmiféle singuláris vagy kiváló elemek nem lépnek fel.

Ha $0<h<m-1$, akkor az (I) egyenletek $V^{(h+1)}$-n kívül még egy másodfokozatú sokaságot is szolgáltathatnak, mely azonban, ha Δ_a az x-ektől független (és természetesen a 0-tól különböző) mennyiség, el is eshetik.

Ha fellép is ez a másodfokozatú sokaság, mégis jogosan használhatjuk az (I) egyenleteket a $V^{(h+1)}$ előállítására; mert azok ezt a sokaságot teljesen meghatározzák. Ha ugyanis megalkotjuk az (I) rendszer teljes resolvensét, ennek a másodfokozatú részlet-resolvensen kívül még ahhoz a $h+1$-edfokozatú resolvenshez is kell vezetnie, a mely $V^{(h+1)}$-t telje-

sen és kizárólagosan értelmezi. (I) ugyanis csak ama két sokaságot szolgáltatja, a melyet *elkülönítve* kell nyernünk, mivel közös elemeik legfölebb $h+2$-edfokozatú sokaságot alkotnak.

Hogy valamely $V^{(h+1)}$ sokaság főelőállításának fogalma természetszerűen most még mily módon bővíthető, az kézzel fogható. Ily bővítésnek kell tekintenünk minden $h+1$ egyenletből álló rendszert, a mely $V^{(h+1)}$ összes elemeit és csak ezeket értelmezi, hacsak kizárjuk egy oly tiszta elsőfokozatú $\psi=0$ sokaság összes elemeit, a melynek $V^{(h+1)}$-vel közös elemei legalább $h+2$-edfokozatú sokaságot alkotnak *.

Még röviden meg akarjuk említeni «a leképezés elméletének» ebből az előállításból folyó alaptételét **.

Minden tiszta $h+1$*-edfokozatú sokaság,* $V^{(h+1)}$*, a mely bármely* $(x_1, \ldots, x_m)$ *sokaságból ered és az* $m-h$*-szorosan kiterjedt* $(z_1, z_2, \ldots, z_{m-h})$ *sokaságból eredő bizonyos elsőfokozatú sokaság közt oly kölcsönösen egyértelmű vonatkozás létesíthető, a melynek legfölebb bizonyos a* $V^{(h+1)}$*-ben foglalt* $h+2$*-edfokozatú sokaságra nézve vannak kivételei.*

Ha $x, x_{h+1}, \ldots, x_{m-1}$-et független változóknak tekintjük, akkor ezen az $(x, x_{h+1}, \ldots, x_{m-1})$-ben foglalt elsőfokozatú sokaság, $[\varphi]_a=0$ a $V^{(h+1)}$-vel a jellemzett kölcsönösen egyértelmű vonatkozásban áll, a melyet épen az (I) egyenletek fejeznek ki; ezekhez még a teljesség kedvéért hozzácsatolhatjuk az ezekből eredő

$$[\varphi_0]_a x_m + [\varphi_m]_a = 0$$

egyenletet.

* A főelőállítás neve (figuration principale) Molk-tól származik, kinek már idézett értekezésében (a 153. lapon) találni a most adott értelemben vett főelőállítást.

** Kronecker, Festschrift, 10. §.

Tetszés szerinti sokaságok előállítása $m+1$ egyenlet segítségével.

11. §. Áttérünk már most KRONECKER-nek következő, bebizonyítás nélkül közlött alapvető tételére*:

Bármely oly $F_j=0$ $(j=1,\ldots,k)$ *egyenletrendszernek, a melyben az ismeretlenek* $x_1,\ldots,x_m$, *tartalma teljesen és kizárólagosan megadható egy legfölebb* $m+1$ *egyenletből álló rendszer segítségével.*

Minthogy magától értetődik, hogy e tétel független az ismeretlenekre alkalmazott oly lineáris transformatiótól, a melynek determinánsa a 0-tól különböző, az adott $F_j=0$ rendszert már olyannak tekinthetjük, a mely a régebben kifejtett értelemben esetleges körülményektől meg van szabadítva. Minthogy azonban most csak az egyenletrendszer tartalmáról van szó, mindenekelőtt a rendszer redukált resolvensét (7. §.), a mely

$$\Psi_t=\prod_{h=0}^{m-1}\prod_{j_h=1}^{\mu_h}P_{hj_h}=0,$$

vehetjük alapúl; azután pedig még feltételezhetjük, hogy az a sokaság, a melyet ismeretes módon a

$$P_{hj_h}=0$$

egyenlet értelmez és a mely része az előállítandó tartalomnak, nincsen meg teljesen a

$$P_{kj_k}=0 \qquad (k<h)$$

értelmezte sokaságban; mert ebben az esetben $\Psi_t=0$ a P_{hj_h} tényező eltávolítása után is már teljesen megadja az $F_j=0$ tartalmát. Annak eldöntésére, vajjon valamely P_{hj_h} ebben az értelemben a tartalom előállítására felesleges-e, csak a

$$P_{kj_k}=0, \quad P_{hj_h}=0 \qquad (P)$$

által összefoglalt egyenletrendszereket kell megvizsgálnunk.

* KRONECKER, Festschrift 10. §.

Ilyen (P) rendszer $P_{hj_h}=0$ következtében oly sokaságot szolgáltat, a melynek fokozatszáma legalább $h+1$. Ha felállítjuk tehát a (P) rendszer összresolvensét, akkor ebben az a részletresolvens, a melynek fokozatszáma a legkisebb, vagy $h+1$-ed- vagy pedig ennél is magasabb fokozatú lesz. Az első esetben tehát annak a sokaságnak, a melyet ez a resolvens értelmez, az irreducibilis $P_{hj_h}=0$ sokaságot teljesen kell tartalmaznia és így $P_{hj_h}=0$ tartalma teljesen benne lesz a $P_{kj_k}=0$ tartalmában. A második esetben $P_{kj_k}=0$ és $P_{hj_h}=0$ közös elemei oly sokaságot alkotnak, a melynek fokozata legfölebb $h+2$ és $P_{kj_k}=0$ csak egy $V^{(h+2)}$ sokaságot tartalmaz $P_{hj_h}=0$-ból.

Miután így minden egyes P_{hj_h}-ra nézve eldöntöttük, vajjon az szükséges-e az $F_j=0$ rendszer teljes tartalmának előállítására, e tartalmat abból az egyenletrendszerből nyerjük, a melyet

$$\psi=\prod_{h=0}^{m-1}\prod_{j_h=1}^{\nu_h} Q_{hj_h}=0$$

szolgáltat, a hol a

$$Q_{kj_k}=0, \quad Q_{hj_h}=0 \qquad (k<h)$$

értelmezte sokaságok közös elemei legalább $h+2$-edfokozatú sokaságot alkotnak.

A

$$\psi(x, x_1, \ldots, x_{m-1}, t_1, \ldots, t_m)=0$$

egyenlet is az $F_j=0$ rendszer resolvense; mert annak a rendszernek a tartalma, a mely úgy származik, ha a $t_1^{a_1}\ldots t_m^{a_m}$ hatványszorzatok együtthatóit egyenként egyenlővé teszszük zérussal, teljesen megegyezik $F_j=0$ tartalmával. Ezt az egyenletet *az $F_j=0$ rendszer minimális resolvensének* nevezhetjük; mert $F_j=0$ tartalmának összefoglalása az első-, másod-, stb. fokozatú sokaságok bizonyos sorozatában feltétlenül tartalmazza azokat a sokaságokat, a melyeket a minimális resolvens szolgáltat. Ha $V^{(h+1)}$ az $F_j=0$ rendszer

első oly irreducibilis sokasága volna, a melyet nem szolgáltat egyszersmind $\psi=0$ is, akkor annak valamely a $\psi=0$-ból származó alacsonyabb fokozatú sokaságban benne kellene lennie és az $F_j=0$ tartalmának jellemzésére felesleges volna. Evvel szemben szükséges azonban minden egyes oly sokaságnak felsorolása, a mely $\psi=0$-ból ered; mert ily sokaságnak azon elemei, a melyeket valamely más, a $\psi=0$-ból eredő sokasággal közösen bír, csupán csak magasabb fokozatú sokaságot alkothatnak.

Ebből egyszermind világos az is, hogy *két egyenletrendszer tartalma akkor és csak akkor lehet ugyanaz, ha minimális resolvenseik ugyanazok.*

Hogy a következőt rövidebben összefoglalhassuk, a minimális resolvenst még a következő módon írjuk:

$$\psi=\psi^{(0)}\psi^{(1)}\ldots\psi^{(m-1)},$$

a hol

$$\psi^{(h)}=\prod_{j_h=1}^{\nu_h} Q_{hj_h}.$$

Most már könnyen bebizonyíthatjuk a következő tételt:

Legyen az $F_j=0$, $(j=1,\ldots,k)$ *egyenletrendszer minimális resolvense* $\psi=0$; *legyen továbbá*

$$G_r^{(h)}=0 \qquad (r=1,2,\ldots) \qquad (\Sigma_{h+1})$$

oly egyenletrendszer, melynek tartalma teljesen magában foglalja az $F_j=0$ *rendszer tartalmát és ezen fölül csak* $h+1$*-ed vagy még magasabb fokozatú sokaságokat ölel föl. Akkor mindig meghatározhatjuk a mennyiségeknek oly* $a_1,\ldots,a_m$ *rendszerét (még raczionális és egész számokból állót is), hogy a*

$$[\psi]_{x=\Sigma a_i x_i}=0, \quad G_r^{(h)}=0 \quad (r=1,2,\ldots) \qquad (\Sigma_{h+2})$$

rendszer tartalma, mely természetesen ismét teljesen magában foglalja az $F_j=0$ *rendszer tartalmát, ezen fölül már csak* $h+2$*-ed vagy még magasabb fokozatú sokaságokból áll.*

A történt megállapítások folytán és a minimális resolvens tulajdonságai alapján a (Σ_{h+1}) minimális resolvense ily alakú lesz:

$$\varrho_{h+1}=\psi^{(0)}\psi^{(1)}\ldots\psi^{(h-1)}\chi^{(h)}\ldots\chi^{(m-1)}=0,$$

hol $\chi^{(h)}$ osztható $\psi^{(h)}$-vel. Ha $\chi^{(h)}\sim\psi^{(h)}$, tételünk — mint közvetetlenül látni — érvényes, akárhogy választjuk is az a mennyiségeket.

Az ellenkező esetben

$$\chi^{(h)}=\psi^{(h)}\chi_1^{(h)}$$

és $\chi_1^{(h)}$ nem ~ 1. A $\chi_1^{(h)}$ irreducibilis tényezői a $\psi^{(h)}$-éitól különbözők lesznek, és ha egyikük $\pi^{(h)}$, akkor $\pi^{(h)}=0$ a minimális resolvens értelmezése szerint nem tartalmazhat valamely $\psi^{(j)}=0$ sokasággal közös oly sokaságot, a melynek fokozatszáma kisebb $h+2$-nél. Vannak tehát olyan $x_i=\xi_i$ mennyiségek, a melyek bizonyos meghatározott, az (A)-ból származó genus-tartományhoz tartoznak és a melyekre nézve $[\pi^{(h)}]=0$, míg $[\psi]$ a 0-tól különböző és ugyanilyen marad akkor is, midőn a t-k helyébe bizonyos $a_1,\ldots,a_m$ mennyiségek rendszerét teszszük (a mely még raczionális és egész számokból is állhat). Ekkor azonban a Σ_{h+2} rendszer minimális resolvense, $\varrho_{h+2}=0$ csakugyan megfelel a tételnek; mert $\psi^{(0)},\psi^{(1)},\ldots,\psi^{(h)}$ a ϱ_{h+2}-nek osztói, a $\pi^{(h)}$ pedig, valamint — az a-k kellő választásánál — $\chi_1^{(h)}$ többi irreducibilis osztója a $[\psi]_{x=\Sigma a_i x_i}=0$ egyenlet hozzálépése miatt nem lehet ilyen. Más $h+1$-ed vagy alacsonyabb fokozatú sokaság végre nem felelhet meg (Σ_{h+2})-nek, mert már (Σ_{h+1})-nek sem felel meg.

Ámde kiindulhatunk valamely $[\psi]_{x=\Sigma a_i x_i}=0$ egyenletből, mint (Σ_1) rendszerből és végre majd a

$$\psi(\Sigma a_{ri}x_i, x_1,\ldots,x_{m-1}, a_{r1},\ldots,a_{rm})=0 \qquad (S_k)$$
$$(r=1,\ldots,k)$$

egyenletrendszerhez jutunk, a melynek minimális resolvense

az $F_j=0$ rendszerével megegyező. Ekkor azonban a két rendszer tartalma is ugyanaz; az (S_k) egyenleteinek száma pedig — a mint az e §. elején kimondott tétel állítja — $\leqq m+1$. Ha ugyanis k az egyenletek száma, az (S_k) rendszer tartalma az $F_j=0$ rendszerétől már csak k-adfokozatú, vagy még ennél is magasabb fokozatú sokaságokban különbözhetik; a $k=m+1$ esetben tehát csak $m+1$-edfokozatú sokaságokban, a melyeknek már nincsen tartalmuk*.

Egyenletrendszerek, a melyeknek tartalma lineáris sokaságot alkot.

12. §. *Lineáris sokaságnak* nevezzük az olyan sokaságot, a melyet lineáris egyenletek rendszere értelmez.

Könnyű felismerni, hogy a lineáris egyenletek valamely

$$c_{i1}x_1+c_{i2}x_2+\cdots+c_{im}x_m+c_{i,m+1}=0 \qquad (1)$$
$$(i=1,\ldots,k)$$

rendszerének összresolvense milyen alakú. Ha ezeknek az egyenleteknek bal oldalai — a mint azt mindig feltételezzük — szabályos formák, (vagy pedig szükség esetén azokat valamely alkalmas lineáris transformatio segítségével ilyenekké átalakítottuk), akkor az x_m együtthatójával, a c_{im} mennyiséggel osztani lehet és az adott rendszer az

$$x=t_1x_1+t_2x_2+\cdots+t_mx_m$$

transformatio alkalmazása után a következő alakot veszi fel:

$$x-x_1t_1-\cdots-x_{m-1}t_{m-1}-X_{im}t_m=0, \qquad (2)$$
$$(i=1,2,\ldots,k)$$

* Vahlen igen érdekes példán kimutatta, hogy valóban vannak esetek, midőn m ismeretlent tartalmazó egyenletrendszer tartalma nem állítható elő kevesebbel, mint $m+1$ egyenlettel. («Bemerkung zur vollständigen Darstellung algebraischer Raumcurven». Journal f. r. u. a. Mathematik. 108. köt. 346. l.).

a hol X_{im} az $x_1, \ldots, x_{m-1}$ mennyiségeknek lineáris formája. Minthogy azonban itt csupa lineáris formával van dolgunk, csak a következő két eset lehetséges. A (2) egyenletek bal oldalai vagy kivétel nélkül egymással æquivalens formák és így tehát bármelyik közülök a teljes elsőfokozatú részlet-resolvens, $D_t=0$; de akkor az $\overline{F}_j$-k (a melyek a III. fej. 18. §-a szerint alkotandók) mindannyian æquivalensek 1-gyel és $D_t=0$ már az összresolvens. Vagy pedig $D_t \sim 1$ és az $\overline{F}_j$ formák azok a formák, a melyek a (2)-ben a bal oldalon állanak. Ekkor tehát

$$\sum_{i=1}^{k} u_i (x - x_1 t_1 - \cdots - x_{m-1} t_{m-1} - X_{im} t_m)$$

és

$$\sum_{i=1}^{k} u'_i (x - x_1 t_1 - \cdots - x_{m-1} t_{m-1} - X_{im} t_m)$$

x_1 szerint vett resultánsa képezendő, és ebben az u-k és u'-k hatványszorzatainak együtthatói lesznek az $F_{j_1}^{(1)}$ formák.

Közvetetlenül felismerjük, hogy ama resultáns és így tehát az $F_{j_1}^{(1)}$ formák is az $x, x_2, \ldots, x_{m-1}$ mennyiségek lineáris formái. Az utóbbiak vagy ismét kivétel nélkül egymással æquivalens formák és akkor úgy, mint előbb bármelyik közülük a rendszer összresolvensét, $D_t^{(1)}=0$-t szolgáltatja; vagy pedig $D_t^{(1)} \sim 1$. Az eljárást hasonló módon folytatva, felismerjük, hogy a lineáris egyenletek rendszerének vagy egyáltalában nincsen tartalma, vagy pedig van oly

$$x - X_1 t_1 - \cdots - X_h t_h - x_{h+1} t_{h+1} - \cdots - x_{m-1} t_{m-1} - X_m t_m = 0 \quad (A)$$

alakú összresolvense, a hol $X_1, \ldots, X_h, X_m$ az $x_{h+1}, \ldots, x_{m-1}$ mennyiségek lineáris formái. A bal oldalon álló formának ugyanis utolsó fejtegetéseink szerint az $x, x_{h+1}, \ldots, x_{m-1}$ mennyiségek lineáris formájának és (e fej. 4. §. szerint) mint teljes $h+1$-edfokozatú részlet-resolvensnek az $x, t_1, \ldots, t_m$

határozatlanok oly homogén formájának kell lennie, a melyben x legmagasabb hatványának együtthatója a t-ket nem tartalmazza. A kérdéses forma tehát az $x, t_1, \ldots, t_m$ határozatlanok sorozatára nézve is lineáris lesz.

Magától értetődik, hogy (A) az (1) rendszernek, ha ennek egyáltalában van tartalma, egyszersmind minimális resolvense is és így ebben az esetben (1)-et az esetleg alkalmazandó lineáris transformatio után egyszersmind az

$$x_i = X_i, \quad x_m = X_m \quad (i=1, \ldots, h) \qquad (A_1)$$

«legegyszerűbb» alakra hoztuk.

Minthogy azonban két egyenletrendszer tartalma csak akkor lehet ugyanaz, ha minimális resolvenseik megegyeznek, ebből a következő tétel foly:

Bármely egyenletrendszer tartalma akkor és csak akkor alkothat lineáris sokaságot, ha minimális resolvense olyan alakú, mint (A) és ekkor e lineáris sokaság raczionális müveletek segítségével megadható a (A_1) alakban.

E mellett még kiemelendő a *homogén lineáris rendszer* esete. Közvetetlenül belátható, hogy homogén lineáris rendszer akkor és csak akkor értelmezhet lineáris sokaságot, ha az $x_i = 0$ $(i=1, \ldots, m)$ elemet tartalmazza.

13. §. *Valamely egyenletrendszer tartalma «$\{A\}$-ban sereget alkot», ha $(\xi_1', \ldots, \xi_m')$ és $(\xi_1'', \ldots, \xi_m'')$-mel egyidejüleg u és v bármely értékei mellett $(u\xi_1' + v\xi_1'', \ldots, u\xi_m' + v\xi_m'')$ is gyökrendszer.*

Az a két (triviális) határeset, a melyben az egyenletrendszernek vagy nincsen tartalma, vagy pedig az egyenletrendszer az $x_1, \ldots, x_m$ változó voltának semmi korlátot sem szab, a következőkben már kizártnak tekinthető.

«Egymástól független»-nek mondjuk az oly k gyökrendszert:

$$\xi_{1j}, \xi_{2j}, \ldots, \xi_{mj}, \qquad (j=1, \ldots, k; k \leq m)$$

a melyre nézve az összes a

$$|\xi_{ij}| \qquad (i=1,\ldots,m, j=1,\ldots,k)$$

matrixból alkotott k-adfokú determinánsok a 0- *tól különbözők.*

Ha az egyenletrendszer igazi, azaz olyan, a mely az $x_1,\ldots,x_m$ változó voltának valóban korlátot szab, tehát nem áll csupa identitásból és tartalma $\{A\}$-ban sereget alkot, akkor csak $m-1$ egymástól független gyökrendszere lehet. Ha ugyanis m egymástól független gyökrendszere volna, akkor az

$$x_i=\sum_{j=1}^{m} u_j \xi_{ij} \qquad (i=1,\ldots,m)$$

lineáris egyenletrendszer determinánsa, $|\xi_{ij}|$ nem volna zérus és így az x_i-k bármely értékrendszerének megfelelőleg meghatározhatnók az u_i-k oly értékrendszerét, a mely ezt az egyenletrendszert kielégítené. A sereg értelmezése szerint azonban akkor $(x_1,\ldots,x_m)$ is gyökrendszer; amaz egyenletrendszernek tehát csupa identitásból kellene állania.

Ha az adott egyenletrendszer tartalma $\{A\}$-ban sereget alkot, akkor ezek szerint mindig van olyan az m-nél kisebb, nem negativ egész szám, k, hogy az egymástól független gyökrendszerek száma pontosan k, de nem több. A sereget ekkor *k-tagú seregnek* nevezzük. (A $k=0$ eset megfelel olyan rendszernek, a melynek csak az egyetlen $x_i=0$ megoldása van.)

Ha a sereg k-tagú és

$$\xi_{1j},\ldots,\xi_{mj} \qquad (j=1,\ldots,k)$$

k egymástól független gyökrendszer, $x_1,\ldots,x_m$ pedig oly gyökrendszer, a mely kielégíti az egyenletrendszert, akkor abban a matrixban, a mely $|\xi_{ij}|$-ből származik, ha ahhoz, mint $k+1$-dik oszlopot $x_1,\ldots,x_m$-et hozzácsatoljuk, minden $k+1$-edfokú determinánsnak 0-sal kell egyenlőnek lennie.

Ha az x ismeretlenek sorozatát és a ξ_{ij} gyökrendszereket alkalmasan rendezzük, feltehetjük, hogy a $|\xi_{ij}|\ (i, j = 1, \ldots, k)$ determináns a 0-tól különböző és ekkor a lineáris egyenleteknek oly rendszere,

$$\zeta x_{k+l} + \zeta_{l1} x_1 + \cdots + \zeta_{lk} x_k = 0, \quad (l=1, \ldots, m-k) \qquad (I)$$

keletkezik, a melyben ζ a 0-tól különböző és ez az adott egyenletrendszer tartalmát teljesen szolgáltatja. A rendszernek most feltételezett tulajdonságai alapján megfelel oly gyökrendszer, a melyben $x_1, \ldots, x_k$ tetszés szerinti értéket vesz fel. Másrészt, minthogy a megoldások sereget alkotnak, szükséges, hogy $\xi_{1j}, \ldots, \xi_{mj}$-vel $(j=1, \ldots, k)$ egyidejűleg

$$x_i = \sum_{j=1}^{k} u_j \xi_{ij} \qquad (i=1, \ldots, m)$$

is gyökrendszer legyen, bármely értékük legyen is az u_j mennyiségeknek. Az

$$x_i = \sum_{i=1}^{k} u_j \xi_{ij} \qquad (i=1, \ldots, k)$$

egyenletekből azonban, bárhogy választottuk is az $x_1, \ldots, x_k$ mennyiségeket, mindig az u_j mennyiségek oly rendszere származik, a mely ezeket az egyenleteket kielégíti. A hozzá tartozó $x_{k+1}, \ldots, x_m$ értékek pedig csakis azok lehetnek, a melyek (I)-t kielégítik; mert ilyen rendszer mindig van és ennek azután (I)-t is ki kell elégítenie. Evvel tehát a következő tételhez jutottunk:

Ha valamely egyenletrendszer tartalma k-tagú sereget alkot, akkor ezt teljesen és kizárólagosan oly m—k-adfokozatú lineáris sokaság állítja elő, a mely tartalmazza a $(0, 0, \ldots, 0)$ *elemet; értelmezését tehát m—k homogén lineáris egyenlet adja, a mely olyan alakú, mint* (I).

Közvetetlenül világos, hogy e tétel megfordítható.

Vajjon valamely egyenletrendszer ilyen-e, azt a minimális resolvens képezésével, azaz raczionális műveletek bizo-

nyos véges sorozatával mindig eldönthetjük, a mely eljárás természetesen a k számot is megadja.

E tétel nagy szerepe az alkalmazásokban azon alapszik, hogy bizonyos problémákban az egyenletrendszernek az a tulajdonsága, hogy tartalma sereget alkot, közvetetlenül felismerhető és ebből azután mindjárt következtethetjük, hogy a minimális resolvens bal oldala az $x, x_{h+1}, \ldots, x_{m-1}$ határozatlanoknak homogén lineáris formája, vagyis hogy ama rendszer tartalmát az (I)-alakú lineáris egyenletek bizonyos rendszere is értelmezi. E mellett még tekintetbe veendő, hogy az ezekben előfordúló ismeretlenek az eredeti $z_1, \ldots, z_m$ ismeretleneknek homogén lineáris formái.

A függvénydeterminány.

14. §. Ha $F_1, \ldots, F_k$ az $x_1, \ldots, x_m$ határozatlanoknak bármely formái és $\varphi(z_1, \ldots, z_k)$ a $z_1, \ldots, z_k$ határozatlanoknak valamely formája, akkor

$$\varphi(F_1, F_2, \ldots, F_k)$$

ismét az $x_1, \ldots, x_m$ határozatlanoknak formája lesz. E formának x_j szerint vett deriváltját a

$$\frac{\partial \varphi}{\partial x_j} = \sum_{i=1}^{k} \frac{\partial \varphi}{\partial F_i} \frac{\partial F_i}{\partial x_j} \qquad (I)$$

képlet szolgáltatja. A differenciálszámolás e szabálya mindaddig, míg csak formákról (vagy egész függvényekről) van szó, egyszerű azonosság, a mely a deriváltnak formális értelmezéséből (II. fej. 5. §.) közvetetlenül nyerhető. Ha x_j helyébe mindenütt $x_j + h_j$ lép, e czélból φ-ben csak $h_1, \ldots, h_m$ együtthatóit kell meghatároznunk és erre elég, ha F_i helyébe mindenütt $F_i + H_i$-t írunk és azután

$$H_i = \sum_{=1}^{m} \frac{\partial F_i}{\partial x_j} h_j$$

-t helyettesítünk, mert az elmaradó tagoknak a keresett együtthatókra nincs befolyásuk. Ép úgy megegyeznek a $h_1, \ldots, h_m$-ben első-dimensiójú tagokra nézve

$$\varphi(F_1+H_1, \ldots, F_k+H_k)$$

és

$$\sum \frac{\partial \varphi}{\partial F_i} H_i;$$

mint h_j együtthatója tehát csakugyan az (I)-ben álló kifejezés származik.

Most különösen az $x_1, \ldots, x_m$ határozatlanoknak m formájából álló

$$F_i(x_1, \ldots, x_m) \qquad (i=1, \ldots, m)$$

rendszer lesz megvizsgálandó. Rövidség kedvéért legyen

$$F_{ij} = \frac{\partial F_i}{\partial x_j}.$$

Az e differenciálhányadosokból alkotott

$$| F_{ij} |_{(i, j=1, \ldots, m)}$$

determinánst *az* $F_1, \ldots, F_m$ *formarendszer* $x_1, \ldots, x_m$ *szerint vett függvénydeterminánsának** nevezzük.

Egy határozatlan esetében e függvénydeterminány egyszerűen a derivált; ha pedig a határozatlanok száma 1-nél nagyobb, a függvénydeterminány a derivált fogalmának igen fontos általánosítását szolgáltatja és ennek megfelőleg $\frac{\partial(F_1, \ldots, F_m)}{\partial(x_1, \ldots, x_m)}$-mel, vagy pedig $\frac{\partial(F)}{\partial(x)}$-szel is jelölhető.

* A függvénydeterminány alapvető tulajdonságait legelőször Jacobi fejtette ki. («De determinantibus functionalibus», Journal f. r. u. a. Math. 22. köt. 319. l. = Werke III. köt. 393. l.). A függvénydeterminány tisztán algebrai elmélete tudtommal itt található először.

Ha $\Phi_1, \ldots, \Phi_m$ az $F_1, \ldots, F_m$ formáknak és $F_1, \ldots, F_m$ az $x_1, \ldots, x_m$ határozatlanoknak formái, akkor $\Phi_1, \ldots, \Phi_m$-et ismét az $x_1, \ldots, x_m$ határozatlanok formáinak tekinthetjük és akkor

$$\frac{\partial \Phi_i}{\partial x_j} = \sum_{r=1}^{m} \frac{\partial \Phi_i}{\partial F_r} \frac{\partial F_r}{\partial x_j},$$

úgy, hogy a determinánsok szorzástétele alapján

$$\frac{\partial (\Phi)}{\partial (x)} = \frac{\partial (\Phi)}{\partial (F)} \frac{\partial (F)}{\partial (x)}.$$

Ha az F formákra az

$$x_i = \sum_{j=1}^{m} a_{ij} z_j \quad (i=1, \ldots, m), \ | a_{ij} | \neq 0 \qquad (T)$$

transformatiót alkalmazzuk, ezek a $z_1, \ldots, z_m$ határozatlanoknak formáiba mennek át és ily értelemben

$$\frac{\partial F}{\partial z_j} = \sum_{j=1}^{m} \frac{\partial F}{\partial x_i} a_{ij},$$

ebből pedig

$$\frac{\partial (F)}{\partial (z)} = | a_{ij} | \frac{\partial (F)}{\partial (x)}.$$

A (T)-vel transformált rendszer függvénydeterminánsa tehát úgy származik, hogy az eredeti rendszer függvénydeterminánsát megszorozzuk a transformatio determinánsával. Minthogy pedig erről az utóbbiról feltételezzük, hogy a 0-tól különböző, azért a két függvénydeterminány vagy egyidejűleg egyenlő 0-sal, vagy pedig mind a kettő a 0-tól különböző.

Az $F_1, \ldots, F_m$ formákat *egymástól függőknek* mondjuk, ha fennáll köztük ilyen alakú azonosság:

$$\sum_{(g)} C_g F_1^{g_1} \ldots F_m^{g_m} = 0,$$

hol a C_g-k nem mindannyian zérusok; ellenkező esetben pedig *egymástól függetlenek.* A C_g-k itt oly raczionális tartomány mennyiségei, a melynek értelmezésébe *nem* lépnek be az $x_1, \ldots, x_m$ határozatlanok. Az $F_1, \ldots, F_m$ formáknak egymástól függő vagy független voltát azonban mindjárt kezdettől fogva, az általánosság megszorítása nélkül úgy értelmezhetjük, hogy *a C mennyiségek az F formák együtthatóival meghatározott raczionális tartományhoz tartozzanak és nem mindannyian egyenlők a zérussal.*

Mert, ha vannak egyáltalában a felállított feltételeknek megfelelő C mennyiségek, ezek a homogén lineáris egyenletek oly rendszerét elégítik ki, a melyben az együtthatók ahhoz az F formák együtthatóival meghatározott raczionális tartományhoz tartoznak. Ezeket az egyenleteket az a kijelentés szolgáltatja, hogy az x-ek minden hatványszorzatának együtthatója zérus. De akkor amaz azonosság érvényes a C-k minden oly értékrendszerére nézve, a mely ezeket a homogén lineáris egyenleteket kielégíti. Ezeknek az egyenleteknek tartalma k-tagú sereget alkot, a hol $k \geqq 1$, minthogy van olyan megoldásuk, a mely a $(0, 0, \ldots, 0)$-tól különböző. És e seregnek ábrázolása értelmében (e fej. 13. §-a) a C mennyiségeknek oly rendszerei is lesznek, a melyek ama raczionális tartományhoz tartoznak.

Az $F_1, \ldots, F_m$ formák egymástól függő vagy független volta a legszorosabban kapcsolatos e formák függvénydeterminánsával. Erre nézve először is a következő tétel érvényes:

Az egymástól függő formák rendszerének függvénydeterminánsa azonosan zérus.

Ezt a tételt úgy bizonyíthatjuk be, hogy kiindulunk abból a most létezőnek feltételezett azonosságból, a mely kifejezi, hogy a formák egymástól függnek és a mely a

$$\Phi(F_1, \ldots, F_m) = 0$$

alakban írható. De épen, mivel ez azonosság,

$$\frac{\partial \Phi}{\partial x_j} = \sum_{i=1}^{m} \frac{\partial \Phi}{\partial F_i} \frac{\partial F_i}{\partial x_j} = 0 \qquad (j=1, \ldots, m)$$

és így tehát

$$|F_{ij}| \frac{\partial \Phi}{\partial F_j} = 0 \qquad (j=1, \ldots, m).$$

Most már könnyen kimutatható, hogy $|F_{ij}|$-t a 0-tól különbözőnek véve, Φ-ben minden egyes C_g együttható szükségképen 0, a mi föltevéseinkkel ellentétben áll. Ekkor ugyanis

$$\frac{\partial \Phi}{\partial F_j} = 0 \qquad (j=1, \ldots, m)$$

volna, ha a bal oldalt az x-ek formájának tekintjük; míg $\frac{\partial \Phi}{\partial F_j}$, mint az F-ek formája nem lehet a j minden értékénél azonosan egyenlő a zérussal. Hisz különben $\Phi = C$ és C a 0-tól különböző volna, a mi képtelenség.

Ha tehát Φ az F-ekben n-ed dimensiójú, akkor a formáknak egymástól függő volta a zérustól különböző függvénydeterminánsmellett bizonyos

$$\Phi_1 (F_1, \ldots, F_m) = 0$$

kapcsolathoz vezetne, a hol Φ_1 olyan a zérustól különböző forma, a melynek dimensiója $n-1$. Így tovább folytatva a következtetést, végre olyan a zérustól különböző lineáris formához, Φ_{n-1}-hez, azaz olyan

$$C_0 + C_1 F_1 + \cdots + C_m F_m = 0$$

vonatkozáshoz jutunk, a hol nem az összes C-k egyenlők a zérussal. Ugyane következtetési mód szerint $\frac{\partial \Phi_{n-1}}{\partial F_j} = C_j$-nek (ha $j=1, \ldots, m$) a zérussal kellene egyenlőnek lennie és, minthogy Φ_{n-1} nem azonosan egyenlő a zérussal, C_0-nak egyrészt a 0-tól különbözőnek kellene lennie, másrészt pedig mégis

$C_0=0$ volna. Az $|F_{ij}|\neq 0$ feltevés tehát ellenmondásra vezet és így evvel a kimondott tétel be van bizonyítva.

15. §. Az utoljára bebizonyított tétel meg is fordítható és így mint részlettétel benne van a következő, most tárgyalandó általános tételben:

(a) Az $F_1, \ldots, F_m$ *formák akkor és csak akkor függetlenek egymástól, ha az* $|F_{ij}|$ *függvénydeterminánsa a* 0*-tól különböző.*

Itt előre kiemeljük, hogy a bebizonyításban kizárólag csak az algebrai mennyiségek elméletébe tartozó segédeszközöket használunk és, a mi a tétel alkalmazásában elengedhetetlen, mindjárt oly módszert is kifejtünk, a mely az $|F_{ij}|=0$ esetben raczionális műveletek segítségével szolgáltat egy $\Phi(F_1, \ldots, F_m)=0$ relácziót, ill. teljesen jellemzi e relácziók összességét.

Az előadandó bebizonyítás áttekinthetőbbé válik, ha egyidőben az

$$F_i(x_1, \ldots, x_m)=w_i, \qquad (i=1, \ldots, m) \qquad (1)$$

egyenletrendszert is tárgyaljuk, a hol $w_1, \ldots, w_m$ *új határozatlanokat* jelentenek és a kimondott tétellel együtt mindjárt az erre az egyenletrendszerre vonatkozó következő tételt is bebizonyítjuk:

(b) Az $F_i=w_i$ *rendszer tartalma m-edfokozatú sokaságot alkot, ha* $|F_{ij}|$ *a* 0*-tól különböző; ha pedig* $|F_{ij}|=0$, *az* $F_i=w_i$ *rendszernek nincsen tartalma**.

* A w-k ama jelentéséhez, hogy új határozatlanok, pontosan kell ragaszkodnunk. Itt ugyanis különösen jellemző módon mutatkozik az az elvi különbség, a mely határozatlanok és korlátlan változók között fennáll. «Határozatlan» w-k esetében az épen kimondott tétel minden kivétel nélkül érvényes. *Ha ellenben a w-k változók*, a tétel — a mint azt kifejezni szokás — *csak «általánosságban» érvényes*, azaz *lehetséges*, hogy érvényességét bizonyos a $(w_1, \ldots, w_m)$-ben fog-

Nem lesz talán felesleges, ha még kiemeljük, hogy fejtegetéseink nem tételezik fel «az algebra alaptételét». Csakis az algebrai mennyiségek forma-elméleti értelmezését használjuk és a mint a IV. fejezet részletes fejtegetései mutatták, az ezekre vonatkozó eredmények csak oly rövidebben írt azonosságok, a melyek az eredeti raczionális tartományból származó formákra vonatkoznak.

Mindenekelőtt megjegyezzük, hogy az *(a)* és *(b)* tételek az $m=1$ esetben érvényesek. Ha $m=1$ (tehát csak egy formánk van, F_1 és egy határozatlanunk, x_1), az «egymástól független» kifejezést nem használhatjuk a közönséges ér-

lalt első vagy magasabb fokozatú sokaságra nézve elveszti. Hogy ebben az esetben a további vizsgálat miképen alakúl, azt röviden mindjárt itt jelezhetjük.

A *(b)* tétel kifejezi, hogy határozatlan w-k mellett az első esetben az $F_i=w_i$ rendszer összresolvense ilyen alakú:

$$\Phi(x, t_1, \ldots, t_m, w_1, \ldots, w_m) = 0;$$

a második esetben pedig ily alakú relácziók állanak fenn:

$$\Psi(w_1, \ldots, w_m) = \sum_{i=1}^{m} \lambda_i (F_i - w_i).$$

Ha $w_1, \ldots, w_m$-nek olyan értékeket tulajdonítunk, a melyek *nem* elégítik ki a $\Psi=0$ relácziót, az $F_i-w_i=0$ rendszernek nem lehet megoldása és így a második eset evvel el van intézve.

Az első esetben képeznünk kell az $F_i=w_i$ rendszer összresolvensét a w-k ama speciális értékrendszerére nézve. A $D_t^{(h)}$ és $f_{j_h}^{(h)}$ formák képezése teljesen ugyanazon a módon történik, mint határozatlan w-k esetében mindaddig, míg az $f_{j_{h+1}}^{(h+1)}$ formák most nem mindannyian egyenlők 0-sal. Közvetetlenül láthatjuk azt is, hogy az $f_{j_{h+1}}^{(h+1)}$ formákkal együtt egyszersmind az ezek után következő $f_{j_{h+2}}^{(h+2)}$,... rendszerek formái is azonosan egyenlők a zérussal. De ez még akkor is megtörténik, ha a megelőző rendszer formáiban pl. az $f_{j_k}^{(k)}$-kban az x_{k+1} legmagasabb hatványának együtthatója mindig egyenlő 0-sal. Ha ezek az együtthatók a következők: $G_i^{(k)}(w_1, \ldots, w_m), \ldots$, akkor a tétel minden esetre érvényes marad mindazokra a $w_1, \ldots, w_m$ rendszerekre nézve, a melyekre nézve $\prod_{(i,k)} G_i^{(k)}$ a 0-tól különböző.

telemben; de ez nem érinti a dolog lényegét (hisz valójában azt kérdezzük, vajjon van-e *egy* határozatlannak oly $\varphi(z)$ formája, a melyre nézve $\varphi(F_1) = 0$). Ebben az esetben a függvénydeterminánsegyszerűen F_1 deriváltja és zérussal egyenlő volta azt jelenti, hogy F_1 nem tartalmazza az x_1 határozatlant; tehát $F_1 = A$. Ha viszont van ilyen reláczió: $\varphi(F_1) = 0$, akkor F_1 szükségképen valamely olyan genus-tartományhoz tartozik, a mely a φ együtthatóival értelmezett raczionális tartományból származik és így tehát az x_1-től független. Minthogy azonban F_1 e raczionális tartományból származó forma, ismét $F_1 = A$. Ha tehát $\frac{\partial F_1}{\partial x_1}$ a 0-tól különböző, nem áll fenn egyetlen $\varphi(F_1) = 0$ reláczió sem és az $F_1 = w_1$ egyenlet x_1 számára véges számú értékrendszert szolgáltat, mert F_1 az x_1 ismeretlent valóban tartalmazza; ha azonban $\frac{\partial F}{\partial x_1} = 0$, tehát $F_1 = A$, akkor ez az a reláczió, a melynek fennállását állítottuk és az $A = w_1$ egyenletnek nincsen tartalma.

E szerint az *(a)* és *(b)* tételek általános bebizonyítására a teljes inductiót alkalmazhatjuk, azaz feltételezhetjük, hogy már be vannak bizonyítva k forma, ill. k egyenlet esetére, a melyek ugyanannyi határozatlant, ill. ugyanannyi ismeretlent tartalmaznak, ha $k < m$ és erre alapíthatjuk a $k = m$ esetre vonatkozó bebizonyítást. Itt is feltételezzük, hogy az F formák lineáris transformatiók segítségével már meg vannak szabadítva esetleges körülményektől. Szembetünő ugyanis, hogy ily lineáris transformatio a tételek érvényességén nem változtat semmit.

A további fejtegetések a függvénydeterminánsa «rangja»*

* Valamely $|a_{ij}|\ (i, j = 1, \ldots, m)$ determináns és valamely $|a_{ij}|\ (i = 1, \ldots, p\ ;\ j = 1, \ldots, q)$ matrix is FROBENIUS szerint («Über lineare Gleichungen etc.» Journal f. Math. 86. köt. 1. l.) *r-edrangú*, ha r a legnagyobb egész szám, a melyre nézve az összes r-edfokú aldeterminánsok nem mindannyian egyenlők a zérussal.

szerint válnak szét. Erre vonatkozólag megjegyzendő, hogy, ha a függvénydeterminánsrangja r, akkor az általánosság megszorítása nélkül feltételezhetjük, hogy az összes

$$|F_{ij}|_{(i=1,\ldots,r;\, j=j_1,\ldots,j_r)}$$

aldeterminánsok, a hol $j_1,\ldots,j_r$ az $1,\ldots,m$ sorozatból bármely módon választott r különböző értéket jelentenek, a zérustól különbözők. Avval, hogy a 0-tól különböző aldeterminánsban fellépő formák épen az $F_1,\ldots,F_r$ formák, csak azt mondjuk, hogy az adott formarendszer formáit megfelelő módon rendeztük és jelöltük. Ha már most pl.

$$|F_{ij}|_{(i,j=1,\ldots,r)}$$

nem egyenlő 0-sal, alkalmazzunk valamely alkalmas módon választott

$$x_\mu = \sum_{\nu=1}^{m} a_{\mu\nu} z_\nu \qquad (\mu=1,\ldots,m)$$
$$|a_{\mu\nu}| \neq 0$$

lineáris transformatiót és vizsgáljuk a transformált formákat. Hogy ezek is az esetleges körülményektől már meg legyenek szabadítva, csak az $a_{\mu\nu}$-ket kell úgy választanunk, hogy bizonyos véges számú algebrai egyenletet *ne* elégítsenek ki.

Ha a bal oldalon $\overline{F}_i$ már a transformált formát jelenti, továbbá

$$\frac{\partial \overline{F}_i}{\partial z_\nu} = \sum_{\mu=1}^{m} \frac{\partial F_i}{\partial x_\mu} a_{\mu\nu};$$

és így tehát a transformált formákra nézve a kérdéses aldeterminánsok egyike a következő lesz:

$$|\overline{F}_{i\nu}|_{(i=1,\ldots,r;\, \nu=j_1,\ldots,j_r)} = \Big|\sum_{\mu=1}^{m} F_{i\mu} a_{\mu\nu}\Big|_{(i=1,\ldots,r;\, \nu=j_1,\ldots,j_r)}$$

és ez a determinánsokra vonatkozó egyik ismeretes tétel* szerint továbbá

$$= \sum_{(s)} A_s \Delta_s,$$

a hol

$$\Delta_s = |F_{ij}|_{(i=1,\ldots,r;\, j=s_1,\ldots,s_r)}, \quad A_s = |a_{ji}|_{(j=s_1,\ldots,s_r;\, i=1,\ldots,r)}$$

és a summatio az $1,\ldots,m$-ből lehetséges összes $s_1,\ldots,s_r$ combinatióra kiterjesztendő. Az α-knak az A_s determinánsok kifejtésében fellépő hatványszorzatai mindannyian különbözők egymástól; e szerint a $\sum_{(s)} A_s \Delta_s$ kifejezésben nem állhat be semmi rövidítés és így

$$|\overline{F}_{iv}|_{(i=1,\ldots,r;\, v=j_1,\ldots,j_r)}$$

a $j_1,\ldots,j_r$ bármely választása mellett az α-knak oly formája, a mely nem egyenlő 0-sal; mert hisz a feltevés szerint $|a_{ji}|_{(i,j=1,\ldots,r)}$ együtthatója, azaz

$$|F_{ij}|_{(i,j=1,\ldots,r)}$$

a 0-tól különböző.

Meghatározhatjuk tehát az α-k oly értékeit, még racionális és egész számúakat is, a melyek a $\sum_{(s)} A_s \Delta_s = 0$ egyenletek egyikét sem elégítik ki; és így az ily módon transformált formák függvénydeterminánsa már csakugyan mutatja az állított tulajdonságot. Elég tehát, ha a felállított tételek bebizonyításánál a transformált formákat vesszük fel alapúl.

16. §. Először most azt az esetet vizsgáljuk, midőn *a függvénydeterminánsrangja* $m-1$ *vagy* m, azaz a függvénydeterminánsnem egyenlő 0-sal, vagy pedig, ha egyenlő 0-sal, van egy a 0-tól különböző $m-1$-edfokú aldeterminánsa. Az előbbiek szerint szabatosan ez úgy fejezhető ki, hogy az összes

* L. pl. Baltzer, Theorie und Anwendung der Determinanten, 4. kiad. 46. l.

$$|F_{ij}|_{(i=1,\ldots,m-1;\, j=j_1,\ldots,j_{m-1})}$$

aldeterminánsok alkalmas lineáris transformatio alkalmazása után a 0-tól különbözők lesznek.

Ekkor mindenekelőtt látjuk, hogy *az*

$$F_i = w_i \qquad (i=1,\ldots,m)$$

egyenletrendszer tartalma nem alkothat az m-diknél alacsonyabb fokozatú sokaságot. Az ellenkező esetben a rendszernek olyan megoldása volna, a melyben x_{m-1} megmarad határozatlannak és ez a megoldás kielégítené az

$$F_i = w_i \qquad (i=1,\ldots,m-1)$$

rendszert akkor is, ha ebben x_{m-1}-et ismét határozatlannak tekintjük és csak $x_1,\ldots,x_{m-2}$, x_m-et veszszük ismeretleneknek. Erre az $m-1$ egyenletből álló és ugyanannyi ismeretlent tartalmazó rendszerre vonatkozólag azonban tételeink érvényesek. Ezeket az egyenleteket tehát véges számú gyökrendszer elégíti ki és az ezekben fellépő mennyiségek az $x_{m-1}, w_1,\ldots,w_{m-1}$ mennyiségeknek meghatározott algebrai függvényei. E megoldások közül azonban az egyiknek a most megvizsgált feltétel mellett ki kellene elégítenie az $F_m=w_m$ egyenletet is; azaz az új határozatlan, w_m a többi határozatlannak algebrai függvénye volna és ez a lehetetlen eredmény mutatja, hogy feltevésünk nem engedhető meg.

Az $F_i = w_i$ rendszer összresolvense tehát vagy az $x, t_1,\ldots,t_m, w_1,\ldots,w_m$ határozatlanoknak formája, még pedig akkor, midőn a rendszernek vannak megoldásai; vagy pedig egyedül a $w_1,\ldots,w_m$ határozatlanoknak formája, midőn a rendszernek nincsenek megoldásai.

Ha először az utóbbi esetet tekintjük közelebbről, a resolvens formára vonatkozó alapvető tétel szerint (III. fej. 18. §. és e fej. 4. §.)

$$\Phi(w_1,\ldots,w_m)\equiv 0 \pmod{F_1-w_1,\ldots,F_m-w_m, x-\sum_{i=1}^{m} x_i t_i},$$

vagy pedig ugyanezt a tényt azonosság alakjában kifejezve:

$$\Phi(w_1, \ldots, w_m) = \sum_{i=1}^{m} \lambda_i (F_i - w_i) + \mu (x - \sum_{i=1}^{m} x_i t_i).$$

Az idézett helyek szerint a bal oldalon tulajdonképen mindig az egység áll; de akkor a w határozatlanok miatt, a melyek most az egyenletrendszer együtthatóival értelmezett raczionális tartományba belépnek, a λ és μ formák együtthatói általánosságban a w-k formáinak hányadosai. Csak a nevezők eltávolítása után keletkezik az azonosság felírt alakja, a hol már mostan $\lambda_1, \ldots, \lambda_m$ és μ az $x, x_1, \ldots, x_m, t_1, \ldots, t_m, w_1, \ldots, w_m$ határozatlanoknak az F formák együtthatóival értelmezett raczionális tartományból származó formái.

Ez az azonosság, a mely helyes, ha $x, w_1, \ldots, w_m$ határozatlanok, helyes marad akkor is, ha a következőket helyettesítjük:

$$w_i = F_i, \quad x = \sum_{i=1}^{m} x_i t_i;$$

és akkor nyerjük, hogy

$$\Phi(F_1, \ldots, F_m) = 0.$$

Ez pedig kifejezi, hogy az F formák egymástól függnek és így szükséges, hogy ebben az esetben a függvénydeterminány egyenlő legyen 0-sal.

Az ellenkező esetben

$$\Phi(x, w_1, \ldots, w_m) = \sum_{i=1}^{m} \lambda_i (F_i - w_i) + \mu (x - \sum_{i=1}^{m} x_i t_i),$$

a hol Φ az x-et valóban tartalmazza. Megmutatjuk, hogy ez az eset *nem* fér össze avval, hogy a függvénydeterminány 0-sal egyenlő. Feltételezve, hogy a függvénydeterminány 0-sal egyenlő, legyen ismét $x = \sum_{i=1}^{m} x_i t_i$ és jelöljük e helyettesítés eredményét úgy, mint előbb szegletes zárójellel; ekkor

$$[\Phi]=\sum_{i=1}^{m}[\lambda_i](F_i-w_i).$$

E kifejezésnek x_j szerint vett deriváltja:

$$\left[\frac{\partial\Phi}{\partial x}\right]t_j=\sum_{i=1}^{m}\left(\left[\frac{\partial\lambda_i}{\partial x_j}\right]+\left[\frac{\partial\lambda_i}{\partial x}\right]t_j\right)(F_i-w_i)+\sum_{i=1}^{m}[\lambda_i]\frac{\partial F_i}{\partial x_j},$$

és ebből, ha a függvénydeterminánsnak $\frac{\partial F_1}{\partial x_j}$ elemeinek megfelelő $m-1$-edfokú aldeterminánsokat φ_j-vel jelöljük,

$$\left[\frac{\partial\Phi}{\partial x}\right]\sum_{j=1}^{m}t_j\varphi_j=\sum_{i=1}^{m}A_i(F_i-w_i),$$

a hol $\Sigma t_j\varphi_j$ a φ_m-mel, az el nem tünő aldeterminánsok egyikével együtt a 0-tól különböző. Ha ebben az azonosságban w_i helyébe ismét F_i-t teszszük, akkor szükségképen

$$\left[\frac{\partial\Phi}{\partial x}\right]_{w_i=F_i}=0.$$

E mellett $\frac{\partial\Phi}{\partial x}=\Phi_1$ az $x, t_1, \ldots, t_m, w_1, \ldots, w_m$ határozatlanoknak oly formája, a mely úgy, mint Φ az $x, t_1, \ldots, t_m$ határozatlanokra nézve homogén és dimensiója, ha e határozatlanok formájának tekintjük, 1-gyel kisebb mint a Φ-é.

Ha Φ_1-ben egyidőben $x=\sum_{i=1}^{m}x_i t_i$, $w_i=F_i$ tétetik, akkor — a mint épen bebizonyítottuk — Φ_1 eltünik; ezt a tényt kifejezhetjük a következő azonossággal:

$$\Phi_1=\sum_{i=1}^{m}\lambda_i^{(1)}(F_i-w_i)+\mu^{(1)}(x-\sum_{i=1}^{m}x_i t_i).$$

Φ_1 itt természetesen Φ-vel együtt a 0-tól különböző forma; az ellenkező eset csak akkor állhatna be, ha Φ nem tartalmazná az x határozatlant, a mi a most vizsgált feltevéssel ellenkezik. Az így nyert azonosságra pontosan ugyanazokat a következtetéseket alkalmazhatjuk, mint az előbbire és így tehát, ha Φ az x-re és a t-kre vonatkozólag s-ed dimensiójú volt, végre olyan

$$\Phi_s(w_1, \ldots, w_m) = \sum_{i=1}^{m} \lambda_i^{(s)} (F_i - w_i) + \mu^{(s)} (x - \sum_{i=1}^{m} x_i t_i)$$

azonossághoz jutunk, a hol Φ_s az $x, t_1, \ldots, t_m$ határozatlanokat már nem tartalmazza és a melyből a $w_i = F_i$, $x = \sum_{i=1}^{m} x_i t_i$ helyettesítések után közvetetlenül a

$$\Phi_s(F_1, \ldots, F_m) = 0$$

reláczió származik. Ugyanez az azonosság azonban azt is mutatja, hogy a $\Phi(x, w_1, \ldots, w_m) = 0$ alakú összresolvens feltevése ellenmondást tartalmaz. Mert ekkor léteznék oly $\xi_1, \ldots, \xi_m$ mennyiség-rendszer, a mely kielégíti az $F_i = w_i$ egyenleteket. Ha pedig az utolsó azonosságban $x_1, \ldots, x_m$ helyébe ezt a rendszert helyettesítenők, és x helyébe $\Sigma \xi_i t_i$-t, akkor $\Phi_s(w_1, \ldots, w_m)$ azonosan 0 volna; pedig származása szerint Φ_s a w-knek el nem tünő formája tartozik lenni.

17. §. Evvel a 15. §. elején felállított tételek az m-ed- és $m-1$-edrangú függvénydeterminánsesetére helyeseknek bizonyúltak. Ha a függvénydeterminánsm-edrangú, azaz nem egyenlő a 0-sal, tehát az $F_1, \ldots, F_m$ formák egymástól függetlenek, ehhez nincs mit hozzátennünk; az ellenkező esetben azonban a formák egymástól való függése még pontosabban jellemzendő.

A resolvens képezése, azaz a raczionális műveletek bizonyos meghatározott sorozata ebben az esetben feltétlenül *egy* bizonyos relációhoz vezet, melyet ismét

$$\Phi(F_1, \ldots, F_m) = 0$$

alakban írhatunk. Ebből, ha $F_i = w_i + F_i - w_i$-t írjuk és azután a $F_i - w_i$-k hatványszorzatai szerint kifejtünk, származik

$$\Phi(w_1, \ldots, w_m) = \Sigma \varphi_i (F_i - w_i),$$

a hol képezésük szerint a Φ és φ_i formák az F-ek együtthatóival értelmezett raczionális tartományból, (R)-ből származnak.

Legyen már most $(\bar{R})$ oly raczionális tartomány, a

mely tartalmazza (R)-t (jelesen valamely ebből származó genus-tartomány), és

$$\Phi = \Phi_1 \dots \Phi_k$$

legyen e tartományban a Φ irreducibilis tényezőkre való felbontása. Ha w_i helyébe ismét az F_i-t irjuk, akkor Φ és így tehát egyik tényezője is egyenlő lesz 0-sal. Legyen e tényező Φ_1; akkor

$$\Phi_1(F_1, \dots, F_m) = 0,$$

a hol Φ_1 az $(\overline{R})$-ben irreducibis formát jelent.

Már most Ψ-t a $w_1, \dots, w_m$ határozatlanok valamely az $(\overline{R})$-ből származó formájának értve, $\Psi(F_1, \dots, F_m) = 0$ akkor és csak akkor lehetséges, ha Ψ az ebben a tartományban irreducibilis Φ_1 formával osztható.

Hogy $w_i = F_i$-re nézve Φ_1-gyel egyidőben minden Φ_1-gyel osztható forma is egyenlő a 0-sal, az közvetetlenül belátható. Ha pedig Ψ nem osztható Φ_1-gyel, Φ_1-nek irreducibilis volta miatt szükségképen $(\Psi, \Phi_1) \sim 1$. Algebrai kapcsolat $F_1, \dots, F_{m-1}$ között nem állhat fenn, mert $|F_{ij}|_{(i,j=1,\dots,m-1)} \neq 0$ lévén, még egy

$$\varphi(F_1, \dots, F_{m-1}, x_m) = 0$$

alakú reláczió sem lehetséges. A Φ_1 és Ψ formák tehát tartalmazzák w_m-et és így w_m szerint vett resultánsukra vonatkozólag

$$\text{Res.} \begin{pmatrix} \Phi_1, & \Psi \\ w_m, & 1 \end{pmatrix} = \psi = W_1 \Phi_1 + W_2 \Psi$$

és ψ a $w_1, \dots, w_{m-1}$ határozatlanoknak a 0-tól különböző formája. Mindamellett, ha w_i helyébe F_i-t teszszük, szükségképen

$$\psi(F_1, \dots, F_{m-1}) = 0$$

volna, a mi — a mint épen kifejtettük — nem lehetséges.

Ha végre (a IV. fej. 18. §-a szerint) arra a genus-tartományra megyünk át, a melyben Φ föltétlenül irreducibi-

lis tényezőkre bomlik, akkor *oly föltétlenül irreducibilis* $\bar{\Phi}(w_1, \ldots, w_m)$ *formát nyerünk, a melynek az a tulajdonsága, hogy a*

$$\Psi(F_1, \ldots, F_m)=0$$

reláczió akkor és csak akkor áll fenn, ha $\Psi(w_1, \ldots, w_m)$ *osztható* $\bar{\Phi}(w_1, \ldots, w_m)$*-mel.*

18. §. Most még azt az esetet vizsgáljuk, midőn *a függvénydeterminánsrangja,* $r<m-1$. A mint tudjuk, ekkor feltételezhetjük, hogy az összes

$$\frac{\partial(F_1, F_2, \ldots, F_r)}{\partial(x_{i_1}, x_{i_2}, \ldots, x_{i_r})}$$

determinánsok különböznek a 0-tól; ellenben, ha $s>r$ és i_s az $i_1, i_2, \ldots, i_r$ számoktól különböző, minden

$$\frac{\partial(F_1, F_2, \ldots, F_r, F_s)}{\partial(x_{i_1}, x_{i_2}, \ldots, x_{i_r}, x_{i_s})}$$

determináns egyenlő 0-sal. Most már az $F_1, \ldots, F_r, F_s$ formákat az $x_{i_1}, \ldots, x_{i_r}, x_{i_s}$ határozatlanok formáinak tekinthetjük, a melyekben azután az együtthatók a többi $m-r-1$ határozatlannak formái; ezen határozatlanok jelei legyenek $z_1, z_2, \ldots, z_{m-r-1}$. E formarendszerre nézve, a melyben a határozatlanok száma már kisebb, tételeink érvényesek. Mivel a függvénydeterminánsrangja pontosan egyenlő a határozatlanoknak az egységgel kisebbített számával, van racionális műveletek segítségével megadott olyan φ forma, a melyre nézve

$$\varphi(F_1, \ldots, F_r, F_s)=0.$$

E forma együtthatói azonban minden esetre még a $z_1, z_2, \ldots$ határozatlanok formái és így ez az azonosság pontosabban a következő módon irandó:

$$\varphi(z_1, z_2, \ldots, F_1, \ldots, F_r, F_s)=0.$$

Ekkor azonban mindig találhatni oly φ formát is, a mely a z határozatlanokat egyáltalában nem tartalmazza és ez az,

a mit épen be kellett bizonyítanunk. Az utolsó azonosságból, ha F_i helyébe $w_i + F_i - w_i$-t írjuk és azután az $F_i - w_i$-k hatványszorzatai szerint kifejtünk, minden esetre származik a következő is:

$$\varphi(z_1, z_2, \ldots, w_1, \ldots, w_r, w_s) = \sum_{\mu=1,\ldots,r,s} \lambda_\mu (F_\mu - w_\mu).$$

Tehát egyszersmind

$$\frac{\partial \varphi}{\partial z_1} = \sum \frac{\partial \lambda_\mu}{\partial z_1}(F_\mu - w_\mu) + \sum \lambda_\mu \frac{\partial F_\mu}{\partial z_1},$$

$$0 = \frac{\partial \varphi}{\partial x_i} = \sum_{(i=i_1,\ldots,i_r)} \frac{\partial \lambda_\mu}{\partial x_i}(F_\mu - w_\mu) + \sum \lambda_\mu \frac{\partial F_\mu}{\partial x_i},$$

a hol a summatio mindig a $\mu = 1, \ldots, r, s$ értékekre terjesztendő ki. Ha most végre a megfelelő aldeterminánsokkal szorzunk és azután összeadunk,

$$\frac{\partial(F_1, \ldots, F_r)}{\partial(x_1, \ldots, x_r)} \frac{\partial \varphi}{\partial z_1} = \Sigma \lambda_\mu^{(1)} (F_\mu - w_\mu).$$

Itt a bal oldalon $\frac{\partial(F_1, \ldots, F_r)}{\partial(x_1, \ldots, x_r)}$ a w határozatlanoktól független és a 0-tól különböző; a $\frac{\partial \varphi}{\partial z_1}$ forma hasonlóképen különböző a 0-tól, mert hiszen különben — a feltevés ellenére — φ a z_1 határozatlant nem is tartalmazná. Ha azonban most $w_\mu = F_\mu$ tétetik, a bal oldal zérus lesz, és e szerint $\frac{\partial \varphi}{\partial z_1} = \varphi_1$ oly forma, a melyre nézve

$$\varphi_1(z_1, z_2, \ldots, F_1, \ldots, F_r, F_s) = 0.$$

Ámde φ_1 a z_1-re vonatkozólag alacsonyabb fokú mint φ úgy, hogy a következtetés e módja végre oly $\Phi(w_1, \ldots, w_r, w_s)$ formához vezet, a mely nem egyenlő 0-sal, a z határozatlanokat nem tartalmazza és a melyre nézve

$$\Phi(F_1, \ldots, F_r, F_s) = 0.$$

Φ-ről azután, ép úgy mint előbb, átmegyünk az $(\bar{R})$ tarto-

mányban irreducibilis Φ_1, ill. a föltétlenül irreducibilis $\bar{\Phi}$ formára. Evvel a következő általános tételhez jutottunk:

Ha az $F_1, \ldots, F_m$ *formarendszer függvénydeterminánsa* r*-edrangú és ennek megfelelőleg* $\frac{\partial(F_1, \ldots, F_r)}{\partial(x_1, \ldots, x_r)}$ *a zérustól különböző, akkor az* $F_1, \ldots, F_r$ *formák függetlenek egymástól, míg az* $F_1, \ldots, F_r, F_s\ (s>r)$ *formák között mindig algebrai kapcsolat áll fenn. Még pedig van* $m-r$ *meghatározott, föltétlenül irreducibilis* $\Phi_s(w_1, \ldots, w_r, w_s)$ *forma, a hol* $s = r+1, \ldots, m$ *és a melyekre nézve*

$$\Phi_s(F_1, \ldots, F_r, F_s)=0.$$

Végre valamely

$$\Psi_s(F_1, \ldots, F_r, F_s)=0$$

reláczió akkor és csak akkor állhat fenn, ha $\Psi_s(w_1, \ldots, w_r, w_s)$ *osztható* $\Phi_s(w_1, \ldots, w_r, w_s)$*-sel.*

Hogy az $F_i = w_i$, $(i = 1, \ldots, m)$ egyenletrendszernek, a hol $w_1, \ldots, w_m$ új határozatlanokat jelentenek, soha sincsen tartalma, ha a függvénydeterminánsrangja kisebb m-nél, igen egyszerű módon következik az előbbiekből. Mert a $\Phi_s(F_1, \ldots, F_r, F_s) = 0$-ból ismét következik, hogy

$$\Phi_s(w_1, \ldots, w_r, w_s) = \sum_{\mu=1, \ldots, r, s} \lambda_\mu (F_\mu - w_\mu).$$

Ha már most léteznék a mennyiségeknek oly rendszere, a melyre nézve valóban $F_\mu(x_1, \ldots, x_m)=w_\mu$ volna, ezt itt behelyettesíthetnők és akkor azt nyernők, hogy $\Phi_s(w_1, \ldots, w_r, w_s) = 0$, habár Φ_s ama határozatlanoknak a 0-tól különböző formája.

Ezek után, ha adva vannak az

$$F_i(x_1, \ldots, x_m) \qquad (i=1, \ldots, k)$$

formák, az előbbiek szerint mindig eldönthető, vajjon azok függnek-e egymástól, vagy sem és az első esetben fel is állíthatjuk a köztük fennálló jellemzetes kapcsolatokat.

Ha ugyanis $k<m$, az adott rendszert m formából álló és m határozatlant tartalmazó rendszerré úgy egészítjük ki, hogy $k+1$-dik, ..., m-dik forma gyanánt hozzácsatoljuk a zérust.

Ha $k>m$, tekintsük ezeket a formákat az $x_1, \ldots, x_m$, $x_{m+1}, \ldots, x_k$ határozatlanok formáinak. Minthogy ekkor $\frac{\partial F_i}{\partial x_{m+1}}, \ldots, \frac{\partial F_i}{\partial x_k}$ mindannyian eltünnek, ebben az esetben a függvénydeterminánsmindig egyenlő 0-sal és ebből láthatjuk, hogy m határozatlannak $m+1$ vagy még ennél is több formája között mindig vannak algebrai kapcsolatok.

HATODIK FEJEZET.

RESULTÁNSOK ÉS DISCRIMINÁNSOK.

(Ú. n. specziális eliminácziò-elmélet.)

Általános formák és az ezekre vonatkozó kérdéstétel.

1. §. *Az m határozatlannak, $x_1, x_2, \ldots, x_m$-nek n-ed dimensiójú általános formája* olyan forma, a mely a dimensio-meghatározással összeférő összes tagokat valóban tartalmazza és a melynek összes együtthatói egymástól különböző új határozatlanok. Vizsgálatunk tárgya most már a következő *állalános formarendszer:*

$$F_i(x_1, \ldots, x_m) = \sum_{(g)} a_g^{(i)} x_1^{g_1^{(i)}} \ldots x_m^{g_m^{(i)}}.$$
$$(i=1, \ldots, k;\ g_1^{(i)} + \cdots + g_m^{(i)} \leqq n_i)$$

Ama határozatlanok complexusát, a melyek mint együtthatók F_i-be belépnek, röviden $a^{(i)}$-vel, az $i=1, \ldots, k$ értékeknek megfelelő összes $a^{(i)}$-k complexusát pedig a-val jelöljük; végre az $x_1, \ldots, x_m$ határozatlanok complexusának jelölésére most az x-et használjuk.

Tekintettel a specziális esetekre, midőn egyes határozatlan együtthatók lépnek be a számolásba, czélszerű most mindjárt ezeknek egyszerűbb jelöléséről is gondoskodni. Részletesebben írva legyen

$$F_i(x_1, \ldots, x_m) = \sum_{j=1}^{m} a_{ij} x_j^{n_i} + \cdots + \sum_{j=1}^{m} c_{ij} x_j + a_{i, m+1},$$

azaz az x_j az F_i formában előfordúló legmagasabb (n_i-dik) hatványának együtthatóját jelöljük a_{ij}-vel, első hatványáét c_{ij}-vel, és az F_i formának az x határozatlanok nélküli tagját $a_{i,\,m+1}$-gyel.

Ezeknek az a és x határozatlanoknak raczionális és egész formái holoid tartományt alkotnak és az ebből származó $F_1, \ldots, F_k$ formák, ha ezeket «modulusrendszernek» tekintjük, olyan congruentiatartományt (I. fej. 10. §.) adnak, a mely ama tartományban benne foglaltatik.

Ha már most $E(a, x)$ az a-knak és x-eknek bármely raczionális és egész formája, akkor raczionális műveletek véges sorozatával eldönthető, vajjon $E(a, x)$ beletartozik-e ama congruentiatartományba, azaz az erre vonatkozólag bevezetett jelöléssel élve, eldönthető, vajjon

$$E(a, x) \equiv 0 \pmod{F_1, \ldots, F_k} \qquad (1)$$

vagy sem és, ha fennáll ily congruentia, ismét raczionális műveletek véges sorozata segítségével *valóban meg is található az*

$$E(a, x) = \sum_{i=1}^{k} H_i F_i \qquad (1a)$$

*előállítás**.

Az $E(a, x)$ forma ily módon követelt alaptulajdonságát (1a)-ban azonosság adja, a melyet még más alakban is írhatunk. Ha ugyanis úgy a jobb, mint a bal oldalon $a_{i,\,m+1}$ helyébe, a hol i az $i=1, \ldots, k$ értékeket veszi föl, mindenütt $a_{i,\,m+1} - F_i$-t írjuk**, a minek jelölésére e fejezetben szögletes zárójelt használunk, akkor — a mint közvetetlenül látni — lesz:

* E «lineáris diophantikus problémának» legáltalánosabb tárgyalását lásd a VII. és VIII. fejezetben.

** Ezt a KRONECKER-féle helyettesítést legegyszerűbb alakjában (egy forma esetében) már a III. fej. 23. §-ában alkalmaztuk.

$$[F_i]=0 \qquad (i=1,\ldots,k)$$

és, minthogy amaz azonosság e változtatás mellett is érvényes marad, továbbá

$$[E(a,x)]=0.$$

Ha most az $a_{1,m+1}$ kivételével minden $a_{i,m+1}$ helyébe ismét $a_{i,m+1}-F_i$-t $(i=2,\ldots,m)$ teszszük, a minek rövid jelölésére a $[\cdots]_1$ jel szolgáljon, akkor

$$[F_i]_1=0 \qquad (i=2,\ldots,k)$$

és

$$[E(a,x)]_1=[H_1]_1 F_1,$$

azaz $[E(a,x)]_1$ osztható F_1-gyel. *Az*

$$E(a,x)\equiv 0 \pmod{F_1,\ldots,F_k}$$

congruentia fönnállásának szükséges és elegendő föltétele e szerint

$$[E(a,x)]_1\equiv 0 \pmod{F_1}. \qquad (2)$$

Ezen épen most szükségesnek bizonyúltt föltétel ugyanis elegendő is, mert bárminő $E(a,x)$-ra nézve

$$E(a,x)=[E(a,x)]_1+K_2F_2+\cdots+K_kF_k,$$

és ez a (2)-vel együtt meg is adja a keresett előállítást.

Mint e jelölés egyszerű alkalmazását mindjárt itt mutatjuk be a következő, igen gyakran használt segédtételt:

Ha $E(a,x)\equiv 0\,(mod.\ F_1,\ldots,F_k)$, *akkor az E forma vagy tartalmazza az összes határozatlanokat, a melyek* F_1*-ben mint együtthatók szerepelnek, vagy pedig már* $E(a,x)\equiv 0\,(mod.\ F_2,\ldots,F_k)$.

Ha ugyanis $a_g^{(1)}$ az F_1 valamely olyan együtthatója, a mely nem fordúl elő $E(a,x)$-ben, akkor ezt az együtthatót $[E(a,x)]_1$ sem fogja tartalmazni; ebből pedig következik, hogy $[H_1]_1=0$, mert különben $[E(a,x)]_1=[H_1]_1F_1$ olyan forma volna, a melyben $a_g^{(1)}$ legalább is az 1 kitevővel ellátva fordúl elő. E szerint tehát $[E(a,x)]_1=0$ és ebből valóban következik,

hogy $E(a, x) \equiv 0 \pmod{F_2, \ldots, F_k}$. Még megjegyzendő, hogy ebben az esetben fennáll az

$$E(a, x) = K_2 F_2 + \cdots + K_k F_k$$

azonosság. Ha már most $E(a, x)$-et az $a^{(1)}$-k hatványszorzatai szerint rendezzük, meggondolva azt, hogy az $F_2, \ldots, F_k$ formák az $a^{(1)}$ határozatlanokat nem tartalmazzák, a két oldalon álló együtthatók összehasonlításából nyerjük, hogy már e hatványszorzatok minden egyes $e(a^{(2)}, \ldots, a^{(k)}, x)$ együtthatójára nézve

$$e(a^{(2)}, \ldots, a^{(k)}, x) \equiv 0 \pmod{F_2, \ldots, F_k}.$$

2. §. Az adott problémát még tovább speczializáljuk, t. i. az a határozatlanoknak oly raczionális és egész $\theta(a)$ formáira szorítkozva, a melyek az x-eket nem is tartalmazzák és a melyekre az általános probléma is könnyen visszavezethető, a mint azt majd később (a 6. §-ban) kimutatjuk.

Az ily $\theta(a)$ formákra vonatkozólag mindenekelőtt a következő fontos tétel érvényes:

Ha $F_1, \ldots, F_k$ az x-eknek igazi formái, azaz, ha ezeknek dimensiója legalább is 1 *és*

$$\theta(a) \equiv 0 \pmod{F_1, \ldots, F_k},$$

a hol $k \leqq m$, akkor ebből következik, hogy $\theta(a) = 0$; azaz, ha a rendszerben az általános formák száma nem nagyobb az x határozatlanok számánál, a zérus az a határozatlanoknak egyetlen raczionális és egész formája, a mely ama congruentiát kielégíti.

E tétel bebizonyítására elég, ha megvizsgáljuk a $k = m$ esetet. Ha ugyanis $k < m$, a rendszert kiegészíthetjük a további $F_{k+1}, \ldots, F_m$ általános formákkal. E kiegészítés után nemcsak $\theta(a) \equiv 0 \pmod{F_1, \ldots, F_k}$, hanem egyszersmind $\theta(a) \equiv 0 \pmod{F_1, \ldots, F_m}$ és ha ebből a congruentiából csakugyan mindig következik, hogy $\theta(a) = 0$, evvel a tétel általánosságban is be van bizonyítva.

Ez a következtetés közvetlenül foly az előbbi fejezet 15. §-ának (*b*) tételéből. Az $F_1, \ldots, F_m$ általános formarendszer függvénydeterminánsa nem zérus; mert pl. már akkor is különböző a zérustól, midőn $F_i = x_i^{n_i}$. Az F_i formának $x_1, \ldots, x_m$ nélküli tagja az $a_{i,\,m+1}$ határozatlan. Az $F_i = 0$ egyenletrendszer tartalma tehát m-edfokozatú sokaságot alkot; azaz e rendszernek van olyan megoldása, a mely az a-knak bizonyos algebrai függvényeiből áll. Ha ezeket belehelyettesítjük az $F_1, \ldots, F_m$ formákba, akkor, minthogy minden egyes F_i zérus lesz, míg θ, a mely az x-eket nem is tartalmazza, e mellett egyáltalában nem változik, a

$$\theta(a) = \sum_{i=1}^{m} H_i F_i$$

azonosságból a bebizonyítandó tételnek megfelelőleg következik, hogy $\theta(a) = 0$.

Didaktikai szempontból kényelmes lehet, ha e fejezet tárgyalása független az eliminázió általános elméletétől. Ezért e tételnek még egy második bebizonyítását is adjuk; elvi különbség azonban nincsen, mert — mint annak idején már említettük — az algebra ú. n. alaptételét az első bizonyításnál sem használtuk.

Most a teljes inductiót alkalmazzuk. Az $m = 1$ esetre a tétel ugyanis közvetetlenül világos. Az, hogy

$$\theta(a) \equiv 0 \,(\text{mod. } F_1),$$

annak a ténynek volna kifejezése, hogy $\theta(a)$ F_1-gyel osztható; ez pedig, minthogy $\theta(a)$ nem tartalmazza az x-eket, nem lehetséges, ha $\theta(a)$ a zérustól különböző.

Feltételezhetjük továbbá, hogy a tétel m határozatlan formáira nézve érvényes és azután $m+1$ határozatlan formáira a következő módon térünk át.

Ha $\theta(a) \equiv 0 \,(\text{mod. } F_1, \ldots, F_{m+1})$, akkor (az 1. §. segédtétele szerint) $\theta(a)$ vagy tartalmazza az a_{11} határozatlant,

vagy pedig $\theta(a) \equiv 0 \pmod{F_2, \ldots, F_{m+1}}$. Az utóbbi esetben $\theta(a)$ vagy tartalmazza az a_{22}-t, vagy pedig a $\theta(a) \equiv 0 \pmod{F_3, \ldots, F_{m+1}}$ congruentiának kell fennállania. Ha mindig a második eset állana be, végre nyernők, hogy $\theta(a) \equiv 0 \pmod{F_{m+1}}$; de mert ez lehetetlen, azért $\theta(a)$-nak az egyik a_{ii} határozatlant kell tartalmaznia és az általánosság megszorítása nélkül feltételezhetjük, hogy ez a_{11}. Hogy ez így legyen, csak alkalmas módon kell rendeznünk az x határozatlanokat és az F formákat.

Ha már most $\theta(a)$-t az a_{11} hatványai szerint rendezzük, akkor:

$$\theta(a) = \theta_0 + \theta_1 a_{11} + \cdots + \theta_r a_{11}^r,$$

a hol $r \geqq 1$ és $\theta_r \neq 0$. A

$$\theta(a) = \sum_{i=1}^{m+1} H_i F_i = H_1 (a_{11} x_1^{n_1} + \cdots) + \sum_{i=2}^{m+1} H_i F_i$$

azonosságból azonban, ha a_{11} legmagasabb hatványának a két oldalon álló együtthatóit összehasonlítjuk, nyerjük, hogy

$$\theta_r = G_1 x_1 + G_2 F_2 + \cdots + G_{m+1} F_{m+1},$$

a hol a G_1 helyébe, ha esetleg H_1 az a_{11}-re nézve az $r-1$-ediknél alacsonyabb fokú, 0 is jöhet. Ha ebben x_1 helyébe a 0-t teszszük, akkor továbbá

$$\theta_r = [G_2]_{x_1=0} [F_2]_{x_1=0} + \cdots + [G_{m+1}]_{x_1=0} [F_{m+1}]_{x_1=0}.$$

De $m+1$ határozatlannak *általános* formáiban az x_1 helyébe a 0-t téve, ezek természetesen m határozatlannak általános formáiba mennek át és minthogy ezekre nézve a tétel érvényes, a 0-tól különbözőnek feltételezett θ_r forma egyenlő volna 0-sal. A $\theta(a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}$ feltevés tehát ellenmondásra vezet, mihelyt $\theta(a)$ nem egyenlő zérussal.

A resultáns értelmezése és alapvető tulajdonságai.

3. §. Az $x_1, \ldots, x_m$ határozatlanoknak $m+1$ általános formájából:

$$F_i(x_1, \ldots, x_m) \qquad (i=1, \ldots, m+1)$$

álló rendszerre nézve, a melyben minden forma dimensiója, $n_1, \ldots, n_{m+1}$ kivétel nélkül $\geqq 1$, a következő tétel érvényes:

A határozatlan a együtthatóknak egy és csak egy — az aequivalentia értelmében teljesen meghatározott — oly raczionális és egész irreducibilis formája létezik, mely az $(F_1, \ldots, F_{m+1})$ *modulusrendszer meghatározta congruentia-tartományhoz tartozik. Ezt a formarendszer resultánsának nevezzük* és a következő módon jelöljük:

$$R = \text{Res.}(F_1, F_2, \ldots, F_{m+1}).$$

Ha a határozatlan a együtthatók helyébe valamely holoid tartománynak bármely oly mennyiségeit helyettesítjük, a melyek csak annak az egy feltételnek vannak alávetve, hogy az így származó formák dimensiója ismét $n_1, \ldots, n_{m+1}$ legyen, akkor a resultánsból származó mennyiséget ismét ama specziális formák resultánsának nevezzük és a következő módon jelöljük:

$$\text{Res.}\begin{pmatrix} F_1, F_2, \ldots, F_m, F_{m+1} \\ x_1, x_2, \ldots, x_m, 1 \end{pmatrix}.$$

Ez a részletes jelölés azért szükséges, mert a formák most más határozatlanokat is tartalmazhatnak.

Kitünik majd, hogy két formának egy határozatlan szerint vett resultánsa, a melynek elméletét a III. fejezetben fejtettük ki, mint specziális eset benne van e fogalomalkotásban.

A resultáns előjele, ezen értelmezés szerint egyelőre nincsen meghatározva; meghatározását későbbre tartjuk fenn.

A tétel közvetetlenül foly az eliminácziő általános el-

méletéből. Az $F_1=0, \ldots, F_m=0$ egyenletrendszer tartalma, mint előbb láttuk, m-edfokozatú sokaságot alkot; az így meghatározott (véges számú) gyökrendszer nem elégítheti ki soha az $F_{m+1}=0$ egyenletet, mert ennek összes együtthatói új határozatlanok. Az $F_1=0, \ldots, F_{m+1}=0$ egyenletrendszernek tehát nincsen tartalma és a resolvens forma elmélete közvetetlenül olyan $\Phi(a)$ raczionális és egész formát ad, melyre nézve

$$\Phi(a) \equiv 0 \,(\text{mod. } F_1, \ldots, F_{m+1}).$$

Már pedig, ha van egyáltalában az a együtthatóknak olyan zérustól különböző raczionális és egész formája, a mely az $(F_1, \ldots, F_{m+1})$ *modulusrendszer meghatározta congruentiatartományhoz tartozik, akkor érvényes a §. elején kimondott tétel és minden ilyen forma osztható lesz R-rel.*

Bontsuk fel ugyanis $\Phi(a)$-t irreducibilis tényezőire:

$$\Phi(a) = P_1(a) \ldots P_r(a).$$

Ha $a_{i,\,m+1}$ helyébe ismét $a_{i,\,m+1} - F_i$-t írjuk, akkor

$$[\Phi(a)] = [P_1(a)] \ldots [P_r(a)] = 0;$$

tehát a tényezők egyike, pl. $[P(a)] = 0$, azaz egyszersmind

$$P(a) \equiv 0 \,(\text{mod. } F_1, \ldots, F_{m+1}).$$

De ekkor nem lehetséges, hogy valamely második, $P(a)$-val *nem* æquivalens, irreducibilis, raczionális és egész $Q(a)$ formára nézve is

$$Q(a) \equiv 0 \,(\text{mod. } F_1, \ldots, F_{m+1})$$

legyen. $P(a)$ és $Q(a)$ ugyanis mind a kettő a zérustól különböző és tartalmazza az összes $a_g^{(i)}$ együtthatókat. Ha ezek közül csak egy is kiesnék, akkor $P(a)$-nak, illetőleg $Q(a)$-nak ahhoz a congruentiatartományhoz kellene tartoznia, a melyet $(F_1, \ldots, F_{m+1})$ az F_i kizárása után meghatároz és így a 2. §. szerint zérussal kellene egyenlőnek lennie.

Ha most a III. fejezetben kifejtett elemi módszer sze-

rint képezzük $P(a)$ és $Q(a)$-nak $a_g^{(i)}$ szerint vett resultánsát, akkor lesz

$$\text{Res.}\begin{pmatrix} P(a), & Q(a) \\ a_g^{(i)}, & 1 \end{pmatrix} = Q_1(a)\,P(a) + P_1(a)\,Q(a) \equiv$$

$$\equiv 0\,(\text{mod. } F_1, \ldots, F_{m+1})$$

és, minthogy ez az a együtthatóknak az $a_g^{(i)}$ kizárásával racionális és egész formája, e resultánsnak zérussal kell egyenlőnek lennie. Így tehát az egymással nem æquivalens, irreducibilis $P(a)$ és $Q(a)$ formák a feltevés ellenére az 1-től különböző közös osztót tartalmaznának. Evvel a tétel már be van bizonyítva.

Ha ugyanis most bármely $\Psi(a) \equiv 0\,(\text{mod. } F_1, \ldots, F_{m+1})$, akkor már e forma valamely $Q(a)$ irreducibilis tényezőjére nézve is $Q(a) \equiv 0$, tehát $P(a) \sim Q(a)$ és $\Psi(a)$ osztható $P(a)$-val.

A resultánsok általános elmélete azonban az elimináczió általános elméletének használata nélkül is kifejtendő. Ezt nem csak didaktikai okokból teszszük, hanem főleg azért, mert evvel együtt megállapítjuk a formarendszer resultánsának recursiv alkotását is lehető egyszerű módon.

4. §. A módszer, a melyet itt használunk, a teljes inductio és ennek megfelelőleg először az $m=1$ esetet kell tisztába hoznunk. E végből csak a III. fej. 14. §-ának eredményei lesznek kiegészítendők. A jelöléseket a mostani általános megállapodásoknak megfelelőleg változtatva, a két forma a következő:

$$F_1(x_1) = a_{11}\,x_1^{n_1} + \cdots + a_{12}$$

$$F_2(x_1) = a_{21}\,x_1^{n_2} + \cdots + a_{22}$$

és az ott felállított Sylvester-féle determináns a most adott pontosabb értelemben is az F_1, F_2 formarendszer resultánsa. Hogy ezt az állításunkat bebizonyítsuk, csak meg kell mutatnunk, hogy *ez a Sylvester-féle determináns az együttha-*

tóknak irreducibilis formája; hogy az (F_1, F_2) modulusrendszer meghatározta congruentiatartományhoz tartozik, azt már a III. fej. 16. §-ából tudjuk.

A kérdéses determinánsnak kifejtése, mint közvetetlenül látni,

$$a_{11}^{n_2} a_{22}^{n_1} + \cdots,$$

a hol a kiírt tag más taggal szemben nem eshetik ki. A bizonyítás magva a következő tényben rejlik:

Ha $\Theta(a)$ *a zérustól különböző és*

$$\Theta(a) \equiv 0 \,(\text{mod. } F_1, F_2),$$

akkor $\Theta(a)$*-nak az* a_{11} *hatványai szerint való kifejtésében, vagyis a*

$$\Theta(a) = \vartheta_0 + \vartheta_1 a_{11} + \cdots + \vartheta_r a_{11}^r$$

kifejezésben ϑ_r*-nek oszthatónak kell lennie* $a_{22}^{n_1}$*-vel*.*

Ugyanis

$$\Theta(a) = H_1 F_1 + H_2 F_2;$$

ha tehát a_{22} helyébe $a_{22} - F_2$-t írjuk, akkor

$$[\Theta(a)]_1 = [H_1]_1 F_1,$$

vagyis

$$[\vartheta_0]_1 + \cdots + [\vartheta_r]_1 a_{11}^r = [H_1]_1 F_1;$$

és ha ebben az a_{11}^r-nek a két oldalon álló együtthatóit összehasonlítjuk, azt találjuk, hogy

$$[\vartheta_r]_1 = K x_1^{n_1},$$

vagyis

$$\vartheta_r = K x_1^{n_1} + L F_2,$$

a hol ϑ_r természetesen nem egyenlő a zérussal, minthogy

* Ez a tétel, valamint a megfelelő általános tétel a 9. §-ban F. MERTENS-től származik. («Über die bestimmenden Eigenschaften der Resultante», Sitzungsberichte d. k. Akad. d. Wiss. in Wien. Math.-nat. wiss. Cl. XCIII. k. II. r. 543. l.)

$\theta(a)$ a zérustól különböző. Szükségképen meg $r \geqq 1$, minthogy az előbbiek szerint $\theta(a)$ minden esetre tartalmazza a_{11}-et. Ha az utoljára nyert azonosságba x_1 helyébe a zérust teszszük, akkor

$$\vartheta_r = (L)_{x_1=0}\, a_{22}\,;$$

tehát ϑ_r minden esetre osztható a_{22}-vel.

Ha már most ϑ_r osztható volna $a_{22}^{n_1-k}$-val, $(k>0)$, de nem volna osztható $a_{22}^{n_1-k+1}$-vel úgy, hogy

$$\vartheta_r = a_{22}^{n_1-k}\,\eta_r,$$

a hol η_r természetesen ismét az a-knak raczionális és egész formája, ebből következnék, hogy

$$[a_{22}^{n_1-k}]_1\,[\eta_r]_1 = K x_1^{n_1},$$

vagyis, hogy

$$(a_{22}-F_2)^{n_1-k}\,[\eta_r]_1 = K x_1^{n_1}.$$

Ámde $(a_{22}-F_2)^{n_1-k}$ osztható $x_1^{n_1-k}$-val, de nem osztható az x_1-nek ennél magasabb hatványával. Ebből tehát következnék, hogy

$$[\eta_r]_1 = M x_1^k,$$

$$\eta_r = M x_1^k + N F_2(x_1)$$

és ha végre x_1 helyébe ismét a 0-t teszszük, lenne

$$\eta_r = (N)_{x_1=0}\, a_{22},$$

azaz η_r osztható volna a_{22}-vel és ϑ_r a feltevés ellenére is $a_{22}^{n_1-k+1}$-vel.

Ha már most a SYLVESTER-féle determinánsnak volnának osztói, ezek közül az egyiknek tartalmaznia kellene a_{11}-et és ennek a_{11} hatványai szerint való kifejtésében a legmagasabb tag a következő alakú volna:

$$a_{11}^{r}\, a_{22}^{n_1}\, A.$$

Szembetünő, hogy a SYLVESTER-féle determináns az $a^{(2)}$ határozatlanoknak n_1-ed dimensiójú homogén formája úgy,

hogy tehát osztói sem lehetnek az $a^{(2)}$-kre nézve magasabb dimensiójúak. Ezért, ha felcseréljük F_1 és F_2 szerepét, abban az osztóban, a mely egy tagot $a_{22}^{n_1}$-vel tartalmaz, ugyanaz a tag osztható volna $a_{11}^{n_2}$-vel. Azaz a feltételezett osztó a következő alakú volna:

$$a_{11}^{n_2} a_{22}^{n_1} A + \cdots .$$

De akkor szükséges, hogy $A=1$ legyen és így tehát amaz osztó teljesen megegyezik a SYLVESTER-féle determinánssal; és ez az a mit be kellett bizonyítani.

5. §. *Az m határozatlan $m+1$ általános formájából álló*

$$F_i(x_1, \ldots, x_m) \qquad (i=1, \ldots, m+1)$$

rendszerre vonatkozólag bebizonyítandó tényeket a következő módon fogalmazzuk. Jelentsék ismét $n_1, \ldots, n_{m+1}$ az $F_1, \ldots, F_{m+1}$ formák dimensióit $(n_i \geqq 1)$ és legyen

$$N = n_1 \ldots n_{m+1}, \quad N_i = \frac{N}{n_i}.$$

Az a együtthatóknak egy és csak egy raczionális és egész formája létezik, a formarendszer ú. n. resultánsa $R(a)$, a melynek a következő tulajdonságai vannak:*

* A mi a resultáns elméletének történetét és meglehetős terjedelmű irodalmát illeti, az Encyclopädie der mathematischen Wissenschaften» I. kötetére utalunk. L. ott NETTO «Über rationale Functionen mehrerer Veränderlichen» cz. czikkének 6.—8. és 14. §-át.

Világos betekintést e bonyolódott képződmény természetébe csak az algebrai mennyiségek elmélete alapján nyerünk. Különösen ki kell itt emelnünk a resultánsnak a 3. §-ban adott első értelmezését és a KRONECKER-féle substitutio alkalmazásának elvét. Sokszoros érintkezése van az itt előadott tárgyalásnak F. MERTENS-nek két dolgozatával a Sitz. Ber. d. Wiener Akad. d. Wiss. XCIII. kötetében 527. l. és CVIII. kötetében II. *a.* 1173. l.; ezekben történt először a KRONECKER-féle substitutio alkalmazása a resultánsok elméletére.

a) *A resultáns az a-knak irreducibilis formája.*

b) $R(a) \equiv 0 \,(mod.\, F_1, \ldots, F_{m+1})$.

Ez a két tulajdonság meghatározza a resultánst az előjel mellőzésével.

c) *A resultáns tartalmazza az*

$$a_{11}^{N_1} a_{22}^{N_2} \ldots a_{m+1,\,m+1}^{N_{m+1}}$$

tagot, +1 együtthatóval ellátva.

Evvel meg van határozva a resultáns előjele.

d) *A resultáns az együtthatók minden egyes $a^{(i)}$ sorozatának N_i-dik dimensiójú homogén formája; tehát az összes a együtthatóknak oly homogén formája, a melynek dimensiója* $\sum_{i=1}^{m+1} N_i$.

e) *A resultáns isobarikus, azaz a resultáns összes tagjainak súlya ugyanaz; még pedig N.* Itt az $a_g^{(i)}$ együttható súlyának nevezzük az $n_i = \sum_{j=1}^{m} g_j$ számot és valamely tag súlyának az egyes ebben tényezőkként szereplő $a_g^{(i)}$-k súlyainak összegét. Ha tehát $a_g^{(i)}$ súlyát $P(a_g^{(i)})$-vel jelöljük, akkor e szerint

$$P(a_{g'}^{(i')} a_{g''}^{(i'')} \ldots) = P(a_{g'}^{(i')}) + P(a_{g''}^{(i'')}) + \cdots$$

Most majd először is kimutatjuk, hogy a resultánsnak (a), (b), (c) tulajdonságaiból már is mindig következnek a (d) és (e) tulajdonságok.

Ha ugyanis $R(a)$ az együtthatók valamely $a_g^{(i)}$ sorozatára vonatkozólag nem volna homogén, hanem

$$R(a) = S_{i0} + \cdots + S_{ir}, \qquad (S_{ir} \neq 0)$$

a hol S_{ik} az $R(a)$ ama tagjainak complexusát jelenti, a melyeknek dimensiója az $a_g^{(i)}$-kre vonatkozólag k, akkor az

$$R(a) = \sum_{i=1}^{m+1} H_i F_i$$

kapcsolatból egyszersmind következik, hogy *

$$S_{ir}=H_{ii}^{(r-1)}F_i+\sum_{j=1}^{m+1}{}^{(i)}H_{ji}^{(r)}F_j,$$

a hol $H_{ji}^{(s)}$ a H_j ama tagjainak complexusát jelenti, a melyeknek dimensiója az együtthatók $a_g^{(i)}$ sorozatára vonatkozólag s. Ekkor azonban a 3. §-ban bebizonyított tételek szerint a resultáns megegyezik S_{ir} egyik irreducibilis tényezőjével. $R(a)-S_{ir}$ tehát osztható $R(a)$-val; de minthogy $R(a)-S_{ir}$ dimensiója az $a_g^{(i)}$-kre vonatkozólag legfölebb $r-1$, az $R(a)$-é pedig r, szükséges, hogy $R(a)-S_{ir}=0$ legyen, azaz $S_{ir}=R(a)$.

A resultáns létezéséből tehát már következik, hogy az az együtthatók minden egyes $a_g^{(i)}$ sorozatának és így az összes a együtthatóknak is homogén formája.

A (c) tulajdonság miatt azonban az $R(a)$ dimensiója az együtthatók $a_g^{(i)}$ sorozatára nézve minden esetre N_i. Az (a), (b) és (c) tulajdonságokból tehát valóban mindig következik a (d) tulajdonság.

Hogy kimutassuk (e) érvényességét is, írjuk, hogy

$$R(a)=T_0(a)+\cdots+T_p(a)+\cdots+T_r(a), \quad (T_r(a)\neq 0)$$

a hol $T_p(a)$ az $R(a)$ ama tagjainak complexusát jelenti, a melyeknek súlya p. Ámde az

$$R(a)=\sum_{i=1}^{m+1}H_iF_i$$

azonosság megtartja érvényességét akkor is, midőn mindenütt

$$a_g^{(i)} \text{ helyébe } a_g^{(i)}x_{m+1}^{n_i-\sum g_j^{(i)}}$$

-et irjuk. De akkor

$$\sum_{p=0}^{r}T_p(a)\,x_{m+1}^p=\sum_{i=1}^{m+1}K_i\Phi_i;$$

* A $\sum_{j=1}^{m+1}{}^{(i)}$ jel azt jelenti, hogy a summatio kiterjesztendő a $j=1,\ldots,m+1$ értékekre a $j=i$ érték kizárásával.

mert $T_p(a)$-ban a tagok mind egyenlő súlyúak lévén, mindegyikhez csak az x_{m+1}^p tényező járul hozzá, míg a jobb oldalon e változtatás következtében F_i átmegy a megfelelő homogén formába (II. fej. 8. §.), Φ_i-be.

Ha már most x_j helyébe, hol $j=1, \ldots, m+1$, mindig $x_j u$-t írjuk, akkor Φ_i-hez csak az u^{n_i} tényező lép hozzá és, ha most ismét x_{m+1} helyébe 1-et teszünk, akkor

$$\sum_{p=0}^{r} T_p(a)\, u^p = \sum_{i=1}^{m+1} L_i F_i,$$

és, ha ebben u^r-nek a két oldalon álló együtthatóit összehasonlítjuk, nyerjük, hogy

$$T_r(a) = \sum_{i=1}^{m+1} M_i F_i.$$

Szükséges tehát, hogy $T_r(a)$ osztható legyen $R(a)$-val, tehát

$$R(a) - T_r(a) = T_0(a) + \cdots + T_{r-1}(a) = R(a)\, Q(a)$$

volna, a mi pedig lehetetlen; mert az egyik oldalon van legalább is egy tag, a melynek súlya $\geqq r$, míg a másik oldalon csakis olyan tagok állanak, a melyeknek súlya $< r$. Ez az ellenmondás csak úgy szünik meg, ha $R(a) = T_r(a)$. E szerint tehát a resultáns minden egyes tagjának súlya r és egyszersmind $R(a) = T_r(a)$.

Minthogy azonban

$$P(a_{11}) = 0, \ldots, P(a_{nn}) = 0, P(a_{m+1, m+1}) = n_{m+1},$$

a resultáns ama tagjának súlya, a mely (c)-ben meg van határozva, $n_{m+1} N_{m+1} = N$.

Az egy határozatlant tartalmazó két formának resultánsára nézve ezek az állítások kivétel nélkül érvényesek. Hogy abban az (a) és (b) tulajdonságok megvannak, azt már előbb bebizonyítottuk; a (c) és (d) tulajdonságot pedig közvetetlenül felismerjük, ha a resultánst (SYLVESTER-

féle determinánst) felírjuk. Hogy ezekből az (*e*) tulajdonság is következik, azt épen most bizonyítottuk be.

6. §. Az 5. §. tételeiből még további fontos következtetéseket vonhatunk. Tekintetbe véve c_{ij} és $a_{i,\,m+1}$ jelentését, a melyet az F_i formának részletes kiírásával állapítottunk meg, t. i. hogy

$$F_i(x_1,\ldots,x_m)=\sum_{j=1}^{m} a_{ij}\,x_j^{n_i}+\cdots+\sum_{j=1}^{m} c_{ij}\,x_j+a_{i,\,m+1},$$

az

$$R(a)=\sum_{i=1}^{m+1} H_i\,F_i$$

azonosságból, ha ennek c_{ij} és $a_{i,\,m+1}$ szerint vett deriváltját képezzük,

$$\frac{\partial R}{\partial c_{ij}}=\sum_{i=1}^{m+1}\frac{\partial H_i}{\partial c_{ij}}\,F_i+H_i\,x_j,$$

$$\frac{\partial R}{\partial a_{i,\,m+1}}=\sum_{i=1}^{m+1}\frac{\partial H_i}{\partial a_{i,\,m+1}}\,F_i+H_i,$$

származik, a miből:

$$\frac{\partial R}{\partial a_{i,\,m+1}}\,x_j\equiv\frac{\partial R}{\partial c_{ij}}\ (\text{mod. } F_1,\ldots,F_{m+1}). \qquad (X_j)$$
$$(j=1,\ldots,m).$$

Ha már most $E(x,a)$ az x-eknek és a-knak valamely olyan raczionális és egész formája, a melynek az x-ekre vonatkozó dimensiója ν, akkor

$$\left(\frac{\partial R}{\partial a_{i,\,m+1}}\right)^{\nu}E(x,a)$$

úgy írható, hogy minden x_j csak a $\dfrac{\partial R}{\partial a_{i,m+1}}\,x_j$ szorzatban fordúljon elő. Az (X_j) congruentiák alapján tehát

$$\left(\frac{\partial R}{\partial a_{i,\,m+1}}\right)^{\nu}E(x,a)\equiv e(a)\ (\text{mod. } F_1,\ldots,F_{m+1}),$$

a hol $e(a)$ egyedül csakis az a-knak raczionális és egész formája. Ezek után:

Annak szükséges és elegendő feltétele, hogy

$$E(x, a) \equiv 0 \,(mod.\, F_1, \ldots, F_{m+1})$$

legyen, az, hogy $e(a) \equiv 0 \,(mod.\, F_1, \ldots, F_{m+1})$, *vagyis tehát hogy* $e(a) \equiv 0 \,(mod.\, R)$ *legyen.*

Hogy az $E(x, a) \equiv 0$-ból közvetetlenül foly $e(a) \equiv 0$, az utolsó congruentiából világos; de ha megfordítva $e(a) \equiv 0$, ebből a congruentiából, mindenütt az $a_{i,\, m+1}$ helyébe $a_{i,\, m+1} - F_i$-t írva, következik, hogy

$$\left[\frac{\partial R}{\partial a_{i,\, m+1}}\right]^{\nu} [E(x, a)] = 0.$$

Ámde az nem lehetséges, hogy

$$\left[\frac{\partial R}{\partial a_{i,\, m+1}}\right] = 0, \text{ azaz } \frac{\partial R}{\partial a_{i,\, m+1}} \equiv 0 \,(\text{mod.}\, F_1, \ldots, F_{m+1});$$

mert $\dfrac{\partial R}{\partial a_{i,\, m+1}}$, a melynek dimensiója $\Sigma N_i - 1$, nem lehet osztható R-rel, a melynek dimensiója ΣN_i. Igy tehát:

$$[E(x, a)] = 0, \text{ azaz } E(x, a) \equiv 0 \,(\text{mod.}\, F_1, \ldots, F_{m+1}).$$

A resultáns recursiv képezése.

7. §. Feltételezve most már, hogy a resultánsra vonatkozó tételek m határozatlannak $m+1$ formája esetében érvényesek, a mint azokat az $m=1$ esetére tényleg bebizonyítottuk, kimutatjuk, hogy azok $m+1$ határozatlannak $m+2$ formája esetében is érvényesek maradnak. Ez lényegében úgy történik, hogy recursiv módszert adunk a resultáns képezésére.

Közvetetlenül világos, hogy az m határozatlannak $m+2$ formájából álló

$$F_i(x_1, \ldots, x_m) = \sum_{(i=1, \ldots, m+2)} a_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$

rendszerből úgy származik a megvizsgálandó rendszer:

$$\bar{F}_i(x_1, \ldots, x_m, x_{m+1}) = \sum_{(i=1, \ldots, m+2)} \bar{a}_g^{(i)} x_1^{g_1} \ldots x_m^{g_m},$$

a mely $m+1$ határozatlannak $m+2$ formájából áll, hogy $\bar{a}_g^{(i)}$-t az új x_{m+1} határozatlan oly általános formájának gondoljuk, a melynek foka $n_i - \Sigma g_j$ (az $a_g^{(i)}$ súlya). Jelesen, ha az

$$F_i(x_1, \ldots, x_m) = \sum_{j=1}^{m} a_{ij} x_j^{n_i} + \cdots + \sum_{j=1}^{m} c_{ij} x_j + a_{i, m+1}$$

jelölést használjuk, lesz

$$\bar{F}_i(x_1, \ldots, x_m, x_{m+1}) = \sum_{j=1}^{m} a_{ij} x_j^{n_i} + \cdots + \sum_{j=1}^{m} \bar{c}_{ij} x_j + \bar{a}_{i, m+1};$$

mert $\bar{a}_{ij}$-nek x_{m+1}-re vonatkozó foka 0 és így tehát $\bar{a}_{ij}$ pontosan ugyanazt az együtthatót jelenti, mint a_{ij}. Általánosságban pedig

$$\bar{a}_{ii} = k_{ii} = l_{ii}, \qquad (i=1, \ldots, m)$$
$$\bar{a}_{i, m+1} = k_{i, m+1} + \cdots + l_{i, m+1} x_{m+1}^{n_i},$$
$$\bar{a}_g^{(i)} = k_g^{(i)} + \cdots + l_g^{(i)} x_{m+1}^{n_i - \Sigma g_j}.$$

A közbeeső együtthatók speciális jelölésére nincs szükségünk.

Ha már most az $\bar{F}_i$ formák közül az egyiket, pl. az utolsót, $\bar{F}_{m+2}$-t elhagyjuk — nevezzük az így származó rendszert S_{m+2}-nek — akkor a megmaradt formákat az $x_1, \ldots, x_m$ határozatlanok oly formáinak tekinthetjük, a melyekben az együtthatók az $\bar{a}_g^{(i)}$-k. Az ilyen rendszerek resultánsára vonatkozólag feltételezett alaptulajdonság szolgáltatja az

$$R_{m+2}(\bar{a}) = \sum_{i=1}^{m+1} H_i \bar{F}_i$$

azonosságot, melyet így is írhatunk:

$$R_{m+2}(\bar{a}) \equiv 0 \,(\text{mod. } \bar{F}_1, \ldots, \bar{F}_{m+2}).$$

Itt $R_{m+2}(\bar{a})$ az x_{m+1} határozatlannak formája és ennek

x_{m+1} nélküli tagját úgy nyerjük, hogy $x_{m+1}=0$ tétetik, vagy pedig, a mi ugyanaz, hogy $\bar{a}_g^{(i)}$ helyébe mindenütt a $k_g^{(i)}$-t irjuk. Ezt a tagot tehát, a mely egyszerűen az m határozatlannak $m+1$ általános formájából álló

$$K_i(x_1, \ldots, x_m) = \sum_{(i=1, \ldots, m+1)} k_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$

formarendszer resultánsa, $R_{m+2}(k)$-val jelölhetjük.

Ha $\bar{N}=\prod_{i=1}^{m+2} n_i$ és $\bar{N}_{m+2}=\frac{\bar{N}}{n_{m+2}}$, akkor továbbá $R_{m+2}(\bar{a})$-nak súlya ismét $\bar{N}_{m+2}$. Minthogy pedig $\bar{a}_g^{(i)}$-nek x_{m+1}-re vonatkozó foka pontosan megegyezik $a_g^{(i)}$ súlyával, $R_{m+2}(\bar{a})$ minden tagjának x_{m+1}-re vonatkozó foka $\bar{N}_{m+2}$. Az x_{m+1} legmagasabb hatványának együtthatóját pedig úgy nyerjük, hogy mindenütt $\bar{a}_g^{(i)}$ helyébe $l_g^{(i)} x_{m+1}^{n_i-\sum g_j}$ jő. E szerint tehát

$$R_{m+2}(\bar{a}) = R_{m+2}(k) + \cdots + R_{m+2}(l)\, x_{m+1}^{\bar{N}_{m+2}},$$

a hol $R_{m+2}(l)$ ismét az m határozatlannak $m+1$ általános formájából álló

$$L_i(x_1, \ldots, x_m) = \sum_{(i=1, \ldots, m+1)} l_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$

formarendszer resultánsa.

Az 5. §. (*c*) tétele szerint továbbá

$$R_{m+2}(k) = k_{11}^{\bar{N}_{m+2,1}} k_{22}^{\bar{N}_{m+2,2}} \ldots k_{m+1,m+1}^{\bar{N}_{m+2,m+1}} + \cdots,$$

a hol

$$\bar{N}_{m+2,i} = \frac{\bar{N}_{m+2}}{n_i}.$$

Teljesen azonos módon még

$$R_{m+2}(l) = l_{11}^{\bar{N}_{m+2,1}} l_{22}^{\bar{N}_{m+2,2}} \ldots l_{m+1,m+1}^{\bar{N}_{m+2,m+1}} + \cdots$$

Ámde az 5. §. (*c*) tételéből következik, hogy $R_{m+2}(k)$, ill. $R_{m+2}(l)$ felírt tagja az egyetlen, a mely csak $k_{11}, k_{22}, \ldots, k_{mm}$-et és $k_{m+1,m+1}$-et, ill. $l_{11}, l_{22}, \ldots, l_{mm}$-et és $l_{m+1,m+1}$-et tartalmazza. Minthogy továbbá

$$\bar{a}_{11}^{\bar{N}_{m+2,1}} \bar{a}_{22}^{\bar{N}_{m+2,2}} \dots \bar{a}_{m+1,\,m+1}^{\bar{N}_{m+2,\,m+1}}$$

kivételével $R_{m+2}(\bar{a})$ minden tagja legalább is egy $\bar{a}_{ij}\,(i \neq j)$ határozatlant tartalmaz, látni, hogy

$$R_{m+2}(\bar{a}) = (k_{11}^{\bar{N}_{m+2,1}} \dots k_{m+1,\,m+1}^{\bar{N}_{m+2,\,m+1}} + \dots) + \dots +$$
$$+ (l_{11}^{\bar{N}_{m+2,1}} \dots l_{mm}^{\bar{N}_{m+2,\,m}} l_{m+1,\,m+1}^{\bar{N}_{m+2,\,m+1}} + \dots)\, x_{m+1}^{\bar{N}_{m+2}}$$

kifejtésében a valóban felírt két tag kivételével minden tag az $\bar{F}_i$ formáknak legalább is egy a $k_{11}, \dots, k_{m+1,\,m+1}$ és $l_{11}, \dots, l_{m+1,\,m+1}$-től különböző együtthatóját tartalmazza.

Végül még bevezetjük az $\bar{F}_i$ formáknak az F_i formáktól független, az eredetileg használtnak megfelelő jelölését, hol zavarok elkerülése végett a határozatlan együtthatók jelölésére az új α symbolumot használjuk; azaz megállapodunk abban, hogy

$$\bar{F}_i(x_1, \dots, x_{m+1}) = \sum_{j=1}^{m+1} \alpha_{ij}\, x_j^{n_j} + \dots + \alpha_{i,\,m+2}.$$

Akkor végül $R_{m+2}(\bar{a})$-t, mint az α-k és x_{m+1} formáját $R_{m+2}(\alpha, x_{m+1})$-nek írva, a következő eredményhez jutunk:

$$R_{m+2}(\alpha, x_{m+1}) = (\alpha_{11}^{\bar{N}_{m+2,1}} \dots \alpha_{mm}^{\bar{N}_{m+2,\,m}} \alpha_{m+1,\,m+2}^{\bar{N}_{m+2,\,m+1}} + \dots) + \dots +$$
$$+ (\alpha_{11}^{\bar{N}_{m+2,1}} \dots \alpha_{mm}^{\bar{N}_{m+2,\,m}} \alpha_{m+1,\,m+1}^{\bar{N}_{m+2,\,m+1}} + \dots)\, x_{m+1}^{\bar{N}_{m+2}}, \quad \text{(I)}$$
$$R_{m+2}(\alpha, x_{m+1}) \equiv 0 \,(\text{mod. } \bar{F}_1, \dots, \bar{F}_{m+2}).$$

E mellett még egyszer kiemeljük, hogy R_{m+2}-nek fel nem írt tagjai közül mindegyik tartalmaz legalább is egy az

$$\alpha_{11}, \dots, \alpha_{m+2,\,m+2},\ \alpha_{m+1,\,m+2},\ \alpha_{m+2,\,m+1}$$

határozatlanoktól különböző határozatlant. Ezt az $\alpha_{m+2,\,m+1}$ és $\alpha_{m+2,\,m+2}$ kivételével már említettük az itt felsorolt határozatlanokról; e kettőt azonban hozzácsatolhatjuk a többiekhez, mert az R_{m+2} képezésénél nem is használtuk az $\bar{F}_{m+2}$ formát.

Az R_{m+2} képezésénél az $\bar{F}_i$ formák rendszeréből kizártuk az $\bar{F}_{m+2}$ formát; teljesen ugyanazt a kifejtést ismétel-

hetjük, ha az $\bar{F}_i$ formák rendszeréből kizárjuk az $\bar{F}_{m+1}$ formát. Az eredmény az előbbitől csak abban különbözik majd, hogy az $m+1$ és $m+2$ indexek, a mennyiben formákra vonatkoznak, helyet cserélnek. Ilyenek az n, R és $\bar{N}$ indexei, valamint az α_{ij}-ben az első helyen álló index és még $\alpha_g^{(i)}$ fölső indexe. Igy tehát

$$R_{m+1}(\alpha, x_{m+1}) = (\alpha_{11}^{\bar{N}_{m+1,1}} \dots \alpha_{mm}^{\bar{N}_{m+1,m}} \alpha_{m+2,m+2}^{\bar{N}_{m+1,m+2}} + \dots) + \dots +$$
$$+ (\alpha_{11}^{\bar{N}_{m+1,1}} \dots \alpha_{mm}^{\bar{N}_{m+1,m}} \alpha_{m+2,m+1}^{\bar{N}_{m+1,m+2}} + \dots)\, x_{m+1}^{\bar{N}_{m+1}}, \quad \text{(II)}$$
$$R_{m+1}(\alpha, x_{m+1}) \equiv 0 \,(\text{mod. } \bar{F}_1, \dots, \bar{F}_{m+2}),$$

a hol R_{m+1}-nek minden ki nem írt tagja ismét legalább is egy az

$$\alpha_{11}, \dots, \alpha_{m+2,m+2}, \alpha_{m+1,m+2}, \alpha_{m+2,m+1}$$

határozatlanoktól különböző határozatlant tartalmaz.

Ha már most R_{m+1}-nek és R_{m+2}-nek x_{m+1} szerint vett resultánsát képezzük, akkor

$$\text{Res.} \begin{pmatrix} R_{m+1}, & R_{m+2} \\ x_{m+1}, & 1 \end{pmatrix} = \alpha_{11}^{K_1} \dots \alpha_{m+2,m+2}^{K_{m+2}} + \dots = H(\alpha), \quad \text{(III)}$$

a hol minden további tag — a mint ez az eddigi fejtegetésekből közvetetlenül következik — legalább is egy az $\alpha_{11}, \dots, \alpha_{m+2,m+2}$ határozatlanoktól különböző határozatlant tartalmaz; és így a felírt tag más taggal szemben ki nem eshetik; ama hatványszorzatnak együtthatója $H(\alpha)$-ban pedig 1 lesz. Ámde két forma resultánsának elemi elméletéből $H(\alpha)$-ra nézve következik, hogy

$$H(\alpha) \equiv 0 \,(\text{mod. } R_{m+1}, R_{m+2})$$

úgy, hogy egyszersmind

$$H(\alpha) \equiv 0 \,(\text{mod. } \bar{F}_1, \dots, \bar{F}_{m+2}).$$

Evvel tehát a 3. §. szerint be van bizonyítva, hogy az $m+1$ határozatlannak $m+2$ formájából álló általános rend-

szernek van resultánsa és ez az előjel mellőzésével minden esetre a $H(\alpha)$ valamely irreducibilis tényezője.

Az 5. §. általános tételének (a) és (b) állításai tehát evvel igazolva vannak.

8. §. Az ebben foglalt utasítás a resultáns képezésére még annyiban nem mondható teljesnek, a mennyiben az $H(\alpha)$ irreducibilis osztóin elvégzendő kisérletek sorozatát követeli. Helyébe azonban oly módszer léphet, a mely csakis k határozatlan $k+1$ formája esetében — ($k \leqq m$) — követeli a resultáns képezését és azután bizonyos legnagyobb közös osztók meghatározását. E módszer egyszermind feltárja a resultánsnak újabb tulajdonságait.

Ha a 6. §. (X_j) képleteit az

$$\bar{F}_i(x_1, \ldots, x_{m+1}) = \sum_{(g)}^{(i=1,\ldots,m+1)} \bar{a}_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$

formarendszerre és ennek $R_{m+2}(\bar{a})$ resultánsára alkalmazzuk, akkor ezekből

$$\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,\,m+1}} x_j \equiv \frac{\partial R_{m+2}(\bar{a})}{\partial \bar{c}_{ij}} \pmod{\bar{F}_1, \ldots, \bar{F}_{m+1}}$$

származik, a melynek alapján, ha $E(x, a)$ helyébe az

$$\bar{F}_{m+2}(x_1, \ldots, x_{m+1}) = \sum_{(g)} \bar{a}_g^{(m+2)} x_1^{g_1} \ldots x_m^{g_m}$$

formát teszszük, úgy mint ott, továbbá következik, hogy

$$\left(\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,\,m+1}}\right)^{n_{m+2}} \bar{F}_{m+2}(x_1, \ldots, x_{m+1}) \equiv$$

$$\equiv \Gamma(\alpha, x_{m+1}) \pmod{\bar{F}_1, \ldots, \bar{F}_{m+1}}.$$

A Γ e mellett az $\bar{F}_{m+2}$-ben fellépő határozatlan együtthatóknak lineáris formája, mert R_{m+2} és ennek deriváltjai azokat nem tartalmazzák. Ebből kiindulva bebizonyíthatjuk, hogy az R_{m+2} és Γ legnagyobb közös osztója az 1. Nevezzük ugyanis e legnagyobb közös osztót D-nek, akkor az, mint R_{m+2} osztója nem tartalmazhat egyetlen $\alpha_g^{(m+2)}$-t sem. Ha

tehát Γ-t mint ezeknek lineáris formáját írjuk, akkor kell, hogy e forma minden együtthatója, tehát az $\alpha_{m+2,\,m+2}$ mellett álló is, azaz

$$\left(\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,\,m+1}}\right)^{n_{m+2}}$$

osztható legyen D-vel. Tehát az

$$R_{m+2}(\bar{a}) \quad \text{és} \quad \frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,\,m+1}}$$

legnagyobb közös osztója is az 1-től különböző volna. De akkor ennek

$$A_0 + A_1 x_{m+1} + \cdots$$

alakúnak kellene lennie, a hol A_0 a 0-tól különböző, mert R_{m+2} nem osztható x_{m+1}-gyel. Így tehát az

$$[R_{m+2}(\bar{a})]_{x_{m+1}=0} \quad \text{és} \quad \left[\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,\,m+1}}\right]_{x_{m+1}=0}$$

formáknak oszthatóknak kellene lenniök A_0-sal. Ámde ezek közül az első forma, mint az $[\bar{F}_i]_{x_{m+1}=0}$ $(i=1,\ldots,m+1)$ formarendszer resultánsa irreducibilis forma és a második az $a_g^{(i)}$-kre vonatkozólag alacsonyabb fokú, mint az első, a miből következik, hogy $A_0 = \pm 1$.

Az $R_{m+2}(\bar{a})$ továbbá az $\alpha_g^{(i)}$ határozatlanoknak homogén formája és így $R_{m+2}(\bar{a})$ minden osztójának is ilyen tulajdonságúnak kell lennie; e szerint $A_1, \ldots$ mind raczionális és egész számok. A feltételezett osztó e szerint az egyetlen x_{m+1} határozatlannak raczionális és egész formája. Ilyen osztót azonban, a mely nem ~ 1-gyel, R_{m+2} nem tartalmazhat, mert ugyanezt az osztót akkor $R_{m+2}(\bar{a})$ is tartalmazná, ha

$$\bar{a}_g^{(i)} = a_g^{(i)}$$

tétetik. Ezt t. i. most *nem* az $x_{m+1}=0$ helyettesítéssel, hanem úgy érjük el, hogy $\bar{a}_g^{(i)}$-ben az $x_{m+1}, x_{m+1}^2, \ldots$ együtthatóiként szereplő határozatlanokat teszszük egyenlővé a

0-sal. De akkor ugyanezt az osztót tartalmazná $[R_{m+2}(\bar{a})]_{x_{m+1}=0}$ is; tehát x_{m+1}-et egyáltalában nem tartalmazhatja és így evvel be van bizonyítva, hogy $(R_{m+2}, \Gamma) \sim 1$.

Ha már most a

$$\Lambda_{m+2} = \text{Res.} \begin{pmatrix} R_{m+2}(\alpha, x_{m+1}), & \Gamma(\alpha, x_{m+1}) \\ x_{m+1} & , \quad 1 \end{pmatrix}$$

formát képezzük, akkor Λ_{m+2} minden esetre a 0-tól különböző és az együtthatók $\alpha_g^{(m+2)}$ sorozatára nézve $\bar{N}_{m+2}$-ed dimensiójú lesz és azonkívül még

$$\Lambda_{m+2} \equiv 0 \,(\text{mod. } \bar{F}_1, \ldots, \bar{F}_{m+2}).$$

Most egymásután az $\bar{F}_1, \ldots, \bar{F}_{m+1}$ formáknak juttatva azt a szerepet, a melyet az eddigi fejtegetésben $\bar{F}_{m+2}$-nek adtunk, *a raczionális és egész formák oly*

$$\Lambda_i(\alpha) \qquad (i=1, \ldots, m+2)$$

sorozata keletkezik, a melyben $\Lambda_i(\alpha)$-nak dimensiója az $\alpha_g^{(i)}$-kre nézve $\bar{N}_i$; továbbá minden egyes Λ_i-re nézve

$$\Lambda_i(\alpha) \equiv 0 \,(\text{mod. } F_1, \ldots, F_{m+2}).$$

Az $\bar{F}_i$ formarendszer resultánsa tehát minden esetre a Λ_i formák egyik közös osztója.

9. §. Megszakítjuk az eddigi gondolatmenetet a következő fontos segédtétel bebizonyításával*:

Ha $\Theta(a)$ nem egyenlő a zérussal és

$$\Theta(a) \equiv 0 \,(\text{mod. } F_1, \ldots, F_{m+1}),$$

akkor $\Theta(a)$-nak az a_{kk} hatványai szerint való kifejtésében:

$$\Theta(a) = \vartheta_0 + \cdots + \vartheta_r a_{kk}^r$$

ϑ_r osztható $R_{ok}^{n_k}$-val, a hol R_{ok} az $(F_k)_{x_k=0}$ kizárásával az

$$(F_1)_{x_k=0}, \ldots, (F_{m+1})_{x_k=0}$$

-ból származó általános formarendszer resultánsa.

* F. Mertens, az i. h.

Akkor ugyanis

$$\theta(a)=\sum_{i=1}^{m+1} H_i F_i$$

és így tehát, ha az $i=k$ kizárásával az $i=1,\ldots,m+1$ értékekre nézve $a_{i,m+1}$ helyébe $a_{i,m+1}-F_i$ jő és ezt a helyettesítést $[\cdots]_k$-val jelöljük, lesz

$$[\vartheta_0]_k+\cdots+[\vartheta_r]_k\, a_{kk}^r=[H_k]_k F_k,$$

vagy pedig, ha ebben a_{kk}^r-nek a két oldalon álló együtthatóit összehasonlítjuk,

$$[\vartheta_r]_k=Kx_k^{n_k}$$

és ebből

$$\vartheta_r=Kx_k^{n_k}+\sum_{i=1}^{m+1}{}^{(k)} L_i F_i,$$

a hol magától értetődik, hogy ϑ_r nem egyenlő zérussal, mert θ a zérustól különböző. Ha az utoljára nyert azonosságban az $x_k=0$-t teszszük, akkor

$$\vartheta_r=\sum_{i=1}^{m+1}{}^{(k)} (L_i)_{x_{k=0}} (F_i)_{x_{k=0}};$$

ϑ_r tehát minden esetre osztható R_{0k}-val.

Ha már most ϑ_r osztható volna $R_{0k}^{n_k-l}$-vel $(l>0)$, de nem volna osztható $R_{0k}^{n_k-l+1}$-vel úgy, hogy

$$\vartheta_r=R_{0k}^{n_k-l}\,\eta_r$$

volna, a hol magától értetődik, hogy η_r ismét az a-knak racionális és egész formája, akkor ebből következnék, hogy

$$[R_{0k}]_k^{n_k-l}\,[\eta_r]_k=Kx_k^{n_k}.$$

Ámde

$$R_{0k}=\sum_{i=1}^{m+1}{}^{(k)} \lambda_i (F_i)_{x_{k=0}},$$

a hol (a 2. §. szerint) λ_i nem egyenlő zérussal és nem tartalmazza a c_{ik} határozatlant (x_k-nak határozatlan együtt-

hatóját F_i-ben), mert ez már az $(F_i)_{x_k=0}$-ból is kiesik. Írhatjuk tehát, hogy

$$R_{0k}=\sum_{i=1}^{m+1}{}^{(k)}\lambda_i\left((F_i)_{x_{k=0}}-F_i\right)+\sum_{i=1}^{m+1}{}^{(k)}\lambda_i F_i$$

és ebből

$$[R_{0k}]_k=\sum_{i=1}^{m+1}{}^{(k)}[\lambda_i]_k\left((F_i)_{x_{k=0}}-F_i\right).$$

Így tehát $(F_i)_{x_{k=0}}-F_i$-vel együtt $[R_{0k}]_k$ is osztható x_k-val; x_k^2-vel ellenben $[R_{0k}]_k$ nem lehet osztható. Ebből ugyanis, hacsak $j\neq k$, következnék, hogy

$$\frac{\partial}{\partial c_{jk}}[R_{0k}]_k=\left[\frac{\partial R_{0k}}{\partial a_{j,m+1}}\right]_k\frac{\partial\left(a_{j,m+1}-F_j\right)}{\partial c_{jk}}=-\left[\frac{\partial R_{0k}}{\partial a_{j,m+1}}\right]_k x_k$$

is osztható x_k^2-vel, tehát $\left[\frac{\partial R_{0k}}{\partial a_{j,m+1}}\right]_k$ osztható x_k-val. E szerint

$$\frac{\partial R_{0k}}{\partial a_{j,m+1}}=K_k' x_k+\sum_{i=1}^{m+1}{}^{(k)}K_i'F_i$$

volna és, ha végre x_k helyébe ismét a 0-t teszszük,

$$\frac{\partial R_{0k}}{\partial a_{j,m+1}}\equiv 0\,(\mathrm{mod.}\,(F_1)_{x_{k=0}},\ldots,(F_{m+1})_{x_{k=0}}),$$

a hol a modulusrendszerben $(F_k)_{x_{k=0}}$ nem fordúl elő; azaz $\frac{\partial R_{0k}}{\partial a_{j,m+1}}$ osztható volna R_{0k}-val, a mi nem lehetséges.

Minthogy tehát $[R_{0k}]_k$ pontosan x_k első hatványával osztható, $[R_{0k}]_k^{n_k-l}$-nek pontosan $x_k^{n_k-l}$-vel kell oszthatónak lennie és így $[\eta_r]_k$ osztható volna x_k^l-vel, η_r pedig R_{0k}-val. E szerint ϑ_r a feltevés ellenére nem csak $R_{0k}^{n_k-l}$-vel, hanem $R_{0k}^{n_k-l+1}$-vel is osztható volna. De ez a következtetés mindaddig ismételhető, míg $l>0$ és így nyerjük a §. elején kimondott tételt.

Ebből közvetetlenűl következtetjük, hogy, *ha az* $F_1,\ldots,F_{m+1}$ *formarendszernek egyálltalában van resultánsa, ennek, mint az* $a_g^{(i)}$ *együtthatók formájának, dimensiója nem lehet alacsonyabb, mint* N_i.

Ez a resultáns ugyanis magában foglalja az $a_{kk}^{r} R_{ok}^{n_k} A$ tagokat, a hol A az a-knak a zérustól különböző formája. Minthogy azonban feltételezzük, hogy a resultánsra vonatkozó tételek $m-1$ határozatlannak m általános formájára már be vannak bizonyítva, $R_{ok}^{n_k}$-nak dimensiója az $a_g^{(i)}$-kre nézve valóban N_i.

10. §. E segédtételek alapján most már a resultáns előállítására szolgáló következő törvényhez jutunk:

Az általános $\bar{F}_i(x_1, \ldots, x_{m+1})\,(i=1, \ldots, m+2)$ *formarendszer resultánsa a* H *és* $\Lambda_i, (i=1, \ldots, m+2)$ *formák legnagyobb közös osztója. A már előbb elintézett elemi* $(m=0)$ *eset kivételével a* Λ *formák alkotására csak az szükséges, hogy előállítsuk* k *határozatlan* $k+1$ *formájának resultánsát, a hol* $k<m+1$.

Az alapvető műveletek tehát, a melyekre végre minden resultáns képezése visszavezethető: Sylvester-féle determinánsok felállítása és bizonyos raczionális és egész formák legnagyobb közös osztójának meghatározása.

A resultáns, a melynek létezését már a 7. §-ban kimutattuk, minden esetre a Λ_i formáknak valamely közös osztója. Minthogy pedig Λ_i az $\bar{F}_i$ forma együtthatóira vonatkozólag $\bar{N}_i$-edfokú, maga a resultáns, R sem lehet ennél magasabb fokú. De — a mint azt már bebizonyítottuk — ennél alacsonyabb fokú sem lehet és ezért, ha

$$\Lambda_i = \Lambda_i' R,$$

a Λ_i' ezeket az együtthatókat már nem tartalmazhatja. A $\Lambda_1', \Lambda_2', \ldots$ mennyiségek legnagyobb közös osztója tehát csak valamely raczionális és egész szám, k lehet. Így tehát

$$(\Lambda_1, \ldots, \Lambda_{m+2}) \sim kR.$$

Minthogy továbbá a 7. §-ban (III) alatt értelmezett H forma minden esetre primitiv forma, azért

$$R \sim (H, \Lambda_1, \ldots, \Lambda_{m+2})$$

AKADÉMIA KÖNYVTÁRA

és evvel a resultáns az előjel mellőzésével meg van határozva.

Minthogy azonban a resultáns okvetetlenül a

$$H(\alpha) = \alpha_{11}^{K_1} \alpha_{22}^{K_2} \dots \alpha_{m+2,\,m+2}^{K_{m+2}} + \cdots$$

formának valamely osztója, annak minden esetre oly tagokat kell tartalmaznia, a melyekben az

$$\alpha_{11}^{k_1} \alpha_{22}^{k_2} \dots \alpha_{m+2,\,m+2}^{k_{m+2}}$$

alakú hatványszorzatok fordúlnak elő és minthogy ez a resultáns az $\alpha_g^{(i)}$-knek $\bar{N}_i$-ed dimensiójú homogén formája, szükségképen $k_i = \bar{N}_i$, azaz csak egy oly tagja lehet, a mely a felállított alakot veszi föl. Ez a tag a következő:

$$\pm \alpha_{11}^{\bar{N}_1} \alpha_{22}^{\bar{N}_2} \dots \alpha_{m+2,\,m+2}^{\bar{N}_{m+2}};$$

mert, ha ennek együtthatója k és nem ± 1 volna, akkor $H(\alpha)$ kiírt tagjának is tartalmaznia kellene a k együtthatót.

Ha már most e tag előjeléül a felsőt választjuk, a resultáns teljesen meg van határozva. Ebben (*a*) és (*b*) mellett megvan az a tulajdonság is, a melyet az 5. §. elején (*c*)-vel jelöltünk és ezekből azután — a mint ott kifejtettük — következnek a (*d*) és (*e*) tulajdonságok is.

A resultáns előjele meg van határozva avval, hogy az $\alpha_{11}^{N_1} \dots \alpha_{m+1,\,m+1}^{N_{m+1}}$ «főtag» előjelét positivnak állapítjuk meg. (Minthogy a teljes inductio segítségével már kimutattuk a resultánsra vonatkozó tételek érvényességét, a tárgyalást ismét az $F_i(x_1, \dots, x_m)$ $(i = 1, \dots, m+1)$ formarendszerre vonatkoztatjuk.) Ha azonban a formákat bármely $F_{i_1}, \dots, F_{i_{m+1}}$ sorrendben írjuk és a határozatlanok sorrendjét is úgy változtatjuk, hogy az $x_{j_1}, \dots, x_{j_m}$ sorrendben következzenek egymásra, a főtag

$$\alpha_{i_1 j_1}^{N_{i_1}} \alpha_{i_2 j_2}^{N_{i_2}} \dots \alpha_{i_m j_m}^{N_{i_m}} \alpha_{i_{m+1} j_{m+1}}^{N_{i_{m+1}}}$$

lesz; és ekkor ennek a tagnak az előjele veendő positivnak. Ha ezt a resultánst R_{ij}-vel jelöljük, akkor minden esetre

$$R_{ij} \equiv 0 \,(\text{mod. } F_1, \ldots, F_{m+1}).$$

Így tehát R_{ij} osztható R-rel és ép úgy R osztható R_{ij}-vel. Az F formák és az x határozatlanok sorrendjének változtatása tehát csak a resultáns előjelének változásával járhat. Az előjel e változásának törvényét meghatározandók, az $a_g^{(i)}$-k bármely speczialis értékeit választhatjuk; csak olyanok zárandók ki, a melyekre nézve a resultáns zérus lesz.

Ha először az

$$F_i = a_{ii} x_i^{n_i} + \cdots + a_{ij} x_j^{n_i} + \cdots$$

formát felcseréljük az

$$F_j = a_{ji} x_i^{n_j} + \cdots + a_{jj} x_j^{n_j} + \cdots$$

formával és azután még x_i-t x_j-vel, akkor a_{ii} átmegy a_{jj}-be, a_{jj} pedig a_{ii}-be; a főtag többi mennyiségei és maga a főtag is változatlanok maradnak. Az x_i és x_j határozatlanok felcserélése tehát csak akkor idéz elő előjelváltozást, ha ugyanaz történik az F_i és F_j formák felcserélésénél.

Könnyen bebizonyítható azután a következő tétel:

Két forma, F_i és F_j felcserélése (és tehát két határozatlan, x_i és x_j felcserélése is) akkor és csak akkor változtatja meg a resultáns előjelét, ha a rendszer összes formáinak dimensiói páratlan számok; azaz

$$\text{Res.} \begin{pmatrix} \cdots F_i, \ldots, F_j \cdots \\ x_1, x_2, \ldots, x_m, 1 \end{pmatrix} = (-1)^N \text{ Res.} \begin{pmatrix} \cdots F_j, \ldots, F_i, \cdots \\ x_1, x_2, \ldots, x_m, 1 \end{pmatrix}$$

és

$$\text{Res.} \begin{pmatrix} F_1, F_2, \ldots, F_{m+1} \\ \ldots, x_i, \ldots, x_j, \ldots, 1 \end{pmatrix} = (-1)^N \text{ Res.} \begin{pmatrix} F_1, F_2, \ldots, F_{m+1} \\ \ldots, x_j, \ldots, x_i, \ldots, 1 \end{pmatrix}.$$

E tétel érvényes az $m=1$ esetben, a mint ezt a SYLVESTER-féle determináns egyszerű megtekintése mutatja. Ez

ugyanis

$$a_{11}^{n_2} a_{22}^{n_1} + \cdots + (-1)^{n_1 n_2} a_{21}^{n_1} a_{12}^{n_2};$$

ha pedig a két forma szerepet cserél, a következőbe megy át:

$$a_{21}^{n_1} a_{12}^{n_2} + \cdots + (-1)^{n_1 n_2} a_{22}^{n_1} a_{11}^{n_2};$$

a tételnek megfelelőleg tehát hozzá lép a $(-1)^{n_1 n_2}$ tényező.

Hogy azt a változást, a melyet az F_i és F_j formák felcserélése a resultánsban előidéz, általánosságban meghatározhassuk, vegyük fel az egyik formát, pl. F_k-t a következő specziális alakban:

$$F_k = a_{kk} x_k^{n_k}.$$

Az $F_1, \ldots, F_{m+1}$ rendszer resultánsa akkor

$$a_{kk}^{N_k} R_{ok}^{n_k},$$

a hol R_{ok} az $(F_1)_{x_k=0}, \ldots, (F_{m+1})_{x_k=0}$ rendszer resultánsa, a melyből ki van zárva $(F_k)_{x_k=0}$. E resultáns ugyanis az $a_g^{(k)}$-knek N_k-ad dimensiójú homogén formája és így tehát F_k-nak felvett specziális alakja mellett csak az $a_{kk}^{N_k}$-val megszorzott része maradhat meg és ez a 9. és 10. §. szerint ilyen alakú.

Ha a bebizonyítandó tételről feltételezzük, hogy $m+1$-nél kevesebb formából álló rendszerekre nézve érvényes, a következtetés m-ről $m+1$-re igazolja majd annak általános érvényességét; mert két forma esetében érvényes. Az F_i és F_j formák felcserélése a most szóban levő resultáns esetében követeli, hogy $(F_i)_{x_k=0}$-t felcseréljük $(F_j)_{x_k=0}$-sal; de akkor R_{ok} átmegy $(-1)^{N_k} R_{ok}$-ba és maga a resultáns a bebizonyítandó tételnek megfelelőleg átmegy a következőbe:

$$(-1)^N a_{kk}^{N_k} R_{ok}^{n_k},$$

a mi bebizonyítandó volt.

A resultánsok szorzástétele.

11. §. Legyen F_i' és F_i'' az $x_1, \ldots, x_m$ határozatlanoknak két általános formája, dimensiójuk pedig n_i' és n_i''; részletesen:

$$F_i' = \sum_{(g)} b_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}, \quad F_i'' = \sum_{(g)} c_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}.$$

Ha az általános $F_1, \ldots, F_{m+1}$ formarendszerben az F_i formát rendre a $F_i' F_i''$, F_i' és F_i'' formákkal helyettesítjük és a megfelelő resultánsokat R, R', R''-nek nevezzük, akkor

$$R = R' R''.$$

Ez a resultánsok szorzástétele.

Hogy e tételt bebizonyíthassuk, gondoljuk meg, hogy

$$R \equiv 0 \,(\text{mod. } F_1, \ldots, F_{i-1}, F_i' F_i'', \ldots)$$

tehát egyszersmind

$$R \equiv 0 \,(\text{mod. } F_1, \ldots, F_{i-1}, F_i', F_{i+1}, \ldots),$$
$$R \equiv 0 \,(\text{mod. } F_1, \ldots, F_{i-1}, F_i'', F_{i+1}, \ldots);$$

és így, minthogy a modulusrendszer «általános» formákból áll, R úgy R'-rel, mint R''-rel is osztható. Ámde R' és R'' irreducibilis és két egymással nem is æquivalens forma, mert mindegyik a határozatlanoknak különböző sorozatait tartalmazza; R tehát osztható $R'R''$-rel is és lesz

$$R = AR'R'',$$

a hol A — mint az az R, R', R'' dimensióiból közvetetlenül látszik — raczionális és egész szám. Ha végre még tekintetbe veszszük, hogy

$$R' = a_{11}^{N_1'} \ldots b_{ii}^{N_i'} \ldots a_{m+1,m+1}^{N_{m+1}'} + \cdots,$$
$$R'' = a_{11}^{N_1''} \ldots c_{ii}^{N_i''} \ldots a_{m+1,m+1}^{N_{m+1}''} + \cdots,$$
$$R = a_{11}^{N_1'+N_2''} \ldots (b_{ii} c_{ii})^{N_i'} \ldots a_{m+1,m+1}^{N_{m+1}'+N_{m+1}''} + \cdots,$$

akkor, minthogy $N_i' = N_i''$, az együtthatók összehasonlításából kitünik, hogy $A = 1$.

E szorzástételt most jelesen arra az esetre alkalmazzuk, midőn az összes F formák általános lineáris formák szorzatai.

Szembetünő, hogy $m+1$ általános lineáris forma:

$$L_i = a_{i1}x_1 + \cdots + a_{im}x_m + a_{i,\,m+1} \qquad (i=1,\ldots,m+1)$$

resultánsa $|a_{ij}|$. Hogy

$$|a_{ij}| \equiv 0 \,(\text{mod. } L_1, \ldots, L_{m+1}),$$

az már a determinánsok elméletének elemeiből ismeretes. E determináns kifejtésében továbbá az $a_{11}, \ldots, a_{m+1,\,m+1}$ főtag az 1 együtthatóval fordúl elő és így végre $|a_{ij}|$ azonosnak bizonyúl a kérdéses resultánssal, ha e determináns a határozatlanok irreducibilis formája.

Hogy $|a_{ij}|$ *az a-knak irreducibilis formája*, a resultánsok elméletétől függetlenül is az $m-1$-ről m-re való következtetés segítségével könnyen bebizonyítható. E determináns — a mint kifejtése mutatja — minden esetre primitiv forma és minden egyes $a_{i1}, a_{i2}, \ldots, a_{im}$ sor lineáris formája. Minden valódi osztója tehát szintén primitiv forma és az a-knak legalább *egy* sorát, pl. $a_{11}, \ldots, a_{1m}$-et *nem* tartalmazza; mert különben a complementáris osztó d' (a melyre nézve $dd' = |a_{ij}|$) egész szám volna, tehát 1-gyel volna egyenlő és d nem lenne valódi osztó. De akkor az

$$|a_{ij}| = \sum_{j=1}^{m} a_{1j} A_{1j}$$

kifejtésében $A_{11}, \ldots, A_{1m}$ szükségképen oszthatók d-vel. Ha $m=2$, tehát $A_{11}=a_{22}$, $A_{12}=-a_{21}$, akkor ezek irreducibilis mennyiségek és így tehát a feltételezett osztó ~ 1. Ha már most feltételezzük, hogy a tétel érvényes $m-1$-re nézve, akkor $A_{11}, \ldots, A_{1m}$, mint olyan $m-1$-edfokú determinánsok, a melyeknek mindegyikében az elemek kivétel nélkül különböző határozatlanok, irreducibilis formák és nem æquivalensek

egymássa ; mert pl. A_{1r} az a_{ir} határozatlant, a mely az összes többi A_{1s}-ekben előfordúl, egyáltalában nem tartalmazza. Az $A_{11}, \ldots, A_{1m}$ mennyiségek legnagyobb közös osztója tehát 1 és így a tétel be van bizonyítva.

Legyen már most *minden egyes* F_i *lineáris formák szorzata*, azaz

$$F_i = \prod_{\mu_i=1}^{n_i} (c_{i1}^{(\mu_i)} x_1 + c_{i2}^{(\mu_i)} x_2 + \cdots + c_{im}^{(\mu_i)} x_m + c_{i,m+1}^{(\mu_i)}),$$

akkor a szorzástételt ismételten alkalmazva származik, hogy

$$\text{Res.}(F_1, \ldots, F_{m+1}) = \prod_{\mu_{m+1}=1}^{n_{m+1}} \cdots \prod_{\mu_1=1}^{n_1} | c_{ij}^{(\mu_i)} |_{(i,j=1,\ldots,m+1)}.$$

Ez a képlet újból mutatja azt a törvényt, a mely szerint a resultáns változik, midőn az F_i és F_j formákat, vagy pedig az x_i és x_j határozatlanokat felcseréljük ; mert ekkor minden egyes determinánsban két oszlop vagy pedig két sor helyet cserél és így a resultánshoz hozzálép a $(-1)^N$ tényező.

Homogén formák rendszerének resultánsa. Invariánstulajdonság.

12. §. Ha az általános

$$F_i(x_1, \ldots, x_m) \qquad (i=1, \ldots, m+1)$$

formarendszerben $a_g^{(i)}$ helyébe $a_g^{(i)} x_{m+1}^{n_i - \Sigma g_j^{(i)}}$ jő, akkor a megfelelő

$$\Phi_i(x_1, \ldots, x_{m+1}) \qquad (i=1, \ldots, m+1)$$

általános homogén formák (II. fej. 8. §.) rendszere származik. Ha továbbá

$$R = \text{Res.} \begin{pmatrix} F_1, F_2, \ldots, F_{m+1} \\ x_1, x_2, \ldots, 1 \end{pmatrix},$$

akkor, minthogy R minden tagjának súlya N, ugyanaz a helyettesítés átvezeti az

$$R=\sum_{i=1}^{m+1} H_i F_i$$

azonosságot a következőbe:

$$Rx_{m+1}^N=\sum_{i=1}^{m+1} H_i \Phi_i.$$

Ha most

$$(\Phi_i(x_1, \ldots, x_{m+1}))_{x_{j-1}}=F_i^{(j)},$$

akkor $F_i^{(j)}$ az x_j kizárásával az x határozatlanoknak ismét általános formája, és e mellett csakis az $a_g^{(i)}$ együtthatóknak bizonyos törvényszerű felcserélése történt. A resultánsra vonatkozó azonosság pedig átmegy a következőbe:

$$Rx_{m+1}^N=\sum_{i=1}^{m+1} H_i^{(j)} F_i^{(j)};$$

és ebből az ismeretes módon (t. i. a KRONECKER-féle helyettesítés révén) következik, hogy

$$R\equiv 0 \,(\text{mod. } F_1^{(j)}, \ldots, F_{m+1}^{(j)}).$$

Ha az $F_i^{(j)}$ rendszernek az x-ek szerint vett resultánsát, a melyekből az x_j ki van zárva, R_j-nek nevezzük, akkor tehát R osztható R_j-vel és minthogy e következtetés — mint azt közvetetlenül látni — meg is fordítható, egyszersmind R_j is osztható R-rel; azaz

$$R_j=\pm R.$$

Kiindulva az $F_i^{(j)}$ formákból, a resultánsra nézve végre még

$$Rx_j^N\equiv 0 \,(\text{mod. } \Phi_1, \ldots, \Phi_{m+1})$$

és ennek megfelelőleg R-t a Φ_i homogén formarendszer resultánsának is nevezzük, vagy ha ezt — tekintettel az előjelre — pontosabban írjuk ki:

$$R = \text{Res.}\begin{pmatrix}\Phi_1, \Phi_2, \ldots, \Phi_{m+1}\\ x_1, x_2, \ldots, x_{m+1}\end{pmatrix}.$$

Még akkor is, ha ebből az értelmezésből indulunk ki, megmaradnak a resultáns alaptulajdonságai, mert *a következő két állítás:*

$$\theta(a)\, x_j^{\nu} \equiv 0 \,(\text{mod. } \Phi_1, \ldots, \Phi_{m+1}),$$
$$\theta(a) \equiv 0 \,(\text{mod. } R),$$

ha különben $\theta(a)$ *az* a*-knak bármely raczionális és egész formája, ugyanazt a tényt fejezi ki.*

Ha $\theta(a)$ osztható R-rel, akkor

$$\theta(a)\, x_j^{N} \equiv 0 \,(\text{mod. } \Phi_1, \ldots, \Phi_{m+1}),$$

míg az első állításból következik, hogy

$$\theta(a) \equiv 0 \,(\text{mod. } F_1^{(j)}, \ldots, F_{m+1}^{(j)});$$

tehát $\theta(a) \equiv 0 \,(\text{mod. } R)$. A mint látni, ν itt oly raczionális és egész szám, a melynek legkisebb értéke meghatározható az adott $\theta(a)$ formából. Jelesen, ha összehasonlítjuk a két oldalon az egyenlő dimensiójú tagokat, kiadódik a

$$\theta(a)\, x_j^{\nu} = \sum_{i=1}^{m+1} H_i \Phi_i$$

specziális előállítás, a hol H_i az x-eknek $\nu - n_i$-ed dimensiójú formája és, ha $\theta(a)$ a zérustól különböző, $\nu \geqq n_i$; mert különben H_i egyenlő volna zérussal és akkor $\theta(a)$-nak is el kellene tünnie. Ez a következtetés még azt is mutatja, hogy a

$$\theta(a)\, x_j^{\nu} \equiv 0 \,(\text{mod. } \Phi_1, \ldots, \Phi_{m+1})$$

congruentiából mindig következik, hogy

$$\theta(a)\, x_r^{\nu_r} \equiv 0 \,(\text{mod. } \Phi_1, \ldots, \Phi_{m+1}). \quad (r=1, \ldots, m+1)$$

Tegyük most fel, hogy az $m+1$ homogén forma:

$$\Phi_i(x_1, \ldots, x_{m+1}), \qquad (i=1, \ldots, m+1)$$

ha ezekre a határozatlan együtthatókat tartalmazó

$$x_j = \sum_{k=1}^{m+1} u_{jk}\, \bar{x}_k$$

(homogén) lineáris transformatiót alkalmazzuk, átmegy a következőbe :

$$\bar{\Phi}_i(\bar{x}_1, \ldots, \bar{x}_{m+1}) = \sum_{(g)} \bar{a}_g^{(i)} \bar{x}_1^{g_1^{(i)}} \bar{x}_2^{g_2^{(i)}} \ldots \bar{x}_{m+1}^{g_{m+1}^{(i)}}, \quad (i=1, \ldots, m+1)$$

a hol e szerint az $\bar{a}_g^{(i)}$-k az $a_g^{(i)}$ és u_{jk} határozatlanoknak raczionális és egész formái ; továbbá legyen

$$\bar{R} = \text{Res.} \begin{pmatrix} \bar{\Phi}_1, \bar{\Phi}_2, \ldots, \bar{\Phi}_{m+1} \\ \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{m+1} \end{pmatrix}.$$

Ha az ennek megfelelő

$$\bar{R}\bar{x}_{m+1}^N = \Sigma H_i \bar{\Phi}_i$$

azonosságra az invers

$$U\bar{x}_k = \sum_{j=1}^{m+1} U_{jk} x_j, \quad U = |u_{ij}|$$

transformátiót alkalmazzuk, akkor, minthogy a H_i-kben mint nevező csak az U-nak hatványa lép fel, a nevezőt eltávolítva, lesz

$$\bar{R}G \equiv 0 \,(\text{mod. } \Phi_1, \ldots, \Phi_{m+1}),$$

hol G az a-któl ment homogén formát jelent. Végre még x_m helyébe 1-et téve, a KRONECKER-féle helyettesítésnél $\bar{R}$ eltünik; $\bar{R}$ tehát osztható R-rel. Ámde $\bar{a}_g^{(i)}$ az $a_g^{(i)}$-knek homogén lineáris formája úgy, hogy $\bar{R}$ és R homogének és az $a_g^{(i)}$-kre vonatkozólag egyenlő dimensiójúak. Így tehát

$$\bar{R} = RV,$$

a hol V az u_{ij}-knek oly raczionális és egész formája, a melynek meghatározására elég, ha az $a_g^{(i)}$-k valamely speciális értékrendszerét használjuk. Minthogy lineáris formák rendszerének resultánsára nézve $V = U$, az általános esetben (úgy mint a 11. §-ban) F_i számára lineáris formák szorzatát választhatjuk és akkor az ottani előállításból a következő általánosságban is érvényes képlet származik :

$$\bar{R} = R\,|u_{ij}|^N,$$

a mely *a resultánsnak ú. n. invariáns-tulajdonságát* fejezi ki.

Homogén egyenletek rendszere.

13. §. A resultánsnak az

$$R \equiv 0 \,(\text{mod. } F_1^{(j)}, \ldots, F_{m+1}^{(j)})$$

congruentiában kifejezett tulajdonsága közvetetlenül mutatja, hogy az $a_g^{(i)}$ mennyiségeket változóknak tekintve, *a resultáns eltünik, mihelyt az* $a_g^{(i)}$ *mennyiségeknek oly értékeket tulajdonítunk, a melyekre nézve az*

$$F_1^{(j)}=0, \quad F_2^{(j)}=0, \ldots \qquad (j=1, \ldots, m+1)$$

egyenletrendszerek közül legalább egynek van megoldása. Hogy azonban a resultáns *csakis* ebben az esetben lesz zérus, az az egyenletrendszerek elméletének alapvető tétele, a melylyel majd most foglalkozunk.

Azt az $m+1$ egyenletrendszert, a mely m ismeretlent tartalmazó bármely k ily $F_i^{(j)}=0$ egyenletből áll, igen egyszerű és a geometriai interpretatio szempontjából fontos módon a

$$\Phi_i(x_1, \ldots, x_{m+1})=0 \qquad (i=1, \ldots, k)$$

rendszer vizsgálatában foglalhatjuk össze, a mely tehát k *homogén*, $m+1$ *ismeretlent tartalmazó egyenletből áll. Azt a megoldást, a melyben az összes ismeretlenek a* 0 *értéket veszik fel* és a mely az együtthatók értékétől függetlenül mindig fellép, *egyszersmindenkorra kizárjuk.*

Ha már most $\xi_1, \ldots, \xi_{m+1}$ nem ilyen gyökrendszer, akkor, ha λ egészen tetszés szerinti mennyiséget jelent, $\lambda\xi_1, \ldots, \lambda\xi_{m+1}$ is a $\Phi_i=0$ egyenletrendszernek gyökrendszere. Ezeket a gyökrendszereket, mint *valódi megoldást* a következőben akarjuk összefoglalni:

$$x_1 : x_2 : \ldots : x_{m+1} = \xi_1 : \xi_2 : \ldots : \xi_{m+1}$$

és valamely második, $\eta_1, \ldots, \eta_{m+1}$ megoldás *ettől nem különbözőnek* tekintendő, ha

$$\xi_1 : \xi_2 : \ldots : \xi_{m+1} = \eta_1 : \eta_2 : \ldots : \eta_{m+1}.$$

Minthogy a ξ mennyiségek közül legalább egy, pl. ξ_j

a 0-tól különböző, mindig van egy és csak egy oly λ_j érték, a melyre nézve $\lambda_j \xi_j = 1$ és ekkor $x_r = \lambda_j \xi_r$ az $F_i^{(j)} = 0$ egyenleteknek egyik gyökrendszere. Viszont $F_i^{(j)} = 0$ minden gyökrendszere a $\Phi_i = 0$ egy olyan megoldását szolgáltatja, a melyben $\xi_j = 1$.

A $\Phi_i = 0$-nak ama megoldásairól, a melyekben $\xi_j = 0$, egyszerű geometriai okokból azt szoktuk mondani, hogy $F_i^{(j)} = 0$-*nak «a végtelenben fekvő» megoldásai.* Ez a megoldás fogalmának olyan bővítése, a melylyel az $F_i = 0$ rendszer elméletében a kivételes eseteket megszüntetjük; ez már az elemekben is megtörténik, midőn pl. két egyenesnek a «végtelenben fekvő» metszéspontját stb. ily módon értelmezzük. (Collineatio.)

A bebizonyítandó tétel most már a következő egyszerű alakban mondható ki:

A $\Phi_i(x_1, \ldots, x_{m+1})$ $(i = 1, \ldots, m+1)$ *rendszer resultánsa akkor és csak akkor tünik el, ha a* $\Phi_i = 0$ *egyenletrendszernek van valódi megoldása.*

Hogy akkor, midőn amaz egyenletrendszernek van valódi megoldása, a resultáns zérussal egyenlő, az az

$$Rx_j^N = \sum_{i=1}^{m+1} H_i^{(j)} \Phi_i$$

azonosságokból tünik ki; tehát ennek a tételnek csakis megfordítását kell fejtegetnünk.

Mindenekelőtt megjegyezzük, hogy az egyes Φ_i formákkal együtt természetesen azok dimensiója, n_i is meg van adva; hogy azonban e formák szabályosak legyenek, most már nem szükséges, mert az $a_g^{(i)}$-ket speciális értékeknek vettük fel. Ezért ismét az

$$x_j = \sum_{k=1}^{m+1} u_{jk} \bar{x}_k$$

általános (homogén) lineáris transformatiót alkalmazzuk, a

mely a Φ_i formákat a szabályos $\bar{\Phi}_i$ formákba vezeti át; az R resultáns ekkor átmegy $\bar{R}=RU^N$-be. A $\Phi_i=0$ bármely «valódi» megoldásának megfelel a $\bar{\Phi}_i=0$ «valódi» megoldása és viszont; R és $\bar{R}$ csak egyidejűleg lehetnek egyenlők a zérussal. A tétel tehát csak a transformált rendszerre vonatkozólag lesz bebizonyítandó.

Ha csupa új határozatlan együtthatóval az $\bar{x}$-eknek

$$V_1, \ldots, V_{m+1} \quad \text{és} \quad W_1, \ldots, W_{m+1}$$

homogén formáit alkotjuk, a melyeknek dimensiói legyenek

$$n-n_1, \ldots, n-n_{m+1},$$

a hol n bármely oly pozitiv egész számot jelenthet, a melyre nézve $n-n_i \geqq 0$ $(i=1, \ldots, m+1)$, akkor

$$\sum_{i=1}^{m+1} V_i \bar{\Phi}_i \quad \text{és} \quad \sum_{i=1}^{m+1} W_i \bar{\Phi}_i$$

az $\bar{x}$-eknek n-ed dimensiójú homogén formái és a

$$\sum_{i=1}^{m+1} V_i \bar{\Phi}_i = 0, \quad \sum_{i=1}^{m+1} W_i \bar{\Phi}_i = 0$$

egyenleteknek akkor és csak akkor lesz valódi megoldásuk, ha ugyanilyen van a $\bar{\Phi}_i=0$ egyenleteknek is. Ha már most a

$$\text{Res.} \begin{pmatrix} \sum_{i=1}^{m+1} V_i \bar{\Phi}_i, & \sum_{i=1}^{m+1} W_i \bar{\Phi}_i \\ \bar{x}_1 \quad , & 1 \end{pmatrix}$$

resultánst képezzük, akkor annak szükséges és elegendő feltételét, hogy a $\bar{\Phi}_i=0$-nak valódi megoldása legyen, úgy fejezhetjük ki, hogy legyen egy olyan nem csupa zérusból álló $\bar{\xi}_2, \ldots, \bar{\xi}_{m+1}$ értékrendszer, a melyre nézve ama resultáns egyenlő a zérussal. Ezekhez az értékekhez (minthogy a formák, a melyeknek resultánsát képezzük, szabályosak) minden esetre hozzácsatolható oly $\bar{\xi}_1$ érték, a melyre nézve

$$\bar{\Phi}_i(\bar{\xi}_1, \ldots, \bar{\xi}_{m+1})=0;$$

ha azonban $\bar{\xi}_i=0\,(i=2,\ldots,m+1)$, akkor a felhozott okból szükségképen egyszersmind $\bar{\xi}_1=0$.

Ha ama resultánst a V_i-kben és W_i-kben fellépő határozatlanoknak hatványszorzatai szerint rendezzük és az együtthatókat $\bar{\Phi}'_{i_1}$-gyel $(i_1=1,\ldots,k_1)$ jelöljük, akkor ama feltételt végre úgy fejezhetjük ki, hogy a

$$\bar{\Phi}'_{i_1}(\bar{x}_2,\ldots,\bar{x}_{m+1})=0 \qquad (i_1=1,\ldots,k_1)$$

homogén egyenletrendszernek legyen valódi megoldása. Itt képezésük szerint a $\bar{\Phi}'_{i_1}$-eknek még az a tulajdonságuk is lesz, hogy

$$\bar{\Phi}'_{i_1}\equiv 0\,(\text{mod. }\bar{\Phi}_1,\ldots,\bar{\Phi}_{m+1}),$$

a mint az a resultánsnak megfelelő tulajdonságából közvetetlenül következik, ha az egyes hatványszorzatok mellett álló együtthatókat összehasonlítjuk.

E következtetések pontos ismétlésével végre arra jutunk, hogy ama szükséges és elegendő feltétel úgy fejezhető ki, hogy a

$$\bar{\Phi}^{(m)}_{i_m}(\bar{x}_{m+1})=0 \qquad (i_m=1,\ldots,k_m)$$

homogén egyenletrendszernek, a hol

$$\bar{\Phi}^{(m)}_{i_m}\equiv 0\,(\text{mod. }\bar{\Phi}_1,\ldots,\bar{\Phi}_{m+1}),$$

legyen valódi megoldása. Hogy e következtetések érvényesek legyenek, csak az szükséges, hogy a $\bar{\Phi}^{(k)}_{i_k}$ formarendszer csupa szabályos formából álljon. Ezt azonban már az első ízben a $\bar{\Phi}_i$ formákra alkalmazott általános lineáris transformatio biztosítja. Ha nem ez az eset forogna fenn, akkor bizonyos lineáris transformatio alkalmazása vezetne szabályos formákra; de a czélt, a melyre evvel törekszünk, már el kellett érnünk amaz általános transformatiónak alkalmazásával, mert ez mint specziális esetet a két lineáris transformatiónak amaz egymásutánját is magában foglalja.

Ámde, mint egy határozatlannak homogén formája,

$$\bar{\Phi}_{i_m}^{(m)} = \varphi_{i_m}^{(m)} \bar{x}_{m+1}^{\nu_{i_m}};$$

a $\bar{\Phi}_i = 0$-nak tehát akkor és csak akkor van valódi megoldása, ha a $\varphi_{i_m}^{(m)}$ formák, a melyek az u_{ij} határozatlanoknak formái, mind egyenlők a zérussal és e mellett még

$$\varphi_{i_m}^{(m)} \bar{x}_{m+1}^{\nu_{i_m}} \equiv 0 \,(\text{mod. } \bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}).$$

Hogy a $\varphi_{i_m}^{(m)}$ mennyiségek szerkezetét pontosabban megállapíthassuk, az $a_g^{(i)}$ mennyiségeket határozatlanoknak fogva fel, a műveleteknek ugyanazt a sorát újból alkalmazzuk a $\bar{\Phi}_i$ formákra. Minthogy az $a_g^{(i)}$-k ama specziális értékeire nézve e formák szabályosak, és homogén voltuk mellett dimensiójuk sem száll alább, az előbbi formákat úgy nyerjük, hogy az általános $\bar{\Phi}_{i_m}^{(m)}$ formákba behelyettesítjük az $a_g^{(i)}$-k értékeit. E végkövetkeztetés csak azt az esetet nem foglalja magában, midőn amaz értékek behelyettesítése következtében valamely $\bar{\Phi}_{i_k}^{(k)}$ forma azonosan zérus lesz; de — mint közvetetlenül belátható — még ebben az esetben is ama specziális formák az általánosaknak képezett formákból származnak; csakhogy ekkor fellép köztük még a formáknak egy további sorozata, a mely az $a_g^{(i)}$-k ama specziális választása mellett elvész.

Annak szükséges és elegendő feltételét tehát, hogy a tetszés szerinti $\bar{\Phi}_i = 0$ egyenletrendszernek legyen valódi megoldása, a

$$\varphi_{i_m}^{(m)} = 0 \qquad (i_m = 1, \ldots, k_m)$$

alakban nyerjük, a hol a $\varphi_{i_m}^{(m)}$-ek az $a_g^{(i)}$-knek és u_{ij}-knek formái; ezeknek tehát az $a_g^{(i)}$-knek tekintetbe jövő specziális értékeire nézve el kell tünniök.

E mellett azonban a $\varphi_{i_m}^{(m)}$-eknek, mint az $a_g^{(i)}$ határo-

zatlanok formáinak az a tulajdonságuk is megvan, hogy

$$\varphi_{i_m}^{(m)} \bar{x}_{m+1}^{\nu_m} \equiv 0 \,(\text{mod. } \bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}),$$

a hol a felírt modulusrendszerben a $\bar{\Phi}_i$-k ismét az általános formákat jelentik, a melyekben az $a_g^{(i)}$-k határozatlanok. Ebből azonban úgy, mint előbb következik, hogy minden egyes $\varphi_{i_m}^{(m)}$ forma oszthatò az általános $\bar{\Phi}_i$ formák $\bar{R}$ resultánsával. Ha tehát $R=0$, akkor egyszersmind minden egyes $\varphi_{i_m}^{(m)}$ is eltünik és így az egyenletrendszernek van valódi megoldása. Evvel pedig a kimondott tétel be van bizonyítva.

Határozott és határozatlan közönséges rendszerek.

14. §. Most közelebbről megvizsgáljuk az olyan m homogén egyenletből álló

$$\Phi_i(x_1, \ldots, x_{m+1}) = 0 \qquad (i=1, \ldots, m)$$

rendszereket, a melyek $m+1$ ismeretlent tartalmaznak. Ezeknek elmélete az előbbiek szerint egybeesik oly m, nem kivétel nélkül homogén $F_i(x_1, \ldots, x_m) = 0$ egyenletével, a mely m ismeretlent tartalmaz. Ilyen rendszereket — a nélkül, hogy erre az elnevezésre súlyt helyeznénk — «közönségeseknek» nevezünk, szemben azokkal, a melyekben az egyenletek száma kisebb, vagy nagyobb m-nél.

A legfontosabb kérdés itt a különböző megoldások számára vonatkozik. Ha ez véges, a rendszert *határozottnak*, az ellenkező esetben pedig *határozatlannak* mondjuk. Az az eset, hogy a valódi megoldások teljesen hiányzanak — mint az majd kitünik — egyáltalában nem fordúlhat elő.

Ha a különböző valódi megoldások száma véges, pl. n, akkor — mint közvetetlenül világos — az

$$x_j = \sum_{k=1}^{m+1} u_{jk} \bar{x}_k$$

általános lineáris transformatio alkalmazása révén származó

$$\bar{\Phi}_i(\bar{x}_1, \ldots, \bar{x}_{m+1}) = 0$$

rendszernek is n megoldása lesz; és ezek közül egyikben sem lesz $\bar{x}_k$ zérussal egyenlő; mert ez az

$$U\bar{x}_k = \sum_{j=1}^{m} U_{jk} x_j$$

miatt csak akkor volna lehetséges, ha $\sum_{j=1}^{m+1} U_{jk} x_j$ oly értékrendszerre nézve, a melyet valamely megoldás szolgáltat, egyenlő zérussal. Legyen már most az n különböző megoldás:

$$\xi_{1r}, \xi_{2r}, \ldots, \xi_{m+1,r}, \qquad (r=1, \ldots, n)$$

a hol az összes mennyiségek, a melyek ugyanabban a sorban állanak, nem lehetnek egyidejűleg a zérussal egyenlők; akkor meghatározhatjuk a mennyiségeknek akárhány sorozatát (még olyanokat is, a melyek csupa raczionális számból állanak), a melyre nézve sem

$$\sum_{j=1}^{m+1} a_{jk} \xi_{jr}, \qquad (r=1, \ldots, n;\ k=1, \ldots, m+1)$$

sem pedig az $|a_{jk}|_{(j,\,k=1,\ldots,m+1)}$ determináns nem tünik el.

Az

$$|a_{jk}| \bar{\xi}_{kr} = \sum_{j=1}^{m+1} a_{jk} \xi_{jr} \qquad (k=1, \ldots, m+1)$$

egyenletek

$$\xi_{jr} = \sum_{k=1}^{m+1} b_{jk} \bar{\xi}_{kr}$$

megoldásaiból bizonyos b_{jk} mennyiségeket kapunk, (a melyek az a_{jk}-kkal egyidejűleg raczionális számok és) a melyek oly tulajdonságúak, hogy, midőn $u_{jk} = b_{jk}$ tétetik, $\sum_{j=1}^{m+1} U_{jk} x_j$ átmegy $\sum_{j=1}^{m+1} a_{jk} x_j$-be. Így tehát egyetlen

$$U\bar{\xi}_{kr} = \sum_{i=1}^{m+1} U_{jk} \xi_{jr} \qquad (k=1, \ldots, m+1;\ r=1, \ldots, n)$$

mennyiség sem lesz egyenlő zérussal, mert ez már akkor

sem történik, midőn az u_{jk} határozatlanok helyébe a b_{jk} mennyiségeket teszszük.

A transformált $\bar{\Phi}_i=0$ rendszernek tehát nincsen olyan valódi megoldása, a melyben valamelyik $\bar{x}_k$ a 0 értéket veszi fel és ebből közvetetlenül következik, hogy a

$$(\bar{\Phi}_i)_{\bar{x}_{m+1}=0}=0 \qquad (i=1,\ldots,m)$$

rendszernek egyáltalában nincsen valódi megoldása (feltéve természetesen azt, hogy az adott rendszernek csak véges számú valódi megoldása van). E tényből végre (a 13. §-ban bebizonyított tétel szerint) az is következik, hogy ebben az esetben

$$\bar{R}_{m+1}(u) = \text{Res.}\begin{pmatrix}(\bar{\Phi}_1)_{\bar{x}_{m+1}=0}, \ldots, (\Phi_m)_{\bar{x}_{m+1}=0} \\ \bar{x}_1 \quad , \ldots, \quad \bar{x}_m\end{pmatrix}$$

szükségképen a zérustól különböző.

Ha pedig a különböző valódi megoldások száma végtelen, akkor mindig van végtelen sok különböző valódi megoldás, melyben $\bar{x}_{m+1}$ nem egyenlő zérussal; a $\bar{\Phi}_i=0$ ezen különböző valódi megoldásainak mindig a $(\bar{\Phi}_i)_{\bar{x}_{m+1}=1}=0$ különböző valódi megoldásai felelnek meg. A $(\bar{\Phi}_i)_{\bar{x}_{m+1}=1}$ legmagasabb dimensiójú tagjai egyszerűen a $(\bar{\Phi}_i)_{\bar{x}_{m+1}=0}$-nak tagjai.

Ha már most a

$$-\bar{x}_j+z, \quad (\bar{\Phi}_i)_{\bar{x}_{m+1}=1} \qquad (i=1,\ldots,m)$$

formarendszer resultánsát képezzük, akkor ennek alaptulajdonságaiból következik, hogy kifejtése a z hatványai szerint a következő:

$$\bar{R}_{m+1}\, z^N+\cdots,$$

a hol $N=n_1 \ldots n_m$ és

$$\bar{R}_{m+1}\, z^N+\cdots\equiv 0\,(\text{mod. } z-\bar{x}_j, (\bar{\Phi}_1)_{\bar{x}_{m+1}=1}, \ldots, (\bar{\Phi}_m)_{\bar{x}_{m+1}=1}).$$

Ha tehát $\bar{\xi}_1, \ldots, \bar{\xi}_m$ a $(\bar{\Phi}_i)_{x_{m+1}=1}=0$ rendszer megoldása és a modulusrendszerben továbbá a következőket helyettesítjük:

$$\bar{x}_j=\bar{\xi}_j, \quad z=\bar{\xi}_j,$$

akkor

$$\bar{R}_{m+1}\bar{\xi}_j^N+\cdots=0$$

és így, ha $\bar{R}_{m+1}$ nem egyenlő a zérussal, $\bar{\xi}_j$ legfölebb N különböző értéket vehet fel.

Evvel tehát a következő tételt nyertük:

A rendszernek véges számú, vagy pedig végtelen sok különböző valódi megoldása van a szerint, a mint az $\bar{R}_{m+1}(u)$ *forma a zérustól különböző, vagy pedig egyenlő zérussal.*

E tételt mindjárt abban a pontosabb fogalmazásban kell értenünk, hogy ama véges szám sohasem zérus, azaz, hogy a rendszernek legalább is egy valódi megoldása van, a mint az majd közvetetlenül kitünik ama rendszereknek most kifejtendő elméletéből, a melyekre nézve $\bar{R}_{m+1}(u)$ nem egyenlő a zérussal.

Megjegyezzük még, hogy $m+1$ ismeretlent tartalmazó m homogén egyenletnek «általánosságban» véges számú különböző valódi megoldása van. Ha ugyanis $\bar{R}_{m+1}(u)$-t részletesen írjuk:

$$\bar{R}_{m+1}(u)=A_0U_0+A_1U_1+\cdots,$$

a hol az U_k-k az u_{jk}-knak hatványszorzatait jelentik és az A-k az $a_g^{(i)}$-knek raczionális és egész formái, akkor az csak abban az esetben nem fog bekövetkezni, ha az $a_g^{(i)}$ együtthatók kielégítik az

$$A_0=0,\quad A_1=0,\ldots$$

egyenleteket *.

15. §. A megelőző §-ban a $\Phi_i(x_1,\ldots,x_{m+1})=0\,(i=1,\ldots,m)$ homogén rendszerre vonatkozólag történt megállapítások közvetetlenül átvihetők az

* Könnyen követhető az az analogia, a mely az előbbi és a jelen fejezet fejtegetései közt fennáll. E mellett azonban figyelnünk kell arra az elvi ellentétre is, hogy ott az egyenletek számát nem korlátozta az ismeretlenek száma, míg másrészt itt a tárgyalandó probléma a «végtelenben» fekvő gyökök hozzácsatolásával ismét más irányban bővült.

$$F_i(x_1, \ldots, x_m) = 0 \qquad (i = 1, \ldots, m)$$

rendszerre.

Ezt a «közönséges» nem homogén rendszert (melyben az ismeretlenek száma megegyezik az egyenletek számával) szintén *határozott*nak, ill. *határozatlan*nak akarjuk nevezni, a mint a különböző valódi megoldások (gyökrendszerek és a végtelenben fekvő megoldások) száma véges, ill. végtelen.

Annak szükséges és elegendő föltétele, hogy ily közönséges rendszer határozott legyen, az előbbiek szerint már ismeretes. Czélszerű és kívánatos azonban a kérdéstétel újból való oly tárgyalása, melynél a megfelelő Φ_i formák általános lineáris transformatioját (azaz geometriailag beszélve, a collineatio elvét) nem használjuk; különben úgy mint előbb csak a resultánsok elméletére támaszkodva, és nem az eliminácziò általános elméletére.

E czélból az $F_i(x_1, \ldots, x_m) = 0$ rendszerhez még hozzácsatoljuk a további

$$-\sum_{j=1}^{m} t_j x_j + z = 0$$

formát, és e formarendszer resultánsát,

$$\text{Res.} \begin{pmatrix} F_1, \ldots, F_m, & z - t_j x_j \\ x_1, \ldots, x_m, & 1 \end{pmatrix}$$

-t az F_i rendszer ($z = \sum_{j=1}^{m} t_j x_j$-re vonatkozó) *eliminánsá*nak nevezzük. Ez részletesen kiírva:

$$E(z; t_1, \ldots, t_m) = R_{m+1} z^N + R'_{m+1} z^{N-1} + \cdots$$

a hol, ha φ_i az F_i legmagasabb (n_i-dik) dimensiójú tagjainak complexusa, a mely mint ilyen homogén forma,

$$R_{m+1} = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix},$$

míg R'_{m+1} stb. a t határozatlanokat is tartalmazhatják.

Ekkor áll a következő tétel:

Az $F_i(x_1, \ldots, x_m)=0$ $(i=1, \ldots, m)$ *rendszer határozott, ill. határozatlan, a mint az* $E(z; t_1, \ldots, t_m)$ *eliminánsnak nevezett forma a* 0*-tól különböző, vagy pedig azonosan zérus.*

Ha ugyanis a $\xi_1, \ldots, \xi_m$ az $F_i=0$ gyökrendszere és a $z, t_1, \ldots, t_m$ bármely mennyiségek, melyek a

$$z-\Sigma t_j \xi_j=0$$

egyenletnek megfelelnek, akkor az E forma — resultáns értelménél fogva — a $z, t_1, \ldots, t_m$ minden ily értékrendszerének helyettesítésénél zérus lesz. Ebből pedig az V. fejezet 7. §-ában használt módszerek szerint, vagy egyszerűbben a jegyzetben adott segédtétel* alapján következik, hogy E osztható $z-\Sigma t_j \xi_j$-vel.

* Az általános eliminációz-elméletnek a szövegben idézett fejtegetéseit (nemcsak ezen a helyen, hanem a később gyakrabban alkalmazandó analog következtetések alkalmával is) a következő egyszerű segédtétel teljesen pótolja.

Legyen $P(z_1, z_2, \ldots)$ *valamely az orthoid* (A) *tartományból származó irreducibilis forma, továbbá tünjék el a* 0*-tól különböző* $\Phi(z_1, z_2, \ldots)$ *forma minden egyes az* {A}*-ból vett oly* $\zeta_1, \zeta_2, \ldots$ *értékrendszerre nézve, a melyre nézve* $P(\zeta_1, \zeta_2, \ldots)=0$; *akkor* Φ *szükségképen osztható* P*-vel.*

A határozatlanok közül valamelyiknek, pl. z_1-nek okvetetlenül elő kell fordúlnia Φ-ben *és* P-ben, mert különben közvetetlenül képezhetünk olyan $\zeta_1, \zeta_2, \ldots$ értékrendszert, a melyre nézve P a zérussal egyenlő és Φ nem tünik el. De akkor, ha Φ nem osztható P-vel, a Φ és P formák z_1 szerint vett resultánsának, a melyet Z-vel jelölünk, a zérustól különbözőnek kell lennie és így

$$Z=Z_1\Phi+Z_2 P.$$

Most már $z_2, z_3, \ldots$ oly értékeit választhatjuk, hogy Z és a z_1 legmagasabb hatványának együtthatója P-ben a zérustól különböző legyen. Ezeknek a $\zeta_2, \zeta_3, \ldots$ értékeknek azonban minden esetre megfelel olyan $z_1=\zeta_1$ érték, a melyre nézve $P=0$; erre az értékrendszerre nézve azután $Z_1\Phi=Z$ és így a feltevés ellenére $Z_1\Phi$, tehát Φ is a zérustól különböző volna.

Ép úgy, ha $x_1 : \ldots : x_m = \eta_1 : \ldots : \eta_m$ az $F_i = 0$ rendszernek egyik a végtelenben fekvő megoldása és $t_1, \ldots, t_m$ bármely oly mennyiségek, melyek a

$$\Sigma t_j \eta_j = 0$$

egyenletnek megfelelnek, akkor az E forma — ismét resultáns értelménél fogva — a $t_1, \ldots, t_m$ minden ily értékrendszer helyettesítésénél 0 lesz, tehát E ismét osztható $\Sigma t_j \eta_j$-vel.

Tehát az $F_i = 0$ rendszer különböző megoldásainak az E forma különböző, nem is æquivalens lineáris tényezői felelnek meg. De az E-nek, ha nem zérus, csak véges számú különböző lineáris tényezője lehet, és így határozatlan rendszer esetében az elimináns azonosan eltünik.

Ha pedig az $F_i = 0$ rendszer határozott, és e szerint úgy gyökrendszereinek, mint a végtelenben fekvő megoldásainak száma véges, legyenek e gyökrendszerek, a mennyiben ilyenek vannak:

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk}, \qquad (k = 1, \ldots, \mu)$$

a végtelenben fekvő összes különböző megoldások pedig szintén, a mennyiben ilyenek vannak:

$$x_1 : \ldots : x_m = \eta_{1l} : \eta_{2l} : \ldots : \eta_{ml}. \qquad (l = \mu+1, \ldots, \nu)$$

Ha már most képezzük a

$$z - \sum_{j=1}^{m} t_j \xi_{jk}, \quad \sum_{j=1}^{m} t_j \eta_{jl} \qquad (k = 1, \ldots, \mu;\ l = \mu+1, \ldots, \nu)$$

formákat, akkor van minden esetre oly $\zeta, \tau_1, \ldots, \tau_m$ értékrendszer, melynek a $z, t_1, \ldots, t_m$ helyébe való helyettesítésénél e formák egyike sem ád zérust. E szerint az

$$F_i = 0, \quad \zeta - \sum_{j=1}^{m} t_j x_j = 0$$

rendszernek nincs megoldása, és $E(\zeta, \tau_1, \ldots, \tau_m)$ nem zérus; tehát az E forma sem lehet azonosan zérus, a mivel előbb kimondott tételünk teljes igazolást nyert.

Határozott rendszer esetében e meggondolások alapján az elimináns alakja még tovább részletezhető.

Ha ugyanis azon kitevőket, melyekkel az előbb megállapított lineáris tényezők az eliminánsban tényleg előfordúlnak c_k ill. c_l-lel jelöljük, az elimináns lesz

$$E(z; t_1, \ldots, t_m) = Q \prod_{k=1}^{\mu} (z - \sum_{j=1}^{m} \xi_{jk} t_j)^{c_k} \prod_{l=\mu+1}^{\nu} (\sum_{j=1}^{m} \eta_{jl} t_j)^{c_l}$$

és Q (mely a rendszer határozott volta miatt minden esetre 0-tól különböző) a z és t-ktől független együttható.

Ha ugyanis Q a $z, t_1, \ldots, t_m$ igazi formája, van egy irreducibilis tényezője P, mely szintén ilyen. Ha már most minden $z, t_1, \ldots, t_m$ értékrendszernél, melyre nézve P eltünik, ama lineáris tényezők egyike legalább 0 volna, e lineáris tényezők szorzata P-vel osztható volna, a mi a c_k és c_l megállapítása folytán pedig nem lehetséges. Van tehát oly $\zeta, \tau_1, \ldots, \tau_m$ értékrendszer, melynek helyettesítésénél Q zérus lesz, az utána álló lineáris tényezők pedig a 0-tól különbözők. Volna tehát az

$$F_i = 0, \quad -\sum_{j=1}^{m} \tau_j x_j + \zeta = 0$$

rendszernek egy oly megoldása, mely a Q egy új lineáris tényezőjét adná. Ez pedig lehetetlen, ha a megoldások fölsorolása már teljes volt.

Határozott $F_i = 0$ rendszer esetében végre tehát akkor és csak akkor van gyökrendszer, ha az elimináns a z-t valóban tartalmazza *.

E gyökrendszerek meghatározását ebben az esetben

* Hogy a gyökrendszerek száma lehet véges és a 0-tól különböző, midőn az elimináns 0, azt már igen egyszerű példák is mutatják; pl. a következő:

$$x_1 = 0, \quad x_2(x_1 + 1) = 0, \quad x_3(x_1 + 1) = 0.$$

igen egyszerű módon visszavezethetjük az egy ismeretlent tartalmazó egyenletek tárgyalására.

Ha meghatározzuk E és $\frac{\partial E}{\partial z}$ legnagyobb közös osztóát és ezt az E-ből eltávolítjuk, a következőt nyerjük:

$$\varrho(z; t_1, \ldots, t_m) = A \prod_{k=1}^{\mu} (z - \Sigma t_j \xi_{jk})$$

és így tehát ϱ discriminánsa a t-knek a zérustól különböző formája. (Könnyű látni, hogy A a t-ktől független). Meghatározhatjuk továbbá a $t_s = a_s$ mennyiségeket oly módon, hogy az a_s-ek pl. raczionális és egész számok és Dscr. $\varrho(z; a_1, \ldots, a_m)$ a zérustól különböző.

Minthogy azonban

$$[\varrho(z; t_1, \ldots, t_m)]_{z=\sum_{j=1}^{m} t_j \xi_{jk}},$$

mint a t-knek formája zérussal egyenlő, annak t_j szerint vett deriváltja is eltünik szükségképen, azaz

$$\left[\frac{\partial \varrho}{\partial z}\right]_{z=\sum_{j=1}^{m} t_j \xi_{jk}} \xi_{jk} + \left[\frac{\partial \varrho}{\partial t_j}\right]_{z=\sum_{j=1}^{m} t_j \xi_{jk}} = 0.$$

Ha most a következőket helyettesítjük:

$$t_s = a_s, \quad z = \zeta_k = \Sigma a_j \xi_{jk},$$

a minek jelölésére a $[\cdots]_a^{(k)}$ jelt használhatjuk, akkor a

$$\varrho(z; a_1, \ldots, a_m) = 0$$

egyenlet egyenesen meghatározza a ζ_k $(k = 1, \ldots, \nu)$ *mennyiségeket és azután* ζ_k*-ból raczionális müveletek segitségével előállithatók a* ξ_{jk} *mennyiségek a*

$$\left[\frac{\partial \varrho}{\partial z}\right]_a^{(k)} \xi_{jk} + \left[\frac{\partial \varrho}{\partial t_j}\right]_a^{(k)} = 0 \qquad (k = 1, \ldots, \nu)$$

egyenletekből. $\left[\frac{\partial \varrho}{\partial z}\right]_a^{(k)}$ ugyanis sohasem lehet egyenlő a zérussal, mert különben ellentétben a $\varrho(z; a_1, \ldots, a_m) = 0$ egyen-

let képezésével $z=\zeta_k$ annak nem egyszerű, hanem többszörös gyöke volna.

Ez az előállítás végre a $\xi_{1k}, \ldots, \xi_{mk}$ *gyökrendszer sokszorosságát* is értelmezi, mint azt a c_k kitevőt, a melylyel a $z - \Sigma t_j \xi_j$ lineáris tényező az E-ben előfordúl; ennek megfelelőleg a $\xi_{1k}, \ldots, \xi_{mk}$ gyökrendszert c_k*-szorosnak* nevezzük, vagy pedig azt mondjuk, hogy *a* $\xi_{1k}, \ldots, \xi_{mk}$ *mennyiségek ebben az esetben* c_k *egybeeső gyökrendszert képviselnek.*

Hasonló módon adják a c_l kitevők a végtelenben fekvő megoldások sokszorosságát.

16. §. Csatlakozva ismét a 14. §. fejtegetéseihez, most a

$$\Phi_i(x_1, \ldots, x_{m+1}) = 0 \qquad (i=1, \ldots, m)$$

rendszer ama feltevés mellett vizsgálandó, hogy annak csak véges számú valódi megoldása van, vagyis hogy a $(\bar{\Phi}_i)_{\bar{x}_{m+1}=0}$ formák resultánsa, a melyet, mint előbb $\bar{R}_{m+1}(u)$-val jelölünk, a zérustól különböző*.

Minthogy homogén lineáris transformatio a kérdéstételen mitsem változtat, úgy, mint előbb áttérhetünk a

$$\bar{\Phi}_i(\bar{x}_1, \ldots, \bar{x}_{m+1}) = 0$$

rendszerre és e mellett az u_{ij} mennyiségeket akár határozatlanoknak tekinthetjük, akár pedig oly határozott (sőt racionális és egész számú) értékeket is tulajdoníthatunk nekik, a melyekre nézve sem $|u_{ij}|$, sem pedig $\bar{R}_{m+1}(u)$ nem egyenlő a zérussal.

Minthogy valódi megoldás esetében $\bar{x}_{m+1}$ sohasem lehet

* Abban az esetben, midőn a valódi megoldások száma végtelen nagy, természetesen az előbbi fejezetben kifejtett KRONECKER-féle általános eliminácziő-elméletet kell alkalmaznunk. Ebben különösen fontos szempontok merülnek fel, ha a végtelenben fekvő megoldásokat a végesektől elkülönítjük, azaz előbb $x_{m+1}=0$-t, azután pedig megint $x_{m+1}=1$-et írunk, a mivel természetesen kiterjeszkedünk az összes megoldásokra.

egyenlő zérussal, $\bar{x}_{m+1}$-et 1-nek is vehetjük (vagy, a mi ugyanaz, a $\bar{\Phi}_i$ formához hozzácsatolhatjuk az $\bar{x}_{m+1}^{n_i}$ nevezőt és azután $\frac{\bar{x}_1}{\bar{x}_{m+1}}$, $\frac{\bar{x}_2}{\bar{x}_{m+1}}$ stbit tekinthetjük majd ismeretleneknek).

A

$$(\bar{\Phi}_i)_{\bar{x}_{m+1}=1}=0$$

egyenletrendszer már most az előbbi §-ban tárgyalt eset alá sorakozik és eliminánsával az

$$\bar{R}_{m+1}(u)\,z^N+\bar{R}'_{m+1}(u)\,z^{N-1}+\cdots+\bar{R}^{(N)}_{m+1}=0$$

egyenletet szolgáltatja, a melyből az összes valódi megoldások meghatározhatók.

Evvel megvan az ú. n. *Bezout-féle tétel, a melynek értelmében m homogén egyenletnek, a melyben m+1 az ismeretlenek száma, vagy végtelen sok, vagy pedig pontosan* $N=n_1 \ldots n_m$ *valódi megoldása van, ha minden egyes ilyen megoldást annyiszor számlálunk, a hányszor azt annak a* 15. §-*ban értelmezett sokszorossága követeli.*

Ha az u_{ij}-ket úgy választjuk, hogy $\bar{R}_{m+1}(u)$ a zérustól különböző, akkor minden egyes megoldás valódi megoldás s egyszersmind véges gyökrendszer is; a homogén lineáris transformatiók amaz algebrai sokaságának megfelelőleg, a melyeknek együtthatói, az u_{ij}-k úgy vannak választva, hogy

$$\bar{R}_{m+1}(u)=0,\ \ldots,\ \bar{R}^{(k-1)}_{m+1}(u)=0,$$

k valódi megoldás mindig «a végtelenben» fekszik, azaz ezekben $\bar{x}_{m+1}=0$. Ez bekövetkezhetik az összes megoldásoknál is, ha egyedül csak $\bar{R}^{(N)}_{m+1}$ különböző a zérustól.

Hogy az elimináns összes együtthatói zérussal egyenlők a nélkül, hogy $|u_{ij}|=0$, az akkor és csak akkor történik, ha a rendszernek végtelen sok különböző valódi megoldása van.

17. §. Legyenek ismét az

$$F_i(x_1,\ldots,x_m)=\sum_{(g)} a_g^{(i)}\,x_1^{g_1}\ldots x_m^{g_m}$$

formák n_i-ed dimensiójú általános formák, a melyeket most a következő módon írunk:

$$F_i = \varphi_i + \cdots,$$

a hol φ_i jelenti az F_i forma n_i-ed dimensiójú tagjainak complexusát; azaz φ_i bizonyos «általános» n_i-ed dimensiójú homogén forma. Akkor természetesen

$$R_{m+1} = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix}$$

a zérustól különböző és a rendszernek N valódi megoldása van, a melyek közül egy sem fekszik a végtelenben és így N gyökrendszere is van. Hogy ezek mind különbözők is, az igen egyszerű módon oly speciális példával igazolható, a melyben az $a_g^{(i)}$ mennyiségeket úgy választjuk, hogy az F_i formák dimensiói ne kisebbedjenek és a melynek mégis pontosan N különböző gyökrendszere van. Ilyen példát szolgáltat az

$$x_1^{n_1} = x_2,\ x_2^{n_2} = x_3,\ \ldots,\ x_i^{n_i} = x_{i+1},\ \ldots,\ x_m^{n_m} = 1$$

rendszer, a mely csak úgy elégíthető ki, ha x_1 valamely N-dik egységgyök és $x_2, \ldots, x_m$ értékeiül az első, második, ... egyenletből származó értékeket veszszük.

Ha már most az

$$F_i = 0 \qquad (i = 1, \ldots, m)$$

rendszerhez hozzácsatoljuk a további

$$F_{m+1} + z = 0$$

egyenletet (a melyben F_{m+1} valamely n_{m+1}-ed dimensiójú általános formát jelent), akkor az 5. és 9. §-ok szerint az F_i formák és $F_{m+1} + z$ resultánsa,

$$R_{m+1}^{n_{m+1}} z^N + \cdots + R,$$

minthogy végtelen megoldások nincsenek, akkor és csak akkor egyenlő zérussal, ha az $F_i = 0$ valamely gyökrendszerére nézve $z + F_{m+1} = 0$.

Az $F_i=0$ rendszernek N gyökrendszerét következőképen jelölve:

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk}, \qquad (k=1, \ldots, N)$$

a hol már most a ξ-k az $a_g^{(i)}$-knek meghatározott algebrai függvényei, ama resultáns akkor és csak akkor egyenlő zérussal, ha z felveszi a

$$-F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}) \qquad (k=1, \ldots, N)$$

értékek valamelyikét. Ezek az értékek, minthogy az F_{m+1} együtthatói ismét új határozatlanok, mind különbözők. Az

$$F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}) = F_{m+1}(\xi_{1l}, \ldots, \xi_{ml})$$

egyenlőségből ugyanis a lineáris tagok együtthatóinak összehasonlítása révén nyernők, hogy

$$\xi_{1k}=\xi_{1l}, \ldots, \xi_{mk}=\xi_{ml},$$

a mi az előbb bebizonyítottakkal ellenkezik.

Az

$$R_{m+1}^{n_{m+1}} z^N + \cdots + R = 0$$

egyenletnek tehát pontosan N különböző gyöke van; ezek t. i. a $-F_{m+1}(\xi_{1k}, \ldots, \xi_{mk})$ mennyiségek és így tehát

$$R = R_{m+1}^{n_{m+1}} \prod_{k=1}^{N} F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}).$$

Másrészt, ha z helyébe a 0-t teszszük, akkor, minthogy evvel nem jár a dimensió kisebbedése, az F_i és $F_{m+1}+z$ formák resultánsa átmegy az $F_1, \ldots, F_{m+1}$ formák resultánsába és ez e szerint R lesz. Így tehát nyerjük, hogy

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, F_{m+1} \\ x_1, \ldots, x_m, \quad 1 \end{pmatrix} = R_{m+1}^{n_{m+1}} \prod_{k=1}^{N} F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}),$$

a hol még

$$R_{m+1} = \text{Res.}\begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix}.$$

Ez a resultánsnak Poisson-tól* eredő előállítása, a

* «Sur l'élimination dans les équations algébriques». Journ de l'école polytechnique, IV. köt. 11. füz. 199. lap.

melyről közvetetlenül láthatjuk, hogy annak az alaknak az általánosítása, a melyben a III. fej. 24. §-a szerint két forma resultánsa előállítható. A ξ_{jk} mennyiségek itt az *általános* $F_i=0$ egyenletekben fellépő határozatlan $a_g^{(i)}$ együtthatóknak algebrai függvényei. A mennyiben azonban oly egyenleteket kellene tárgyalnunk. a melyekben az együtthatók határozott mennyiségek, a resultánsnak ez az alakja ismét *symbolikus,* mert ekkor fel kell tennünk, hogy azt előbb a régi alakba számítottuk át.

A resultánsnak Poisson-tól eredő ez az előállítása a symmetrikus formák fogalmának oly általánosításához vezet, a melylyel mindjárt tüzetesebben is foglalkozunk, mert mélyebb betekintést enged e képződmények természetébe és különösen az ú. n. discriminánsvizsgálatát könnyíti meg lényegesen.

A mennyiségek több rendszerének symmetrikus formái*.

18. §. Legyen

$$x_{ij} \qquad (i=1,\ldots,m;\, j=1,\ldots,n)$$

mn határozatlan, a mely közül az ugyanabban az oszlopban állók:

$$x_{1j}, x_{2j}, \ldots, x_{mj}$$

egy-egy «rendszert», jelesen az épen felírtak a (j) rendszert alkotják. A (j) és (k) rendszerek felcserélése e szerint a határozatlanoknak olyan felcserélése, a melynél egyidejűleg i minden értékénél x_{ij} lép x_{ik} helyébe és viszont. Az adott n

* E formák elméletét, a mely tulajdonképen Waring-ig vezethető vissza, pontosabban legelőször Schläfli fejtette ki. («Über die Resultante eines Systems mehrerer algebraischer Gleichungen» (Denkschr. d. kais. Akad. d. Wiss. in Wien. Math.-naturwiss. Cl. IV. k. 2. r. 1852.)

rendszernek minden lehetséges felcserélését tehát az

$$\begin{pmatrix}(1), & (2), & \ldots, & (n)\\ (j_1), & (j_2), & \ldots, & (j_n)\end{pmatrix}$$

jelképpel jelölhetjük, a hol $j_1, j_2, \ldots, j_n$ az $1, \ldots, n$ számokat jelentik, valamely tetszés szerinti sorrendben.

Az x_{ij} rendszerek symmetrikus formája olyan forma, a mely a rendszerek bármely felcserélése mellett változatlan marad.

A dolog természete szerint minden ilyen symmetrikus forma AX-alakú tagokból áll, a hol A ama holoid tartomány valamely mennyisége, a melyből a forma származik és X az x_{ij}-knek hatványszorzata; részletesen tehát

$$X = x_{1j_1}^{a_{11}} \ldots x_{mj_1}^{a_{m1}} x_{1j_2}^{a_{12}} \ldots x_{mj_2}^{a_{m2}} \ldots x_{1j_k}^{a_{1k}} \ldots x_{mj_k}^{a_{mk}}$$

és $k \leqq n$. Ha e hatványszorzatra az n rendszer összes lehetséges felcseréléseit alkalmazzuk és az így származó *különböző* hatványszorzatok összegét képezzük, akkor ez az összeg, a mely röviden a következő módon jelölhető:

$$\Sigma X,$$

az x_{ij} rendszerek symmetrikus formája. Ha ugyanis az ilyen felcserélést két különböző hatványszorzatra alkalmazzuk, újból különböző hatványszorzatok keletkeznek; az összes különböző hatványszorzatok összege tehát az elrendezés mellőzésével változatlan marad.

Az ilyen különösen egyszerű szerkezetű ΣX symmetrikus formát, a melyet az X hatványszorzat értelmez, *typikus symmetrikus formának*, vagy röviden «*typus*»-nak nevezzük; és közvetetlenül világos, hogy minden symmetrikus forma az

$$A_0 T_0 + A_1 T_1 + \cdots + A_s T_s$$

alakban írható, a hol $T_0, T_1, \ldots, T_s$ különböző typusokat, jelesen T_0 az 1-et jelenti és $A_0, A_1, \ldots, A_s$ az adott formának együtthatói.

A typusok közül első sorban említjük *az elemi symmetrikus formákat, a melyek minden egyes* $x_{1j}, \ldots, x_{mj}$ *mennyiség-rendszerre nézve lineárisak* és így tehát részletesen írva következő alakúak:

$$\sum_{(j)} x_{r_1 j_1} x_{r_2 j_2} \ldots x_{r_k j_k},$$

a hol $k \leqq n$, $j_1, \ldots, j_k$ az $1, \ldots, n$ sorozat k különböző számát, $r_1, \ldots, r_k$ pedig az $1, \ldots, m$ sorozat bármely egyenlő vagy különböző számait jelentik. A k-ad dimensiójú elemi symmetrikus formák számát a

$$(t_1 x_{11} + t_2 x_{21} + \cdots + t_m x_{m1}) \ldots (t_1 x_{1k} + t_2 x_{2k} + \cdots + t_m x_{mk})$$

kifejezés tagjainak száma szolgáltatja, ha ezt a t-k formájának tekintjük. Ebben ugyanis valamely $t_{r_1} \ldots t_{r_k}$ hatványszorzat együtthatója a következő alakban írható kifejezés:

$$x_{r_1 1} x_{r_2 2} \ldots x_{r_k k} + \cdots;$$

továbbá a különböző hatványszorzatok és e kifejezések kiírt első tagjai, valamint ezek az első tagok és a különböző k-ad dimensiójú elemi symmetrikus formák kölcsönösen egyértelműleg felelnek meg egymásnak. *A k-ad dimensiójú elemi symmetrikus formák száma* tehát (a II. fej. 8. §-a szerint)

$$\binom{m+k-1}{k}$$

és *az összes elemi symmetrikus formák száma*

$$\sum_{k=1}^{n} \binom{m+k-1}{k} = \binom{m+n}{n} - 1.$$

Ha valamennyi rendszerben a mennyiségek száma, $n=1$, akkor a mennyiségek *egyetlen* $x_{11}, x_{12}, \ldots, x_{1n}$ sorozatának a II. fej. 10. §-ában tárgyalt elmélet értelmében vett elemi symmetrikus formáit nyerjük, úgy hogy amaz elmélet, mint specziális eset beleilleszkedik ezekbe a fejtegetésekbe. Az elemi symmetrikus formák száma tehát csak akkor egyenlő

a határozatlanok számával, ha $m=1$; minden más esetben pedig ennél nagyobb. E szerint lényeges különbség van az előbb tárgyalt specziális eset és a jelen általános fejtegetések közt. A mennyiségek egy sorozatának elemei symmetrikus formái egymástól függetlenek voltak (II. fej. 15. §.); most ezek közt algebrai kapcsolatoknak kell fennállaniok és az egymástól függetlenek száma nem lehet nagyobb, mint mn (V. fej. 15. és 18. §.). Bebizonyítjuk erre vonatkozólag a következő tételt*:

Az elemi symmetrikus formák közt pontosan mn egymástól független forma van.

E tétel a legegyszerűbben úgy igazolható, hogy tényleg felállítjuk az egymástól független formáknak egy ilyen sorozatát.

Ilyent alkotnak az

$$x_{i1}, x_{i2}, \ldots, x_{in} \qquad (i=1, \ldots, m)$$

sorozatoknak (a szó előbbi egyszerűbb értelmében vett) elemi symmetrikus formái, a melyek jelölésére

$$e_r^{(i)} = \Sigma x_{ik_1} x_{ik_2} \ldots x_{ik_r}$$

szolgáljon. Akkor a

$$\frac{\partial(\ldots, e_r^{(i)}, \ldots)}{\partial(\ldots, x_{ir}, \ldots)}$$

függvénydeterminánsvalóban a zérustól különböző, mert egyenesen a

$$\frac{\partial(e_1^{(i)}, \ldots, e_n^{(i)})}{\partial(x_{i1}, \ldots, x_{in})}, \qquad (i=1, \ldots, m)$$

számra nézve m függvénydeterminánsszorzata és ez az utóbbi (a II. fej. 15. §-a szerint) egyszerűen

$$\prod_{r,s}(x_{ir}-x_{is}) \qquad (r, s=1, \ldots, n;\ r<s).$$

Evvel tételünk be van bizonyítva.

* Fr. Junker, Math. Annalen, 38. k. 91. l.

19. §. A nélkül, hogy az ehhez csatlakozó általános elméletet tovább fejtegetnők, közvetetlenül a következő, alkalmazásában fontos alaptételre térünk át:

Bármely raczionális, az $x_{1j}, \ldots, x_{mj}$, *számra nézve n rendszerre vonatkozólag symmetrikus forma előállítható mint az elemi symmetrikus formák raczionális formája.*

Közvetetlenül belátható, hogy elég, ha a tételt a typusokra bizonyítjuk be. A typusokat most meg akarjuk különböztetni az egyes tagokban fellépő különböző rendszerek száma szerint és a bizonyítást először az oly («egyformájú») typusokra vonatkozólag adjuk, a melyekben minden egyes tag csak egy rendszer határozatlanait tartalmazza.

Legyen

$$T_j = \sum_{i=1}^{m} t_i x_{ij}, \qquad (j=1, \ldots, n),$$

a hol $t_1, \ldots, t_m$ új határozatlanokat jelentenek, akkor a T_j mennyiségek elemi symmetrikus formái közvetetlenül képezési törvényük szerint a t-knek oly homogén formái, a melyeknek együtthatói egyenesen az $x_{1j}, \ldots, x_{mj}$ mennyiségrendszereknek elemi symmetrikus formái és e szerint

$$\sum_{j=1}^{n} T_j^a$$

is a t-knek oly homogén formája lesz, a melynek együtthatói raczionális és egész módon épűlnek fel amaz elemi symmetrikus formákból. Hogy tehát a

$$T^{(1)} = \Sigma x_{1j}^{a_1} x_{2j}^{a_2} \ldots x_{mj}^{a_m}$$

typust nyerjük, csak $a = a_1 + \cdots + a_m$-et kell irnunk és a

$$\sum_{j=1}^{n} T_j^a = \sum_{j=1} (t_1 x_{1j} + t_2 x_{2j} + \cdots + t_m x_{mj})^a$$

előállításban $t_1^{a_1} \ldots t_m^{a_m}$ együtthatóját meghatároznunk, a mely egyrészt bizonyos polynomiális együttható és $T^{(1)}$ szorzata,

másrészt pedig amaz elemi symmetrikus formáknak raczionális és egész formája lesz.

Ha már most feltételezzük, hogy az előállítás e módja lehetséges oly typusokra nézve, a melyeknek tagjai $k-1$, vagy pedig ennél kevesebb különböző rendszerből vannak összeállítva, akkor ép oly módon állíthatjuk elő azon («k-formájú») typusokat is, a melyeknek tagjai k különböző rendszer határozatlanait tartalmazzák. Ha ugyanis

$$T^{(k)} = \Sigma x_{1j_1}^{a_{11}} \ldots x_{mj_1}^{a_{m1}} x_{1j_2}^{a_{12}} \ldots x_{mj_2}^{a_{m2}} \ldots x_{1j_k}^{a_{1k}} \ldots x_{mj_k}^{a_{mk}}$$

ilyen typus, akkor e két typus:

$$T^{(1)} = \Sigma x_{1j_1}^{a_{11}} \ldots x_{mj_1}^{a_{m1}},$$

$$T^{(k-1)} = \Sigma x_{1j_2}^{a_{12}} \ldots x_{mj_2}^{a_{m2}} \ldots x_{1j_k}^{a_{1k}} \ldots x_{mj_k}^{a_{mk}}$$

szorzata bizonyára előállítható mint az elemi symmetrikus formák raczionális és egész formája. Másrészt azonban, ha mindazokat a tagokat veszszük, a melyekben j_1 különböző $i_2, \ldots, j_k$-tól, a szorzás végrehajtása szolgáltatja a $T^{(k)}$ typust, megszorozva bizonyos raczionális és egész számmal. A szorzat összes többi tagjai legfölebb $k-1$ különböző rendszerhez tartozó határozatlanokat tartalmaznak és így legfölebb «$k-1$-formájú» typusokba foglalhatók össze. Evvel tehát valóban megvan $T^{(k)}$-nek keresett előállítása.

20. §. Legyen már most

$$F_i(x_1, \ldots, x_m) = 0 \qquad (i=1, \ldots, m) \qquad (1)$$

«általános» egyenletrendszer, azaz olyan, a melyben F_i «általános» n_i-ed dimensiójú formát jelent. Ennek az egyenletrendszernek e szerint $N=n_1 \ldots n_m$ gyökrendszere van:

$$\xi_{1j}, \xi_{2j}, \ldots, \xi_{mj}, \qquad (j=1, \ldots, N)$$

a hol a ξ mennyiségek az $a_g^{(i)}$ együtthatók algebrai függvényei.

Ha e fej. 15. §-a szerint az eliminánst képezzük, az

$$R_{m+1} z^N + R'_{m+1} z^{N-1} + \cdots + R^{(N)}_{m+1} = 0 \qquad (2)$$

egyenletet nyerjük, a melynek gyökei a következő N lineáris forma:

$$\sum_{i=1}^{m} t_j \xi_{ij}. \qquad (j=1, \ldots, N) \qquad (3)$$

E mellett

$$R_{m+1} = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix} = r_0,$$

a hol φ_i az F_i n_i-ed dimensiójú tagjainak összfoglalatja; tehát R_{m+1} a $\varphi_1, \ldots, \varphi_m$ formák együtthatóinak raczionalis és egész, irreducibilis formáját jelenti. A resultánsnak előbb kifejtett tulajdonságaiból továbbá közvetetlenül következik, hogy $R^{(p)}_{m+1}$ a t-knek olyan p-ed dimensiójú homogén formája, a melynek együtthatói ismét az $a^{(i)}_g$ együtthatóknak raczionális és egész homogén formái; még pedig ezeknek dimensiója $a^{(i)}_g$-re nézve N_i és így tehát az összes a-kra nézve $\sum_{i=1}^{m} N_i$.

E szerint legyen most már

$$R^{(p)}_{m+1} = r_{p1} T_1 + r_{p2} T_2 + \cdots,$$

a hol a T-k a t-knek különböző p-ed dimensiójú hatványszorzatai és megfelelőleg

$$R_{m+1} = r_0.$$

Ha már most a (3) alatti gyökök elemi symmetrikus formáit képezzük és jelölésükre a megszokott

$$\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_N$$

jeleket használjuk, akkor közvetetlenül látjuk, hogy ezek a t-knek oly homogén formái, a melyeknek együtthatói egyenesen a $\xi_{1j}, \ldots, \xi_{mj}$ mennyiség-rendszereknek elemi symmetrikus formái. Ezeknek bizonyos sorrendben való jelölésére szolgáljanak:

$$\mathfrak{E}_1, \mathfrak{E}_2, \ldots, \mathfrak{E}_\mu.$$

Könnyű látni, hogy minden egyes $\mathfrak{E}$ föllép mint együtthatható; pl.

$$\Sigma \xi_{r_1 j_1} \xi_{r_2 j_2} \ldots \xi_{r_k j_k}$$

a $t_{r_1} t_{r_2} \ldots t_{r_k}$ együtthatója $\mathfrak{f}_k$-ban. Másrészt

$$r_0 \mathfrak{f}_k = (-1)^k R^{(k)}_{m+1}.$$

Ha tehát a különböző hatványszorzatok együtthatóit összehasonlítjuk, *a* $\xi_{1j}, \ldots, \xi_{mj}$ *mennyiség-rendszereknek összes elemi symmetrikus formái egyenesen a* $(-1)^k \frac{r_{kl}}{r_0}$ *alakban adódnak ki* és ez a következő általános tételhez vezet:

A $\xi_{1j}, \ldots, \xi_{mj}$ *mennyiség-rendszereknek minden racionális symmetrikus formája előállítható mint az* $\frac{r_{kl}}{r_0}$ *mennyiségek raczionális formája,* a hol az összes r-ek az $a_g^{(i)}$-knek raczionális és egész formái.

Az e tétel szerint valamely symmetrikus formára vonatkozólag nyert

$$S(\ldots, \xi_{ij}, \ldots) = \sum_{(g)} C_g \left(\frac{r_{k_1 l_1}}{r_0}\right)^{g_1} \left(\frac{r_{k_2 l_2}}{r_0}\right)^{g_2} \ldots \qquad (S)$$

előállítás úgy értendő, hogy, ha a jobb oldalon minden egyes $\frac{r_{kl}}{r_0}$ mennyiség helyébe a megfelelő elemi symmetrikus formát teszszük, oly azonosság származik, a mely érvényes marad akkor is, ha a ξ_{ij}-k bármily határozatlan mennyiségeket jelentenek.

E helyettesítés révén azonban a jobb oldalon olyan kifejezés származik, a mely egy $\xi_{1j}, \ldots, \xi_{mj}$ rendszer mennyiségeire nézve legfeljebb d'-ed dimensiójú lehet, ha a jobb oldalon álló forma az $\frac{r_{kl}}{r_0}$ mennyiségekre vonatkozó dimensiója d'.

Ha tehát az S symmetrikus forma valamely $\xi_{1j}, \ldots, \xi_{mj}$ *rendszerre nézve d-ed dimensiójú* (a mikor természetesen minden rendszerre nézve ugyanolyan), *akkor* r_0^d *S előállítható mint az* r_{kl}*-ek és* r_0 *raczionális homogén formája*

Az (S)-ben ugyanis a jobb oldalon álló formának dimensiója bármely $\xi_{1j}, \ldots, \xi_{mj}$ rendszerre nézve — a mint épen láttuk — nem nagyobb d'-nél. Ha már most valóban $d' > d$ volna, akkor, ha (S)-ben a jobb oldalon az $\frac{r_{kl}}{r_0}$-ok helyébe a megfelelő elemi symmetrikus formákat teszszük, szükségképen mindama tagok összegének, a melyeknek dimensiója $d+1, d+2, \ldots$ külön-külön el kellene tünnie, a mi az $\mathfrak{C}$-k közt most fennálló algebrai kapcsolatok miatt csakugyan megtörténhetik. Így tehát még egy második

$$S(\ldots, \xi_{ij}, \ldots) = \Sigma C_h \left(\frac{r_{k_1 l_1}}{r_0}\right)^{h_1} \left(\frac{r_{k_2 l_2}}{r_0}\right)^{h_2} \ldots$$

előállítást is nyerünk, a hol a jobb oldalon álló forma dimensiója d és evvel megadja a kimondott tételt.

E mellett azonban, ellentétben az $m=1$ specziális esettel, lehetséges, hogy r_0-nak valamely a d-diknél alacsonyabb hatványa mellett is már $r_0^a S$ az r_{kl}-eknek és r_0-nak raczionális és homogén formája, ha t. i. a ξ_{ij}-k nem határozatlanokat, hanem *kizárólag* az (1) gyökrendszereit jelentik. Mert tekintettel az ily gyökrendszerek közt esetleg fönnálló kapcsolatra * lehetséges, hogy két oly S és S' formára nézve, a melyek az egyes $\xi_{1j}, \ldots, \xi_{mj}$ mennyiség-rendszerekre nézve különböző dimensiójúak, mégis $S = S'$.

Mint azonnal alkalmazandó példát képezzük a

$$\prod_{j=1}^{N} I(\xi_{1j}, \ldots, \xi_{mj})$$

symmetrikus formát, a hol

$$I = \left| \frac{\partial F_i}{\partial x_j} \right|_{(i, j=1, \ldots, m)}$$

az $F_1, \ldots, F_m$ formarendszer függvénydeterminánsát jelenti.

* Ily kapcsolatokat ismerünk a geometriából; példáúl idézzük a két 3-adrendű görbe metszéspontjaira vonatkozó tételt.

Az I dimensiója $x_1, \ldots, x_m$-re nézve $\sum_{i=1}^{m} n_i - m$ úgy, hogy

$$r_0^{\sum n_i - m} \prod_{j=1}^{N} I(\xi_{1j}, \ldots, \xi_{mj})$$

mint az r_0 és r_{kl}-ek $\Sigma n_i - m$-ed dimensiójú formája állítható elő. Minthogy azonban r_{kl} és r_0, valamint I az együtthatók $a_g^{(i)}$ sorozatára nézve N_i-ed, ill. első dimensiojú racionális és homogén formák, az így értelmezett forma dimensiója az együtthatók $a_g^{(i)}$ sorozatára nézve $N_i(\sum_{i=1}^{m} n_i - m) + N$, az összes a együtthatókra nézve $\sum_{i=1}^{m} N_i(\sum_{i=1}^{m} n_i - m) + mN$.

Ennek megfelelőleg általánosságban is $r_0^d S(\ldots, \xi_{ij}, \ldots)$ bármely specziális $F_1, \ldots, F_m$ formarendszerre nézve, hacsak az egyes formák dimensiói, $n_1, \ldots, n_m$ nem szállnak alább, megtartja jelentését, mint *bizonyos az F-ek specziális együtthatóiból képezendő mennyiségek symbolikus értelmezése*, ha t. i. megállapodunk abban, hogy *először* történik az átszámítás az a-k formájába és *azután* ama specziális értékek behelyettesítése. Ez szembetünőleg általánosítása a III. fej. 24. §-ában bevezetett symbolikus előállításnak.

21. §. Az előbbi példában tárgyalt kifejezésre nézve a 17. § értelmében

$$r_0^{\sum n_i - m} \prod_{j=1}^{N} I(\xi_{1j}, \ldots, \xi_{mj}) = \text{Res.} \begin{pmatrix} F_1, \ldots, F_m, I \\ x_1, \ldots, x_m, 1 \end{pmatrix},$$

hacsak a resultáns definicziója nem veszti el értelmét. Minthogy állandóan feltételezzük, hogy $n_i \geqq 1$, ez csak akkor történhetik, midőn a függvénydeterminánsdimensiója zérus. Ez pedig akkor és csak akkor áll be, midőn az összes formák lineárisak. Ha ez általános formákra nézve más esetben is történnék, akkor úgy volna az $F_i = x_i^{n_i}$ specziális esetben is; minthogy azonban ekkor az

$$N x_1^{n_1 - 1} \ldots x_m^{n_m - 1}$$

függvénydeterminánsdimensiója $\Sigma n_i - m$ is nem zérus, állításunk be van bizonyítva. Lineáris formák rendszerének

kivételes esetében ama symmetrikus forma, mint közvetetlenül látni, $=I=r_0$.

Könnyen felismerhető továbbá az is, hogy *ama kifejezés, midőn mint az* $a_g^{(i)}$*-k raczionális formáját állítjuk elő, osztható* r_0*-sal.* A lineáris formák kivételes esetében ez nyilvánvaló; ha azonban valóságos resultánssal van dolgunk, annak az a-k oly értékei mellett, a melyekre nézve $r_0=0$, el kell tünnie. Ha ugyanis φ_i ismét az F_i legmagasabb dimensiójú tagjainak complexusát jelenti, akkor a $\varphi_i=0$ egyenleteknek van valódi megoldásuk; hisz épen ez az r_0 zérus voltának jelentése. Az I legmagasabb dimensiójú tagjainak complexusát $\left|\frac{\partial \varphi_i}{\partial x_j}\right|$ szolgáltatja. Minthogy azonban a φ-k homogén formák, azért (ha t. i. a determináns h-dik oszlopát megszorozzuk x_h-val és azután ehhez hozzáadjuk az $x_1, \ldots, x_m$-mel megszorzott első, $\ldots$, m-dik oszlopot)

$$x_h \left|\frac{\partial \varphi_i}{\partial x_j}\right| = A_{1h}\varphi_1 + \cdots + A_{mh}\varphi_m .$$

V $\varphi_i=0$ egyenletek ama valódi megoldása tehát kielégíti a $\left|\frac{\partial \varphi_i}{\partial x_j}\right|=0$ egyenletet is; azaz az $F_1=0, \ldots, F_m=0, I=0$ rendszernek van egy a végtelenben fekvő valódi megoldása és a resultáns e szerint szükségképen 0, ha az a-k értékrendszere olyan, hogy $r_0=0$. Minthogy azonban r_0 irreducibilis és így egyszersmind $r_0=0$ irreducibilis sokaság, ebből az V. fej. 7. §-ában használt módszerek szerint, vagy egyszerűbben a 15. § jegyzetében adott segédtétel alapján következik, hogy ama resultáns osztható r_0-sal. E szerint tehát

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, I \\ x_1, \ldots, x_m, 1 \end{pmatrix} = r_0 D,$$

a hol D az $a_g^{(i)}$-knek raczionális formája, mert a resultánsnak r_0-sal való oszthatóságára vonatkozó következtetés a raczionális számok tartományára, (1)-re vonatkozik. D azonban szükségképen *raczionális és egész* forma. Ha ugyanis D'

primitiv raczionális és egész forma, p, q pedig raczionális és egész számok, akkor minden esetre

$$D = \frac{p}{q} D'.$$

Minthogy azonban r_0 irreducibilis raczionális és egész forma, p szükségképen osztható q-val.

E szerint tehát a lineáris formákból álló rendszerre is érvényes eredmény, hogy

$$r_0^{\Sigma n_i - m - 1} \prod_{j=1}^{N} I(\xi_{1j}, \ldots, \xi_{mj})$$

az $a_g^{(i)}$*-knek raczionális és egész formája. Ezt az* $F_1, F_2, \ldots, F_m$ *formarendszer discriminánsának nevezzük* és Dscr. $(F_1, \ldots, F_m)$-mel, vagy pedig szükség esetén Dscr. $\binom{F_1, \ldots, F_m}{x_1, \ldots, x_m}$-mel jelöljük. Ezt az elnevezést megtartjuk akkor is, ha az $a_g^{(i)}$ együtthatók akármily értékeket vesznek fel, a mi természetesen úgy értendő, hogy ezek a specziális értékek a discriminánsnak, mint az $a_g^{(i)}$-k raczionális és egész formájának kész kifejezésébe helyettesítendők.

A függvénydeterminány irreducibilis volta.

22. §. A következőkben alkalmazandó fontos segédtétel, melynek bizonyítását itt közbeiktatjuk, így szól:

Az $F_i(x_1, \ldots, x_m)$, $(i=1, \ldots, m)$ *általános formarendszernek, hol* $n_i \geqq 1$, *függvénydeterminánsa I, mint az a-k és x-ek raczionális és egész formája, irreducibilis.*

Csupa lineáris forma,

$$L_i = \sum_{j=1}^{m} c_{ij} x_j \qquad (i=1, \ldots, m)$$

esetében e függvénydeterminány $|c_{ij}|$, melyről már e fejezet 11. §-ában kimutattuk, hogy a c-k irreducibilis raczionális és egész formája.

Áttérve tehát arra az esetre, midőn nem minden egyes F_i dimensiója az egység, az F_i lineáris tagjainak complexusát L_i-vel jelölhetjük; tehát

$$L_i = \sum_{j=1}^{m} c_{ij} x_j \qquad (i=1, \ldots, m)$$

és

$$I = |c_{ij}| + C_1 X_1 + C_2 X_2 + \cdots,$$

a hol $X_1, X_2, \ldots$ az x-eknek az 1-től különböző hatványszorzatait jelentik.

Az I minden osztója ép úgy, mint I maga is, az $a_g^{(i)}$-k minden sorozatára nézve homogén; még pedig bármely sorozatra nézve vagy lineáris, úgy mint I, vagy pedig azt a sorozatot egyáltalában nem is tartalmazza. Kell továbbá, hogy ez az osztó

$$d = A_0 + A_1 X_1 + A_2 X_2 + \cdots$$

alakú legyen, hol A_0, az x-ektől ment tag, a zérustól különböző; mert különben ebből $|c_{ij}| = 0$ következnék. A complementáris osztó azután

$$d' = A'_0 + A'_1 X_1 + A'_2 X_2 + \cdots$$

volna úgy, hogy

$$A_0 A'_0 = |c_{ij}|.$$

Így tehát vagy A_0, vagy pedig A'_0 egyenlő ± 1-gyel; és minthogy d es d' minden egyes $a_g^{(i)}$ sorozatra nézve, a melyet tartalmaz, homogén és lineáris, e két valódi osztó egyikében az X hatványszorzatok mellett álló együtthatók kivétel nélkül raczionális és egész számok lesznek.

Az I valamely ilyen osztója tehát szükségképen akkor is az I osztója maradna, ha az $a_g^{(i)}$ mennyiségeket bármely módon egész számoknak választanók. Tehát ismét írhatjuk, hogy pl. $F_i = L_i$ és ekkor d vagy d' a $|c_{ij}|$-nek is osztója, tehát az x-eket sem tartalmazza, azaz $= \pm 1$. I-nek e szerint valóban csak ± 1 és $\pm I$ lehetnek osztói.

A 11. §-ban és itt előadott módszerekkel ép úgy kimutatható, hogy az általános *formarendszer függvénydeterminánsa, a melyben minden egyes forma dimensiója* $\geqq 1$, *mint az a-knak és x-eknek formája, a IV. fej.* 18. §-*a értelmében föltétlenül irreducibilis forma.*

A discrimináns alaptulajdonságai.

23. §. Ha $F_1, \ldots, F_m$ ismét általános formarendszer ($n_i \geqq 1$) és I annak függvénydeterminánsa, akkor a 17. és 21. § szerint

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, I \\ x_1, \ldots, x_m, 1 \end{pmatrix} = r_0^{\Sigma n_i - m} \prod_{k=1}^{N} I(\xi_{1k}, \ldots, \xi_{mk}),$$

$$\text{Dscr.}\begin{pmatrix} F_1, \ldots, F_m \\ x_1, \ldots, x_m \end{pmatrix} = r_0^{\Sigma n_i - m - 1} \prod_{k=1}^{N} I(\xi_{1k}, \ldots, \xi_{mk});$$

és így tehát, ha a formarendszer discriminánsát röviden D-vel jelöljük, lesz

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, I \\ x_1, \ldots, x_m, 1 \end{pmatrix} = r_0 D.$$

Innen kezdve kizárjuk a csupa lineáris formából álló rendszert, azaz föltételezzük, hogy $N > 1$.

Akkor bebizonyíthatjuk, hogy *az előbbi fejtegetésekben raczionális és egész formának felismert discrimináns az* $(F_1, \ldots, F_m, I)$ *modulusrendszer meghatározta congruentia-tartományhoz tartozik;* azaz, hogy

$$D \equiv 0 \pmod{I, F_1, \ldots, F_m}. \qquad \text{(I)}$$

Minthogy e tulajdonság az $I, F_1, \ldots, F_m$ formarendszer resultánsában megvan, minden esetre

$$r_0 D = K_0 I + \sum_{i=1}^{m} K_i F_i$$

és, ha ebben az azonosságban, a hol $K_0, \ldots, K_m$ az a-knak és x-eknek raczionális és egész formáit jelentik, ismét

$a_{i,\,m+1}\,(i=1,\ldots,m)$ helyébe az $a_{i,\,m+1}-F_i$-t

írjuk, akkor, minthogy r_0 és I az $a_{i,\,m+1}$ határozatlanokat nem is tartalmazza, lesz

$$r_0\,[D] = [K_0]\,I,$$

a hol a $[\cdots]$ jel úgy, mint előbb azt jelenti, hogy a jelzett helyettesítést végrehajtottuk. Minthogy azonban r_0 nem tartalmazza az x-eket, I pedig irreducibilis forma, ebből, hacsak I az x határozatlanokat tartalmazza, következik, hogy $[D]$-nek oszthatónak kell lennie I-vel és ez csak más kifejezésmódja az (I) congruentiának.

Evvel tételünk be is van bizonyítva, mert nem csupán lineáris formákból álló rendszer esetében a függvénydeterminánsz az x határozatlanoknak legalább is egyikét mindig tartalmazza. Ha ugyanis e rendszert az $n_1,\ldots,n_m$ dimenziószámok megtartása mellett pl. a következőre speczializáljuk:

$$x_1^{n_1},\ldots,x_i^{n_i},\ldots,x_m^{n_m}$$

és itt pl. $n_i>1$, akkor a függvénydeterminánsz,

$$N\ldots x_i^{n_i-1}\ldots$$

még mindig tartalmazza az x_i határozatlant.

24. §. A további fejtegetések miatt pontosabban kell ismernünk az *oly rendszer discriminánsát, a melynek minden formája általános lineáris formák szorzata.*

E czélból először meg kell állapítanunk, hogy milyen alakú ebben az esetben a függvénydeterminánsz. Közvetetlenül látjuk, hogy, ha az egyik forma mint szorzat állítható elő, pl.

$$F_1 = F_1' F_1'',$$

akkor a függvénydeterminánsz:

$$\frac{\partial(F_1' F_1'', F_2,\ldots,F_m)}{\partial(x_1, x_2,\ldots,x_m)} = F_1'' \frac{\partial(F_1', F_2,\ldots,F_m)}{\partial(x_1, x_2,\ldots,x_m)} + F_1' \frac{\partial(F_1'', F_2,\ldots,F_m)}{\partial(x_1, x_2,\ldots,x_m)}.$$

Ennek az azonosságnak ismételt alkalmazása révén, ha általánosságban

$$F_i = L_{i1} \dots L_{i\mu_i} \dots L_{in_i}, \qquad (i=1, \dots, m) \qquad \text{(I)}$$

nyerjük, hogy

$$\frac{\partial(F_1, \dots, F_m)}{\partial(x_1, \dots, x_m)} = \sum \frac{F_1 \dots F_m}{L_{1\mu_1}, \dots, L_{m\mu_m}} \frac{\partial(L_{1\mu_1}, \dots, L_{m\mu_m})}{\partial(x_1, \dots, x_m)},$$

a hol a summatio kiterjesztendő mindazokra az $1\mu_1, \dots, m\mu_m$ számpárokra, melyekben $\mu_1, \dots, \mu_m$ egymástól függetlenül az $(1, \dots, n_1), \dots, (1, \dots, n_m)$ sorozatok bármely számait jelentik. Ha már most úgy, mint előbb (a 11. §-ban)

$$L_{i\mu_i} = c_{i1}^{(\mu_i)} x_1 + \dots + c_{im}^{(\mu_i)} x_m + c_{i,m+1}^{(\mu_i)},$$

akkor a resultánsokra vonatkozó szorzástétel szerint

$$r_0 = \prod_{\mu_m=1}^{n_m} \dots \prod_{\mu_1=1}^{n_1} | c_{ij}^{(\mu_i)} |_{(i,j=1,\dots,m)}$$

és az $F_i = 0$ rendszer ama $\xi_{1\mu_1}, \dots, \xi_{m\mu_m}$ gyökrendszerre nézve, a mely kielégíti az

$$L_{1\mu_1} = 0, \; L_{2\mu_2} = 0, \dots, L_{m\mu_m} = 0$$

lineáris rendszert, a függvénydeterminánsa a következő értéket veszi fel:

$$\left(\frac{F_1 \dots F_m}{L_{1\mu_1} \dots L_{m\mu_m}} \right)_{\xi_{1\mu_1}, \dots, \xi_{m\mu_m}} | c_{ij}^{(\mu_i)} |,$$

a hol a hányados az első tényezőben csak azt jelenti, hogy az $F_1 \dots F_m$ szorzatból $L_{1\mu_1}, \dots, L_{m\mu_m}$ rendre eltávolítandók. Végre tehát az (I)-ben értelmezett formarendszer discriminánsa

$$r_0^{\Sigma n_i - m} \prod_{\mu_m=1}^{n_m} \dots \prod_{\mu_1=1}^{n_1} \left(\frac{F_1 \dots F_m}{L_{1\mu_1} \dots L_{m\mu_m}} \right)_{\xi_{1\mu_1}, \dots, \xi_{m\mu_m}}.$$

A $\xi_{1\mu_1}, \dots, \xi_{m\mu_m}$ mennyiségek mindegyike azonban két forma hányadosa; e hányadosokban a nevező $| c_{ij}^{\mu_i} |$, a számláló pe-

dig hasonló szerkezetű determináns, a hol csak a j-dik oszlop elemeinek helyébe a $-c_{i,m+1}^{(\mu_i)}$ elemek lépnek. A productum jele alatt álló általános tényező tehát, a mely $\Sigma n_i - m$ lineáris tényezőből áll, egész lesz, ha $r_0^{\Sigma n_i - m}$-ből épen a $|c_{ij}^{(\mu_i)}|^{\Sigma n_i - m}$ tényezőt csatoljuk hozzá. A Dscr. $(F_1, \ldots, F_m)$-et szolgáltató kifejezés ily módon származó tényezői tehát a következő alakúak:

$$c_{k1}^{(\nu_k)} \{ |c_{ij}^{(\mu_i)}| \}_1 + \cdots + c_{km}^{(\nu_k)} \{ |c_{ij}^{(\mu_i)}| \}_m + c_{k,m+1}^{(\nu_k)} |c_{ij}^{(\mu_i)}|,$$

a hol $\{ |c_{ij}^{(\mu_i)}| \}_r$ azt a determinánst jelenti, a mely a $|c_{ij}^{(\mu_i)}|$ determinánsból úgy származik, hogy ebben az r-dik oszlopban a $c_{1r}^{(\mu_1)}, \ldots, c_{mr}^{(\mu_r)}$ elemek helyébe rendre a $-c_{1,m+1}^{(\mu_1)}, \ldots, -c_{m,m+1}^{(\mu_m)}$ elemeket helyettesítjük és a k, ν_k számpár nem egyezik meg az $1, \mu_1$; $2, \mu_2, \ldots$, vagy m, μ_m számpárokkal. E szerint e tényezők, a melyeknek száma $N(\Sigma n_i - m)$ és a melyekben a $c_{ij}^{(\mu_i)}$ mennyiségek kivétel nélkül különböző határozatlanokat jelentenek, a $c_{k1}^{(\nu_k)}, \ldots, c_{k,m+1}^{(\nu_k)}$ határozatlanokra vonatkozólag mindig lineárisok és kettő közülük sohasem æquivalens egymással. Az egyes ilyen tényezőket teljesen megadják a $(k, \nu_k), (1, \mu_1), \ldots, (m, \mu_m)$ számpárok és két különböző tényező, a melyben t. i. épen ezek a számpárok nem egyeznek meg mindannyian, különböző határozatlanokat is tartalmaz. Minden egyes ilyen tényező irreducibilis is, mert a lineárisan fellépő $c_{k1}^{(\nu_k)}, \ldots, c_{k,m+1}^{(\nu_k)}$ határozatlanok együtthatóinak, a

$$\{ |c_{ij}^{(\mu_i)}| \}_1, \ldots, \{ |c_{ij}^{(\mu_i)}| \}_m$$

mennyiségeknek nincsen az 1-től különböző közös osztójuk. Ebből következik, hogy e tényezők közül egyik sem lehet osztható valamely $|c_{ij}^{(\mu_i)}|$ determinánssal, mert amaz irreducibilis tényező dimensiója $m+1$ és így egyetlen olyan osztója sem lehet, a melynek dimensiója m.

Ezek szerint tehát az (I)-ben megadott formarendszer

discriminánsa egyszerűen a következő resultáns-szorzat*:

$$\text{Res.}(L_{1\mu_1}, L_{2\mu_2}, \ldots, L_{m\mu_m}, L_{k\nu_k}), \qquad \text{(II)}$$

a hol a szorzás kiterjesztendő mindazokra a resultánsokra, a melyek úgy származnak, hogy $\mu_i = 1, \ldots, n_i$ és minden egyes $(\mu_1, \ldots, \mu_m)$ combinatióhoz rendre hozzácsatolunk minden $L_{k\nu_k}$-t, a hol (k, ν_k) valamely az $(1, \mu_1), \ldots, (m, \mu_m)$ számpároktól különböző számpár.

Ha tehát valamely formarendszer minden egyes formája általános lineáris formák szorzata, akkor discriminánsa csupa különböző irreducibilis formák szorzata és nem osztható r_0-sal. (Itt r_0 — a mint azt már többször megállapítottuk — ama homogén formarendszer resultánsa, a melyben minden forma egy-egy eredeti forma legmagasabb dimensiójú tagjait tartalmazza).

25. §. Áttérünk már mostan arra az alapvető tételre, hogy *az általános formarendszer discriminánsa az* $a_g^{(i)}$ *együtthatóknak irreducibilis raczionális és egész formája* **.

E discrimináns, mint az $a_g^{(i)}$-k raczionális és egész formája bizonyára a következő alakú:

$$D = r_0^c P_1^{c_1} \ldots P_k^{c_k};$$

hogy minden esetre $c=0$, $c_1 = \cdots = c_k = 1$, az épen tárgyalt speciális esetből következik. Ha ugyanis az $a_g^{(i)}$-k helyébe a $c_{ij}^{(\mu_i)}$-k ama homogén formáit helyettesítjük, a melyek $F_i = L_{i1}, \ldots, L_{i\mu_i}$-ben mint együtthatók szerepelnek, akkor D nem zérus, tehát $r_0, P_1, \ldots, P_k$ is a zérustól különbözők. Ha tehát a c-k nem vennék fel az említett értékeket, D

* Minden egyes determinánsnak itt, szemben az előbbi előállítással, a $(-1)^m$ előjele van. Számuk, $N(\Sigma n_i - m)$ azonban mindig páros.

** Ezt a tételt KRONECKER a «Festschrift» 10. §-ában csak mellékesen említi; bizonyítását egy későbbi — fájdalom meg nem jelent — értekezésnek tartotta fenn.

osztható volna r_0-sal, vagy pedig többszörös tényezőket tartalmazna, a mi pedig az előbbiek szerint lehetetlen. E szerint D minden esetre a következő alakú:

$$D = P_1, \ldots, P_k.$$

A 23. § fejtegetései szerint tehát továbbá

$$[P_1] \ldots [P_k] \equiv 0 \,(\mathrm{mod.}\, I);$$

minthogy pedig az I függvénydeterminánsirreducibilis forma, azért valamelyik P-re nézve — legyen ez P_1 —

$$[P_1] \equiv 0 \,(\mathrm{mod.}\, I)$$

volna, azaz

$$P_1 \equiv 0 \,(\mathrm{mod.}\, F_1, \ldots, F_m, I).$$

Tulajdonítsunk már most az $a_g^{(i)}$-knek tetszés szerint választott oly értékeket, a melyekre nézve P_r zérus lesz. Akkor erre az értékrendszerre nézve r_0 vagy egyenlő a zérussal, vagy pedig nem. Az utóbbi esetben Res. $(F_1, \ldots, F_m, I)$ eltünik a nélkül, hogy r_0 is zérus volna; az

$$F_1 = 0, \ldots, F_m = 0, I = 0$$

egyenleteknek tehát van közös véges megoldásuk. Ha $F_1, \ldots, F_m, I$-ben ezt behelyettesítjük $x_1, \ldots, x_m$ helyébe, akkor az utolsó congruentiából következik, hogy az $a_g^{(i)}$-k ugyanazon értékrendszere mellett P_1 is egyenlő a zérussal. Mindezeket összefoglalva tehát látjuk, hogy az $a_g^{(i)}$-k minden olyan értékrendszere mellett, a melyre nézve P_r zérus, vagy r_0, vagy pedig P_1 egyenlő a zérussal és így tehát $r_0 P_1$ is eltünik. A 21. §-ban fejtegetett következtetési mód, jelesen az ott a jegyzetben előadott egyszerű segédtétel szerint tehát $r_0 P_1$-nek oszthatónak kell lennie P_r-rel, a mi azonban nem lehetséges, mert a feltevés szerint úgy r_0, mint P_1 a P_r-től különböző irreducibilis formákat jelentenek. A D tehát P_1 mellett nem tartalmazhat más irreducibilis osztót és így $D \sim P$, a mi épen bebizonyítandó volt.

26. §. Legyen ismét az $F_i(x_1, \ldots, x_m)$ általános forma-

rendszerre nézve $N>1$ és az egyes $F_i(x_1, \ldots, x_m)$ formáknak megfelelő homogén formák $\Phi_i(x_1, \ldots, x_{m+1})$; legyen továbbá úgy, mint előbb,

$$F_i^{(k)} = (\Phi_i(x_1, \ldots, x_{m+1}))_{x_k=1},$$

tehát $F_i^{(m+1)} = F_i$; legyen továbbá az eddigi jelöléseknek megfelelőleg

$$\varphi_i^{(k)} = (\Phi_i(x_1, \ldots, x_{m+1}))_{x_k=0}$$

és azután még

$$\varrho_k = \text{Res.}(\varphi_1^{(k)}, \ldots, \varphi_m^{(k)}).$$

A $\varphi_i^{(m+1)}$ forma tehát az a homogén forma, a melyet eddig φ_i-vel jelöltünk és ϱ_{m+1} az eddigi r_0. Közvetetlenül belátható, hogy $\varrho_1, \ldots, \varrho_{m+1}$ csupa egymástól különböző irreducibilis forma.

Legyen már most D az $F_1, \ldots, F_m$ formarendszer előbb értelmezett discriminánsa és $a_g^{(i)} = \alpha_g^{(i)}$ valamely olyan értékrendszer, a melyre nézve D a zérussal egyenlő, míg ellenben $\varrho_1, \ldots, \varrho_{m+1}$ a zérustól különbözők. E specziális választásnak megfelelőleg az $F_i=0$ egyenleteknek van oly véges gyökrendszerük, mely az

$$|F_{ij}| = 0 \qquad (i, j=1, \ldots, m)$$

egyenletet is kielégíti; még pedig, ha e gyökrendszert $\xi_1, \ldots, \xi_m$-mel jelöljük, a $\varrho_k \neq 0$ föltétel következtében egy ξ sem lehet egyenlő 0-sal.

Legyen már most $H^{(k)}$ a $\Phi_1, \ldots, \Phi_m$ formák függvénydeterminánsa $x_1, \ldots, x_{m+1}$ szerint, *a mely határozatlanok sorozatából az x_k ki van zárva;* akkor a

$$\Phi_1=0, \ldots, \Phi_m=0, H^{(k)}=0 \qquad (\Sigma_k)$$

egyenletrendszer egyszerűen az x_k határozatlan bevezetésével homogénné lett

$$F_1^{(k)}=0, \ldots, F_m^{(k)}=0, \; I^{(k)}=0$$

egyenletrendszer; ha t. i.

$$I^{(k)} = |F_{ij}^{(k)}|_{(i=1, \ldots, m;\; j=1, \ldots, m+1 \quad j \neq k)}.$$

A $H^{(k)}$ függvénydeterminánsok között a következő kapcsolat áll fönn:

$$x_{m+1} H^{(k)} \equiv \pm x_k H^{(m+1)} \pmod{\Phi_1, \ldots, \Phi_m},$$

a miről közvetetlenül meggyőződünk, ha $H^{(k)}$-ban $(k \neq m+1)$ az utolsó oszlop elemeit megszorozzuk x_{m+1}-gyel, és a megelőző oszlopok elemeit rendre $x_1, \ldots, x_m$-mel (az x_k kizárásával) megszorozva, azokhoz hozzáadjuk és végre még tekintetbe veszszük a

$$\sum_{j=1}^{m+1} {}^{(k)} x_j \Phi_{ij} = -x_k \Phi_{ik} + n_i \Phi_i$$

egyenlőséget.

E szerint, ha $\alpha_g^{(i)}$ az előbb megállapított módon választott együttható-rendszer, a $\xi_1, \ldots, \xi_{m+1}$ gyökrendszer, a melyben $\xi_1, \ldots, \xi_m$ az előbb adott értékek, ξ_{m+1} pedig 1, nemcsak a (Σ_{m+1}) rendszernek, hanem bármely (Σ_k) rendszernek is valódi megoldása; és így továbbá még $\frac{\xi_j}{\xi_k}$, $(j=1, \ldots, m+1; j \neq k)$ valódi megoldása az

$$F_1^{(k)} = 0, \ldots, F_m^{(k)} = 0, I^{(k)} = 0$$

egyenletrendszernek. Ebben az esetben tehát az $F_i^{(k)}$ rendszer discriminánsa, melyet $D^{(k)}$-val jelölhetünk, szintén zérus.

Minden olyan $\overline{\alpha}_g^{(i)}$ értékrendszerre nézve, a melynek helyettesítésénél $D=0$, vagy az egyik ϱ lesz egyenlő zérussal, vagy pedig $D^{(k)}=0$ úgy, hogy $\varrho_1 \varrho_2 \cdots \varrho_{m+1} D^{(k)}$ okvetetlenül 0. Ezért (a 21. § segédtétele szerint) e mennyiség osztható lesz D-vel. Ámde D irreducibilis és egyetlen ϱ sem lehet osztható D-vel, mint az közvetetlenül világos annak az esetnek vizsgálatából, a hol az F-ek lineáris formák szorzatai; mert akkor ϱ irreducibilis tényezőinek dimensiója m, a D-éinek dimensiója pedig $m+1$. Szükséges tehát, hogy $D^{(k)}$ osztható legyen D-vel, azaz e két irreducibilis forma

csak előjelben különbözhetik egymástól; vagy általánosabban kifejezve:

A $D^{(1)}, D^{(2)}, \ldots, D^{(m+1)}=D$ *discriminánsok csak előjelben különbözhetnek egymástól.*

A $\xi_1, \ldots, \xi_{m+1}$ gyökrendszer megfelel továbbá a

$$\Phi_1=0, \ldots, \Phi_m=0, \sum_{k=1}^{m+1} t_k H^{(k)}=0$$

rendszernek is, a hol $t_1, \ldots, t_{m+1}$ új határozatlanokat jelentenek és e rendszer resultánsa minden az előbbi módon jellemzett $\alpha_g^{(i)}$ rendszerre nézve a zérussal egyenlő; azaz ama resultáns a t-knek oly homogén formája, a mely részletesen írva a következő:

$$\Sigma A_g t_1^{g_1} \ldots t_{m+1}^{g_{m+1}}, \qquad (g_1+\cdots+g_{m+1}=N)$$

a hol minden egyes együtthatónak is megvan ugyanaz a tulajdonsága. E szerint $\varrho_1 \ldots \varrho_{m+1} A_g$ osztható lesz D-vel és, minthogy egyetlen ϱ sem osztható D-vel, minden egyes A_g-nek oszthatónak kell lennie D-vel. Könnyű azonban felismerni, hogy D *az* A_g *együtthatóknak legnagyobb közös osztója.* A t_k^N-nek együtthatóját ugyanis úgy nyerjük, ha a t_k kivételével minden egyes t-t 0-nak, t_k-t pedig 1-nek veszszük. De akkor ama resultáns átmegy a $\Phi_1, \Phi_2, \ldots, \Phi_m, H^{(k)}$ rendszer resultánsába, vagyis az

$$F_1^{(k)}, F_2^{(k)}, \ldots, F_m^{(k)}, I^{(k)}$$

rendszer resultánsába is, azaz $\varrho_k D$-be. Minthogy pedig $\varrho_1, \ldots, \varrho_{m+1}$-nek nincsen az 1-től különböző közös osztójuk, a D közös osztó egyszersmind amaz A együtthatóknak is legnagyobb közös osztója.

Most ép úgy, mint a resultáns esetében, a $\Phi_1, \ldots, \Phi_m$, számra nézve *m homogén forma discriminánsa* egyenesen az $F_1, \ldots, F_m$ formák discriminánsa legyen. E mellett az x határozatlanoknak még bizonyos elrendezése tartandó szem előtt; ha ez nincsen megadva, a discrimináns előjele hatá-

rozatlan marad, a mi azonban természetszerűen megfelel a discrimináns mostani értelmezésének, a mely szerint az bizonyos formák legnagyobb közös osztója.

Evvel a homogén formarendszer discriminánsának KRONECKER-től* eredő következő értelmezéséhez jutunk, a mely a discriminánsnak egyszersmind egyik fontos tulajdonságát fejezi ki:

Ha $\Phi_i(x_1, \ldots, x_{m+1})$ $(i=1, \ldots, m)$ *általános homogén formák, a melyeknek dimensiói* $n_1, \ldots, n_m$, $(N>1)$ *és* Φ_{m+1} *oly általános homogén lineáris formát jelent, a melynek együtthatói új határozatlanok, akkor a*

$$\Phi_1, \ldots, \Phi_m, \; |\Phi_{ij}|_{(i,j=1,\ldots,m+1)}$$

formák resultánsa tartalmaz egy a Φ_{m+1} *forma együtthatóitól független tényezőt és épen ez a* $\Phi_1, \ldots, \Phi_m$ *formarendszer discriminánsa.*

Közvetetlenül felismerjük ugyanis, hogy $\Phi_{m+1} = \sum_{k=1}^{m+1} t_k x_k$ esetében $\sum_{k=1}^{m+1} t_k H^{(k)} = |\Phi_{ij}|$.

E tétel még általánosabban és pontosabban következőképen fogalmazható:

Ha Φ_{m+1} *oly* n_{m+1}*-ed dimensiójú általános formát jelent, melynek összes együtthatói ismét új határozatlanok, akkor a*

$$\Phi_1, \ldots, \Phi_m, \; |\Phi_{ij}|_{(i,j=1,\ldots,m+1)}$$

formák resultánsa:

$$n_{m+1}^N \text{ Res.}(\Phi_1, \ldots, \Phi_{m+1}) \text{ Dscr.}(\Phi_1, \ldots, \Phi_m).$$

Tekintetbe véve, hogy

* Festschrift, 10. §. Az idézett helyen adott általánosabb tétel, mely arra az esetre vonatkozik, midőn Φ_{m+1} dimensiója n_{m+1}, mint a szöveg fejtegetéseiből kitünik, oda módosítandó, hogy ama resultánsnak a t-ktől független tényezője *nem* Dscr.$(\Phi_1, \ldots, \Phi_m)$, hanem n_{m+1}^N Dscr.$(\Phi_1, \ldots, \Phi_m)$.

$$\text{Res.}(\Phi_1, \ldots, \Phi_m, x_{m+1}) = \varrho_{m+1},$$

és fölhasználva a resultánsok szorzástételét, a meghatározandó resultánst R-rel jelölve, nyerjük, hogy

$$\varrho_{m+1} R = \text{Res.}(\Phi_1, \ldots, \Phi_m, x_{m+1} \mid \Phi_{ij} \mid),$$

vagyis az $x_{m+1} \mid \Phi_{ij} \mid$ egyszerű átalakításával:

$$\varrho_{m+1} R = \text{Res.}\left(\Phi_1, \ldots, \Phi_m, \sum_{k=1}^{m+1} n_k \Phi_k H_k\right)$$

$$= \text{Res.}\left(F_1, \ldots, F_m, \sum_{k=1}^{m+1} n_k F_k I_k\right),$$

hol H_k, ill. I_k a Φ_i, ill. F_i, $(i=1, \ldots, m+1;\ i \neq k)$ formáknak függvénydeterminánsa $x_1, \ldots, x_m$ szerint. Tehát végre a resultáns Poisson-tól eredő alakját (17. §) használva,

$$R = \varrho_{m+1}^{\sum_{j=1}^{m+1} n_j - m} \prod_{k=1}^{N} n_{m+1} F_{m+1}(\xi_{1k}, \ldots, \xi_{mk})\, I(\xi_{1k}, \ldots, \xi_{mk})$$

és

$$R = n_{m+1}^{N} \varrho_{m+1}^{n_{m+1}} \prod_{k=1}^{N} F_{m+1}(\xi_{1k}, \ldots, \xi_{mk})\, \varrho_{m+1}^{\sum_{i=1}^{m} n_i - m - 1} \prod_{k=1}^{N} I(\xi_{1k}, \ldots, \xi_{mk}),$$

a mi már is a keresett resultánsnak a tételben adott alakja.

A discrimináns invariáns-tulajdonsága.

27. §. A discriminánsnak most kifejtett új értelmezése végre még a következő tételhez vezet, a melyben az előbbi § összes jelöléseit megtartottuk:

Ha $N>1$, akkor a $\Phi_1, \ldots, \Phi_m$ formarendszer discriminánsának eltünése szükséges és elegendő feltétele annak, hogy a

$$\Phi_1 = 0, \ldots, \Phi_m = 0, \sum_{k=1}^{m+1} t_k H^{(k)} = 0 \qquad (\Sigma)$$

egyenletrendszernek, a hol $t_1, \ldots, t_{m+1}$ határozatlanoknak, $x_1, \ldots, x_{m+1}$ pedig ismeretleneknek tekintendők, oly valódi megoldása legyen, mely a t-któl független mennyiségekből áll.

E rendszernek akkor van valódi megoldása, ha a

$$\Sigma A_g t_1^{g_1} \dots t_{m+1}^{g_{m+1}} \qquad (g_1 + \dots + g_{m+1} = N)$$

resultáns eltünik; azaz, minthogy a t-k határozatlanok, ha minden egyes A_g együttható zérus, vagyis más szóval, ha a Φ formák $a_g^{(i)}$ együtthatói gyanánt olyan értékrendszereket választunk, a melyek az $A_g = 0$ egyenletrendszert kielégítik.

Ámde, mint már előbb (26. §) láttuk, $A_g = DA'_g$ és így tehát $D = 0$ minden esetre elegendő feltétel. Ha pedig megfordítva valamely $a_g^{(i)}$ együtthatórendszer olyan, hogy a (Σ) egyenleteknek van a t-ktől független mennyiségekből álló valódi megoldása, akkor ebben valamelyik x, pl. x_k nem zérus és így az

$$F_1^{(k)} = 0, \dots, F_m^{(k)} = 0, \mid F_{ij}^{(k)} \mid = 0$$

egyenleteknek is megfelel valamely véges gyökrendszer. Ámde

$$D \equiv 0 \,(\text{mod. } F_1^{(k)}, \dots, F_m^{(k)}, \mid F_{ij}^{(k)} \mid);$$

ha tehát az e congruentia jelezte azonosságban az x-ek helyébe ama gyökrendszert helyettesítjük, akkor az együtthatók ama rendszerére nézve szintén $D = 0$ és evvel a tétel be van bizonyítva.

Ez a tétel lényegében már tartalmazza *a discriminánsnak ú. n. invariáns-tulajdonságát,* a melyet most részletesebben is kifejtünk.

A

$$\Phi_1, \dots, \Phi_m, \Phi_{m+1} = \sum_{k=1}^{m+1} t_k x_k$$

formák az

$$x_j = \sum_{k=1}^{m+1} u_{jk} \bar{x}_k \qquad (T)$$

lineáris transformatio alkalmazása után — a már előbb használt jelöléssel élve — ismét a következőkbe menjenek át:

$$\bar{\Phi}_1, \dots, \bar{\Phi}_m, \bar{\Phi}_{m+1}.$$

Akkor

$$\frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j} = \frac{\partial \overline{\Phi}_i}{\partial x_1} u_{1j} + \cdots + \frac{\partial \overline{\Phi}_i}{\partial x_{m+1}} u_{m+1,j},$$

a hol az alkalmazott jelöléseket természetszerűen tovább fejlesztve, $\frac{\partial \overline{\Phi}_i}{\partial x_k}$ azt a formát jelenti, a mely $\frac{\partial \Phi_i}{\partial x_k}$-ból származik, ha erre a (T) transformatiót alkalmazzuk. E szerint

$$\left| \frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j} \right| = \left| \frac{\partial \overline{\Phi}_i}{\partial x_j} \right| |u_{ij}|$$

és így tehát a

$$\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}, \left| \frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j} \right|$$

rendszer resultánsa csak $|u_{ij}|$-nek egy tényezőként szereplő hatványában különbözik a

$$\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}, \left| \frac{\partial \overline{\Phi}_i}{\partial x_j} \right|$$

rendszer resultánsától. Ez azonban a (T) transformatio alkalmazásával

$$\Phi_1, \ldots, \Phi_{m+1}, \left| \frac{\partial \Phi_i}{\partial x_j} \right|$$

rendszer resultánsából származik; és így e két resultáns közt ép olyan kapcsolatnak kell fennállania. Tehát

$$\text{Res.}\left(\bar{\Phi}_1, \ldots, \bar{\Phi}_m, \left| \frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j} \right|\right) = |u_{ij}|^K \text{Res.}\left(\Phi_1, \ldots, \Phi_m, \left| \frac{\partial \Phi_i}{\partial x_j} \right|\right).$$

Ha az itt a két oldalon föllépő resultánsokat a 26. § utolsó tételében meghatározott alakban írjuk, lesz

$$\text{Res.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}) \text{ Dscr.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_m) =$$
$$= |u_{ij}|^K \text{ Res.}(\Phi_1, \ldots, \Phi_{m+1}) \text{ Dscr.}(\Phi_1, \ldots, \Phi_m).$$

Itt $\text{Res.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1})$ és $\text{Res.}(\Phi_1, \ldots, \Phi_{m+1})$ e fejezet 12. §-a értelmében csakis $|u_{ij}|$ egy tényezőként szereplő hatványában különböznek. Tehát a két oldalon álló discriminánsok közt ugyanily kapcsolat áll fönn. Azaz hasonlóképen, mint

a resultáns, *a discrimináns is a következő azonosság kifejezte invariáns-tulajdonságot* mutatja:

$$\bar{D} = \text{Dscr.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_m) = |u_{ij}|^{N(\Sigma n_i - m)} D.$$

Az $|u_{ij}|$ kitevőjének ebben foglalt pontos meghatározását igazolja azon körülmény, hogy adott dimensiójú formákra nézve e kitevő nem változik, bárhogyan választjuk is az $a_g^{(i)}$-ket. Ha tehát lineáris formák szorzatát veszszük és a discriminánsnak a 24. §-ban erre az esetre nyert szorzatalakját használjuk, azt tapasztaljuk, hogy a transformatio alkalmával minden egyes tényezőként szereplő determinánshoz pontosan $|u_{ij}|$ járul hozzá mint szorzó és így ama tényezők száma, $N(\Sigma n_i - m)$ lesz a keresett kitevő.

A megoldások sokszorossága.

28. §. A Φ_i formarendszer discriminánsának előadott tulajdonságait most átviszszük a $\Phi_i = 0$ egyenletrendszerre. Ajánlatos hogy e tárgyalásban a határozott és határozatlan rendszer eseteit szétválaszszuk.

Mindenekelőtt a következő tételnek szigorú és tisztán algebrai bizonyításával foglalkozunk:

A határozott $\Phi_i(x_1, \ldots, x_{m+1}) = 0 \; (i = 1, \ldots, m)$ *rendszer discriminánsa akkor és csak akkor lesz zérus, ha e rendszernek többszörös megoldása van.*

A határozott rendszer feltevésének megfelelőleg (a 14. § szerint) $\bar{R}_{m+1}(u)$ különböző a zérustól és a resultánsnak invariáns-tulajdonsága miatt másrészt elégséges, ha az u_{ij} mennyiségek helyébe olyan értékrendszert teszünk, a melyre nézve $|u_{ij}| \neq 0$. Ha még továbbá az u_{ij} mennyiségeket úgy választjuk, hogy $\bar{R}_{m+1}(u)$ a zérustól különböző legyen, akkor a kérdés vissza van vezetve oly

$$F_i(x_1, \ldots, x_m) = 0 \qquad (i = 1, \ldots, m)$$

egyenletrendszer vizsgálatára, a melynek $z=\Sigma t_j x_j$-re vonatkozó eliminánsa az

$$E(z)=R_{m+1}z^N+R'_{m+1}z^{N-1}+\cdots+R^{(N)}_{m+1}=0$$

egyenletet adja, a hol $R^{(k)}_{m+1}$ a t-knek oly k-ad dimensiójú formája, a melynek együtthatói ahhoz a raczionális tartományhoz tartoznak, a melyből az F_i formák származnak; még pedig R_{m+1} e raczionális tartománynak valamely zérustól különböző mennyisége.

Ámde az adott rendszernek akkor és csak akkor van többszörös megoldása, ha az $E(z)=0$ egyenlet gyökeinek száma kisebb N-nél; tehát akkor ha ennek az egyenletnek többszörös gyökei vannak, vagyis végre, ha Dscr. $E(z)$ eltünik. Magától értetődik, hogy Dscr. $E(z)$ itt a t-k formájának tekintendő.

Az $F_i=0$ egyenleteknek a 15. § értelmében meghatározott gyökrendszerei legyenek

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk}, \qquad (k=1,\ldots,\nu)$$

a hol $\nu \leqq N$; most épen a $\nu < N$, $\nu = N$ eseteket kell szétválasztanunk.

Minthogy

$$F_i(\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk}) = 0,$$

minden esetre

$$F_i(x_1, \ldots, x_m) = \sum_{j=1}^{m}(x_j-\xi_{jk})\,G_{ij}(x, \xi^{(k)}) \qquad (i=1,\ldots,m)$$

írható, a hol a könnyen érthető $G_{ij}(x, \xi^{(k)})$ rövidítés jelentése

$$G_{ij}(x, \xi^{(k)}) = G_{ij}(x_1, \ldots, x_m, \xi_{1k}, \ldots, \xi_{mk}).$$

A G_{ij}-k különféle módon választhatók; pl. úgy, hogy F_i-nek az $x_j-\xi_{jk}$-k hatványszorzatai szerint való kifejtésében először mindazokat a tagokat, a melyek $x_1-\xi_{1k}$-t tartalmazzák, összefoglaljuk az $(x_1-\xi_{1k})\,G_{i1}$ alakban, a hátra-

levők közül ismét mindazokat, a melyek $x_2-\xi_{2k}$-t tartalmazzák az $(x_2-\xi_{2k})G_{i2}$ alakban s í. t. Bármely módon történjék azonban a G_{ij}-knek ez a választása, a II. fej. 5. §-a szerint minden esetre

$$G_{ij}(\xi^{(k)}, \xi^{(k)}) = F_{ij}(\xi^{(k)}), \; F_{ij} = \frac{\partial F_i}{\partial x_j}.$$

Legyen már most a G_{ij}-kből képezett determináns

$$|\, G_{ij}(x, \xi^{(k)})\,|_{(i, j=1, \ldots, m)} = H(x, \xi^{(k)}),$$

akkor az aldeterminánsokat megfelelően jelölve:

$$H(x, \xi^{(k)})(x_j-\xi_{jk}) = \sum_{i=1}^{m} H_{ij}(x, \xi^{(k)})\, F_i(x_1, \ldots, x_m).$$

Ha $x_j=\xi_{jh}$ és $h+k$, a jobb oldal eltünik, míg a $\xi_{jh}-\xi_{jk}$ mennyiségek nem mindannyian egyenlők a zérussal; e szerint

$$H(\xi^{(h)}, \xi^{(k)}) = 0, \qquad (h+k)$$

míg az előbbiek értelmében

$$H(\xi^{(k)}, \xi^{(k)}) = |\, F_{ij}(\xi^{(k)})\,| = I(\xi^{(k)}).$$

Ha már most az egyes gyökrendszereket c_k sokszorosságuknak megfelelőleg c_k-szor írjuk, az mN mennyiségből álló

$$\xi_{1r}, \xi_{2r}, \ldots, \xi_{mr} \qquad (r=1, \ldots, N)$$

rendszer keletkezik, és ennek megfelelőleg a

$$\Delta = |\, H(\xi^{(h)}, \xi^{(k)})\,|_{(h, k=1, \ldots, N)}$$

determináns okvetetlenül zérussal egyenlő, ha két $\xi^{(h)}$ és $\xi^{(k}$ gyökrendszer nem különböző egymástól; mert ekkor a h-dik sor megegyezik a k-dik sorral. N különböző gyökrendszer esetében csak a fődiagonálisban álló elemek különbözők a 0-tól és a determináns értéke e szerint

$$\prod_{k=1}^{N} |\, F_{ij}(\xi^{(k)})\,|.$$

Ebből azonban következik, hogy a most vizsgált esetben, midőn többszörös gyök nincs és $R_{m+1} \neq 0$, mindig

$$\Delta = \prod_{k=1}^{N} F_{ij}(\xi^{(k)}).$$

Szembetünő, hogy Δ a $\xi^{(i)}$ gyökrendszerek symmetrikus formája, mert, ha $\xi^{(h)}$-t felcseréljük $\xi^{(k)}$-val, akkor Δ-ban egyidejűleg a h-dik és k-dik sor és ép úgy a h-dik és k-dik oszlop helyet cserél; ép úgy változatlan marad a jobb oldalon álló szorzat is.

A 20. § jelölését használva tehát

$$\Delta = \frac{\varphi(r_0, \ldots, r_{kl}, \ldots)}{r_0^a},$$

$$\prod_{k=1}^{N} F_{ij}(\xi^{(k)}) = \frac{\psi(r_0, \ldots, r_{kl}, \ldots)}{r_0^b},$$

a hol φ és ψ homogén formákat jelentenek és $r_0 = R_{m+1} \neq 0$. Ha most már Dscr. $E(z)$ a zérustól különböző, bizonyára lesz

$$r_0^b \varphi = r_0^a \psi.$$

Ha ugyanazt a meggondolást elvégezzük az általános egyenletrendszer esetében, ezek szerint ez az egyenlet fennáll az $a_g^{(i)}$ együtthatók minden olyan rendszerére nézve, a melyre nézve r_0 és a Dscr. $E(z)$ forma összes együtthatói nem egyidejűleg zérusok; tehát az együtthatók minden olyan rendszerére nézve, a melyre nézve $r_0 A$, a hol A a Dscr. $E(z)$ forma valamely együtthatója, különböző a zérustól. De akkor érvényes az együtthatók bármely rendszerére nézve is és minthogy feltételeztük, hogy r_0 különböző a zérustól, végre a következő általánosan érvényes meghatározáshoz jutunk:

$$r_0^{\Sigma n_i - m - 1} \Delta = r_0^{\Sigma n_i - m - 1} \prod_{k=1}^{N} F_{ij}(\xi^{(k)}) = \text{Dscr.}(F_1, \ldots, F_m).$$

A discrimináns tehát feltétlenül zérussal egyenlő, ha $R_{m+1} \neq 0$ *és két gyökrendszer,* $\xi^{(h)}$ *és* $\xi^{(k)}$ *nem különbözik egymástól,* vagyis tehát, ha az egyenletrendszernek többszörös megoldása van, a mi az utolsó egyenletből szembetünő ; mert hisz ebben az esetben Δ egyenlő a zérussal.

29. §. Hogy a tételt, a melyre a 28. §-ban reámutattunk, teljesen bebizonyítsuk, még ki kell mutatnunk, hogy (ismét az $R_{m+1} = r_0 \neq 0$ feltétel mellett) megfordítva *a discrimináns eltünéséből mindig következik, hogy az egyenletrendszernek többszörös megoldása van.*

E tényre abból a körülményből következtethetünk, hogy az $E(z)$ elimináns a 15. § szerint az

$$F_1, \ldots, F_m, z - \Sigma t_j x_j$$

rendszer resultánsa ; tehát fennáll az

$$E(z) \equiv 0 \,(\text{mod. } F_1, \ldots, F_m, z - \Sigma t_j x_j)$$

congruentia, a melyből az

$$E\left(\sum_{j=1}^{m} t_j x_j\right) = \sum_{i=1}^{m} K_i F_i$$

azonosság foly. Ha a z-t megtartjuk mint $\sum_{j=1}^{m} t_j x_j$ rövidítését, akkor x_j szerint deriválva, ebből

$$\frac{\partial E}{\partial z} t_j = \sum_{i=1}^{m} \frac{\partial K_i}{\partial x_j} F_i + \sum_{i=1}^{m} K_i F_{ij}.$$

Ha már mostan $\xi^{(k)}$ olyan gyökrendszer, a melyre nézve $|F_{ij}(\xi^{(k)})| = 0$, akkor legyenek az r-edfokú aldeterminánsok a legalacsonyabb fokúak, a melyek még mindannyian eltünnek.

Ha $r=1$, tehát $F_{ij}(\xi^{(k)})$ mindig zérussal egyenlő, akkor az utolsó azonosságból következik, hogy $z = \Sigma t_j \xi_{jk}$ a $\frac{\partial E}{\partial z} = 0$

egyenletnek is gyöke és így tehát e gyök — a mint azt állítottuk — az $E(z)=0$ egyenletnek többszörös gyöke.

Ha $r>1$, akkor az $r-1$-edfokú aldeterminánsokat megfelelően választva és ezekkel, a melyek közt egy a zérustól különböző is van, szorozva, lesz

$$\frac{\partial E}{\partial z}\Sigma t_j d_j = \sum_{i=1}^{m} K_i' F_i,$$

és ha ebben ismét az $x_j=\xi_{jk}(j=1,\ldots,m)$ helyettesítést végezzük, akkor, minthogy az egyik d_j minden esetre a zérustól különböző, $z=\Sigma t_j \xi_{jk}$ kielégíti a $\frac{\partial E}{\partial z}=0$ egyenletet; tehát ismét azt találjuk, hogy $z=\Sigma t_j \xi_{jk}$ az $E(z)=0$ egyenletnek többszörös gyöke.

Evvel a 28. § tétele teljesen be van bizonyítva.

30. §. Az eddigi fejtegetések végre befejezéshez jutnak, ha még bebizonyítjuk, hogy *határozatlan rendszer discriminánsa mindig zérussal egyenlő.*

Határozatlan az olyan rendszer, a melynek végtelen sok valódi megoldása van. E szerint tehát most olyan megoldás is végtelen sok lesz, a melyben egy és ugyanaz a határozatlan a zérustól különböző értékeket vesz föl. Ha ugyanis csak véges volna azoknak a megoldásoknak száma, a melyekben rendre $x_1,\ldots,x_{m+1}$ különböző a zérustól, akkor a megoldások összességének száma is véges volna. Ha végül ama határozatlant x_{m+1}-gyel jelöljük, ez csak a határozatlanok megnevezésének változtatása és így végre feltételezhetjük, hogy az

$$F_i(x_1,\ldots,x_m)=0$$

egyenletrendszernek végtelen sok (véges) gyökrendszere van; azaz az $F_i=0$ rendszert olyan sokaság elégíti ki, a melynek fokozat-száma kisebb m-nél.

Feltételezhetjük továbbá, hogy az $F_i=0$ rendszer az

által, hogy az $x_1, \ldots, x_m$ határozatlanokat oly lineáris transformatiónak vetettük alá, a melynek determinánsa a zérustól különböző, az V. fejezet értelmében esetleges körülményektől meg van szabadítva; mert az eredeti és transformált rendszer discriminánsa egyidejűleg zérus, vagy zérustól különböző.

Az V. fej. 9. §-ának jelöléseit* használva, látjuk, hogy a $\Delta_a F_i = 0$ rendszer ki van elégítve, ha $x_{h+1}, \ldots, x_{m-1}$-et meghagyva határozatlanoknak, x-et, mint algebrai függvényt a

$$\varphi(x, a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1}) = 0 \qquad (1)$$

egyenletből meghatározzuk és azután $x_1, \ldots, x_h$-t a

$$\left[\frac{\partial \varphi}{\partial x}\right]_a x_i + [\varphi_i]_a = 0 \qquad (i=1, \ldots, h) \qquad (2)$$

egyenletekből számítjuk ki, míg x_m meghatározására az

$$x = \sum_{i=1}^{m} a_i x_i, \quad \text{vagy a} \quad \left[\frac{\partial \varphi}{\partial x}\right]_a x_m + [\varphi_m]_a = 0 \qquad (3)$$

egyenlet szolgál. (Itt $h < m-1$ úgy, hogy az értelmezett sokaság, $V^{(h+1)}$ legfölebb $m-1$-edfokozatú).

A $\varphi(x, t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1})$ forma továbbá irreducibilisnek tételezendő fel; az a_i értékeket pedig, a melyeket a t_i-k helyébe teszünk, úgy választottuk, hogy $\varphi(x, a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1})$ discriminánsa az $x_{h+1}, \ldots, x_m$ határozatlanoknak a 0-tól különböző formája, a melyet úgy, mint az idézett helyen Δ_a-val, vagy pedig $\Delta_a(x_{h+1}, \ldots, x_{m-1})$-gyel jelölünk.

* Hogy itt belépnek az általános eliminácziő-elmélet fejtegetései, nem csak természetszerű, hanem szükséges is és nem talán a folytonossági vizsgálat «mesterséges» elkerülésének következménye. Hisz valamely az m-ediknél alacsonyabb fokozatú sokaságban egyesített gyökrendszerek «folytonosságára» épen csak amaz előállításból következtethetünk.

De akkor

$$\Delta_a = \lambda\varphi + \mu\left[\frac{\partial\varphi}{\partial x}\right]_a;$$

tehát

$$\Delta_a x_i + \mu\,[\varphi_i]_a = 0 \qquad (i=1,\ldots,h);$$

valamint $\Delta_a F_i=0$, ha $x_1,\ldots,x_h,x_m$ helyébe az előbb adott értékeket teszszük, x pedig az (1)-ben értelmezett algebrai függvényt jelenti és azonkívül még

$$\sum_{i=1}^{m} a_i x_i = x.$$

Az utóbbi azonban ismét az F_i-ben foglalt határozatlanoknak csak homogén lineáris transformatióját jelenti. Ha ez F_i-t átvezeti $G_i(x, x_1,\ldots,x_{m-1})$-be, akkor ismét Dscr. $(G_1,\ldots,G_m)$ és Dscr. $(F_1,\ldots,F_m)$ egyidejűleg zérus, vagy zérustól különböző.

Ha Δ_a-nak elég magas hatványával szorzunk úgy, hogy $\Delta_a^{c_i} G_i$ az $x_1,\ldots,x_h$ mennyiségeket csak a $\Delta_a x_1,\ldots,\Delta_a x_h$ szorzatokba foglalva tartalmazza, akkor

$$\Delta_a^{c_i} G_i \equiv H_i(x, x_{h+1},\ldots,x_{m-1})\,(\text{mod.}\ldots,\Delta_a x_i + \mu\,[\varphi_i]_a,\ldots)$$

és H_i zérus lesz, ha x az (1)-ben értelmezett algebrai függvényt jelenti és így tehát H_i osztható φ-vel. Ebből végre következik a

$$\Delta_a^{c_i} G_i \equiv 0\,(\text{mod.}\,\psi_1,\ldots,\psi_h,\psi_{h+1}) \qquad (C)$$

congruentia, a hol a következő rövidítéseket alkalmaztuk:

$$\psi_i = \Delta_a x_i + \mu\,[\varphi_i]_a, \qquad (i=1,\ldots,h)$$

$$\psi_{h+1} = \varphi$$

és a (C)-ben fellépő modulusrendszer elemeinek száma, $h+1<m$. A (C)-t még a

$$\Delta_a^{c_i} G_i = \sum_{j=1}^{m} C_{ij}\,\psi_j$$

alakban is írhatjuk, a hol $\psi_{h+2},\ldots,\psi_m$ egyszerűen zérusnak

veendő és ebből nyerjük, hogy

$$\Delta_a^{c_i} \frac{\partial G_i}{\partial x_r} = \sum_{j=1}^{m} \frac{\partial C_{ij}}{\partial x_r} \psi_j + \sum_{j=1}^{m} C_{ij} \frac{\partial \psi_j}{\partial x_r} + K_{ir} G_i.$$

$$(r=0, 1, \ldots, m-1)$$

Minthogy pedig az (1) és (2)-vel értelmezett sokaság elemeire nézve G_i, valamint $\psi_j=0$, azért ugyanekkor

$$\Delta_a^{c_i} \frac{\partial G_i}{\partial x_r} = \sum_{j=1}^{m} C_{ij} \frac{\partial \psi_j}{\partial x_r}$$

és végre ugyanazokra az elemekre nézve

$$\Delta_a^{c_1+\cdots+c_m} \left| \frac{\partial G_i}{\partial x_r} \right| = |C_{ij}| \left| \frac{\partial \psi_j}{\partial x_r} \right|.$$

Minthogy azonban a jobb oldalon legalább is egy ψ_j azonosan egyenlő a zérussal, és így ugyanaz áll $\left| \frac{\partial \psi_j}{\partial x_r} \right|$-re nézve is, Δ_a pedig a határozatlanoknak a zérustól különböző formája, azért végre ama sokaság összes elemeire nézve $\left| \frac{\partial G_i}{\partial x_r} \right| = 0$.

Ámde

$$\text{Dscr.}\,(G_1, \ldots, G_m) \equiv 0 \left(\text{mod.}\, G_1, \ldots, G_m, \left| \frac{\partial G_i}{\partial x_r} \right| \right)$$

és, ha a jobb oldalon $x, x_1, \ldots, x_{m-1}$ helyébe ama sokaság bármely elemét teszszük, $x_{h+1}, \ldots, x_{m-1}$-et mindig határozatlanoknak értve, akkor a modulusrendszer minden eleme, tehát a G-k discriminánsa is és evvel együtt az $F_1, \ldots, F_m$ rendszer discriminánsa is egyenlő lesz a zérussal, a mit be kellett bizonyítanunk.

Most már a 28. és 30. §§ eredményeit könnyen összefoglalhatjuk a következőben:

A $\Phi_i=0\,(i=1, \ldots, m)$ rendszernek «általánosságban» N különböző megoldása van; evvel szemben a rendszert *singulárisnak* nevezzük, midőn a különböző megoldások száma vagy kisebb N-nél, azaz a rendszernek «többszörös» meg-

oldásai vannak, vagy pedig a különböző megoldások száma nagyobb N-nél, azaz végtelen nagy. Evvel a következő tételhez jutottunk:

A $\Phi_i (i=1,\ldots, m)$ formák discriminánsának eltünése szükséges és elegendő föltétele annak, hogy a $\Phi_i=0$ egyenletrendszer singuláris legyen.

A lineáris formák rendszerének esete, melyet az eddigiekben állandóan kizártunk, mint könnyű látni, egész elemi úton intézhető el. Ily egyenletrendszer, melynek együtthatói m sorból és $m+1$ oszlopból álló matrixot adnak, akkor és csak akkor singuláris, ha minden e matrixból keletkező m-edfokú determináns eltűnik.

HETEDIK FEJEZET.

LINEÁRIS DIOPHANTIKUS PROBLÉMÁK.

(Általános tételek és az algebrai elmélet.)

A probléma felállítása.

1. §. Legyen A bárminő holoid tartomány, mely tehát akár valódi holoid tartomány, akár pedig orthoid tartomány lehet és $[A, x_1, \ldots, x_m]$ e tartományból származó formatartomány. Ha azután

$$F_{i0}, F_{i1}, \ldots, F_{il} \qquad (i=1, \ldots, k)$$

e tartományhoz tartozó formák, meghatározandók azok az

$$X_1, \ldots, X_l$$

formák, a melyek ugyanahhoz a tartományhoz tartoznak és az

$$F_{i0} = F_{i1} X_1 + F_{i2} X_2 + \cdots + F_{il} X_{il} \qquad (I)$$
$$(i=1, \ldots, k)$$

egyenletrendszert kielégítik. E felfogásban (I) *lineáris diophantikus egyenletek rendszere,* a hol tehát ellentétben a kérdés eddigi felállításával, mint megoldások csak azok a mennyiségek jönnek tekintetbe, melyek az $[A, x_1, \ldots, x_m]$ formatartományhoz tartoznak.

A következőkben különösen két eset lesz vizsgálandó, először, midőn A orthoid tartomány, másodszor pedig az az eset, midőn A a raczionális és egész számok tartománya. Az első esetben a probléma az algebrába tartozik, a másodikban pedig az arithmetikába, ha e két tudományágat a IV. fej.

8. §-ának értelmében különítjük el egymástól. E két alapvető esetre visszavezethető az algebrai mennyiségek elméletének minden ide tartozó problémája.

A lineáris diophantikus egyenletrendszer megoldásának problémája mindkét esetben két egyszerűbb alapproblémára bontható és, hogy az ismételéseket elkerüljük, e visszavezetést mindjárt valamivel általánosabb alakban végezzük.

Ha Γ holoid tartomány és a γ-k a Γ tartományhoz tartoznak, akkor a

$$\sum_{j=1}^{l} \gamma_{ij} \xi_j = \gamma_{i0} \qquad (i=1, \ldots, k) \qquad \text{(II)}$$

«lineáris diophantikus egyenletek rendszerének megoldása Γ-ban» az ugyanehhez a tartományhoz tartozó $\xi_1, \ldots, \xi_l$ mennyiségek mindama rendszereinek meghatározását követeli, a melyek ezt az egyenletrendszert kielégítik. Ha végtelen sok ilyen mennyiség-rendszer van, akkor magától értetődik, hogy a «meghatározás» helyébe az a követelés lép, hogy azokat meghatározott módon teljesen leírjuk.

A Γ tartományt röviden *diophantikus tartománynak* nevezzük, ha minden

$$\gamma_1 \xi_1 + \gamma_2 \xi_2 + \cdots + \gamma_l \xi_l = 0 \qquad (1)$$

homogén lineáris diophantikus egyenletnek megfelelőleg *véges* számmal meghatározhatók a tartományhoz tartozó mennyiségek olyan

$$\xi_{1h}, \xi_{2h}, \ldots, \xi_{lh} \qquad (h=1, \ldots, r) \qquad (2)$$

rendszerei, hogy nemcsak — a mint ez magától értetődik —

$$\xi_j = \mu_1 \xi_{j1} + \mu_2 \xi_{j2} + \cdots + \mu_r \xi_{jr}, \quad (j=1, \ldots, l) \qquad (3)$$

a hol $\mu_1, \ldots, \mu_r$ a Γ tartomány tetszés szerinti mennyiségei, mindig ama diophantikus egyenlet megoldása, hanem megfordítva is bármely $\xi_1, \ldots, \xi_l$ megoldás erre az alakra hozható. Ezt a tulajdonságot a következő szavakkal fejezzük ki: *Dio-*

phantikus tartományban bármely homogén diophantikus egyenlet megoldásai véges sereget alkotnak. Csatlakozva már előbb használt elnevezésekhez (V. fej. 13. §) ezt a sereget r-tagúnak nevezzük. A μ_i-k bármely választása mellett a (2) rendszerekkel egy időben természetesen a (3) rendszerek is megoldások; de ha Γ-ra nézve nincsen további megállapodásunk, egyáltalában nincsen kizárva az a lehetőség sem, hogy amaz r rendszer, bármilyen nagy szám is r, sohasem elégséges az *összes* megoldások előállítására. «Diophantikus» tartomány esetében épen ez nem történik meg.

Ily értelemben be lesz bizonyítandó később, hogy minden formatartomány, a mely orthoid tartományból, vagy pedig az [1] tartományból származik, diophantikus tartomány.

Diophantikus tartományban a lineáris diophantikus egyenletek (II) *rendszerének teljes megoldása a következő két alapproblémára vezethető vissza:*

1) *Ama véges sereg meghatározása, a mely egy egyetlen homogén lineáris diophantikus* (1) *egyenletet kielégít.*

2) *Annak eldöntése, vajjon valamely lineáris diophantikus egyenletnek, a mely*

$$\gamma_1 \xi_1 + \cdots + \gamma_l \xi_l = 1 \qquad (4)$$

alakú, van-e megoldása és egy megoldásának meghatározása, ha ilyen egyáltalában van.

E két feladat tárgyalása után minden lineáris diophantikus rendszer teljes megoldása véges számú lépésben történhetik. Hogy miképen, az épen most lesz első sorban tárgyalandó.

Mindenekelőtt világos, hogy ekkor a (4) egy megoldásának ismerete után e megoldások összessége is teljesen leírható. Ha ez a megoldás a következő:

$$\xi_{10}, \ldots, \xi_{l0},$$

akkor minden más megoldás kielégíti a

$$\gamma_1(\xi_1-\xi_{10})+\cdots+\gamma_l(\xi_l-\xi_{l0})=0$$

homogén egyenletet. Az összes megoldások tehát a

$$\xi_j=\xi_{j0}+\mu_1\xi_{j1}+\cdots+\mu_r\xi_{jr} \qquad (j=1,\ldots,l) \qquad (5)$$

alakban állíthatók elő, a hol a μ-k a Γ tartomány tetszés szerinti mennyiségei.

Ha másodszor az adott egyenlet a következő:

$$\gamma_1\xi_1+\cdots+\gamma_l\xi_l=\gamma$$

és γ az 1-től különböző, akkor ennek az egyenletnek megoldásai megvannak a

$$\gamma_1\xi_1+\cdots+\gamma_l\xi_l-\gamma\eta=0$$

egyenlet megoldásai között; még pedig oly módon, hogy az utóbbi egyenlet minden olyan megoldása, a melyben $\eta=1$, az adott egyenlet egyik megoldását szolgáltatja és viszont. Ámde az utóbbi egyenlet általános megoldásában η alakja a következő:

$$\eta=\mu_1\eta_1+\cdots+\mu_r\eta_r$$

és így tehát még csak a μ mennyiségeket kell a

$$\mu_1\eta_1+\cdots+\mu_r\eta_r=1$$

feltételnek megfelelőleg meghatároznunk. Ebből a μ-ket az (5)-höz hasonló szerkezetű kifejezések alakjában nyerjük és az egyenlet általános megoldása:

$$\xi_j=\xi'_{j0}+\nu_1\xi'_{j1}+\cdots+\nu_s\xi'_{js}, \qquad (j=1,\ldots,l) \qquad (6)$$

a hol a ν-k ismét a Γ tartomány tetszés szerinti mennyiségei.

Hogy most már a (II) diophantikus rendszer általános megoldása szintén véges számú lépésben állítható elő, egyszerű módon kimutatható a k-ról $k-1$-re való átmenettel. Ha ugyanis a (II) első egyenletének

$$\sum_{j=1}^{l}\gamma_{1j}\xi_j=\gamma_{10}$$

általános megoldását a (6) alakban előállítottuk, akkor ezt az előállítást a többi egyenletbe a ξ_j-k helyébe téve, a ν_j

mennyiségekre vonatkozó szükséges és elegendő feltételeket nyerjük, a melyek e mennyiségek meghatározására egyenesen $k-1$ lineáris diophantikus egyenletből álló rendszert szolgáltatnak. Ezt ily módon folytatva, végre egy egyenlethez és (II) megoldásainak végleges előállításához jutunk, a melynek ismét a (6)-ban jellemzett alakja van.

Modulusrendszerek vagy osztórendszerek.

2. §. Mielőtt a felállított probléma megoldásának menetét tovább követnők, még egy ahhoz csatlakozó fogalommal kell megismerkednünk, a mely az algebrai mennyiségek elméletében alapvető jelentőségű. Ép ezért legjobbnak tartjuk, ha ezt a fogalmat mindjárt elejétől fogva felhasználjuk az ide tartozó eredmények fogalmazásában.

Ha az $X_1, \ldots, X_l$ mennyiségek meghatározásától eltekintünk, akkor azt a tényt, hogy az

$$F = F_1 X_1 + \cdots + F_l X_l$$

diophantikus egyenletnek az $[A, x_1, \ldots, x_m]$ formatartományban van megoldása, kifejezhetjük az

$$F \equiv 0 \pmod{F_1, \ldots, F_l}$$

congruentiával is, a hol természetesen az a formatartomány, a melyre nézve ezt a tényállást megállapítjuk, egyszer mindenkorra adva van*.

Ha $l=1$, ez az állítás egyszerűen azt fejezi ki, hogy F az $[A, x_1, \ldots, x_m]$ tartományban osztható F_1-gyel. Az általá-

* Hogy e kijelentés helyessége ama tartomány választásától függ, az már igen egyszerű példán is igazolható. Így pl. a raczionális formák tartományában

$$1 \equiv 0 \pmod{x+2, x+4};$$

de ugyanaz az állítás a raczionális és egész formák tartományában helytelen.

nos esetben tehát *az oszthatóság fogalmának bővítésével* van dolgunk, a hol az F_1 osztó, vagyis egytagú modulus helyébe az l-tagú $(F_1, \ldots, F_l)$ modulusrendszer lép, a melyet ebben a felfogásban KRONECKER* szerint osztórendszernek is nevezünk.

Ezt az analogiát tovább fűzve, végre F-nek az

$$F \equiv 0 \pmod{F_1, \ldots, F_l}$$

congruentiával megadott tulajdonságát még úgy fejezzük ki, hogy *F tartalmazza az $(F_1, \ldots, F_l)$ modulusrendszert (osztórendszert)***.

E kifejezésmód természetszerű bővítése a következő meghatározásokhoz vezet:

I. *Az $(M_1, \ldots, M_h)$ modulusrendszer (osztórendszer) tartalmazza az $(N_1, \ldots, N_g)$ modulusrendszert, ha az első modulusrendszer minden eleme tartalmazza a második modulusrendszert;* azaz a congruentia jelölését használva, ha

$$M_i \equiv 0 \pmod{N_1, \ldots, N_g}. \qquad (i=1, \ldots, h)$$

II. *Két modulusrendszer (osztórendszer) aequivalens, ha mindegyikük tartalmazza a másikat.* Ennek jelölésére szolgáljon:

$$(M_1, \ldots, M_h) \simeq (N_1, \ldots, N_g).$$

A $h=1$, $g=1$ esetben azután a $\simeq$ jel jelentése pontosan ugyanaz, mint az előbb használt $\sim$ jelé.

Ebből közvetetlenül nyerjük a következő egyszerű tételt: *Ha M tartalmazza az $(M_1, \ldots, M_h)$ modulusrendszert, akkor*

$$(M_1, \ldots, M_h) \simeq (M, M_1, \ldots, M_h).$$

* KRONECKER «Festschrift» 20. §.

** A $\sqrt{-5}$ tartomány példája, a melyet az I. fejezetben tárgyaltunk, különösen pedig az ottani 9. § mutatja, hogy bizonyos tények kifejezésére már akkor is szükséges ez a fogalom-alkotás, midőn az A tartományban maradunk, a nélkül, hogy ahhoz új határozatlanokat csatolnánk hozzá, vagyis midőn az $F, F_1, \ldots, F_l$ mennyiségek mindannyian az A tartomány mennyiségei.

Valódi modulusrendszer az olyan, a melyet az absolut egység nem tartalmaz; a melyre nézve tehát nem érvényes az $(M_1, \ldots, M_h) \simeq 1$ æquivalentia. Minden valódi modulusrendszer e szerint valódi congruentiatartományt határoz meg (I. fej. 10. §).

Még a legnagyobb közös osztó fogalmát is át kell vinnünk a modulus- vagy osztórendszerre. (Most, midőn a vonatkozás a congruentiatartományra háttérbe lép és inkább azokkal a tulajdonságokkal lesz dolgunk, a melyek magukban a rendszerekben mutatkoznak, főleg az osztórendszer elnevezést használjuk.) Ez a következő megállapodással történik:

III. *Az* $(M_1, \ldots, M_h, N_1, \ldots, N_g)$ *osztórendszert az* $(M_1, \ldots, M_h)$ és $(N_1, \ldots, N_g)$ *osztórendszerek legnagyobb közös tartalmának nevezzük,* a melyet az a tulajdonság jellemez, hogy az oly osztórendszert, a melyet az első osztórendszer tartalmaz, egyszersmind a második és harmadik osztórendszer is tartalmazza, valamint megfordítva is. Ezen állítás helyessége a megfelelő meghatározásokból közvetetlenül kitünik. Minden osztórendszer, a melynek megvan az épen kimondott tulajdonsága, szükségképen $\simeq (M_1, \ldots, M_h, N_1, \ldots, N_g)$, mert ezt az osztórendszert tartalmazza és viszont ez tartalmazza amazt. Két osztórendszer legnagyobb közös tartalma tehát a most előadott æquivalentia-meghatározás szerint egyértelműleg van megadva.

IV. *Két osztórendszerről,* $(M_1, \ldots, M_h)$ és $(N_1, \ldots, N_g)$*-ről végre azt mondjuk, hogy relativ törzs-osztórendszerek, ha legnagyobb közös tartalmuk,* $(M_1, \ldots, M_h, N_1, \ldots, N_g) \simeq 1$.

Hogy a fogalmakat — különösen képleteinkben — erősebben kiemeljük, czélszerűnek mutatkozott a $\simeq$ jel bevezetése. Ez szűkebb æquivalentia jelölésére szolgál, mint a milyent az előbb használt $\sim$ jellel jelöltünk. Következetesen

ragaszkodva az utóbbi jel eddigi jelentéséhez,

$$(M_1, \ldots, M_h) \sim (N_1, \ldots, N_g)$$

kifejezi, hogy az $M_1, \ldots, M_h$ mennyiségek minden közös osztója egyszersmind az $N_1, \ldots, N_g$ mennyiségeknek is közös osztója és viszont; ez pedig megtörténhetik a nélkül is, hogy

$$(M_1, \ldots, M_h) \simeq (N_1, \ldots, N_g)$$

volna. Igy pl. a raczionális és egész formák tartományában

$$(x+2, x+4) \sim 1$$

a nélkül, hogy

$$(x+2, x+4) \simeq 1;$$

mert nincsenek olyan A és B formák, a melyekre nézve

$$A(x+2)+B(x+4)=1.$$

Ennek egyszerű oka az, hogy $x+2$ és $x+4$ az $(x, 2)$ kéttagú osztórendszert tartalmazzák, 1 pedig ezt nem tartalmazza.

Az $\simeq$ jel — a mint közvetetlenül látni — kifejezi, hogy mindazokat az osztórendszereket, a melyeket $M_1, \ldots, M_h$ tartalmaz, tartalmazza egyszersmind $N_1, \ldots, N_g$ is és viszont; ha pedig az $\sim$ jelt alkalmazzuk, ez csak a közönséges osztókra (egytagú osztórendszerekre) áll.

Ha az $\sim$ jel használatát csak magában álló mennyiségekre szorítanók, akkor e különbség elesnék; mert az, hogy $M \sim N$, már ugyanannyit mond, mint $M \simeq N$.

De épen nem jelentéktelen dolog, hogy e szűkebb és bővebb æquivalentiát ezentúl még jelöléseinkben is megkülönböztethetjük; különben már a legnagyobb közös osztó előbb használt egyszerű jelölésével is ellenkezésbe jutnánk.

A hol a szövegben ezentúl egyszerűen aequivalens osztórendszerekről lesz szó, mindig a $\simeq$ értelmezte aequivalentia értendő.

3. §. Ha az osztórendszerek között bizonyos törvény-

szerű kapcsolatot létesítünk, akkor azon osztórendszerek összességét, a melyeket az $[A, x_1, \ldots, x_m]$ tartomány mennyiségeiből alkothatunk, ismét «tartomány»-ba foglaljuk össze: *az* $[A, x_1, \ldots, x_m]$ *tartománynak osztó-tartományába.* E kapcsolás, az ú. n. *compositio* törvénye, egyszerűen az legyen, hogy *az*

$$(\ldots, M_i, \ldots)_{(i=1,\ldots,h)} \quad \text{és} \quad (\ldots, N_j, \ldots)_{(j=1,\ldots,g)}$$

osztórendszerekből egy harmadik, az

$$(\ldots, M_i N_j, \ldots)_{(i=1,\ldots,h;\, j=1,\ldots,g)}$$

jellemezte osztórendszer alkotandó.

Az utóbbi rendszerről azt mondjuk, hogy *az előbbi kettőből össze van téve vagy componálva;* amaz előbbi rendszerek *a compositio tényezői*, vagy pedig (az egytagú rendszerek szorzásával fönnálló szembetünő analogia miatt) röviden az utóbbi rendszer tényezői, a melyet ennek megfelelőleg az első két rendszer *szorzatának* is nevezünk.

A compositio értelmezése, mint æquivalentia az

$$(\ldots, M_i, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, M_i N_j, \ldots)_{(i=1,\ldots,h;\, j=1,\ldots,g)}$$

alakban is írható, a hol a componálandó rendszereket egyszerűen egymás mellé írjuk. Ezen irásmód jogosúlt volta egyszerűen abból a tényből következik, hogy a compositiónál æquivalens rendszerek egymást teljesen helyettesíthetik. Ennek kifejezése a következő közvetetlenül belátható tétel: Abból, hogy

$$(M_1, \ldots, M_h) \simeq (M'_1, \ldots, M'_{h'}),$$

mindig következik, hogy

$$(\ldots M_i N_j, \ldots) \simeq (\ldots, M'_{i'} N_j, \ldots)._{(i=1,\ldots,h;\, i'=1,\ldots,h';\, j=1,\ldots,g)}$$

Értelmezése szerint a compositióra érvényes a commutativ elv ép úgy, mint a szorzásra, a melybe ez az új kapcsolat átmegy, ha $h=1$ és $g=1$.

E meghatározások a következő, egyszerűsége mellett is fontos tételre vezetnek:

Ha valamely osztórendszer úgy az $(M_1, \ldots, M_h)$, *mint az* $(N_1, \ldots, N_g)$ *osztórendszert tartalmazza és ezek relativ törzsosztórendszerek, akkor amaz osztórendszer ezeknek szorzatát is tartalmazza.*

Nyilvánvaló, hogy e tételt csak egytagú F osztórendszerre kell bebizonyítanunk. Hogy ama rendszerek relativ törzsosztórendszerek, azaz

$$(M_1, \ldots, M_h, N_1, \ldots, N_g) \simeq 1,$$

az részletesen kiírva annyit jelent, hogy vannak az $[A, x_1, \ldots, x_m]$ tartományban olyan U_i, V_j mennyiségek, a melyekre nézve

$$\sum_{i=1}^{h} M_i U_i + \sum_{j=1}^{g} N_j V_j = 1.$$

Másrészt, ha G_i, H_j ismét az $[A, x_1, \ldots, x_m]$ tartomány mennyiségei, akkor

$$F = \sum_{i=1}^{h} G_i M_i = \sum_{j=1}^{g} H_j N_j$$

és így

$$N_j F = \sum_{i=1}^{h} G_i M_i N_j, \qquad (j=1, \ldots, g)$$

$$M_i F = \sum_{j=1}^{g} H_j M_i N_j. \qquad (i=1, \ldots, h)$$

Ha tehát rendre V_j, U_i-vel szorzunk és azután összeadunk, akkor

$$F = 0 \ (\text{mod.} \ldots, M_i N_j, \ldots).$$

Ebből jelesen még a következő speciális tétel foly:

Ha $(M_1, N_1) \simeq 1$, *akkor egyszersmind*

$$(M_1 N_1, M_2, \ldots, M_h) \simeq (M_1, M_2, \ldots, M_h)(N_1, M_2, \ldots, M_h).$$

Hogy a bal oldalon álló osztórendszer a jobb oldalon álló szorzatot tartalmazza, az épen bebizonyított tételnek következménye. Az ugyanis szembetünő, hogy a két tényezőt

tartalmazza és ezek M_1 és N_1-gyel egy időben relativ törzsosztórendszerek; hogy pedig megfordítva a jobb oldalon álló szorzat amaz osztórendszert is tartalmazza, ép oly könnyen belátható. A szorzat alakjában adott osztórendszer elemei $M_1 N_1$ és továbbá csupán csak $M_2, M_3, \ldots$, vagy M_h-val osztható mennyiségek.

Tovább követve a közönséges oszthatóság tételeivel fönnálló analogiát, még a következő tételhez jutunk:

Ha az $(N_1, \ldots, N_g)$ *osztórendszernek nem minden eleme* 0 *és*

$$(\ldots, M_i, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, M'_{i'}, \ldots)(\ldots, N_j, \ldots),$$
$$(i=1, \ldots, h;\ i'=1, \ldots, h';\ j=1, \ldots, g)$$

akkor az $(\ldots, M_i^g, \ldots)$ *osztórendszer tartalmazza a* $(\ldots, M'_{i'}, \ldots)$ *osztórendszert és egyszersmind a* $(\ldots, M_{i'}^{\prime g}, \ldots)$ *osztórendszer is tartalmazza az* $(\ldots, M_i, \ldots)$ *osztórendszert.*

A feltevés szerint ugyanis

$$M_i N_s = \sum_{j=1}^{g} L_{ij}^{(s)} N_j, \qquad (s=1, \ldots, g)$$

és ebben az $L_{ij}^{(s)}$-k a M'-ek lineáris formái; továbbá pedig

$$\sum_{j=1}^{g} (L_{ij}^{(s)} - \delta_{sj} M_i) N_j = 0,$$

a hol, mint már ismételten, $\delta_{sj}=1$, ha $s=j$ és $\delta_{sj}=0$, ha $s \neq j$. Minthogy azonban az N_j-k nem mindannyian 0-sal egyenlők, még

$$|L_{ij}^{(s)} - \delta_{sj} M_i|_{(j, s=1, \ldots; g)} = 0,$$

és ebből valóban következik, hogy

$$M_i^g \equiv 0 \ (\text{mod.} \ldots, M'_{i'}, \ldots).$$

Teljesen azonos módon következik az is, hogy

$$M_{i'}^{\prime g} \equiv 0 \ (\text{mod.} \ldots, M_i, \ldots).$$

Különösen kiemelendő még a következő speciális eset:

Ha az $(N_1, \ldots, N_g)$ *osztórendszernek nem minden eleme* 0 *és*

$$(\ldots, M_i, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, N_j, \ldots),$$

akkor egyszersmind

$$(\ldots, M_i, \ldots) \simeq 1.$$

Az épen bebizonyított általános tétel szerint az 1 tartalmazza az $(\ldots, M_i, \ldots)$ osztórendszert és magától értetődik, hogy viszont ez az osztórendszer tartalmazza az 1 «osztórendszer-t»; tehát valóban

$$(\ldots, M_i, \ldots) \simeq 1.$$

Hogy az általános tétel megállapította feltevésekből *épen nem következik*, hogy

$$(\ldots, M_i, \ldots) \simeq (\ldots, M_i', \ldots),$$

nagyon is figyelemre méltó tény, a mely megérdemli, hogy egyszerű példával megvilágítsuk.

Az $[A, x, y]$ formatartományban, a mely valamely tetszés szerinti holoid A tartományból származik,

$$(x^2, y^2)(x, y) \simeq (x^3, x^2y, xy^2, y^3)$$
$$(x^2, xy, y^2)(x, y) \simeq (x^3, x^2y, xy^2, y^3);$$

de azért az

$$(x^2, y^2) \quad \text{és} \quad (x^2, xy, y^2)$$

osztórendszerek *mégsem aequivalensek,* mert — a mint szembetünő — az

$$xy \equiv 0 \pmod{x^2, y^2}$$

congruentia lehetetlen. Az általános tétel értelmében azonban (x^2, xy, y^2)-et tartalmazza az (x^4, y^4) és (x^2, y^2)-et az (x^4, x^2y^2, y^4).

4. §. Hogy az analogia, a mely az osztórendszerek és közönséges osztók (egytagú osztórendszerek) elmélete közt fennáll, ilyen módon megszakad, lényegében e rendszerek olyan tulajdonságán fordúl meg, a mely az épen említett legegyszerűbb esetben még nem mutatkozik.

Lehetséges ugyanis, hogy $(M_1, \ldots, M_h)$ *az* $(N_1, \ldots, N_g)$

osztórendszert tartalmazza és még sem állítható elő mint ezen utóbbi és valamely harmadik $(N_1', \ldots, N_{g'}')$ *osztórendszer szorzata.* A «tartalmazás» fogalma tehát jóval bővebb, mint az «oszthatóság» fogalma. Ezt már egyszerű példán is láthatjuk. Közvetetlenül belátható, hogy (x^2, y^2) az (x, y) osztórendszert tartalmazza; de azért még sincsenek olyan $X_1, \ldots, X_k$ formák, a melyekre nézve

$$(x^2, y^2) \simeq (x, y)(X_1, \ldots, X_k).$$

Az eredményt mindjárt általánosabban fogalmazva, kimutatjuk, hogy az (x^2, y^2) osztórendszernek egyáltalában nincsen «valódi» felbontása. Ha ugyanis

$$(x^2, y^2) \simeq (X_1, \ldots, X_k)(Y_1, \ldots, Y_l),$$

akkor bebizonyítható, hogy az egyik tényező szükségképen az egységgel, a másik pedig az (x^2, y^2) rendszerrel æquivalens. Minden esetre írhatjuk, hogy

$$X_i \equiv a_i + b_i x + c_i y + d_i xy \pmod{x^2, y^2},$$
$$Y_j \equiv p_j + q_j x + r_j y + s_j xy \pmod{x^2, y^2}.$$

Hogy már most a feltevésnek megfelelőleg

$$X_i Y_j \equiv 0 \pmod{x^2, y^2}$$

legyen, szükséges, hogy egyszersmind

$$a_i p_j = 0, \qquad (i=1, \ldots, k; j=1, \ldots, l)$$

legyen; azaz, hogy vagy az $a_1, \ldots, a_k$ mennyiségek, vagy pedig a $p_1, \ldots, p_l$ mennyiségek mindannyian eltünjenek. Ha már most pl. a p mennyiségek nem mindannyian egyenlők a zérussal, akkor ismét az összes b, c és d mennyiségeknek a zérussal egyenlőknek kell lenniök, és így végre az $(X_1, \ldots, X_k)$ osztórendszer tartalmazza az (x^2, y^2) osztórendszert. Minthogy ennek megfordítottja is érvényes, azért

$$(X_1, \ldots, X_k) \simeq (x^2, y^2),$$

innen még:

$$(Y_1, \ldots, Y_l) \simeq 1.$$

Valamely osztórendszer felbonthatatlan vagy irreduci-

bilis, ha nincsen «valódi» felbontása, azaz, ha csak oly módon bontható fel két tényezőre, hogy az egyik tényező az adott rendszerrel, a másik tényező pedig ekkor az előbb bebizonyítottakhoz képest az egységgel æquivalens. A tárgyalt példa azonban mutatja, hogy *felbonthatatlan osztórendszer mégis tartalmazhat olyan osztórendszereket, a melyek sem az egységgel, sem pedig az adott osztórendszerrel nem aequivalensek.*

Valamely osztórendszer *törzsrendszer* (törzs-osztórendszer, törzs-modulusrendszer), ha bármely szorzat ezt csak akkor tartalmazhatja, ha egyik tényezője is már tartalmazza.*

Ebben az értelemben minden törzsmennyiség, ha azt egytagú osztórendszernek tekintjük, törzsrendszer; ilyen pl. az (x, y) osztórendszer is. De felbonthatatlansága mellett sem törzsrendszer (x^2, y^2), a melyet (x^2, y) (x^2, y) tartalmaz, habár az (x^2, y) tényezők — a mint közvetetlenül belátható — az (x^2, y^2) osztórendszert nem tartalmazzák.

Minden törzsrendszer irreducibilis; mert felbontása olyan szorzatot szolgáltatna, a melynek egyik tényezője már is tartalmazná ama törzsrendszert, míg természetesen az adott törzsrendszer azt a tényezőt is tartalmazza. E tényező tehát a törzsrendszerrel, a másik tényező pedig az

* A «Festschrift»-ben KRONECKER az «irreducibel» és «prim» elnevezéseket még megkülönböztetés nélkül használja felbonthatatlan rendszerek jelölésére. Az evvel járó alkalmatlanságok azonban később az élesebb megkülönböztetésre vezettek. (KRONECKER, Über einige Anwendungen der Modulsysteme auf elementare algebraische Fragen, Journal f. r. n. a. Math. XCIX. k. 337. l., Werke III. 1. k. 158. l.) A törzsrendszernek a szövegben előadott értelmezése tartalmilag megegyezik KRONECKER értelmezésével, de formailag egyszerűbb, mert nem támaszkodik a «fokozat» fogalmára.

egységgel volna æquivalens. E tétel megfordítása, mint azt már az (x^2, y^2) példája mutatja, nem helyes.

Absolut törzsrendszer végre *az olyan, a mely csakis az egységgel vagy pedig az adott rendszerrel aequivalens osztórendszereket tartalmaz*.*

A raczionális és egész formák tartományában — mint már említettük — minden $F(x_1, \ldots, x_m)$ törzsforma (egytagú) törzsrendszert szolgáltat; ez azonban, ha F legalább egy x határozatlant valóban tartalmaz, nem absolut törzsrendszer. Ekkor ugyanis az $a_1, \ldots, a_m$ raczionális és egész számok mindig meghatározhatók oly módon, hogy $F(a_1, \ldots, a_m)$ sem 0-sal, sem pedig ± 1-gyel nem egyenlő és így valamely p törzsszámmal osztható. De akkor

$$F(x_1, \ldots, x_m) = \sum_{i=1}^{m} G_i(x_i - a_i) + pc$$

és így tehát F tartalmazza az

$$(x_1 - a_1, \ldots, x_m - a_m, p)$$

* Hogy az így értelmezett $(P_1, P_2, \ldots)$ rendszer mindig törzsrendszer e szó előbb meghatározott értelmében, egyszerűen belátható, de mégis bebizonyítandó állítás.

Ha ugyanis az

$$(F_1, F_2, \ldots)(G_1, G_2, \ldots)$$

szorzat tartalmazná a $(P_1, P_2, \ldots)$ osztórendszert, akkor ezt az

$$(F_1, F_2, \ldots, P_1, P_2, \ldots)(G_1, G_2, \ldots)$$

osztórendszer is tartalmazná. Ámde $(P_1, P_2, \ldots)$ e tényezők közül az elsőt minden esetre tartalmazza és így az e rendszerre vonatkozó feltevés szerint vagy

$$(F_1, F_2, \ldots, P_1, P_2, \ldots) \simeq (P_1, P_2, \ldots)$$

és ekkor már $(F_1, F_2, \ldots)$ is tartalmazza a $(P_1, P_2, \ldots)$ rendszert, vagy pedig

$$(F_1, F_2, \ldots, P_1, P_2, \ldots) \simeq 1,$$

a midőn a másik tényező, $(G_1, G_2, \ldots)$ tartalmazza a $(P_1, P_2, \ldots)$ rendszert.

osztórendszert, a mely sem nem $\simeq 1$, sem pedig $\simeq F$. A második esetben ugyanis p-nek oszthatónak kellene lennie F-fel; de ez nem lehetséges. Az első esetben pedig olyan $H_0, H_1, \ldots, H_m$ formáknak kellene létezniök, a melyekre nézve

$$\sum_{i=1}^{m} H_i(x_i - a_i) + H_0 p = 1$$

és ez az azonosság még akkor is helyes maradna, ha $x_i = a_i$ és ekkor azt szolgáltatná, hogy 1 osztható p-vel. Így tehát ez a feltevés is képtelenségre vezet.

Ellenben minden orthoid (A) tartományból származó $[A, x_1, \ldots, x_m]$ formatartományban az $(x_1 - a_1, \ldots, x_m - a_m)$ osztórendszer, a hol $a_1, \ldots, a_m$ az (A) tartomány mennyiségei, absolut törzsrendszer. Ha ugyanis ama rendszer az $(X_1, \ldots, X_k)$ rendszert tartalmazza, akkor minden esetre

$$X_i \equiv c_i \,(\text{mod. } x_1 - a_1, \ldots, x_m - a_m)$$

lévén, ha $(X_1, \ldots, X_k)$ nem æquivalens az adott rendszerrel, legalább egy c_i-nek a 0-tól különbözőnek kell lennie, mert különben minden i-re nézve $X_i \equiv 0 \,(\text{mod. } x_1 - a_1, \ldots, x_m - a_m)$ volna; tehát a két rendszer valóban tartalmazná egymást és így

$$(X_1, \ldots, X_k) \simeq (x_1 - a_1, \ldots, x_m - a_m)$$

lenne. Ha azonban c_i a zérustól különböző, akkor

$$c_i \equiv 0 \,(\text{mod. } X_i, x_1 - a_1, \ldots, x_m - a_m);$$

tehát egyszersmind

$$c_i \equiv 0 \,(\text{mod. } X_1, \ldots, X_k)$$

és, minthogy orthoid tartományban c_i-vel oszthatunk, végre

$$1 \equiv 0 \,(\text{mod. } X_1, \ldots, X_k),$$

azaz

$$(X_1, \ldots, X_k) \simeq 1.$$

Véges osztó-lánczok.

5. §. Hogy az algebrai mennyiségek elméletében fellépő tartományok diophantikus tartományok, azon általános tulajdonságukból következik, a melyet majd most részletesen kifejtünk.

Legyen A valamely (valódi vagy nem valódi) holoid tartomány,

$$(S_1), (S_2), \ldots, (S_k), \ldots$$

pedig legyen az osztórendszerek olyan határtalan sorozata, a melyeknek elemei az A tartomány mennyiségei. Ezen kivül még azt a feltételt szabjuk, hogy minden egyes (S_k) osztórendszert a megelőző (S_{k-1}) osztórendszer tartalmazza.

Az osztórendszerek ilyen sorozatát röviden *osztó-lánczoknak* mondjuk és *végesnek* nevezzük az $(S_1), (S_2), \ldots, (S_r), \ldots$ osztó-lánczot akkor, ha olyan pozitiv egész számot, r-t jelölhetünk ki, hogy, ha a bármely positiv egész szám, mindig $(S_{r+a}) \simeq (S_r)$.

Ha $(S_k) \simeq (G_1, \ldots, G_c)$, akkor, minthogy a feltevés szerint (S_k) tartalmazza (S_{k+1})-et, ez minden esetre a

$$(G_1, \ldots, G_c, G_{c+1}, \ldots, G_d)$$

alakban írható és azután (S_k) és (S_{k+1}) közé iktathatjuk (interpoláljuk) a további

$$((S_k), G_{c+1}), ((S_k), G_{c+1}, G_{c+2}), \ldots, ((S_k), G_{c+1}, \ldots, G_{d-1})$$

rendszereket. Ha ezt mindenütt megteszszük, akkor, minthogy (S_1) elé mindig még $S_0 = 0$-t is tehetünk, bizonyos specziális alakú

$$F_1, (F_1, F_2), (F_1, F_2, F_3, \ldots), \ldots$$

osztó-lánczot nyerünk és magától értetődik, hogy ez akkor és csak akkor véges, ha az adott osztó-láncz is ilyen.

Vannak tartományok, a melyekben minden osztó-láncz véges. Így lesz az mindig, ha A orthoid tartomány; mert

hiszen ilyen tartományban minden a 0-tól különböző mennyiség æquivalens az egységgel.

Ugyanaz a tulajdonsága megvan az [1] tartománynak is. Ebben az esetben minden osztórendszer, $(S_k) \simeq d_k$, hol d_k valamely meghatározott pozitiv egész szám, és, minthogy (S_{k-1}) tartalmazza (S_k)-t, $d_k \leq d_{k-1}$. Igy tehát sohasem növekedő pozitiv egész számok bizonyos

$$d_1, d_2, d_3, \ldots$$

sorozata keletkezik és, ha e számok közül a legkisebb d_k, akkor okvetetlenül $(S_k) \simeq (S_{k+1}) \simeq (S_{k+2})$ stb.

Az idevágó alapvető tétel a következő:

Ha minden az A *tartomány mennyiségeiből alkotott osztó-láncz véges, akkor ugyanez áll az* A*-ból származó és m határozatlant tartalmazó formák tartományáról,* $[A, x_1, \ldots, x_m]$*-ről is.*

Minthogy a feltevés szerint a tétel $m=0$ esetében helyes, annak általános érvényességét az $m-1$-ről m-re való következtetés segítségével bizonyíthatjuk be.

Másrészt azonban az előbbi fejtegetések szerint olyan speciális osztó-lánczokra szorítkozhatunk, a melyekben

$$(S_k) \simeq (F_1, \ldots, F_k)$$

és végre még a formák $F_1, F_2, \ldots$ sorozatát is bizonyos «legegyszerűbb» alakra hozhatjuk. Közvetetlenül világos ugyanis, hogy F_r helyébe minden olyan F_r' forma tehető, a melyre nézve

$$F_r' \equiv F_r \,(\text{mod. } F_1, \ldots, F_{r-1}).$$

Ennek megfelelőleg F_r helyébe majd azt a G_r formát teszszük, a mely az F_r-rel mod. $(F_1, \ldots, F_{r-1})$ congruens formák között x_m-re vonatkozólag a lehetőleg legalacsonyabb fokú. Ha $F_r \equiv 0 \,(\text{mod. } F_1, \ldots, F_{r-1})$, akkor magától értetődik, hogy F_r az osztó-láncz alkotásánál egészen elhagyható. Az ezek

szerint legegyszerűbb alakjában felírt

$$\ldots, (G_1, G_2, \ldots, G_k), \ldots \qquad (k=1, 2, 3, \ldots)$$

osztó-láncznak azonban a végesben teljesen meg kell szakadnia; azaz bizonyos meghatározott k-tól kezdve $G_{k+1}=0$, $G_{k+2}=0, \ldots$ Ha ezt az épen állított tényt bebizonyítjuk, avval természetesen tételünk is közvetetlenül nyilvánvalóvá lesz.

Először is kimutatjuk, hogy a $G_1, G_2, \ldots$ formák sorozata csak véges számmal tartalmazhat olyan formákat, a melyek x_m-re vonatkozólag meghatározott, pl. n-ed fokúak. Legyen ugyanis

$$G'_1, G'_2, \ldots$$

az ilyen formák határtalan sorozata és e szerint

$$G'_r = \alpha_r x_m^n + \cdots,$$

a hol α_r az $x_1, \ldots, x_{m-1}$ határozatlanoknak az A-ból származó formája. Minthogy azonban tételünk $m-1$ határozatlannak az A-ból származó formáira nézve érvényes, az

$$\alpha_1, \alpha_2, \ldots, \alpha_l, \ldots$$

sorozatnak megfelelőleg van olyan pozitiv egész szám r, hogy

$$\alpha_{r+a} \equiv 0 \,(\text{mod. } \alpha_1, \ldots, \alpha_r),$$

bármely pozitiv egész számot jelentsen is a. Jelesen, ha

$$\alpha_{r+a} = \beta_{1a}\alpha_1 + \beta_{2a}\alpha_2 + \cdots + \beta_{ra}\alpha_r,$$

akkor

$$G'_{r+a} \equiv G'_{r+a} - \beta_{1a}G'_1 - \beta_{2a}G'_2 - \cdots - \beta_{ra}G'_r \,(\text{mod. } G'_1, \ldots, G'_r)$$

és abból, hogy a jobb oldalon álló formának x_m-re vonatkozó foka *nem* éri el n-t, az következnek, hogy G'_{r+a} még nem volt a feltételezett «legegyszerűbb» alakra hozva. Ha ez megtörtént, akkor a $G_1, G_2, \ldots$ sorozatban álló x_m-re vonatkozólag n-edfokú formák száma szükségképen véges lesz.

Ugyane feltevések mellett azonban a $G_1, G_2, \ldots$ formáknak

x_m-re vonatkozó foka bizonyos meghatározott pozitiv egész számot, N-t nem haladhat túl. Ha ennek ellenkezője történnék, a $G_1, G_2, \ldots$ sorozatból kiválaszthatnók a formáknak olyan végtelen

$$G'_{n_1}, G'_{n_2}, G'_{n_3}, \ldots$$

sorozatát, a melyben G'_{n_r}-nek x_m-re vonatkozó foka n_r és $n_1, n_2, n_3, \ldots$ növekedő positiv egész számoknak végtelen sorozata. E mellett G'_{n_r} a következő specziális alakú volna:

$$G'_{n_r} = \alpha_r x_m^{n_r} + \cdots,$$

a hol

$$\alpha_1, \alpha_2, \ldots, \alpha_l, \ldots$$

ismét az $x_1, x_2, \ldots, x_{m-1}$, számra nézve $m-1$ határozatlannak az A tartományból származó formái és most is okvetetlenül léteznék olyan meghatározott pozitiv egész szám, r, hogy

$$\alpha_{r+a} \equiv 0 \,(\text{mod. } \alpha_1, \alpha_2, \ldots, \alpha_r),$$

bármely pozitiv egész számot jelentsen is a. Ha részletesen írva

$$\alpha_{r+a} = \beta_{1a}\alpha_1 + \beta_{2a}\alpha_2 + \cdots + \beta_{ra}\alpha_r,$$

akkor

$$G'_{n_{r+a}} \equiv G'_{n_{r+a}} - \beta_{1a} x_m^{n_{r+a}-n_1} G'_{n_1} - \cdots - \\ - \beta_{ra} x_m^{n_{r+a}-n_r} G'_{n_r} (\text{mod. } G'_{n_1}, \ldots, G'_{n_r})$$

lenne és, minthogy a jobb oldalon álló formának x_m-re vonatkozó foka nem éri el n_{r+a}-t, ebből ismét az következnék, hogy $G'_{n_{r+a}}$ a feltevés ellenére nincsen a «legegyszerűbb» alakra hozva. Ha ez megtörtént, akkor a formák fokainak száma, valamint a minden fokhoz tartozó formák száma is csak véges lehet és így tehát egyáltalában csakis véges számú a 0-tól különböző G forma van. Evvel tehát a felállított tétel be van bizonyítva.

Jelesen bármely orthoid formatartományban, valamint

akárhány határozatlan raczionális és egész formáinak tartományában minden osztó-láncz véges.

Ebből közvetetlenül foly a következő tétel, a melyet a homogén formákra való egészen lényegtelen megszorítással legelőször HILBERT* állított fel:

Az orthoid formák bármely sokaságából, vagy pedig a raczionális és egész formák bármely sokaságából is mindig kiválaszthatók véges számmal olyan $F_1, F_2, \ldots F_k$ *formák, hogy a sokaság minden más formája a* $\sum_{i=1}^{k} H_i F_i$ *alakban állítható elő, a hol* $H_1, H_2, \ldots H_k$ *ismét orthoid, ill. raczionális és egész formák.*

Ha ez nem történhetnék, akkor a formáknak olyan határtalan

$$F_1, F_2, \ldots, F_r, \ldots$$

sorozatát találhatnók, hogy az $F_r \equiv 0 (\text{mod. } F_1, \ldots, F_{r-1})$ congruentia sohasem állhatna fenn, a mi az imént bebizonyított tétel szerint lehetetlen.

6. §. Az osztó-lánczok véges voltát az $[(A), x_1, \ldots, x_m]$ és $[[1], x_1, \ldots, x_m]$ tartományokban — és ezt különösen hangsúlyozandónak tartjuk — csak existentia-bizonyítással mutattuk ki; de azért ennek a mi czéljainkra mégis egyenesen alapvető fontossága van.

Közvetetlenül következik belőle, hogy *az* $[(A), x_1, \ldots, x_m]$ *és* $[[1], x_1, \ldots, x_m]$ *tartományok csakugyan diophantikus tartományok.*

* «Über die Theorie der algebraischen Formen». (Math. Annalen XXXVI. k. 473. l.). Raczionális formákra vonatkozó új bizonyítását GORDAN adta (Göttinger Nachrichten 1899, 240. l.). Az osztórendszerek elmélete a tétel tartalmának fentebbi egyszerű kifejezését szolgáltatja és evvel együtt az itt előadott lényegesen rövidebb és átlátszóbb bizonyítását.

A
$$\sum_{i=1}^{l} F_i X_i = 0$$
diophantikus egyenlet bármely $\xi_1, \xi_2, \ldots, \xi_l$ megoldásából a megfelelő
$$\xi = \xi_1 u_1 + \xi_2 u_2 + \cdots + \xi_l u_l$$
forma keletkezik, a hol $u_1, u_2, \ldots, u_l$ új határozatlanokat jelentenek. Az épen bebizonyított tételt a formák e sokaságára alkalmazva, azt nyerjük, hogy ebben véges számmal olyan
$$\xi^{(j)} = \xi_{1j} u_1 + \cdots + \xi_{lj} u_l \qquad (j=1, \ldots, k)$$
formák vannak, melyeknek segítségével a ξ sokaság minden formája a
$$\xi = \alpha_1 \xi^{(1)} + \cdots + \alpha_k \xi^{(k)}$$
alakban állítható elő, a hol $\alpha_1, \ldots, \alpha_k$ ismét az $x_1, \ldots, x_m, u_1, \ldots, u_l$ határozatlanoknak az (A), ill. [1] tartományból származó formái. Minthogy azonban a ξ-k az u-knak homogén, lineáris formái, szükséges, hogy már
$$\xi = \alpha_{10} \xi^{(1)} + \cdots + \alpha_{k0} \xi^{(k)}$$
és így tehát
$$\xi_i = \alpha_{10} \xi_{i1} + \cdots + \alpha_{k0} \xi_{ik} \qquad (i=1, \ldots, l)$$
legyen, a hol α_{j0} az α_j formának az u-któl ment tagját jelenti; és épen ez az, a mit be kellett bizonyítanunk.

Evvel kapcsolatban mindjárt megjegyezzük, hogy a következtetés e módja szóról-szóra alkalmazható még akkor is, ha a
$$\Sigma F_i X_i \equiv 0 \,(\text{mod. } G_1, G_2, \ldots)$$
congruentiával van dolgunk. Tehát *az ilyen congruentia megoldásai is véges sereget alkotnak.*

Itt is — legalább egyelőre — még csak existentia-bizonyítással van dolgunk és tulajdonképeni feladatunk, — hogy e sereget az algebrai, ill. arithmetikai műveletek véges sorában valóban előállítsuk, — evvel még nincsen meg-

oldva. Épen erre a problémára nézve fontos a főtételünkből levonható most következő folyomány.

7. §. *Legyenek*

$$F_1, F_2, \ldots, F_k$$

az $x_1, x_2, \ldots, x_m$ *határozatlanoknak olyan formái, a melyeknek együtthatói az* $[(A), z_1, \ldots, z_r]$, *ill. az* $[[1], z_1, \ldots, z_r]$ *tartományból származnak. Legyen már most adva az* $[(A), x_1, \ldots, x_m, z_1, \ldots, z_r]$, *ill.* $[[1], x_1, \ldots, x_m, z_1, \ldots, z_r]$ *tartomány olyan tulajdonságú G formáinak különben bármilyen sokasága, hogy minden G-nek megfelelőleg meghatározható egy az* $[(A), z_1, \ldots, z_r]$, *ill.* $[[1], z_1, \ldots, z_r]$ *tartományhoz tartozó, a G-vel különben változó H forma, a melyre nézve*

$$HG \equiv 0 \pmod{F_1, \ldots, F_k};$$

akkor van az $[(A), z_1, \ldots, z_r]$, *ill.* $[[1], z_1, \ldots, z_r]$ *tartományban olyan K forma is, hogy ama sokaság minden G formájára nézve*

$$KG \equiv 0 \pmod{F_1, \ldots, F_k}.$$

Ha e sokaság G formáira ismét az 5. § végső tételét alkalmazzuk, akkor véges számmal találunk abban olyan $G_1, G_2, \ldots, G_s$ formákat, hogy

$$G = \sum_{i=1}^{s} T_i G_i.$$

Ha tehát $H_1, \ldots, H_s$ azok a formák, a melyekre nézve

$$H_i G_i \equiv 0 \pmod{F_1, \ldots, F_k},$$

akkor, ha

$$K = H_1 H_2 \ldots H_s,$$

ez a K forma okvetetlenül olyan tulajdonságú, hogy az adott sokaság minden G formájára nézve:

$$KG \equiv 0 \pmod{F_1, \ldots, F_k}.$$

Ha most továbbá F_i *az* $x_1, \ldots, x_{i-1}$ *határozatlanokat nem tartalmazza és* x_i *hatványai szerint rendezve* $Z_i x_i^{n_i} + \cdots$ *alakú, a hol* Z_i *az x határozatlanok egyikét sem tartalmazza, ha továbbá* Dscr. $\binom{F_1, \ldots, F_k}{x_1, \ldots, x_k}$ *a zérustól különböző; akkor*

ama K forma a megfelelő tartomány lineáris diophantikus egyenleteinek megoldása után szintén véges számú lépésben meghatározható.

Ha feltételezzük, hogy van olyan az x-eket nem tartalmazó H forma, a melyre nézve

$$HG \equiv 0 \,(\text{mod. } F_1, \ldots, F_k),$$

akkor G az $x_1, \ldots, x_k$ minden olyan értékrendszerére nézve, a mely az $F_1 = 0, \ldots, F_k = 0$ egyenleteket kielégíti, eltünik. Alkalmazva a közönséges osztási eljárást, a

$$G = F_1 Q_1 + R_1,$$
$$R_1 = F_2 Q_2 + R_2,$$
$$\ldots\ldots$$

egyenlőségeket nyerjük, melyekből

$$G = F_1 Q_1 + F_2 Q_2 + \cdots + F_k Q_k + R_{k+1},$$

a hol azonban R_{k+1} szükségképen a zérussal azonosan egyenlő, mert x_i-re vonatkozó foka nem éri el az n_i-t és mégis eltünik arra az $n_1 \ldots n_k$ különböző értékrendszerre nézve, a mely az $F_1 = 0, \ldots, F_k = 0$ egyenleteket kielégíti. A G ezen előállítása mellett a $Q_1, \ldots, Q_k$-ban mint nevezők csak a Z_i-k hatványszorzatai szerepelnek. Ha tehát $Z = Z_1 \ldots Z_k$, akkor szükségképen van olyan meghatározott pozitiv egész szám r, hogy már

$$Z^r G \equiv 0 \,(\text{mod. } F_1, \ldots, F_k);$$

tehát Z^r a K-ra kiszabott feltételt kielégíti. Így tehát tételünk igazolása már csak azon múlik, hogy meghatározzuk ezt az r számot úgy, hogy megfeleljen a föltételnek, bárhogyan választjuk is a G formát. E számra nézve könnyű kijelölni oly szükséges feltételt, a melyről azután majd felismerjük, hogy elegendő feltétel is. Ha ugyanis valamely G'-re nézve fennáll a

$$Z^{r+1} G' \equiv 0 \,(\text{mod. } F_1, \ldots, F_k),$$

congruentia, akkor szükséges, hogy fennálljon már a

$$Z^r G' \equiv 0 \,(\text{mod. } F_1, \ldots, F_k)$$

congruentia is. Minthogy magától értetődik, hogy ennek megfordítottja is érvényes, szükséges, hogy a

$$Z^r G = \sum_{i=1}^{k} F_i X_i$$

és a

$$Z^{r+1} G' = \sum_{i=1}^{k} F_i Y_i$$

diophantikus egyenletekből G-re, ill. G'-re vonatkozólag ugyanazok a megoldások származzanak. Ha már most ismeretes valamely olyan véges meghatározott eljárás, a mely ezeknek az egyenleteknek megoldását szolgáltatja, tehát

$$G = \Sigma G_j U_j$$
$$G' = \Sigma G'_h V_h$$

meg van adva, akkor ez a feltétel azt fejezi ki, hogy minden G_j-nek tartalmaznia kell a $(\ldots, G'_h, \ldots)$ osztórendszert és minden G'_h-nak a $(\ldots, G_j, \ldots)$ osztórendszert, vagyis kell, hogy

$$(\ldots, G_j, \ldots) \simeq (\ldots, G'_h, \ldots)$$

legyen.

Így tehát az $r = 0, 1, 2, \ldots$ számoknak megfelelőleg az osztórendszerek olyan $(S_0), (S_1), (S_2), \ldots$ sorozata származik, a melyeknek æquivalentiáját feltevésünk szerint ismét véges számú lépés után megitélhetjük. Véges számú kisérlet után azonban olyan r számhoz kell jutnunk, a melyre nézve $(S_r) \simeq (S_{r+1})$, és *az így meghatározott szám megfelel a felállított követeléseknek.*

Mert ha volna olyan Γ forma, a melyre nézve legelőször csak

$$Z^{r+k}\Gamma \equiv 0 \,(\text{mod. } F_1, \ldots, F_k),$$

a hol k valamely pozitiv egész számot jelent, akkor okvetetlenül fönnállana a

$$Z^{r+1}(Z^{k-1}\Gamma) \equiv 0 \,(\text{mod. } F_1, \ldots, F_k);$$

congruentia; tehát — a mint épen bebizonyítottuk — egy-

szersmind

$$Z^{r+k-1}\Gamma \equiv 0 \,(\text{mod. } F_1, \ldots, F_k).$$

Ha már mostan $k-1$ nem zérus, ezt az eljárást csak addig kell ismételnünk, míg végre a

$$Z^r\Gamma \equiv 0 \,(\text{mod. } F_1, \ldots, F_k)$$

congruentiát nyerjük és evvel az ilyen Γ forma létezésének feltevését helytelennek bizonyítottuk.

Az algebrai és arithmetikai probléma szétválasztása.

8. §. Hogy az osztórendszerek elméletének és ennek alkalmazásainak biztos alapját megvethessük, mindenekelőtt szükséges, hogy minden adott esetben eldönthessük, vajjon két adott rendszer közül az egyik tartalmazza-e a másikat, vagy sem? Annak a kérdésnek az eldöntése, vajjon két osztórendszer æquivalens-e, ebben benne van mint specziális eset. Ama kérdés azután közvetetlenül annak az eldöntésére vezetendő vissza, vajjon a tartomány valamely F mennyisége tartalmazza-e az $(F_1, \ldots, F_k)$ osztórendszert, azaz, vajjon az

$$F = F_1X_1 + \cdots + F_kX_k$$

diophantikus egyenletnek van-e megoldása. Így tehát az e fejezet elején felállított lineáris diophantikus problémának teljes megoldása egyszersmind teljes feleletet ád azon kérdésekre is, a melyek az osztórendszerekre vonatkoznak.

A további tárgyalásban külön választandó az a két eset, midőn az alapúl felvett A tartomány orthoid tartomány, vagy pedig valódi holoid tartomány; mert e két eset nemcsak az alkalmazandó módszerek tekintetében, hanem az előadandó tények jelentésében és értelmezésében is lényegesen különböző szempontokat tár elénk.

A mennyiben az adott tartomány orthoid tartomány, vagy pedig ha az valamely [A] valódi holoid tartomány volt,

de a további tárgyalásban a mellérendelt (A) orthoid tartomány mennyiségeit is használjuk — hiszen ez ugyanaz, mintha mindjárt elejétől fogva az (A) tartományt vettük volna fel alapúl — olyan fejtegetéssel van dolgunk, a mely a már többször kifejtett értelemben kizárólag az algebrába tartozik és ezért az elméletet ebben az esetben *a lineáris diophantikus rendszerek algebrai elméletének* nevezzük.

Evvel ellentétben *a lineáris diophantikus rendszerek arithmetikai elméletének* azt az esetet nevezzük, midőn kizárólag csak a raczionális és egész formák tartományára szorítkozunk. E megszorításra mindenekelőtt az a körülmény indít, hogy a mennyire az algebrai mennyiségek elmélete van szóban és nem az «algebrai» elmélet amaz egyszerű esete lép fel, kizárólag olyan problémákkal van dolgunk, a melyek ezzel az «arithmetikai» elmélettel teljesen megoldhatók*.

Magától értetődik, hogy a fellépő problémák megoldá-

* Megjegyezhetjük mindjárt itt, hogy a VIII. fej. ide tartozó fejtegetései sokkal szélesebbkörű módszereket nyújtanak. Hogy csak a legegyszerűbb esetet említsük, azok majdnem szóról szóra átvihetők az olyan teljes holoid tartományokra, a melyekben minden mennyiségnek teljes maradékrendszere van. Ennek értelme a következő:

Ha A az [A] tartomány valamely mennyisége, akkor mindig van a tartománynak véges számú olyan

$$A_0, A_1, \ldots, A_{k-1}$$

mennyisége (a hol ezt a k számot az A teljesen meghatározza), hogy az [A] tartomány minden B mennyisége az A modulusra nézve az A_i mennyiségek közűl egygyel és csak egygyel congruens.

Az algebrai mennyiségek elmélete értelmében egyébként holoid tartományoknak általános elmélete nem is lehetséges. Hiszen pl. azoknak az analitikai függvényeknek összessége, a melyeket mindig összetartó hatványsorok értelmeznek, szintén holoid tartományt alkot.

sának mindig csak az olyat tekintjük, a mely az adott mennyiségekből kiindulva a műveleteknek csupán véges sorát követeli és e műveletek ismét csak a négy alapművelet alkalmazásából és adott mennyiségek legnagyobb közös osztójának meghatározásából állanak. A részletezett lineáris diophantikus problémáknak, valamint az általános arithmetika ezekkel kapcsolatos problémáinak (l. a IX. fej.) teljes megoldását ebben az értelemben tudtommal ez a munka adja legelőször*

A lineáris diophantikus rendszerek algebrai elmélete.

9. §. Ha (A) már most orthoid tartomány, akkor e fej. 1. §-ának fejtegetései szerint először is *egy egyetlen homogén lineáris egyenlet:*

$$F_1X_1+\cdots+F_kX_k=0$$

megoldásainak seregét kell meghatároznunk; evvel azután meg van adva az ilyen egyenletekből álló rendszer megoldásainak serege is.

Itt az $m-1$-ről m-re való következtetés alkalmazható, azaz

* Az «algebrai» elmélet előmunkálatai gyanánt tekinthetők az összes vizsgálatok, melyek NOETHER tételére (l. e fej. 12. §-át) vonatkoznak. Ezek a két határozatlant tartalmazó formák esetének felelnek meg.

Az «arithmetikai» elméletre vonatkozólag megemlítendő HENSEL két dolgozata: «Über die Zurückführung der Divisorensysteme auf eine reducirte Form» (Journ. f. d. r. u. a. Math. CXVIII. és CXIX. k.). E dolgozatok az olyan osztórendszerek redukált alakját határozzák meg, a melyeknek elemei *egy* határozatlant tartalmazó racionális és egész formák és két *ilyen* osztórendszer æquivalentiájának speciálisabb problémájára vonatkozólag azt az eredményt nyeri HENSEL, hogy æquivalentia akkor és csak akkor áll fönn, ha a megfelelő redukált formák ugyanazok.

Ugyanevvel a kérdéssel foglalkozott HANCOCK is (Journ. f. d. r. u. a. Math. CXIX. k.).

a következtetés $[(A), x_1, \ldots, x_{m-1}]$-ről $[(A), x_1, \ldots, x_m]$-re. Magában az (A) tartományban a dolog fölötte egyszerű. Ha a

$$\gamma_1\xi_1+\gamma_2\xi_2+\cdots+\gamma_k\xi_k=0$$

egyenletben legalább egy együttható, pl. γ_1 a zérustól különböző, akkor annak teljes megoldása közvetetlenül mint $k-1$ tagú sereg áll elő a következő alakban:

$$\xi_1=-\frac{\gamma_2}{\gamma_1}\mu_2-\cdots-\frac{\gamma_k}{\gamma_1}\mu_k,$$

$$\xi_i=\mu_i. \qquad (i=2,\ldots,k)$$

Ha továbbá a

$$\gamma_1\xi_1+\gamma_2\xi_2+\cdots+\gamma_k\xi_k=1$$

egyenletben pl. γ_1 különböző a zérustól, akkor annak egyik megoldása közvetetlenül felírható:

$$\xi_1=\frac{1}{\gamma_1},\ \xi_2=\cdots=\xi_k=0.$$

Evvel tehát (A)-ban a két alapprobléma meg van oldva és a lineáris rendszerek elméletét erre az esetre teljesen elintéztük.

Feltételezhetjük, hogy a homogén, lineáris diophantikus rendszer megoldására $[(A), x_1, \ldots, x_{m-1}]$-ben jól értelmezett eljárás áll rendelkezésünkre, a mint ez (A)-ról valóban áll és e feltevés alapján megállapítjuk azt az eljárást, a mely az $[(A), x_1, \ldots, x_m]$ tartományban ugyanazt a czélt szolgálja.

Minthogy lineáris transformatio a problémán mit sem változtat, mindjárt feltételezhetjük, hogy az $F_1, \ldots, F_k$ formák mind szabályosak. Ezt feltételezve az

$$F_1X_1+F_2X_2+\cdots+F_kX_k=0 \qquad (1)$$

egyenlet megoldása, a melylyel együtt a homogén rendszerek megoldása is elintézettnek tekinthető, következőképen alakúl:

Minthogy F_1 szabályos, az $X_2, \ldots, X_k$ ismeretlen formák okvetetlenül az

$$X_i = F_1 Y_i + R_i \qquad (i=2, \ldots, k)$$

alakban írhatók, a hol R_i-nek x_m-re vonatkozó foka legfölebb n_1-1, ha n_1 az F_1 formának dimensiója. Maga az egyenlet azután a következő alakot veszi fel:

$$F_1(X_1+F_2Y_2+\cdots+F_kY_k)+F_2R_2+\cdots+F_kR_k=0. \qquad (2)$$

Az $F_2R_2+\cdots+F_kR_k$ formának x_m-re vonatkozó foka legfölebb a legnagyobb az n_i+n_1-1 $(i=2, \ldots, k)$ számok közül, a hol n_i az F_i forma dimensióját jelenti és így tehát az $X_1+F_2Y_2+\cdots+F_kY_k$ formának x_m-re vonatkozó foka nem nagyobb, mint s, az n_i-1 számok közül a legnagyobb. Ha tehát az adott egyenletekben részletesen kiírjuk, hogy

$$R_i = U_{i0}x_m^{n_1-1}+U_{i1}x_m^{n_1-2}+\cdots+U_{i,n_1-1}, \qquad (i=2, \ldots, k)$$

$$X_1+\sum_{i=2}^{k}F_iY_i = V_0x_m^s+V_1x_m^{s-1}+\cdots+V_s,$$

a hol az U-k és a V-k az $[(A), x_1, \ldots, x_{m-1}]$ tartománynak egyelőre még ismeretlen formáit jelentik, akkor az x_m hatványainak együtthatóit egyenként zérussal egyenlítve, az U-kra és V-kre vonatkozó szükséges és elegendő feltételeknek olyan rendszerét nyerjük, a mely egyenesen homogén, lineáris diophantikus egyenletek rendszere az $[(A), x_1, \ldots, x_{m-1}]$ tartományban és a melyet a feltevés szerint teljesen meg tudunk oldani. Így tehát (2) rendszerünk általános megoldását a következő alakban nyerjük:

$$R_i = \sum_{j=1}^{l} G_{ji}W_j, \qquad (i=2, \ldots, k)$$

$$X_1+\sum_{i=2}^{k}F_iY_i = \sum_{j=1}^{l}H_jW_j$$

és azután az (1) egyenlet általános megoldását is az

$$X_1 = -\sum_{i=2}^{k}F_iY_i+\sum_{j=1}^{l}H_jW_j,$$

$$X_i = F_1Y_i+\sum_{i=1}^{l}G_{ji}W_j$$

alakban, a hol H_j, G_{ji} adott, Y_i, W_j pedig tetszés szerinti formákat jelentenek. A nyert megoldás tehát legfölebb $k+l-1$-tagú sereg alakjában lép fel.

A második alappробléma, t. i. *annak eldöntése, hogy az*

$$F_1X_1+\cdots+F_kX_k=1$$

diophantikus egyenletnek vannak-e egyáltalában megoldásai és ha vannak, egyiköknek meghatározása (még akkor is, ha a jobb oldalon az 1 helyén bármely F forma áll), az épen részletezett módszer szerint ismét az $[(A), x_1, \ldots, x_{m-1}]$ tartományra vezethető vissza; de az általános eliminációelmélet fejtegetései alapján (V. fej. 4. és 5. §) is teljesen letárgyalható. Ez a nem épen elemi, de mivel mélyebbre ható, magában is fontos módszer, néhány sorban részletezhető.

Ha az $F_i=0$ $(i=1, \ldots, k)$ egyenletrendszer összresolvense az æquivalentia-meghatározás értelmében az 1-től különböző, akkor az $F_i=0$ egyenleteknek van gyökrendszerük. Ekkor azonban ama diophantikus egyenletnek nem lehet megoldása; mert olyan X_i formákra nézve, a melyek ama diophantikus egyenletet kielégítik, annak identitássá kell válnia, a melynek akkor is érvényesnek kellene maradnia, midőn az x_i-k helyébe az említett gyökrendszert teszszük; de ez a $0=1$ lehetetlenséghez vezetne.

Ha azonban az egyenletrendszer összresolvense æquivalens az egységgel, akkor a III. fej. 18. §-ában leírt műveletsorozat segítségével a resolvensforma számára egyenesen az

$$1=\sum_{i=1}^{k} G_iF_i$$

azonosságot nyerjük, azaz az adott diophantikus egyenlet egyik megoldását.

A főosztályhoz tartozó osztórendszerek (a melyeknek elemei orthoid tartományból származó formák).

10. §. Ha olyan $(F_1, F_2, \ldots, F_k)$ osztórendszerrel van dolgunk, a melynek elemei orthoid tartományból származó formák, az $F_j=0$ egyenletrendszer, vagyis az ezen egyenletrendszer értelmezte sokaság fokozatszámát egyszersmind *az osztórendszer fokozatszámának* nevezzük. Aequivalens osztórendszerek fokozatszámai tehát ugyanazok és a fokozatszám akkor sem változik, ha az osztórendszert az x határozatlanoknak valamely (homogén) lineáris transformatiójával olyan osztórendszerbe vezetjük át, a melynek elemei azután a z határozatlanoknak formái.

Az itt tekintetbe vett diophantikus problémák esetében az ilyen transformatio a kérdésen mit sem változtat és ezért, a hol ez épen szükségesnek mutatkozik, *már elejétől fogva feltételezzük, hogy az osztórendszerre, azaz annak összes elemeire az ilyen «általános» transformatiót már is alkalmaztuk.* Ez az «általános» jelző annyit jelent, hogy a transformatio együtthatói *nem* elégítenek ki bizonyos meghatározott algebrai egyenleteket.

Valamely osztórendszerről akkor mondjuk, hogy a *főosztályhoz tartozik, midőn olyan* $(F_1, F_2, \ldots, F_k)$ *osztórendszerrel aequivalens, a melynek az a tulajdonsága, hogy* $(F_i, \ldots, F_k)$ *pontosan* $k-i+1$*-ed fokozatú**. A következőkben feltételezzük, hogy a főosztályhoz tartozó osztórendszer már ebben az alakban van megadva. Magától értetődik, hogy a $k \leqq m$ fölvétel czéljainkra elégséges; mert az $m+1$ fokozatszámnak csupán csak az egységgel æquivalens osztórend-

* Különben könnyű kimutatni, hogy ily értelemben minden k-tagú és k-adfokozatú osztórendszer a főosztályhoz tartozik.

szerek felelnek meg és ezeknek tulajdonságai az épen kimondottal ki is vannak merítve.

Az ilyen k-ad fokozatú k-tagú osztórendszer egyik alaptulajdonsága még úgy is kifejezhető, hogy az

$$F_j = 0 \qquad (j=1,\ldots,k)$$

egyenletrendszernek, a melyben $x_1,\ldots,x_k$ tekintendők az ismeretleneknek, míg együtthatói az $x_{k+1},\ldots,x_m$ határozatlanoknak az (A) orthoid tartományból származó formái, véges (a 0-tól különböző) számú gyökrendszere van. (Ha $k=m$, az együtthatók nem tartalmaznak határozatlanokat.)

A főosztály értelmezéséből közvetetlenül folyó megjegyzés, hogy $(F_1, F_2,\ldots, F_k)$-*val egy időben* $(F_i,\ldots, F_k)$ *is a főosztályhoz tartozik.* Evvel azt a tényt fejezzük ki, hogy az $F_i=0,\ldots, F_k=0$ egyenletrendszernek is véges, a 0-tól különböző számú gyökrendszere van, ha az x-ek közül $k-i+1$-et ismeretlennek, $m-k+i-1$-et pedig az együtthatókban fellépő határozatlanoknak tekintünk. (Az F-ekre alkalmazott általános lineáris transformatio következtében teljesen közömbös, hogy az x-eknek e szétválasztása miképen történik.)

Ha most már az

$$F_1=0,\ldots, F_k=0$$

rendszer összresolvensét alkotjuk, oly módon, hogy e czélból a

$$z_1=t_{11}x_1+t_{12}x_2+\cdots+t_{1m}x_m$$

új ismeretlent vezetjük be, akkor ez $R_1(z_1, x_{k+1},\ldots, x_m)=0$, és lesz:

$$R_1\left(\sum_{i=1}^{k} t_{1i}x_i,\ x_{k+1},\ldots,\ x_m\right)=\sum_{j=1}^{k}\lambda_{1j}F_j.$$

Itt az általános eliminácziő-elmélet fejtegetései értelmében a z_1 legmagasabb hatványának együtthatója R_1-ben az x-ektől független mennyiség, és R_1 a z_1 igazi formája. Az V. fej. 2. és 3. §-ával való összehasonlítás kedveért még

megjegyzendő, hogy most a könnyebb áttekintés végett x_k és x_m jelentését fölcseréltük.

Tudjuk továbbá, hogy, ha $R_1=0$-t mint egyenletek complexusát fogjuk fel, azaz, ha az együtthatókat, a melyek a t_{1i}-k különböző hatványszorzatai mellett állanak, külön-külön zérussal egyenlítjük, akkor az $R_1=0$ és $F_j=0$ rendszerek gyökrendszerei ugyanazok.

E tényt úgy is fejezhetjük ki, hogy, a mennyiben a t-ktől független mennyiségekre szorítkozunk, az

$$F_1=0,\ F_2=0,\ \ldots,\ F_k=0$$

rendszernek ugyanazon gyökrendszerek felelnek meg, mint az

$$R_1\left(\sum_{i=1}^{k} t_{1i}x_i,\ x_{k+1},\ \ldots,\ x_m\right)=0,\ F_2=0,\ \ldots,\ F_k=0$$

egyenletrendszernek és viszont.

Ha mostan az utóbbi egyenletrendszerre ugyanazokat a műveleteket alkalmazzuk, jelesen a

$$z_2=t_{21}x_1+t_{22}x_2+\cdots+t_{2m}x_m$$

új ismeretlen bevezetésével az összresolvenst alkotjuk, lesz ismét

$$R_2\left(\sum_{i=1}^{k} t_{2i}x_i,\ x_{k+1},\ \ldots,\ x_m\right)=\lambda_{21}R_1+\sum_{j=2}^{k}\lambda_{2j}F_j,$$

a hol, minthogy, a mint majd bebizonyítjuk, a most vizsgált rendszer is k-ad fokozatú, R_2-nek a z_2-re vonatkozólag ugyanazon tulajdonságai vannak, mint R_1-nek a z_1-re vonatkozólag. Az $R_2=0$ egyenlet, ha ezt az előbb megállapított módon fogjuk fel, ismét az $F_1=0,\ \ldots,\ F_k=0$ gyökrendszereit szolgáltatja és csak ezeket, ha t. i. a t-ktől független mennyiségekre szorítkozunk.

Ezt így folytatva, a formáknak következő sorozata keletkezik:

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$R_\mu\Big(\sum_{i=1}^{m} t_{\mu i}x_i,\ x_{k+1},\dots,x_m\Big)=\sum_{\varrho=1}^{\mu-1}\lambda_{\mu\varrho}R_\varrho+\sum_{j=\mu}^{k}\lambda_{\mu j}F_j,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$R_k\Big(\sum_{i=1}^{m} t_{ki}x_i,\ x_{k+1},\dots,x_m\Big)=\sum_{\varrho=1}^{k-1}\lambda_{k\varrho}R_\varrho+\lambda_{kk}F_k.$$

A $t_{\mu i}$ mennyiségeket most már speciális módon (mint racionális és egész számokat is) úgy választhatjuk és választjuk is, hogy az $R_1, R_2, \dots, R_k$ formák alakja megmaradjon; egyszersmind pedig a $|t_{\mu i}|_{(\mu, i=1,\dots,k)}$ determináns a 0-tól különböző legyen. Ha azután

$$z_\mu=\sum_{i=1}^{m} t_{\mu i}x_i \qquad (\mu=1,\dots,k)$$

-t úgy tekintjük, mint lineáris transformatiót és végre z helyébe ismét x-et írunk, akkor evvel az adott osztórendszer alkalmas transformatiója után *a formák következő sorozatát kapjuk:*

$$R_\mu(x_\mu, x_{k+1},\dots,x_m)=\sum_{\varrho=1}^{\mu-1}\lambda_{\mu\varrho}R_\varrho+\sum_{j=\mu}^{k}\lambda_{\mu j}F_j, \qquad (R_\mu)$$
$$(\mu=1,\dots,k)$$

a hol az R_μ-k kivétel nélkül az x_μ oly igazi formái, a melyekben az x_μ legmagasabb hatványának együtthatója a többi x-ektől független mennyiség, míg az F_j-k is szabályosaknak vehetők; mert először is olyan transformatiót alkalmazhatunk, a mely ezt megvalósítja és a további transformatiókat mindig úgy választhatjuk, hogy ez a tulajdonság megmaradjon.

Az R_μ formasorozat létezése azonban még azon eddig be nem bizonyított föltevésen fordúl meg, hogy minden

$$R_1=0,\dots,\ R_{i-1}=0,\ F_i=0,\dots,\ F_k=0$$

rendszer, mely most úgy értendő, hogy k egyenletből áll, együtthatói pedig a t-k formái, csakugyan k-adfokozatú. Az

$F_i=0, \ldots, F_k=0$ rendszer a föltevés szerint $k-i+1$-edfokozatú, és e szám nem változik, ha az F formákat, mint az $((A), t_{11}, \ldots)$ orthoid tartományból származókat fogjuk föl, mert ez által az összresolvens képezésén mi sem változik. Egyenletrendszerünk továbbá már is az «esetleges körülményektől» ment; mert hisz ez úgy van, ha az ismeretlenekre oly (homogén) lineáris transformatiót alkalmazunk, melynek együtthatói raczionális és egész számok; e transformatiót pedig már eredetileg is az F-eken végrehajtottnak gondolhatjuk. Ép oly kevéssé változik az egyenletrendszer «általános» jellege, ha a

$$z_\mu=\sum_{i=1}^{m} t_{\mu i}\, x_i \qquad (\mu=1, 2, \ldots, i-1)$$

egyenletek alapján $x_1, \ldots, x_{i-1}$ helyett az új $z_1, \ldots, z_{i-1}$ ismeretleneket vezetjük be. De ekkor az $R_\mu=0$ egyenletekből az $x_{k+1}, \ldots, x_m$ minden értékrendszerének megfelelnek a $z_1, \ldots, z_{i-1}$ bizonyos véges (a 0-tól különböző) számú értékei, míg végre azután az $F_i=0, \ldots, F_k=0$ egyenletek az $x_i, \ldots, x_k$ ugyanily számú értékeket adnak, a mi épen bebizonyítandó volt.

Legyenek már most az $F_j=0$ rendszernek a feltevés szerint véges, a 0-tól különböző számú gyökrendszerei, midőn ismeretleneknek $x_1, \ldots, x_k$-t tekintjük, míg $x_{k+1}, \ldots, x_m$ az együtthatókban fellépő határozatlanok, a következők:

$$\xi_{1\nu}, \xi_{2\nu}, \ldots, \xi_{k\nu}; \qquad (\nu=1, 2, \ldots, r)$$

akkor az $R_\mu=0$ egyenletet is kielégítik ezek a gyökrendszerek, azaz *irhatjuk, hogy*

$$R_\mu=A_\mu \prod_{\nu=1}^{s}(x_\mu-\xi_{\mu\nu})^{c_{\mu\nu}}, \qquad (r \leqq s)$$

a hol A_μ az eredeti orthoid tartományhoz tartozik, tehát 1-nek is vehető. R_μ-nek $x_\mu-\xi_{\mu\nu}$ hatványai szerint való kifejtése e jelölés értelmében a $c_{\mu\nu}$-dik hatványnyal kezdődik, vagy — a mint azt még másképen is mondhatjuk — R_μ-nek

az $x_1-\xi_{1\nu}, x_2-\xi_{2\nu}, \ldots, x_k-\xi_{k\nu}$ hatványszorzatai szerint való kifejtése, minthogy a többi tagok hiányzanak, a $c_{\mu\nu}$-ed dimensiójú tagokkal kezdődik, a melyek benne a legalacsonyabb dimensiójúak.

11. §. Az a kérdés, vajjon valamely osztórendszer, vagy a mi egyre megy, valamely magában álló forma az $(F_1, \ldots, F_k)$ osztórendszert tartalmazza-e, a megfelelő lineáris diophantikus egyenlet megoldásával véges számú lépésben eldönthető. E megoldás azonban avval a kellemetlenséggel jár, hogy minden egyes Φ formára nézve külön elvégzendő. Evvel szemben alapvető fontosságú, hogy *megjelölhetjük a Φ formán elvégzendő állandó müveletek olyan véges sorozatát, a melylyel bármely Φ formáról eldönthető, vajjon az adott $(F_1, \ldots, F_k)$ osztórendszert tartalmazza-e, vagy sem.* Ezt a kérdést a főosztályhoz tartozó osztórendszerek esetében most teljesen el akarjuk intézni.

A főosztályhoz tartozó elsőfokozatú osztórendszerek, azaz magukban álló egyes formák esetében ez egyszerűen a közönséges oszthatósági probléma és az általános eset egyenesen erre lesz visszavezetendő; még pedig a következő alapvető tétel szerint:

Hogy eldönthessük, vajjon valamely tetszés szerinti Φ forma a főosztály $(F_1, \ldots, F_k)$ osztórendszerét tartalmazza-e, meg kell határoznunk az

$$R_\mu(x_\mu, x_{k+1}, \ldots, x_m), \qquad (\mu=1, \ldots, k)$$

és a további $\lambda_{\mu\nu}$ formákat, a melyek az

$$R_\mu(x_\mu, x_{k+1}, \ldots, x_m)=\sum_{\nu=1}^{\mu-1}\lambda_{\mu\nu}R_\nu+\sum_{j=\mu}^{k}\lambda_{\mu j}F_j \qquad (R_\mu)$$

jelezte kapcsolatban állanak, hol továbbá $R_\mu=A_\mu x_\mu^{k_\mu}+\cdots$, A_μ az x-eket nem tartalmazza és $k_\mu \geqq 1$. Azután akkor és csak akkor lesz

$$\Phi \equiv 0 (\text{mod. } F_1, \ldots, F_k), \qquad (C)$$

AKADÉMIAI KÖNYVTÁR

ha

$$\lambda_{11}\lambda_{22}\ldots\lambda_{kk}\Phi\equiv 0(\text{mod. } R_1,\ldots,R_k), \qquad (K)$$

és az utóbbi formának megfelelő

$$\lambda_{11}\ldots\lambda_{kk}\Phi=\sum_{i=1}^{k}K_iR_i$$

előállításából azután a Φ formának

$$\Phi=\sum_{i=1}^{m}H_iF_i$$

előállítását is megkapjuk.

Hogy az R és λ formák ilyen sorozata az osztórendszerre esetleg alkalmazandó transformatio után mindig meghatározható, azt az előbbi §-ban bizonyítottuk be.

Mielőtt a kimondott tétel bebizonyítására áttérnénk, még néhány előleges megjegyzést akarunk itt közbeszúrni.

Vajjon a (K)-ban kifejezett feltétel ki van-e elégítve, vagy sem, az a közönséges osztási eljárással mindig eldönthető. Ha ugyanis

$$\Psi=\sum_{i=1}^{k}K_iR_i,$$

akkor írhatjuk, hogy

$$K_i=M_iR_1+N_i; \qquad (i=2,\ldots,k)$$

azután Ψ a

$$\Psi\{(M_2R_2+\cdots+M_kR_k)R_1+\sum_{i=2}^{k}N_iR_i$$

alakot veszi fel, és ebben R_1 együtthatója a «hányados», $\sum_{i=1}^{k}N_iR_i$ pedig a «maradék», mely Ψ-nek R_1-gyel való «osztás-a» alkalmával fellép. Az osztási eljárás ismételt alkalmazása révén végre

$$\Psi=\sum_{i=1}^{k}Q_iR_i,$$

származik, a hol tehát Q_i-nek az $x_1,\ldots,x_{i-1}$ határozatlanokra vonatkozó foka kisebb, mint az $R_1,\ldots,R_{i-1}$ formák foka ugyanazokra a határozatlanokra vonatkozólag.

A $\Psi \equiv 0 (\mathrm{mod.}\, R_1, \ldots, R_k)$ *feltétel tehát akkor és csak akkor van kielégítve, ha a közönséges osztási eljárást ismételten alkalmazva, a k-dik osztás után a «zérus» maradékhoz jutunk és ebben az esetben meg is van mindjárt a* $\Psi = \Sigma Q_i R_i$ *előállítás.*

Ha tehát $G(x_{k+1}, \ldots, x_m)$ oly forma, a melyben az $x_1, \ldots, x_k$ határozatlanok *nem* fordulnak elő és $G\Psi \equiv 0 (\mathrm{mod.}\, R_1, \ldots, R_k)$, akkor egyszersmind $\Psi \equiv 0 (\mathrm{mod.}\, R_1, \ldots, R_k)$; mert amaz osztási eljárást alkalmazva, az összes Q_i-k rendre oszthatók lesznek G-vel.

A bebizonyítandó tételt egyelőre helyesnek feltételezve ebből következik, hogy *akkor, midőn*

$$G(x_{k+1}, \ldots, x_m)\, \Phi \equiv 0 (\mathrm{mod.}\, F_1, \ldots, F_k),$$

mindig egyszersmind lesz $\Phi \equiv 0 (\mathrm{mod.}\, F_1, \ldots, F_k)$.

A megelőző megjegyzés szerint ugyanis abból, hogy

$$\lambda_{11} \ldots \lambda_{kk} G\Phi \equiv 0 (\mathrm{mod.}\, R_1, \ldots, R_k),$$

mindig az is következik, hogy

$$\lambda_{11} \ldots \lambda_{kk} \Phi \equiv 0 (\mathrm{mod.}\, R_1, \ldots, R_k).$$

Hogy végre a bebizonyítandó tétel $k=1$ esetében helyes, közvetetlenül belátható. Ebben az esetben

$$R_1 = \lambda_{11} F_1$$

és a tétel csak azt a triviális tényt fejezi ki, hogy, midőn $\lambda_{11}\Phi$ osztható $R_1 = \lambda_{11} F_1$-gyel, Φ is osztható F_1-gyel.

A tétel általános bebizonyítása tehát ismét teljes inductióval végezhető; ez pedig a következőkben úgy fog megtörténni, hogy feltételezve a tétel helyességét a főosztály $k-1$-tagú osztórendszerei esetében, kimutatjuk, hogy a k-tagú osztórendszerek esetében is érvényes.

Ez igen egyszerűen, a következő módon történik. Abból, hogy

$$\Phi = \sum_{i=1}^{k} H_i F_i,$$

következik, hogy

$$\lambda_{11}\Phi = H_1\lambda_{11}F_1 + \sum_{i=2}^{k} H_i' F_i,$$

vagy pedig, mivel

$$R_1 = \lambda_{11}F_1 + \lambda_{12}F_2 + \cdots + \lambda_{1k}F_k,$$

továbbá még az is, hogy

$$\lambda_{11}\Phi = H_1' R_1 + \sum_{i=2}^{k} H_i'' F_i.$$

Viszont azonban az utóbbi kapcsolatból foly, hogy

$$\lambda_{11}\Phi = H_1'\lambda_{11}F_1 + \sum_{i=2}^{k} H_i''' F_i,$$

vagyis

$$\lambda_{11}(\Phi - H_1' F_1) = \sum_{i=2}^{k} H_i''' F_i;$$

tehát egyszersmind

$$\lambda_{11}F_1(\Phi - H_1' F_1) = \sum_{i=2}^{k} H_i''' F_1 F_i$$

és

$$R_1(\Phi - H_1' F_1) = \sum_{i=2}^{k} H_i' F_i.$$

Ámde $(F_2, \ldots, F_k)$ a főosztály $k-1$ tagú osztórendszere, a melyben, hacsak a kezdetben választott lineáris transformatiót kellően határoztuk meg, $x_2, \ldots, x_k$ azok a határozatlanok, a melyekre a további műveletek vonatkoznak. E határozatlanokat azonban R_1 nem tartalmazza. Így tehát

$$\Phi - H_1' F_1 = \sum_{i=2}^{k} H_i F_i.$$

E szerint a

$$\Phi \equiv 0 \,(\text{mod. } F_1, \ldots, F_k),$$
$$\lambda_{11}\Phi \equiv 0 \,(\text{mod. } R_1, F_2, \ldots, F_k)$$

congruentiák egy időben érvényesek vagy nem érvényesek és $\lambda_{11}\Phi$ megfelelő előállításából ismeretes műveletek segítségével nyerhető a Φ előállítása is.

Ha ugyanezt az eljárást az $(R_1, F_2, \ldots, F_k)$ osztórendszerre alkalmazzuk, ép úgy jutunk a

$$\lambda_{11}\lambda_{22}\Phi \equiv 0 \,(\text{mod. } R_1, R_2, F_3, \ldots, F_k)$$

congruentiához és így tovább haladva végre a

$$\lambda_{11}\ldots\lambda_{kk}\Phi \equiv 0 \,(\text{mod. } R_1, \ldots, R_k)$$

congruentiát nyerjük, a mivel tételünk teljesen be van bizonyítva.

Noether tételének általánosítása.

12. §. *Legyenek már most a főosztályhoz tartozó k-tagú* $(F_1, \ldots, F_k)$ *osztórendszer elemei olyan formák, a melyek az orthoid* (A) *tartományból származnak és mint ilyenek csakis az* $x_1, \ldots, x_k$, *tehát számra nézve k határozatlant tartalmazzák. Az előbbivel szemben e szerint most* $m=k$.

Annak szükséges és elegendő feltétele, hogy Φ ezt az osztórendszert tartalmazza,

$$\Lambda\Phi \equiv 0 \,(\text{mod. } R_1, \ldots, R_k), \qquad (K)$$

a hol rövidség kedvéért $\Lambda = \lambda_{11}\ldots\lambda_{kk}$ áll, most már olyan congruentia-feltételek sorozatára bontható fel, a melyek az $F_1=0, \ldots, F_k=0$ egyenletrendszer egyes gyökrendszereire vonatkoznak, *ha egyidejüleg* (A) *helyébe azon* (A)*-ból származó genus-tartományt veszszük alapúl, a melyet az* $F_i=0$ *egyenletrendszer értelmez.*

R_μ-t a következő módon értelmeztük:

$$R_\mu = (x_\mu - \xi_{\mu 1})^{c_{\mu 1}} \ldots (x_\mu - \xi_{\mu\nu})^{c_{\mu\nu}} \ldots,$$

a hol a $\xi_{\mu 1}, \ldots, \xi_{\mu\nu}, \ldots$ sorozat, mely az $R_\mu=0$ egyenlet gyökeit adja, tehát az x_μ ismeretlennek az $F_j=0$ gyökrendszereiben fellépő értékeit tartalmazza és e szerint, ha $\nu \neq \nu'$,

$$\left((x_\mu - \xi_{\mu\nu})^{c_{\mu\nu}}, (x_\mu - \xi_{\mu\nu'})^{c_{\mu\nu'}}\right) \sim 1.$$

Még tekintetbe veendő, hogy az F-ekre alkalmazandó lineáris transformatiót mindig úgy választhatjuk, hogy minden egyes ismeretlen a különböző gyökrendszerekben különböző érté-

keket vegyen fel. Ha tehát ama genus-tartományt veszszük alapúl, akkor (a 3. § szerint) az $(R_1, \ldots, R_k)$ osztórendszer olyan tényezőkre bomlik, a melyeknek alakja a következő:

$$((x_1-\xi_{1\nu_1})^{c_1\nu_1}, (x_2-\xi_{2\nu_2})^{c_2\nu_2}, \ldots, (x_k-\xi_{k\nu_k})^{c_k\nu_k}),$$

a hol $\xi_{1\nu_1}, \ldots, \xi_{k\nu_k}$ egyenként és egymástól függetlenül az $x_1, \ldots, x_k$ ismeretleneknek az $F_j=0$ gyökrendszereiben fellépő értékeit futják át.

Ha ezeket a tényezőket röviden $\{\nu_1, \ldots, \nu_k\}$-val jelöljük, akkor a $\xi_{1\nu_1}, \ldots, \xi_{k\nu_k}$ és $\xi_{1\nu'_1}, \ldots, \xi_{k\nu'_k}$ mennyiségek, a melyek két különböző tényezőben, $\{\nu_1, \ldots, \nu_k\}$-ban és $\{\nu'_1, \ldots, \nu'_k\}$-ban előfordúlnak, nem lesznek mindannyian egyenlők. Különbőző tényezőknek tehát nincsen közös tartalmuk és így e fej. 3. §-a szerint a (K) congruentiát, a (K)-val egyenlő jelentésű

$$\Delta\Phi \equiv 0 \,(\mathrm{mod.}\, \{\nu_1, \ldots, \nu_k\}) \qquad (K'_\nu)$$

congruentiák rendszere teljesen pótolja.

E mellett két eset lehetséges a szerint, a mint a $\xi_{1\nu_1}, \ldots, \xi_{k\nu_k}$ mennyiségek az $F_j=0$ gyökrendszerét alkotják, vagy pedig nem. Az utóbbi esetnek megfelelő congruentiák azonban azonosan vannak kielégítve és egészen elhagyhatók; mert — mint könnyen kimutatható — ekkor

$$\Delta \equiv 0 \,(\mathrm{mod.}\, \{\nu_1, \ldots, \nu_k\}).$$

Minden esetre ugyanis

$$\Delta F_j \equiv 0 \,(\mathrm{mod.}\, \{\nu_1, \ldots, \nu_k\}),$$

és minthogy most az $x_1=\xi_{1\nu_1}, \ldots, x_k=\xi_{k\nu_k}$ értékekre nézve legalább egy az F_j-k közűl *nem* tünik el,

$$(F_j, \{\nu_1, \ldots, \nu_k\}) \sim 1;$$

de ekkor ΔF_j, mely F_j-t és $\{\nu_1, \ldots, \nu_k\}$-t is tartalmazza, e fejezet 3. §-a szerint tartalmazza e két osztórendszer szorzatát is; azaz valóban:

$$\Delta \equiv 0 \,(\mathrm{mod.}\, \{\nu_1, \ldots, \nu_k\}).$$

Ha tehát $F_1=0, \ldots, F_k=0$ gyökrendszereit ismét a kö-

vetkező módon jelöljük:

$$\xi_{1\nu}, \xi_{2\nu}, \ldots, \xi_{k\nu}, \qquad (\nu=1, \ldots, r)$$

akkor (K) *helyébe a következő congruentia-rendszer lép:*

$$\Lambda\Phi \equiv 0 \pmod{(x_1-\xi_{1\nu})^{c_{1\nu}}, (x_2-\xi_{2\nu})^{c_{2\nu}}, \ldots, (x_k-\xi_{k\nu})^{c_{k\nu}}} \quad (K_\nu)$$
$$(\nu=1, \ldots, r).$$

Szorosan a bizonyítás szavai szerint a congruentiák e rendszere csak olyan $\Phi = \sum_{i=1}^{k} H_i F_i$ előállítást szolgáltatna, a melyben a H_i formák együtthatói bizonyos az (A) tartományból származó genus-tartományhoz tartoznak. Ebből azonban mindig a Φ_i olyan előállítása is következik, a melyben a H_i-k az (A) tartományból származó formák*.

A (K) és (K_ν) feltételek tehát kölcsönösen helyettesítik egymást.

A (K_ν) feltételek most már olyan alakra hozhatók, a melynek a következőkben alapvető jelentősége van:

Legyenek $\xi_{1\nu}, \ldots, \xi_{k\nu}$, $(\nu=1, \ldots, r)$ az $F_j=0$ *egyenletrendszer összes különböző gyökrendszerei és* $c_{i\nu}$ *a* $\xi_{i\nu}$ *gyök sokszorossága az* $R_i=0$ *egyenletben; akkor annak szükséges és elegendő feltétele, hogy* Φ *a főosztály k-tagú* $(F_1, \ldots, F_k)$ *osztórendszerét tartalmazza a következő módon is kimondható: Kell, hogy meghatározhatók legyenek olyan* $K_{\nu 1}, \ldots, K_{\nu k}$ *formák, melyekre nézve*

$$\Lambda\Phi - \sum_{i=1}^{k} K_{\nu i} R_i$$

* Ha ugyanis $\Lambda\Phi \equiv 0 \pmod{R_1, \ldots, R}$, akkor egy

$$\Lambda\Phi = \sum_{i=1}^{k} K_i R_i$$

előállítás a közönséges osztási eljárással, azaz raczionális műveletek segítségével nyerhető és ép úgy jutunk ettől ismét raczionális műveletek segítségével a

$$\Phi = \sum_{i=1}^{k} H_i F_i$$

előállításhoz.

-nek az $x_1-\xi_{1\nu},\ldots,x_k-\xi_{k\nu}$ *hatványszorzatai szerint való kifejtésében nem fordúlnak elő olyan tagok, a melyeknek dimensiója* $\leqq\sum_{i=1}^{k} c_{i\nu}-k$.

A kimondott feltétel minden esetre szükséges feltétel; mert hiszen vannak olyan K formák is, a melyekre nézve ama kifejezés azonosan egyenlő a zérussal. Hogy pedig elegendő is e feltétel, abból látható, hogy $\Delta\Phi-\sum_{i=1}^{k} K_{\nu i}R_i$ kifejtésében minden tagnak legalább egy $x_i-\xi_{i\nu}$ tényezőt kell tartalmaznia a $c_{i\nu}$ kitevővel ellátva. Ha minden ilyen tényező kitevője $\leqq c_{i\nu}-1$ volna, akkor épen az illető tag dimensiója nem volna nagyobb $\Sigma c_{i\nu}-k$-nál. Így e föltétel mellett

$$\Delta\Phi-\sum_{i=1}^{k} K_{\nu i}R_i\equiv 0\,(\mathrm{mod.}\,(x_1-\xi_{1\nu})^{c_{\nu 1}},\ldots,(x_k-\xi_{k\nu})^{c_{k\nu}})$$

és egyszerűsítve

$$\Delta\Phi\equiv 0\,(\mathrm{mod.}\,(x_1-\xi_{1\nu})^{c_{1\nu}},\ldots,(x_k-\xi_{k\nu})^{c_{k\nu}}).$$

13. §. E fejtegetések alapján végre *Noether tételének** általánosítását nyerjük, a melynek az algebrai mennyiségek elméletében, különösen ezen elmélet alkalmazásainak egész sorozatában alapvető jelentősége van.

Legyenek $\xi_{1\nu},\ldots,\xi_{k\nu},(\nu=1,\ldots,r)$ *az* $F_1=0,\ldots,F_k=0$ *egyenletrendszer összes különböző gyökrendszerei, ha abban* $x_1,\ldots,x_k$*-t tekintjük ismeretleneknek; legyenek továbbá a*

* A kérdéses tételt az irodalomban eddig egyedül tárgyalt $k=2$ esetre, a mely az algebrai görbék, ill. az egy változós algebrai függvények elméletére vonatkozik, legelőször Noether M. mondta ki. («Zur Theorie des eindeutigen Entsprechens algebraischer Gebilde von beliebig vielen Dimensionen» Math. Annalen II. k. 314. l. Szigorúbb tárgyalással pedig: «Über einen Satz aus der Theorie der algebraischen Functionen». Math. Annalen VI. k. 351. l.). A tétel további irodalmára vonatkozó részletes adatokat adja Brill és Noether «Bericht über die Entwicklung der Theorie der algebraischen Functionen» cz. munkája. («Jahresberichte der deutschen Mathematiker-Vereinigung» III. köt. 347. l.)

λ_{jj} formának az $x-\xi_{1\nu}, \ldots, x_k-\xi_{k\nu}$ hatványszorzatai szerint való kifejtésében az $l_{j\nu}$-ed dimensiójú tagok a legalacsonyabb dimensiójúak, a melyek abban egyáltalában előfordúlnak, vagyis az V. fej. 6. §-ában bevezetett kifejezésmód szerint legyen $\xi_{1\nu}, \ldots, \xi_{k\nu}$ a $\lambda_{jj}=0$ sokaság $l_{j\nu}$-szeres eleme; $c_{i\nu}$ pedig legyen úgy, mint előbb az R_i-re nézve hasonló jelentésű szám. Akkor annak szükséges és elegendő feltétele, hogy Φ az $(F_1, \ldots, F_k)$ osztórendszert tartalmazza, következőképen mondható ki:

Kell, hogy meghatározhatók legyenek olyan tulajdonságú $H_{1\nu}, \ldots, H_{k\nu}$ formák, melyekre nézve

$$\Phi - \sum_{i=1}^{k} H_{i\nu} F_i$$

-nek az $x_1-\xi_{1\nu}, \ldots, x_k-\xi_{k\nu}$ hatványszorzatai szerint való kifejtésében ne forduljanak elő d_ν-ed vagy ennél alacsonyabb dimensiójú tagok. E mellett minden esetre elegendő, a

$$d_\nu = \sum_{j=1}^{k} (c_{j\nu} - l_{j\nu}) - k$$

fölvétel.

Az előrebocsátott fejtegetés után e tétel bebizonyítása igen egyszerű. De mielőtt e bizonyításra áttérnénk, még egy (az előbbi § tételére vonatkozó) megjegyzést akarunk közbeszúrni. A $\Phi \equiv 0 \pmod{F_1, \ldots, F_k}$ fönnállására kimondott szükséges és elegendő feltétel ép úgy, mint az előbbi (a 11. §-ban) algebrai feltétel; azaz a négy alapművelet és adott orthoid formák legnagyobb közös osztójának meghatározása segítségével véges számú lépésben döntjük el, vajjon ama feltétel kielégíthető-e.

A tétel természete szerint $H_{i\nu}$ ama tagjainak, a melyeknek dimensiója d_ν-t túlhaladja, az itt fejtegetendő kérdésre nincsen befolyásuk; elégséges tehát, ha a $H_{i\nu}$-ket olyan d_ν-ed dimensiójú általános formáknak veszszük fel, a

melyeknek együtthatói valamely meghatározott genus-tartományhoz, azaz valamely orthoid tartományhoz tartoznak. Ama feltétel e szerint a H-k együtthatóira vonatkozó lineáris diophantikus egyenletek rendszerét szolgáltatja, a melynek részletes tárgyalásába nem bocsátkozunk. Annál kevésbbé teszszük ezt, mert annak gyakorlati eldöntésére, hogy létezik-e ilyen $\Phi = \sum_{i=1}^{k} H_i F_i$ előállítás, valamint a H_i formák meghatározására a 11 § tétele sokkal egyszerűbb eszközöket nyújt.

Nœther tételének fontossága kiválóan azokban a tulajdonságokban nyilvánúl, a melyeket az az osztórendszert tartalmazó Φ formák számára megállapít. Különösen kiemeljük mindjárt azt a körülményt, hogy *a most megadott szükséges és elegendő feltételek — mint az közvetetlenül belátható — az $x_1, \ldots, x_k$ határozatlanokra alkalmazott (homogén) lineáris transformatiótól függetlenek.*

Ha most végre a tétel bebizonyítására térünk át, a feltétel szükséges volta ismét nyilvánvaló; mert hiszen olyan H_i formák is vannak, a melyekre nézve $\Phi - \sum_{i=1}^{k} H_i F_i$ azonosan egyenlő a zérussal.

Hogy a feltétel elegendő voltát kimutathassuk, mindenekelőtt megjegyzendő, hogy

$$\Psi \equiv 0 \,(\text{mod. } \{a+1\}),$$

a hol $\{a+1\}$-et a kifejezésmód egyszerűsítése kedvéért az

$$(\ldots, (x_1 - \xi_{1\nu})^{g_1} (x_2 - \xi_{2\nu})^{g_2} \ldots (x_k - \xi_{k\nu})^{g_k}, \ldots)$$
$$(g_1 + g_2 + \cdots + g_k = a+1)$$

osztórendszer rövid jelképe gyanánt használjuk, azt a tényt fejezi ki, hogy a Ψ formának az $x_1 - \xi_{1\nu}, x_2 - \xi_{2\nu}, \ldots$ hatványszorzatai szerint való kifejtése a-dik, vagy pedig annál alacsonyabb dimensiójú tagokat nem tartalmaz.

Ha már mostan a kimondott feltételnek megfelelőleg van olyan tulajdonságú $H_{i\nu}$ formarendszer, hogy

$$\Phi - \sum_{i=1}^{k} H_{iv} F_i \equiv 0 \,(\mathrm{mod.}\, \{d_v+1\}),$$

akkor

$$\lambda_{11}\Phi - H_{1v}\lambda_{11} F_1 - \sum_{i=2}^{k} \lambda_{11} H_{iv} F_i \equiv 0 \,(\mathrm{mod.}\, \{d_v+l_{1v}+1\}).$$

Ha tehát $\lambda_{11} F_1$ helyébe R_1-et vezetjük be, akkor olyan H'_{iv} formarendszer is van, a melyre nézve

$$\lambda_{11}\Phi - H'_{1v} R_1 - \sum_{i=2}^{k} H'_{iv} F_i \equiv 0 \,(\mathrm{mod.}\, \{d_v+l_{1v}+1\}).$$

Ha ismét λ_{22}-vel szorzunk, R_2-t bevezetjük és ezt így tovább folytatjuk, végre a

$$\Lambda\Phi - \sum_{i=1}^{k} K_{vi} R_i \equiv 0 \,(\mathrm{mod.}\, \{d_v + \sum_{j=1}^{k} l_{jv} + 1\})$$

congruentiához jutunk.

Ámde, ha $d_v \geqq \sum_{j=1}^{k} (c_{jv} - l_{jv}) - k$, akkor

$$d_v + \sum_{j=1}^{k} l_{jv} + 1 \geqq \sum_{j=1}^{k} c_{jv} - k + 1$$

és evvel a 12. § feltétele teljesülvén, a tétel be van bizonyítva.

Magától értetődik, hogy egyáltalában nincsen kizárva (sőt a legegyszerűbb «általános» feltevéseket kivéve valóban úgy is van), hogy a d_v szám azon értéke, a melyet mindig használhatunk, t. i. $\sum_{=1}^{k} (c_{jv} - l_{jv}) - k$, a szükségesnél nagyobb.

Beállhat az az eset, hogy az adott feltétel helyett már a

$$\Phi - \sum_{i=1}^{k} H_{iv} F_i \equiv 0 \,(\mathrm{mod.}\, \{d_v\})$$

föltétel is elégséges. Ekkor azonban kell, hogy minden d_v-ed dimensiójú hatványszorzat is kielégítse az

$$(x_1 - \xi_{1v})^{h_1} \ldots (x_k - \xi_{kv})^{h_k} \equiv 0 \,(\mathrm{mod.}\, \{d_v+1\})$$
$$(h_1 + \cdots + h_k = d_v)$$

feltételt és ez egyszersmind elegendő is. Vajjon ez a congruentia-feltétel teljesül-e, az a diophantikus egyenletek bizonyos sorozata oldhatóságának vizsgálatával, tehát véges számú lépésben dönthető el. Tehát d_ν vagy a legkisebb szám, a mely a Nœther-féle feltételekbe belép, vagy pedig $d_\nu - 1$ vehető helyette. Ezt az eljárást folytatva az algebrai műveletek sorozata bizonyos legkisebb e_ν számhoz vezet úgy, hogy *annak eldöntésére, vajjon fennáll-e a* $\Phi \equiv 0 \pmod{F_1, \ldots, F_k}$ *congruentia, szükséges és elegendő, ha* Φ*-t a* $\sum_{i=1}^{k} H_i F_i$*-nek az* $x_1 - \xi_{1\nu}, \ldots, x_k - \xi_{k\nu}$ *hatványszorzatai szerint való kifejtésével az* e_ν*-ed dimensiójú tagokig (bezárólag) összehasonlítjuk* míg, ha $e'_\nu < e_\nu$, így csak szükséges, de *nem* elegendő feltételhez jutunk.

Az így értelmezett és algebrailag is meghatározott e_ν számot a következőkben a $\xi_{1\nu}, \ldots, \xi_{k\nu}$ *gyökrendszer charakteristikájának* nevezzük. Az általánosított Nœther-féle tétel alkalmazásaira fontos, hogy az egyes gyökrendszerek e charakteristikáját az $(F_1, \ldots, F_k)$ osztórendszer általános tulajdonságaiból pontosabban meghatározhassuk.

A gyökrendszerek charakteristikájának elmélete az «egyszerű» esetben.

14. §. Legyen ismét az $F_i = 0, (i = 1, \ldots, k)$ egyenletrendszer, a melyben $x_1, \ldots, x_k$-t ismeretleneknek tekintjük, k-adfokozatú és legyen

$$\xi_{1\nu}, \xi_{2\nu}, \ldots, \xi_{k\nu}$$

véges számú gyökrendszereinek egyike.

Továbbá F_i-nek az $x_1 - \xi_{1\nu}, x_2 - \xi_{2\nu}, \ldots$ hatványszorzatai szerint való kifejtése kezdődjék az $a_{i\nu}$-ed dimensiójú tagokkal, a melyeknek complexusát φ_i-vel jelöljük úgy, hogy

$$F_i = \varphi_i + \varphi_i^{(a_{i\nu}+1)} + \cdots;$$

ezt a tényt pedig csatlakozva a már használt jelölésekhez, az

$$F_i \equiv 0 \pmod{\{a_{iv}\}}$$

congruentiával fejezzük ki, a hol természetesen $a_{iv} \geqq 1$.

Most az ú. n. «*egyszerű esetet*»* vizsgáljuk, a melyet az a feltevés jellemez, *hogy a* $\varphi_i = 0$ *egyenletrendszernek csak ez az egy* $x_j = \xi_{jv}$ *megoldása van.* Magától értetődik, hogy ekkor

$$r_v = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_k \\ z_1, \ldots, z_k \end{pmatrix} \neq 0,$$

a hol a kifejezésmód rövidsége kedvéért $z_j = x_j - \xi_{jv}$ legyen.

Ha még

$$A_v = a_{1v}\, a_{2v} \ldots a_{kv},$$

akkor a mostani feltevés mellett

$$r_v\, z_j^{A_v} = \mu_{j1}\varphi_1 + \cdots + \mu_{jk}\varphi_k, \tag{1}$$

a hol magától értetődik, hogy μ_{ji} a $z_1, \ldots, z_k$ határozatlanoknak $A_v - a_{vj}$-dik dimensiójú homogén formája.

Ha most még a 10. § utasítása szerint a $\varphi_1, \ldots, \varphi_k$ formákra vonatkozó $R_1, \ldots, R_k$ formasorozatot alkotjuk, akkor $R_1 = 0, \varphi_2 = 0, \ldots, \varphi_k = 0$ egyenleteknek is csak ez az egy gyökrendszerük lesz: $z_1 = 0, \ldots, z_k = 0$ s í. t. Így tehát mindig egyrészt az egyszerű esettel, másrészt pedig homogén formákkal van dolgunk. A 13. § elején kimondott tétel szerint meghatározott c_{jv} és l_{jv} számok tehát olyanok lesznek, hogy $c_{jv} - l_{jv} = a_{jv}$ és ebből közvetetlenül következik, hogy *a* $z_j = 0$ *gyökrendszer charakteristikája a* $\varphi_i = 0$ *egyenletrendszerre vonatkozólag nem nagyobb* $\sum_{i=1}^{k} a_{iv} - k$*-nál.*

* Ezt az elnevezést a $k=2$ esetében NOETHER alkalmazta először (i. h.) Ha (A) a complex számok összessége, akkor «a k-dimensiós tér geometriájával» van dolgunk és a geometria kifejezésmódja szerint az «egyszerű eset» az, midőn a $(\xi_{1v}, \ldots, \xi_{kv})$ pont az összes $F_i = 0$ ($k-1$-dimensiós) sokaságoknak pontja ugyan, de nincsen olyan «egyenes», a mely e pontban az összes $F_i = 0$ sokaságoknak a_{iv}-edrendű érintője volna.

15. §. Hogy ugyanez érvényes most az $F_i=0$ egyenletrendszer esetében is, a további bebizonyítás tárgya.

E célból előbb megmutatjuk, hogy *mindig választhatunk oly* $M_i (i=1,\ldots,k)$ *formákat, a melyeknek a* z*-k hatványszorzatai szerint való kifejtése pontosan az* $A_\nu - a_{i\nu}$*-ed dimensiójú tagokkal kezdődik, míg*

$$z_1^{A_\nu} - \sum_{i=1}^{k} M_i F_i$$

-nek a z*-k hatványszorzatai szerint való kifejtéséből kiesnek mindazok a tagok, a melyeknek dimensiója valamely elég nagynak választott* g *számnál kisebb.*

Ennek megfelelőleg írjuk, hogy

$$M_i = M_{i0} + M_{i1} + M_{i2} + \cdots$$

és úgy, mint előbb

$$F_i = \varphi_i + \varphi_i^{(a_{i\nu}+1)} + \varphi_i^{(a_{i\nu}+2)} + \cdots .$$

Az M_i e kifejtése úgy értelmezendő, hogy abban M_{ih} a z-knek $A_\nu - a_{i\nu} + h$-ad dimensiójú homogén formája.

Ekkor először is szükséges, hogy

$$\sum_{i=1}^{k} M_{i0} \varphi_i = z_1^{A_\nu}$$

legyen és ezt úgy érjük el, ha M_{i0}-t (1) szerint a következő módon választjuk:

$$M_{i0} = \frac{1}{r_\nu} \mu_{1i}.$$

Így tehát az M_{i1} formákat úgy kell meghatároznunk, hogy

$$\sum_{i=1}^{k} M_{i1} \varphi_i = -\sum_{i=1}^{k} M_{i0} \varphi_i^{(a_{i\nu}+1)}$$

legyen. Itt a jobb oldalon a z-knek $A_\nu + 1$-dik dimensiójú homogén formája áll; ámde már

$$A_\nu = a_{1\nu} \ldots a_{k\nu} > \sum_{i=1}^{k} (a_{i\nu} - 1)$$

és így tehát ama tételek szerint, a melyeket a $\varphi_i=0$ egyenletrendszerre vonatkozólag bebizonyítottunk, elérhető, hogy

$$-\sum_{i=1}^{k} M_{i0}\varphi_i^{(a_{iv}+1)} = \sum_{i=1}^{k} \mu_{i1}\varphi_i$$

legyen; és ennek megfelelőleg M_{i1}-et a következő módon választhatjuk:

$$M_{i1}=-\mu_{i1}.$$

Ha a jellemzett egyszerű eljárást folytatjuk, akkor az

$$M_i=M_{i0}+M_{i1}+\cdots+M_{i,\,g-a_{iv}}$$

formák valóban kielégítik a megszabott feltételeket. Ha végre g-t nagyobbnak választjuk A_v+e_v-nél, akkor $z_1^{A_v}-\sum_{i=1}^{k} M_i F_i$-nek a z-k hatványszorzatai szerint való kifejtésében minden tag mint két oly tényező szorzata lesz előállítható, a mely mind a kettő a z-knek hatványszorzata; még pedig az egyik, (P') A_v-ed dimensiójú lesz, a másiknak, (P''-nek) pedig dimensiója nagyobb lesz e_v-nél, a hol e_v a $z_j=0$ gyökrendszer karakteristikája $F_i=0$-ra vonatkozólag. Ennek megfelelőleg:

$$z_1^{A_v}-\sum_{i=1}^{k} M_i F_i=\sum_{h=1}^{H} P'_h P''_h.$$

Ha már most minden tagot a 10. §-ban értelmezett

$$\frac{R_1(x_1)}{(x_1-\xi_{1v})^{c_{1v}}} = (x_1-\xi_{1v})^{c_{11}}\ldots$$

formával megszorzunk és ismét $z_j=x_j-\xi_{jv}$, akkor nyerjük, hogy

$$\bar{R}_1(x_1)=\sum_{i=1}^{k} \bar{M}_i F_i+\sum_{h=1}^{H} P'_h\left(P''_h(x_1-\xi_{11})^{c_{11}}\ldots\right).$$

Minthogy megfelelőleg választott lineáris transformatio alkalmazása után két különböző gyökrendszer kivétel nélkül különböző mennyiségekből áll, azért a hozzácsatolt tényezőnek $x_1-\xi_{1v},\ldots,x_k-\xi_{kv}$ hatványszorzatai szerint való kifejtése el nem tünő, 0-ad dimensiójú tagot szolgáltat és

így tehát a $\bar{R}_1(x_1), \bar{M}_1, \ldots, \bar{M}_k$ formák kifejtése ugyanazon hatványszorzatok szerint ugyanolyan dimenziójú tagokkal kezdődik, mint a $z_1^{A_\nu}$ és $M_1, \ldots, M_k$ formáké.

Látjuk továbbá, hogy a

$$P_h''(x_1-\xi_{11})^{c_{11}}\ldots$$

formák Nœther tételének feltételeit kielégítik. A $\xi_{1\nu}, \ldots, \xi_{k\nu}$ gyökrendszer esetében ez egyszerű következménye annak a körülménynek, hogy a P_h''-nak az $x_1-\xi_{1\nu}, \ldots, x_k-\xi_{k\nu}$ hatványszorzatai szerint való kifejtése csak olyan tagokat tartalmaz, a melyeknek dimenziója e_ν-nél nagyobb. A többi gyökrendszer esetében ez kitünik abból a tényből, hogy a vizsgált forma osztható $(x_1-\xi_{11})^{c_{11}}$-gyel stb.-vel és így tehát a 12. § (K_ν) congruentiáját kielégíti.

E szerint tehát

$$\sum_{h=1}^{H} P_h'\left(P_h''(x_1-\xi_{11})^{c_{11}}\ldots\right)=\sum_{i=1}^{k}\bar{N}_i F_i$$

és az $\bar{N}_i$ formáknak az $x_1-\xi_{1\nu}, \ldots, x_k-\xi_{k\nu}$ hatványszorzatai szerint való kifejtései a P_h' megfelelő tulajdonsága miatt olyan tagokkal kezdődnek, a melyeknek dimenziója nem lehet kisebb A_ν-nél.

Ha tehát

$$\bar{M}_i+\bar{N}_i=\lambda_{1i},$$

akkor

$$\bar{R}_1(x_1)=\sum_{i=1}^{k}\lambda_{1i}F_i,$$

a hol $\bar{R}_1(x_1)$-nek ama hatványszorzatok szerint való kifejtése pontosan A_ν-ed dimenziójú tagokkal kezdődik, a λ_{1i}-é pedig olyanokkal, a melyeknek dimenziója legalább $A_\nu-a_{i\nu}$.

Most már az $\bar{R}_1(x_1), F_2, \ldots, F_k$ formarendszerrel teljesen ugyanazon a módon bánhatunk el, mert ekkor a 14. § értelmezése szerint mindig ismét az «egyszerű» esettel van dolgunk. Így tehát olyan

$$\bar{R}_\mu(x_\mu)=\sum_{\varrho=1}^{\mu-1}\bar{\lambda}_{\mu\varrho}\bar{R}_\varrho+\sum_{j=\mu}^{k}\lambda_{\mu j}F_j \qquad (\bar{R}_\mu)$$
$$(\mu=1,\ldots,k)$$

formasorozathoz jutunk, a mely a 13. § tételében alkalmazható. Ámde most az ott fellépő $c_{j\nu}-l_{j\nu}$ szám legfölebb $a_{j\nu}$ lehet és így tehát a következő tételhez jutunk:

Ha $\xi_{1\nu},\ldots,\xi_{k\nu}$ *az* $F_i=0$ *sokaság* $a_{i\nu}$*-szeres eleme, akkor az «egyszerű» esetben a* $\xi_{1\nu},\ldots,\xi_{k\nu}$ *gyökrendszer charakterisztikája az* $F_1=0,\ldots,F_k=0$ *egyenletrendszerre vonatkozólag nem nagyobb* $\Sigma a_{i\nu}-k$*-nál.*

Hilbert tétele.

16. §. Ha $F_i(x_1,\ldots,x_m)$ $(i=1,\ldots,k)$ ismét az (A) orthoid tartományból származó formák, de

$$(F_1, F_2,\ldots, F_k)$$

most egészen tetszés szerinti osztórendszer, akkor közvetetlenül belátható, hogy valamely Φ forma a

$$\Phi\equiv 0 \pmod{F_1, F_2,\ldots, F_k}$$

congruentiának csak úgy felelhet meg, azaz csak úgy lehet $\Phi=\sum_{i=1}^{k}H_iF_i$, ha a $\Phi=0$ egyenletet az $F_i=0$ egyenletrendszer minden gyökrendszere kielégíti. De már a főosztályhoz tartozó osztórendszerek esete is mutatja, hogy ez a szükséges feltétel épenséggel nem elegendő. Ebben az esetben a következő tétel érvényes, a melyet teljes általánosságában Hilbert D.* állított fel:

Legyenek

$$G_1, G_2,\ldots, G_l$$

bármilyen formák és az $F_i=0$ *egyenletrendszer minden gyök-*

* «Über die vollen Invariantensysteme». Math. Ann. XLII. köt. 320. lap.

rendszerére nézve legyen $G_j \equiv 0$. *Akkor van olyan az* $(F_1, \ldots, F_k)$ *osztórendszer meghatározta pozitiv egész szám* r, *a melynek az a tulajdonsága, hogy mindig*

$$G_{j_1} G_{j_2} \ldots G_{j_r} \equiv 0 \pmod{F_1, \ldots, F_k},$$

ha $G_{j_1}, \ldots, G_{j_r}$ *a* $G_1, \ldots, G_l$ *sorozat tetszés szerinti formái.*

A helyett, hogy HILBERT bizonyításának bonyolódott menetét követnők, megmutatjuk, hogy e tétel az V. fejezetben kifejtett általános eliminácziό-elmélet egyszerű corollariuma.

Mindenekelőtt megjegyezzük, hogy a tételünkben kifejezett tényállás teljesen független az F és G formákon egyidejűleg végzett bármely (homogén) lineáris transformatiótól. Ezt a körülményt a bizonyításban is fölhasználjuk, és föltételezzük, hogy az $F_i = 0$ egyenletrendszer összresolvensének fölállítását megelőző transformatiót úgy választottuk, hogy ennek következtében a G formák is mind szabályosokká váljanak*.

Legyen azután a $\Phi_t = 0$ az $F_i = 0$ egyenletrendszer összresolvense (V. fej. 4. §) és P_{hj_h} a Φ_t valamely iereducibilis osztója. Akkor a föltevés szerint G_j eltünik minden oly értékrendszerre nézve, a mely kielégíti a

$$P_{hj_h}\left(\sum_{i=1}^{m} t_i x_i,\ x_{h+1}, \ldots, x_{m-1}\right) = 0$$

egyenleteket, a hol a t-ket határozatlanoknak tekintjük. Ha most x_m helyébe bevezetve x-et, G_j a t_m megfelelő hatványával szorozva átmegy $\bar{G}_j$-be, akkor $\bar{G}_j$-nek oszthatónak kell lennie $P_{hj_h}(x, x_{h+1}, \ldots, x_{m-1})$-gyel. Mert különben a közönséges osztási eljárás egy

$$R = \bar{G}_j - P_{hj_h} Q$$

* Azt az esetet, hogy valamely G az x-eket nem is tartalmazza, természetesen nem kell tekintetbe vennünk.

kifejezéshez vezetne, mely x-ben a P_{hj_h}-nál alacsonyabb fokú és nem 0. Ha pedig ekkor az

$$x_{h+1}=\xi_{h+1}, \ldots, x_{m-1}=\xi_{m-1}$$

értékeket úgy választjuk, hogy P_{hj_h} discriminánsa x szerint ne legyen 0, akkor ennek megfelelőleg van egy

$$x=\sum_{i=1}^{h} t_i \xi_i' + \sum_{j=h+1}^{m-1} t_j \xi_j + t_m \xi_m'$$

érték, melyre nézve P_{hj_h} zérus és R nem zérus. Erre nézve $\bar{G}_j$ sem volna zérus, azaz G_j ama a $P_{hj_h}=0$ egyenleteknek megfelelő értékrendszer helyettesítésénél a föltevés ellenére nem tünnék el. Hasonlóképen kell, hogy $\bar{G}_j$ a Φ_t bármely más irreducibilis osztójával is osztható legyen.

Ha tehát r a legnagyobb kitevő, a melylyel valamely irreducibilis tényező a Φ_t-ben előfordúl, akkor

$$\bar{G}_{j_1} \bar{G}_{j_2} \ldots \bar{G}_{j_r}$$

osztható Φ_t-vel és igy tehát ép úgy, mint ez a forma maga kielégíti a

$$\bar{G}_{j_1} \bar{G}_{j_2} \ldots \bar{G}_{j_r} \equiv 0 \,(\text{mod. } F_1, \ldots, F_k, x-\Sigma t_i x_i)$$

congruentiát. Ha azután x helyébe $\sum_{i=1}^{m} t_i x_i$-t írjuk és a két oldalon a t-k hatványszorzatainak együtthatóit összehasonlítjuk, akkor valóban úgy, mint bebizonyítandó volt,

$$G_{j_1} G_{j_2} \ldots G_{j_r} \equiv 0 \,(\text{mod. } F_1, \ldots, F_k).$$

NYOLCZADIK FEJEZET.

A LINEÁRIS DIOPHANTIKUS PROBLÉMÁK ARITHMETIKAI ELMÉLETE.

Az absolut törzsrendszerek $[[1], x_1, \ldots, x_k]$-ban.

1. §. Legyenek $S_1, S_2, \ldots$ az $x_1, x_2, \ldots, x_k$ határozatlanoknak bármilyen raczionális és egész formái. Ha az $(S_1, S_2, \ldots)$ osztórendszert, a melyet most röviden az (S) jelképpel jelölünk, megfelelő módon választjuk, megtörténhetik, hogy van az $[[1], x_1, \ldots, x_k]$ tartomány formáinak olyan *véges* sorozata:

$$C_0, C_1, \ldots, C_{s-1},$$

hogy az említett tartomány minden formája a C formák közül egygyel és csak egygyel congruens mod. (S). Az (S) osztórendszernek ezt a tulajdonságát a következőkben avval a kifejezésmóddal jelezzük, hogy «*van az* (S) *osztórendszernek megfelelő* $C_0, \ldots, C_{s-1}$ *teljes maradékrendszer*». E mellett magától értetődik, hogy bármely C_i felcserélhető minden más olyan C_i' formával, a mely C_i-vel congruens mod. (S).

Ha továbbá valamely az (S) osztórendszernek megfelelő teljes maradékrendszer ismeretes és adva van olyan eljárás, a melylyel mindig meghatározhatjuk a maradékrendszernek azt a C_i formáját, mely valamely adott F formával congruens, akkor az

$$AX \equiv B \,(\mathrm{mod.}\,(S))$$

«lineáris congruentia megoldása» elintézettnek tekinthető;

e mellett két olyan megoldás, a mely congruens mod. (S), nem tekintendő különbözőnek. Minthogy most csupán csak a $C_0, C_1, \ldots, C_{s-1}$ gyökök lehetségesek, mindössze véges számú kisérlettel megállapítandó, hogy az $AC_0, AC_1, \ldots, AC_{s-1}$ mennyiségek közül melyik congruens a B mennyiséggel (a mely maga $\equiv C_j$).

Ha pedig az adott osztórendszer absolut törzs-osztórendszer — az ilyent ezentúl (P)-vel jelöljük — és A *nem* $\equiv 0 (\text{mod. } (P))$, akkor az

$$AX \equiv B (\text{mod. } (P))$$

congruentiának egy és csak egy gyöke van.

Ekkor ugyanis $(A, (P)) \simeq 1$, minthogy (P) tartalmazza ezt az osztórendszert, a mely nem lehet $\simeq (P)$-vel; az ellenkező esetben ugyanis feltevésünk ellenére $A \equiv 0 (\text{mod. } (P))$ volna.

Ebből az æquivalentiából azonban egy

$$\lambda A + \mu_0 P_0 + \mu_1 P_1 + \cdots = 1,$$

azonosság fönnállása következik, vagyis olyan λ forma létezése, a melyre nézve

$$\lambda A \equiv 1 (\text{mod. } (P)),$$

és így tehát

$$X \equiv \lambda B (\text{mod. } (P)).$$

Ez a mennyiség, minthogy a congruentiát valóban kielégíti, ennek egyetlen gyöke.

Az előbb megállapított feltevések értelmében e gyök a kisérletek véges sorozatával nyerhető.

Ha az (S) osztórendszer ismét megfelel a fentebbi feltételeknek, akkor az $x_1, \ldots, x_k, x_{k+1}, \ldots, x_m$ határozatlanok raczionális és egész formáinak «oszthatósága mod. (S)» elemi elméletben tárgyalható.

«Valamely F forma mod. (S) osztható a G formával», ha van olyan harmadik forma H, hogy

$$F \equiv GH (\text{mod. } (S)).$$

Minthogy most (S) az $x_{k+1}, \ldots, x_m$ határozatlanokat nem tartalmazza, csak úgy lehet $F - GH \equiv 0 \pmod{(S)}$, ha $x_{k+1}, \ldots, x_m$ különböző hatványszorzatainak minden egyes együtthatója már magában is $\equiv 0 \bmod (S)$; ebből pedig következik, hogy G és H, ha elhagyjuk belőlük azokat a tagokat, a melyek $\equiv 0 \bmod (S)$, (a mi hiszen itt, a hol az F, G, H formák mindig $\bmod (S)$ értendők, nem idéz elő változást), az $x_{k+1}, \ldots, x_m$ határozatlanokra vonatkozólag nem lehetnek magasabb fokúak mint F. Minthogy végre $x_{k+1}, \ldots, x_m$ különböző hatványszorzatainak együtthatói csakis a teljes maradékrendszerben fellépő formák lehetnek, látjuk, hogy *F-nek csak véges számmal lehetnek osztói és világos, hogy ezek a kisérletek véges sorozatával meghatározhatók; még pedig úgy, hogy a G osztóval együtt mindjárt a «complementáris» osztót, H-t is megkapjuk.*

Teljes analogiában a raczionális és egész formák oszthatóságának közönséges elméletével azt mondjuk, hogy *az F és G formák* «$\bmod (S)$ *aequivalensek*», ha az egyiknek osztói $\bmod (S)$ ugyanazok, mint a másikéi, vagyis tehát, ha F osztható G-vel és G osztható F-fel $\bmod (S)$.

Végre F «$\bmod (S)$ irreducibilis», ha F minden osztója az egységgel, vagy magával F-fel æquivalens $\bmod (S)$.

Most áttérünk a specziális

$$(M^{(k)}) = (M_k, \ldots, M_2, M_1, n_0)$$

osztórendszer vizsgálatára, hol n_0 valamely az 1-től különböző raczionális és egész pozitiv szám és általánosságban

$$M_i = x_i^{n_i} + \varphi_{i1} x_i^{n_i - 1} + \cdots + \varphi_{in_i},$$

míg $\varphi_{i1}, \ldots, \varphi_{in_i}$ az $x_i, x_{i+1}, \ldots, x_k$ *kizárása után* ismét az $x_1, \ldots, x_k$ határozatlanoknak raczionális és egész formái; $\varphi_{11}, \ldots, \varphi_{1n_1}$ tehát raczionális és egész számok.

Ha már most valamely tetszés szerinti $F(x_1, x_2, \ldots, x_k)$ formára a közönséges osztási eljárást alkalmazzuk, a következőket nyerjük:

$$F = M_k Q_k + R_k,$$
$$R_k = M_{k-1} Q_{k-1} + R_{k-1},$$
$$\ldots\ldots\ldots\ldots$$
$$R_2 = M_1 Q_1 + R_1;$$

ha továbbá R_1-ben a számbeli együtthatók helyébe a mod. n_0 legkisebb nem negativ maradékokat írjuk, vagyis tehát, ha

$$R_1 = n_0 Q_0 + R_0,$$

akkor végre

$$F \equiv R_0 (\text{mod. } M_k, \ldots, M_1, n_0).$$

Képezésénél fogva azonban R_0-nak x_i-re vonatkozó foka nem lépheti túl $n_i - 1$-et, míg, mint az $x_1, \ldots, x_k$ hatványszorzatainak együtthatói, R_0-ban csakis a $0, 1, \ldots, n_0 - 1$ számok szerepelhetnek.

Az így nyert formák azonban, a melyeknek száma nyilvánvalóan $n_0^{n_1 n_2 \cdots n_k}$, mindannyian különbözők mod. $(M^{(k)})$. Ha ugyanis ezeket következőképen jelöljük:

$$\varrho_0, \varrho_1, \ldots,$$

akkor, minthogy $\varrho_r - \varrho_s$-nek x_i-re vonatkozó foka sem éri el n_i-t és számbeli együtthatói az előjelt mellőzve nem lépik túl $n_0 - 1$-et, amaz osztási eljárást alkalmazva,

$$\varrho_r - \varrho_s = G_k M_k + G_{k-1} M_{k-1} + \cdots + G_1 M_1 + G_0 n_0$$

-ból $\varrho_r - \varrho_s$-nek ép oly előállítása származnék, a hol $G_k = 0, \ldots, G_1 = 0$ és azután $\varrho_r - \varrho_s$ osztható n_0-sal úgy, hogy végre a számbeli együtthatókra szabott feltétel következtében ϱ_r azonosan $= \varrho_s$.

E szerint tehát $\varrho_0, \varrho_1, \ldots$ az $(M^{(k)})$ osztórendszernek megfelelő teljes maradékrendszer, a melyre e § összes fejtegetései alkalmazhatók.

2. §. Az épen értelmezett $(M^{(k)})$ osztórendszert még

specziálisabban akarjuk választani; még pedig legyen e specziálisabb rendszer

$$(P^{(k)}) = (P_k, P_{k-1}, \ldots, P_1, p_0),$$

a hol p_0 valamely természetes törzsszám és P_i olyan racziónális és egész forma, amelyben az összes az M_i-re vonatkozólag megállapított tulajdonságok megvannak, és mely továbbá még irreducibilis mod. $(P^{(i-1)})$, vagyis mod. $(P_{i-1}, \ldots, P_1, p_0)$. Az így értelmezett rendszereknek, a melyeket röviden «*k*+1-*ed-fokozatú P-rendszereknek*»* nevezünk, a következő két tétel ad alapvető fontosságot az algebrai mennyiségek elméletében.

I. *Minden* $(P^{(k)})$ *rendszer absolut törzsrendszer ama racziónális és egész formák tartományában, a melyek más határozatlanokat nem tartalmaznak, mint a melyek a*

* A racziónális és egész formák tartományában a *P*-rendszer a törzsszám-fogalom természetszerű analogonja és nélkülözhetetlen, ha az arithmetikai problémákat ezekben a tartományokban tárgyaljuk. Eddig ezek közül csak az $m=1$ eset volt részletesebb vizsgálat tárgya; még pedig először Schönemann értekezésében (Journal f. r. u. a. Mathematik 31. és 32. k.). Ez a legegyszerűbb eset már Gauss hagyatékában is található (Werke, II. k. 197. l.); de Gauss-nak ez a vizsgálata csak később került nyilvánosságra.

E szerint tehát e fejezet egész tartalma új és az algebrai mennyiségek arithmetikai elméletének lényeges hézagát tölti be. Csak az itt kifejtett eredmények képesítenek bennünket arra, hogy az általános arithmetika két nagy problémáját — az alaprendszerek valóságos felállítását és valamely egész mennyiség irreducibilis tényezőkre való valóságos felbontását — a IX. fejezetben teljesen megoldhassuk.

Ehhez azonban mint alapvető fontosságú új módszeres segédeszközök kozzájárulnak a III. fejezetben értelmezett resolvens forma fogalma és Kronecker eliminácziő-elméletének erre támaszkodó általánosítása.

E rövid megjegyzés arra való, hogy reámutasson azon elméletek szükséges és következetes voltára, melyeket a szerző e könyvben kifejteni megkisérelt.

$P_k, \ldots, P_1, p_0$ *formákban előfordúlnak; továbbá egyszerűen törzsrendszer ama formák tartományában a melyek azokon kívül még a további* $x_{k+1}, \ldots, x_m$ *határozatlanokat is tartalmazzák.*

II. *Az* $x_1, \ldots, x_k$ *határozatlanok raczionális és egész formáinak tartományában minden absolut törzsrendszer aequivalens valamelyik* $(P^{(k)})$ *rendszerrel úgy, hogy ezek a rendszerek bizonyos meghatározott «kanonikus» alakban az absolut törzsrendszerek összességét megadják.*

A második tételt csak előlegesen említjük, hogy a P-rendszerek jelentőségére már itt reámutassunk; bebizonyításához, a melyet a 8. §. tartalmaz, még további segédeszközök szükségesek. Most csak az első tétellel foglalkozunk.

A $(P^{(k)})$ rendszerrel egy időben meg vannak adva a

$$(P^{(0)}) = (p_0),$$
$$(P^{(1)}) = (P_1, p_0),$$
$$\ldots\ldots\ldots$$
$$(P^{(k-1)}) = (P_{k-1}, \ldots, P_1, p_0)$$

rendszerek is, a melyek közül mindegyik tartalmazza a következőt, valamint végre $(P^{(k-1)})$ is a $(P^{(k)})$-t.

A $k=0$-nak megfelelő $(P^{(0)})$ osztórendszer tulajdonképen a p_0 törzsszám; a tétel tehát ebben a legegyszerűbb esetben minden esetre helyes. Általános érvényességére a teljes inductio segítségével következtetünk úgy, hogy feltételezve helyességét $(P^{(0)}), \ldots, (P^{(k)})$-re nézve, ezen az alapon bebizonyítjuk, hogy helyes a $(P^{(k+1)})$ esetében is.

Ennek a teljes inductio segítségével elvégzendő bebizonyításnak lényeges alapját találjuk a raczionális és egész formák ama tulajdonságaiban, melyek akkor mutatkoznak, midőn azokat mod. $(P^{(k)})$ vizsgáljuk, a hol $(P^{(k)})$-ről már feltételezzük, hogy az $[[1], x_1, \ldots, x_k]$ tartományban absolut törzsrendszer.

A mi először az $x_1, \ldots, x_k$ határozatlanoknak racionális és egész formáit illeti, van a $(P^{(k)})$ rendszernek megfelelő teljes maradékrendszer; az előbb felállított

$$\varrho_0, \varrho_1, \ldots$$

formák ilyent szolgáltatnak, a hol még $\varrho_0 = 0$, $\varrho_1 = 1$-nek vehető.

Ezek a ϱ formák, habár csak véges számmal vannak, «tartományt» alkotnak, a melyben az összeadás és szorzás a következő módon értelmezhető. ϱ_r és ϱ_s összege, ill. szorzata legyen a maradékrendszer ama formája, a mely az algebra közönséges szabályai szerint alkotott $\varrho_r + \varrho_s$-sel, ill. $\varrho_r \varrho_s$-sel congruens mod. $(P^{(k)})$. Ha azonban megállapítjuk, hogy az összes formák, a melyek $\equiv \varrho_r$ mod. $(P^{(k)})$, csak ugyanannak a ϱ_r formának különböző jelei, akkor azt is mondhatjuk, hogy a ϱ formák összeadása és szorzása az algebra közönséges szabályai szerint megy végbe; e mellett csak azért, hogy ezeket a kapcsolatokat a szó közönséges értelmében vett összeadástól és szorzástól megkülönböztethessük, most a megfelelő kijelentésekben az előbbitől különböző egyenlőségi jelt akarunk használni. Mint ilyen közvetetlenül kínálkozik a «$\equiv$ mod. $(P^{(k)})$» jel. Így tehát az

$$F \equiv \varrho_r \,(\text{mod. } (P^{(k)}))$$

kijelentésnek kettős értelme van, a mely nagyon egyszerű, majdnem magától értetődő, de, minthogy az arithmetikai vizsgálatok módszerére nézve egyenesen alapvető jelentőségű, mégis részletesen volt fejtegetendő.

A teljes maradékrendszer, a melyet ily módon «tartomány»-nak tekintünk, vagy — a mint még mondhatjuk — az «$[[1], x_1, \ldots, x_k]$ (mod. $(P^{(k)})$) tartomány» mennyiségei az összeadás és szorzás közönséges törvényét követik; minthogy $P^{(k)}$ törzsrendszer, abból, hogy

$$AB \equiv 0 \,(\text{mod. } P^{(k)}),$$

mindig következik, hogy

$$vagy\ A\equiv 0\ vagy\ B\equiv 0 \pmod{P^{(k)}};$$

végre az $AX\equiv B \pmod{P^{(k)}}$ congruentiának, ha A nem $\equiv 0$, mindig egy és csakis egy gyöke van. A tartomány az absolut egységet is tartalmazza és így tehát az orthoid tartomány minden tulajdonságát mutatja *egynek kivételével*, mert most az

$$1, 1+1, \ldots$$

sorozatban a zérus is előfordúl.

A kifejezés rövidségéért az olyan tartományt, a melyben az

$$1, 1+1, \ldots$$

sorozat a zérust tartalmazza, de a melyben különben a holoid, ill. orthoid tartomány minden tulajdonsága megvan, *pseudoholoid*, ill. *pseudoorthoid* tartománynak nevezzük.

Az $[[1], x_1, \ldots, x_k] \pmod{(P^{(k)})}$ *tartomány tehát pseudoorthoid tartomány.*

Pontosan ugyanazok a meggondolások mutatják, hogy *az* $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m] \pmod{(P^{(k)})}$ *tartomány pseudoholoid* tartomány. E mellett az $x_1, \ldots, x_m$ határozatlanoknak formáit csak úgy kell írnunk, mint az $x_{k+1}, \ldots, x_m$ határozatlanoknak formáit és az $x_1, \ldots, x_k$ határozatlanoknak együtthatókként szereplő formáit ismét mod. $(P^{(k)})$ kell vennünk; különösen, minthogy a feltevés szerint $(P^{(k)})$ ebben a tartományban is törzsrendszer, abból, hogy

$$FG\equiv 0 \pmod{(P^{(k)})},$$

most is következik, hogy

$$vagy\ F\equiv 0,\ vagy\ G\equiv 0 \pmod{P^{(k)}};$$

és ez ismét csak úgy lehetséges, ha F vagy G minden együtthatója (abban a felfogásban, hogy ezek az $x_1, \ldots, x_k$ határozatlanoknak formái) $\equiv 0 \pmod{(P^{(k)})}$. E tartomány

tehát csak egyetlen egy «zérust» tartalmaz. Végre pl. az

$$x_{k+1} X \equiv 1 \,(\text{mod. } P^{(k)})$$

congruentiának nincsen megoldása, mert az ellenkező feltevésből az is következnék, hogy

$$0 \equiv 1 \,(\text{mod. } P^{(k)}).$$

Az $[[1], x_1, \ldots, x_m] (\text{mod. } (P^{(k)}))$ pseudoholoid tartományból ismét az $([1], x_1, \ldots, x_m) (\text{mod. } (P^{(k)}))$ tartomány származik, az előbbinek mellérendelt pseudoorthoid tartománya (l. az I. fej. 4. §-át), a mely az összes $\frac{F}{G}$ formahányadosokból áll, a hol G különböző a 0-tól mod. $(P^{(k)})$.

Ezen az alapon épül fel azután az

$$[[1], x_1, \ldots, x_m] (\text{mod. } (P^{(k)}))$$

tartomány formáinak oszthatósági elmélete, a melyet nem kell részletesen fejtegetnünk, mert szóról szóra megegyezik a III. fej. 1., 2., 4.—17. §-ainak eredményeivel, hacsak mindenütt az «$=$» jelt a «$\equiv$ mod. $(P^{(k)})$» jellel helyettesítjük.

Ez kitünik abból, hogy a holoid, ill. orthoid tartományoknak az a tulajdonsága, a mely most hiányzik, csak abban a tételben nyer alkalmazást, mely szerint minden forma szabályossá válik bizonyos olyan meghatározott transformatio alkalmazása után, a melynek determinánsa 1 és együtthatói raczionális, ill. raczionális és egész számok. E tétel azonban, eltekintve a 3. §-tól, a mely kevésbbé fontos részletet tárgyal, csak a resolvens forma elméletében és az erre támaszkodó további fejtegetésekben (18. és köv. §) talál alkalmazást*.

E mellett azonban belép még az a további *lényeges*

* Hogy a viszonyok itt hogyan alakulnak, azt majd később a 4. §-ban fejtjük ki.

egyszerűsítés, hogy az $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m] \pmod{(P^{(k)})}$ tartomány, a melynek formáit most mint az $x_{k+1}, \ldots, x_m$ határozatlanoknak az $[[1], x_1, \ldots, x_k] \pmod{(P^{(k)})}$ tartományból vett együtthatókkal ellátott formáit tekintjük, *teljes pseudoholoid tartomány*, mert az utóbbi tartomány pseudoorthoid tartomány. A «teljes» jelző, mint előbb, ismét úgy értendő, hogy a tartomány tetszés szerinti két formájának mindig van — most természetesen a $(P^{(k)})$ modulusra vonatkozólag vett — «legnagyobb közös osztója», a melynek előállítására a III. fej. 11. §-ában pontos utasításunk van.

3. §. A III. fej. 15. és 16. §-a alapján most a következő tételekhez jutunk:

Ha

$$F = A_0 x^m + \cdots, \quad G = B_0 x^n + \cdots$$

két oly forma, a melynek együtthatói az

$$[[1], x_1, \ldots, x_k, x_{k+1}, \ldots] \pmod{(P^{(k)})}$$

pseudoholoid tartományhoz tartoznak, továbbá A_0 *és* B_0 *nem egy időben* $\equiv 0 \bmod (P^{(k)})$, *akkor*

$$\text{Res.} \begin{pmatrix} F, & G \\ x, & 1 \end{pmatrix} \equiv 0 \pmod{(P^{(k)})}$$

szükséges és elegendő feltétele annak, hogy az F és G formáknak legyen olyan legnagyobb közös osztójuk $\bmod (P^{(k)})$, *a mely az x-et valóban tartalmazza, azaz az*

$$[[1], x_1, \ldots, x_k, x_{k+1}, \ldots]$$

tartomány egyetlen mennyiségével sem congruens $\bmod (P^{(k)})$.

Továbbá most is lesz

$$\text{Res.} \begin{pmatrix} F, & G \\ x, & 1 \end{pmatrix} \equiv G_1 F + F_1 G \pmod{(P^{(k)})},$$

a hol G_1*-nek az x-re vonatkozó foka legfölebb* $n-1$, F_1*-é pedig legfölebb* $m-1$.

Erre az alapra építve, a 2. §-ban jelzett bebizonyítás most már igen könnyen elvégezhető.

$(P^{(k)})$ absolut törzsrendszer az $[[1], x_1, \ldots, x_k]$ tartományban; hogy $(P^{(k+1)})$ is az az $[[1], x_1, \ldots, x_k, x_{k+1}]$ tartományban, részletesebben úgy fejezhető ki, hogy, ha $F_1, F_2, \ldots$ e tartomány bármely formái és $(P^{(k+1)})$ az $(F_1, F_2, \ldots)$ osztórendszert tartalmazza a nélkül, hogy $(F_1, F_2, \ldots) \simeq (P^{(k+1)})$, akkor fen kell állania az $(F_1, F_2, \ldots) \simeq 1$ æquivalentiának.

Az épen részletezett esetben $(F_1, F_2, \ldots)$ nem tartalmazhatja a $(P^{(k+1)})$ osztórendszert; mert hisz ekkor, minthogy ennek megfordítottja is fennáll, $(F_1, F_2, \ldots) \simeq (P^{(k+1)})$ volna. Az F formák közt tehát legalább *egy*, pl. F_1 olyan, a mely $(P^{(k+1)})$-t *nem* tartalmazza és így más kifejezésmód szerint *nem* $\equiv 0 \bmod. (P^{(k+1)})$. Így tehát

$$F_1 \equiv \varrho \,(\bmod. (P^{(k+1)})),$$

a hol ϱ az előbb $(P^{(k+1)})$-re vonatkozólag megadott teljes maradékrendszer egyik formája és nem zérus. Így tehát ϱ az $x_1, \ldots, x_{k+1}$ határozatlanoknak oly raczionális és egész formája, a melynek x_i-re vonatkozó foka nem éri el n_i-t és együtthatói a $0, 1, \ldots, p_0 - 1$ sorozatból vett számok, a melyek nem tünhetnek el mindannyian.

Most minden esetre meghatározható olyan λ forma, hogy

$$\lambda\varrho \equiv 1 \,(\bmod. (P^{(k+1)})).$$

Ha ϱ, a mi hiszen szintén előfordúlhat, pozitiv egész szám, a mely ekkor kisebb p_0-nál, akkor e czélból olyan a 0-tól különböző egész számot kell választanunk, a mely a

$$\lambda\varrho \equiv 1 \,(\bmod. p_0)$$

congruentiát kielégíti. Ha ellenben ϱ az $x_1, \ldots, x_{k+1}$ határozatlanoknak igazi formája és pl. x_i e sorozat utolsó határozatlana, a mely ϱ-ban valóban előfordúl, akkor megjegyzendő, hogy ϱ az x_i-re vonatkozólag legfölebb $n_i - 1$-edfokú, míg P_i olyan $x_i^{n_i} + \cdots$ alakú forma, a mely $\bmod. (P^{(i-1)})$ irreducibilis és az $x_{i+1}, \ldots$ határozatlanokat hasonlóképen

nem tartalmazza. Nem lehetséges tehát, hogy ϱ osztható P_i-vel és így tehát ϱ-nak és P_i-nek egyáltalában nem lehet olyan közös osztója, a mely x_i-t tartalmazza. Ha tehát ϱ és P_i-nek x_i szerint vett resultánsát σ_{i-1}-gyel jelöljük, akkor

$$\sigma_{i-1} \equiv \lambda_{i-1}\varrho + \mu_{i-1}P_i \,(\mathrm{mod.}\,(P^{(i-1)}))$$

és σ_{i-1} különböző mod.$(P^{(i-1)})$ a 0-tól. A feltevés szerint tehát okvetetlenül meghatározhatunk olyan α formát, a melyre nézve

$$\alpha\sigma_{i-1} \equiv 1 \,(\mathrm{mod.}\,(P^{(i-1)})).$$

Így tehát

$$\alpha\lambda_{i-1}\varrho \equiv 1 - \alpha\mu_{i-1}P_i \,(\mathrm{mod.}\,(P^{(i-1)})),$$

vagy a mi ugyanaz:

$$\lambda\varrho \equiv 1 \,(\mathrm{mod.}\,(P^{(i)})),$$

hol $\lambda = \alpha\lambda_{i-1}$. Egyszersmind tehát

$$\lambda\varrho \equiv 1 \,(\mathrm{mod.}\,(P^{(k+1)})).$$

Most végre

$$(F_1, P_{k+1}, \ldots, P_1, p_0) \simeq (\varrho, P_{k+1}, \ldots, P_1, p_0)$$

olyan rendszer, a mely $(P^{(k+1)})$-gyel együtt minden esetre az $(F_1, F_2, \ldots)$ rendszert is tartalmazza. Ugyanaz állítható a

$$(\lambda\varrho, P_{k+1}, \ldots, P_1, p_0) \simeq (1, P_{k+1}, \ldots, P_1, p_0) \simeq 1$$

rendszerről is és így — a mit ép be akartunk bizonyítani —

$$(F_1, F_2, \ldots) \simeq 1.$$

Még a 2. §-ban felállított I. tétel második részét kell bebizonyítanunk és ennek megfelelőleg kimutatnunk, hogy $(P^{(k)})$ az $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m]$ tartományban törzsrendszer. Hogy itt már nem absolut törzsrendszer, közvetetlenül abból a körülményből következtethető, hogy akkor $(P^{(k)})$ a $(P^{(k+1)})$-t is tartalmazza.

Ha az $x_1, \ldots, x_m$ határozatlanoknak formáit az $x_{k+1}, \ldots, x_m$ határozatlanoknak az $[[1], x_1, \ldots, x_k]$ tartományból vett együtthatókkal ellátott formáinak tekintjük, akkor ilyen forma csak

úgy lehet $\equiv 0 \bmod. (P^{(k)})$, ha ugyanaz áll minden egyes együtthatójáról.

Ha már most $FG \equiv 0 (\bmod. (P^{(k)}))$ volna és mindamellett sem F, sem pedig G nem lenne $\equiv 0 \bmod. (P^{(k)})$, akkor e formák a következő alakban volnának előállíthatók:

$$F = A_g x_{k+1}^{g_{k+1}} \ldots x_m^{g_m} + \cdots,$$
$$G = B_h x_{k+1}^{h_{k+1}} \ldots x_m^{h_m} + \cdots,$$

a hol a kiírt tagok a «legmagasabbak», a melyeknek együtthatója különböző $\bmod. (P^{(k)})$ a 0-tól. Ekkor azonban FG legmagasabb tagja

$$A_g B_h x_{k+1}^{g_{k+1}+h_{k+1}} \ldots x_m^{g_m+h_m}$$

volna és a feltevés ellenére $A_g B_h$ nem volna $0 \bmod. (P^{(k)})$, mert az $[[1], x_1, \ldots, x_k]$ tartományhoz tartozó A_g és B_h formák egyike sem $0 (\bmod. (P^{(k)}))$.

4. §. Legyenek $A_0, A_1, \ldots, A_n$ az $x_1, \ldots, x_m$ határozatlanoknak raczionális és egész formái és legyen (S) valamely osztórendszer, a mely szintén ilyen formákból áll; akkor a következő specziális diophantikus egyenletről:

$$A_0 X^n + A_1 X^{n-1} + \cdots + A_n \equiv 0 (\bmod. (S)),$$

a hol A_0 nem $0 (\bmod. (S))$, azt mondjuk, hogy «n-edfokú congruentia egy ismeretlennel».

A magasabbfokú congruentiák elméletének tárgyalására itt nem terjeszkedünk ki; ebből csak a következő igen egyszerű tételre lesz szükségünk:

Ha (S) törzsrendszer és A_0 nem $0 (\bmod. (S))$, akkor az

$$A_0 X^n + A_1 X^{n-1} + \cdots + A_n \equiv 0 (\bmod. (S))$$

congruentiának nem lehet n-nél több $\bmod. (S)$ *különböző gyöke.*

Ha ugyanis $X_1, \ldots, X_n, X_{n+1}$ ilyen gyökök volnának, akkor abból, hogy

$$A_0 X_i^n + A_1 X_i^{n-1} + \cdots + A_n \equiv 0 \pmod{(S)},$$
$$(i=1, \ldots, n+1)$$

a determinánsok elméletének elemei szerint következnék, hogy

$$A_0 \mid X_i^{j-1} \mid \equiv 0 \pmod{(S)},$$

a hol $\mid X_i^{j-1} \mid$ ismeretes módon az X_i-kből alkotható különbségek szorzatát jelenti. Minthogy azonban A_0 nem 0 (mod. (S)), kettőnek az $X_1, \ldots, X_{n+1}$ sorozat mennyiségei közül a feltevés ellenére is congruensnek kellene lennie (mod. (S)).

Teljes analogiában a II. fej. 17. §-ával fennáll továbbá a következő tétel:

Legyenek $F_i(z_1, z_2, \ldots)$ $(i=1, 2, \ldots)$ *oly formák, a melyeknek együtthatói az* $x_1, \ldots, x_m$ *határozatlanoknak racionális és egész formái és a melyek különbözők a* 0*-tól* mod. $(P^{(k)})$, *a hol* $k<m$; *akkor akárhány hasonlóképen az* $[[1], x_1, \ldots, x_m]$ *tartományhoz, sőt már az* $[[1], x_1, \ldots, x_{k+1}]$ *tartományhoz is tartozó olyan* $\alpha_1, \alpha_2, \ldots$ *mennyiséget határozhatunk meg, hogy minden egyes* $F_i(\alpha_1, \alpha_2, \ldots)$ *különböző* mod. $(P^{(k)})$ *a* 0*-tól.*

Egy z határozatlan esetében az $x_{k+1}, x_{k+1}^2, x_{k+1}^3, \ldots$ sorozat mennyiségei kivétel nélkül különbözők mod. $(P^{(k)})$ és, ha n az $F(z)$ formának z-re vonatkozó foka, akkor közülük legfölebb n elégítheti ki az $F(z) \equiv 0 \pmod{(P^{(k)})}$ congruentiát. Az adott sorozat minden más mennyisége tehát bizonyára kielégíti a felállított követelést. Az átmenet $F(z)$-ről $F(z_1, z_2, \ldots)$-re, valamint arra az esetre, midőn a formák száma tetszés szerinti, ép úgy történik, mint az idézett helyen.

Itt azonban a $k<m$ feltétel *lényeges feltétel*, mert különben az $[[1], x_1, \ldots, x_m]$ tartományban mod. $(P^{(m)})$ teljes maradékrendszer léteznék és így nem állíthatnók fel a mod. $(P^{(m)})$ incongruens mennyiségeknek *végtelen* sorozatát. Így pl. az $x^p - x$ forma nem $\equiv 0 \pmod{p}$ és mégis minden

raczionális és egész számra nézve érvényes, hogy

$$a^p - a \equiv 0 \pmod{p}.$$

Ennek megfelelőleg most *az a tétel, a mely valamely formának szabályos formába való transformatiójára vonatkozik* (II. fej. 19. §), a következőképen módosítandó:

Legyenek $F_i(z_1, z_2, \ldots, z_r)$ $(i=1, 2, \ldots)$ a $z_1, z_2, \ldots, z_r$ *határozatlanoknak bármely olyan formái, a melyeknek együtthatói az* $[[1], x_1, \ldots, x_m]$ *tartományhoz tartoznak; akkor, ha ismét* $k<m$, *akárhány olyan lineáris transformatio jelölhető ki, a melynek determinánsa egyenlő* 1*-gyel, együtthatói ugyanahhoz a tartományhoz tartoznak és e lineáris transformatiók alkalmazása után az* F_i *formák olyan formákba mennek át, a melyek* mod. $(P^{(k)})$ *szabályosak.*

Ebben a mod. $(P^{(k)})$ szabályos forma olyannak értendő, a melyben, ha dimensiója n, a $z_1^n, z_2^n, \ldots$ együtthatói mindannyian különbözők mod. $(P^{(k)})$ a 0-tól.

Ha részletesen írva

$$F_i = \sum_{(g)} A_g^{(i)} z_1^{g_1} z_2^{g_2} \ldots z_r^{g_r}, \qquad (i=1, \ldots, k)$$

akkor a

$$z_1 = y_1, \quad z_j = u_{j1} y_1 + y_j \qquad (j=2, \ldots, r)$$

specziális lineáris transformatio alkalmazása után, a melynek determinánsa — bárhogyan is határozzuk majd meg az u_{j1}-eket — 1-gyel egyenlő, F_i átmegy a

$$\overline{F}_i = \sum_{(g)} A_g^{(i)} y_1^{g_1} (u_{21} y_1 + y_2)^{g_2} \ldots (u_{r1} y_1 + y_r)^{g_r}$$

formába, a hol y_1^n-nek együtthatója

$$\Sigma A_g^{(i)} u_{21}^{g_2} \ldots u_{r1}^{g_r},$$

ha a summatiót mindazokra a tagokra terjesztjük ki, a melyekben $g_1 + g_2 + \cdots + g_r = n$.

A mint épen bebizonyítottuk, az $u_{21}, \ldots, u_{r1}$ mennyiségek, ha nem is mindig mint raczionális és egész számok,

de minden esetre már mint az $[[1], x_1, \ldots, x_m]$ tartomány formái úgy választhatók, hogy y_1^n együtthatója ne legyen 0 mod. $(P^{(k)})$, míg $y_2^n, \ldots$ együtthatója $\overline{F}_i$-ben ugyanaz, mint z_2^n együtthatója F_i-ben.

Ennek az eljárásnak folytatása végre ép úgy, mint a II. fej. 18. §-ában, olyan lineáris transformatiókat szolgáltat, a melyek a fenn felállított feltételeket kielégítik és a melyeknek alkalmazása után az $F_i(z_1, z_2, \ldots)$ formák olyan $\overline{F}_i(\overline{z}_1, \overline{z}_2, \ldots)$ formákba mennek át, a melyek az összes $\overline{z}_1, \overline{z}_2, \ldots$ határozatlanokra nézve mod. $(P^{(k)})$ szabályosak.

*

Hogy a raczionális és egész formák oszthatóságának elméletét formálisan is teljesen egységesen fogalmazhassuk, czélszerűnek mutatkozik a $(P^{(-1)})$ *jelkép bevezetése*, mely — ha úgy tetszik — 0-nak is vehető. Az $F_1 \equiv F_2 \pmod{(P^{(-1)})}$ kijelentés egyszerűen azt fejezze ki, hogy $F_1 = F_2$.

A «raczionális és egész formák elmélete mod. $(P^{(k)})$» ezután $k = -1$ esetére a régebben kifejtett tételeket is megadja.

Osztórendszerek mod. $(P^{(k)})$.

5. §. Előbbi megállapodásainknak természetszerű bővítése a következő definicziókhoz vezet.

I. *Az* $(M_1, \ldots, M_h)$ *osztórendszer «tartalmazza* mod. $(P^{(k)})$» *az* $(N_1, \ldots, N_g)$ *osztórendszert, ha az első osztórendszer minden eleme kielégíti az*

$$M_i \equiv 0 \pmod{N_1, \ldots, N_g, (P^{(k)})}$$

congruentiát.

II. *Két osztórendszer (szükebb értelemben) aequivalens* mod. $(P^{(k)})$, *ha mindegyikük tartalmazza* mod. $(P^{(k)})$ *a másikat.* Ennek jelölésére szolgál:

$$(M_1, \ldots, M_h) \simeq (N_1, \ldots, N_g) \,(\mathrm{mod.}\,(P^{(k)})).$$

Ugyanezt különben már az eddigi jelölésekkel is kifejezhetjük. Közvetetlenül belátható ugyanis, hogy az

$$\big(M_1, \ldots, M_h, (P^{(k)})\big) \simeq \big(N_1, \ldots, N_g, (P^{(k)})\big)$$

æquivalentia ugyanezt a tényállást jellemzi.

Itt is megkülönböztetendő az épen értelmezett szűkebb értelemben vett æquivalentia a bővebb értelemben vett æquivalentiától, a melynek jelölésére az $\sim$ jel szolgál. E jelt használva,

$$(M_1, \ldots, M_h) \sim (N_1, \ldots, N_g) \,(\mathrm{mod.}\,(P^{(k)}))$$

azt jelenti, hogy $M_1, \ldots, M_h$ minden közös osztója mod. $(P^{(k)})$ egyszersmind az $N_1, \ldots, N_g$-nek is közös osztója mod. $(P^{(k)})$ és viszont.

Magukban álló mennyiségek (egytagú osztórendszerek) esetében $M \sim N \,(\mathrm{mod.}\, P^{(k)})$ és $M \simeq N \,(\mathrm{mod.}\, P^{(k)})$ jelentése ugyanaz.

Ezek után két osztórendszer «*legnagyobb közös tartalmát* mod. $(P^{(k)})$» ismét úgy értelmezhetjük, mint a VII. fej. 2. §-ában és két osztórendszerről $(M_1, \ldots, M_h)$ és $(N_1, \ldots, N_g)$-ről azt mondjuk, hogy «*relativ törzs-osztórendszerek* mod. $(P^{(k)})$», ha

$$(M_1, \ldots, M_h, N_1, \ldots, N_g) \simeq 1 \,(\mathrm{mod.}\,(P^{(k)})),$$

vagyis

$$\big(M_1, \ldots, M_h, N_1, \ldots, N_g, (P^{(k)})\big) \simeq 1.$$

A VII. fej. 3. §-ának fejtegetései is szóról szóra érvényesek maradnak, ha az ott alkalmazott æquivalentia helyett most æquivalentiát mod. $(P^{(k)})$ értünk; a mely esetre vonatkozólag külön kiemelendő a következő fontos tétel:

III. *Ha az* $(N_1, \ldots, N_g)$ *osztórendszernek nem minden eleme* $\equiv 0 \,\big(\mathrm{mod.}\,(P^{(k)})\big)$ *és*

$$(\ldots, M_i, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, M_{i'}', \ldots)(\ldots, N_j, \ldots) \,(\mathrm{mod.}\,(P^{(k)})),$$
$$(i=1, \ldots, h;\ i'=1, \ldots, h';\ j=1, \ldots, g)$$

akkor az $(\ldots, M_i^g, \ldots)$ *osztórendszer tartalmazza* mod. $(P^{(k)})$

a $(\ldots, M'_{i'}, \ldots)$ *osztórendszert és ép úgy* $(\ldots, M'^{g}_{i'}, \ldots)$ *az* $(\ldots, M_i, \ldots)$ *osztórendszert.*

Ha most már olyan formákat vizsgálunk, a melyeknek együtthatói az

$$[[1], x_1, \ldots, x_m] \pmod{(P^{(k)})}$$

tartományhoz tartoznak, akkor — mint már említettük — a III. fej. 5—8. §-ának Kronecker alaptételére vonatkozó fejtegetései feltétlenül érvényesek maradnak, hacsak ismét az $=$ jel helyébe a $(P^{(k)})$ modulusra vonatkozó congruentia jelölését teszszük; e mellett csak arra kell ügyelnünk, hogy az $x_1, \ldots, x_m$ határozatlanoknak így megállapított jelentése miatt az ott használt betűk helyett a formák határozatlanait most másképen, pl. $z_1, \ldots, z_n$-nel kell jelölnünk. Ép úgy lép most $Q_1, \ldots, Q_i$ az ott használt $P_1, \ldots, P_i, \ldots$ betűk helyébe, minthogy ezek jelenleg a $(P^{(k)})$ osztórendszer elemeit jelentik. Azután analogiában a III. fej. 6. §-ának elején kimondott tétellel Kronecker *alaptételének* következő, messzeható *általánosítását* nyerjük:

IV. Legyenek

$$F_j \equiv \sum_{(g)} A_g^{(j)} z_1^{g_1} \ldots z_n^{g_n} \pmod{(P^{(k)})} \qquad (j=1, 2, \ldots h)$$

a $z_1, \ldots, z_n$ határozatlanoknak olyan formái, a melyek mod. $(P^{(k)})$ különbözők a 0-tól és a melyeknek együtthatói az $[[1], x_1, \ldots, x_m] \pmod{P^{(k)}}$ pseudoholoid tartományhoz tartoznak; e formák szorzata legyen

$$F = F_1 \ldots F_h \equiv \Sigma C_g z_1^{g_1} \ldots z_n^{g_n} \pmod{(P^{(k)})};$$

legyen továbbá

$$Q_i = A_{i_1}^{(1)} A_{i_2}^{(2)} \ldots A_{i_h}^{(h)}$$

h olyan együttható szorzata, a mely közül mindegyik másmás formából van véve.

Akkor van a mennyiségeknek oly $H_1, \ldots, H_\nu$ sorozata,

a melyek az $A^{(1)}, \ldots, A^{(h)}$ együtthatóknak oly raczionális és egész, homogén formái, a melyek különbözők mod. $(P^{(k)})$ a 0-tól; valamint a mennyiségeknek oly további $L_{i\sigma}^{(s)}$ sorozata, a melyek a C_g mennyiségeknek raczionális és egész, homogén és lineáris formái úgy, hogy

$$H_s Q_i \equiv \sum_{\sigma=1}^{\nu} L_{i\sigma}^{(s)} H_\sigma \pmod{(P^{(k)})}. \quad {}_{(s=1,\ldots,\nu)} \quad (K)$$

Minthogy most az $[[1], x_1, \ldots, x_m] \pmod{(P^{(k)})}$ tartomány teljes pseudoholoid tartomány, a III. fej. 8. §-ának további következtetései is alkalmazhatók és így azt találjuk, hogy

$$(Q_1, \ldots, Q_i, \ldots) \sim (C_1, \ldots, C_g, \ldots) \pmod{(P^{(k)})},$$

azaz *a* $(Q_1, \ldots, Q_i, \ldots)$ *és* $(C_1, \ldots, C_g, \ldots)$ *forma-sorozatok legnagyobb közös osztója* mod. $(P^{(k)})$ *ugyanaz.*

Kronecker alaptétele azonban még más irányban is bővítendő; ha ugyanis a kérdéstételben, a mint az osztórendszerek bevezetése után ez önként kínálkozik, a $(Q_1, \ldots, Q_i, \ldots)$ és $(C_1, \ldots, C_g, \ldots)$ osztórendszerek bővebb értelemben vett æquivalentiájáról azoknak szűkebb értelemben vett æquivalentiájára megyünk át. Magától értetődik, hogy ekkor $(C_1, \ldots, C_g, \ldots)$ tartalmazza a $(Q_1, \ldots, Q_i, \ldots)$ osztórendszert, de megfordítva csak a következő, megszorítása mellett is alapvető tétel érvényes:

V. *Mindig van olyan pozitiv egész szám* ν, *hogy*

$$(Q_1^\nu, \ldots, Q_i^\nu, \ldots)$$

a $(C_1, \ldots, C_g, \ldots)$ *osztórendszert* mod. $(P^{(k)})$ *tartalmazza.*

E tétel helyessége közvetetlenül kitünik a (K) congruentiából, ha az e §-ban III. alatt adott tételt alkalmazzuk.

Az $L_{i\sigma}^{(s)}$ formák jelentése szerint a $(\ldots, H_s Q_i, \ldots)$ osztórendszer tartalmazza mod. $(P^{(k)})$ a $(\ldots, H_s C_g, \ldots)$ osztórend-

szert és magától értetődik, hogy megfordítva $(\ldots, H_s C_g, \ldots)$ is tartalmazza $(\ldots, H_s Q_i, \ldots)$-t. Mind a kettő azonban componált rendszer és ha azokat mint a compositio tényezőinek szorzatát írjuk fel, lesz

$$(\ldots, H_s, \ldots)(\ldots, Q_i, \ldots) \simeq (\ldots, H_s, \ldots)(\ldots, C_g, \ldots) \pmod{(P^{(k)})}.$$

Ebből pedig III. szerint közvetetlenül kiadódik a kimondott tétel.

A resolvens formák elmélete mod. $(P^{(k)})$.

6. §. Hogy valamely $F_1, \ldots, F_h$ formarendszer resolvens formájának a III. fej. 18. §-ában kifejtett elméletét pontosan és minden változtatás nélkül az $[[1], x_1, \ldots, x_m] \pmod{(P^{(k)})}$ tartomány formáira alkalmazhassuk, az F formákat az $x_{k+2}, \ldots, x_m$ határozatlanoknak oly formáinak tekintjük, a melyeknek együtthatói az $[[1], x_1, \ldots, x_k, x_{k+1}] \pmod{(P^{(k)})}$ tartományhoz tartoznak. Minthogy e tartomány végtelen sok nem congruens formát tartalmaz, mindig lesz akárhány oly lineáris transformatio, melynek determinánsa $\equiv 1$, együtthatói az $[[1], x_1, \ldots, x_k, x_{k+1}] \pmod{(P^{(k)})}$ pseudoholoid tartományhoz tartoznak és a melynek alkalmazása után akárhány F forma egyidőben az $x_{k+2}, \ldots, x_m$ határozatlanokra nézve szabályossá válik.

Az analogia az idézett helyen egyedül tárgyalt $k = -1$ esettel ekkor teljes lesz, hacsak figyelembe veszszük azt a körülményt, hogy a raczionális egész számok helyébe most az $[[1], x_1, \ldots, x_k, x_{k+1}] \pmod{(P^{(k)})}$ tartomány formái lépnek.

E mellett az az eset, midőn az F formák az $x_{k+2}, \ldots, x_m$ határozatlanokat egyáltalában nem tartalmazzák, mint különösen egyszerű eset, elsőnek tárgyalandó. Jelöljük a formákat ekkor a következő módon:

$$f_j(x_1, \ldots, x_k, x_{k+1}) \pmod{(P^{(k)})}.$$

Ha $f_1, \ldots, f_k$ legnagyobb közös osztója mod. $(P^{(k)})$ pl. $\sim d$, tehát

$$f_j \equiv d f_j' \ (\text{mod. } (P^{(k)}))$$

és

$$(f_1', \ldots, f_h') \sim 1 \ (\text{mod. } (P^{(k)})),$$

akkor

$$d \sum_{j=1}^{h} f_j' w_j \equiv 0 \ (\text{mod. } f_1, \ldots, f_h, (P^{(k)}))$$

az «$f_1, \ldots, f_h$ resolvens formája mod. $(P^{(k)})$».

Ehhez mindjárt hozzácsatoljuk azt a megjegyzést, hogy a

$$\sum_{j=1}^{h} f_j X_j \equiv 1 \ (\text{mod. } (P^{(k)}))$$

congruentia megoldhatóságának kérdése, valamint egyik gyökének meghatározása, ha e congruentia egyáltalában megoldható, már itt intézhető el. (Ha $k=-1$, akkor egyenlettel van dolgunk, a melyben az összes ismeretlenek együtthatói raczionális egész számok.)

Ama congruentia megoldhatóságának szükséges és elegendő feltétele

$$(f_1, \ldots, f_h) \sim 1 \ (\text{mod. } (P^{(k)})),$$

a hol, a bővebb értelemben vett æquivalentia jelét ($\sim$) használjuk, és így $(f_1, \ldots, f_h)$ az $f_1, \ldots, f_h$ formák legnagyobb közös osztóját jelenti.

E feltétel szükséges voltát abból ismerjük fel, hogy $f_1, \ldots, f_h$-val együtt $\Sigma f_j X_j = 1$-nek is oszthatónak kell lennie mod. $(P^{(k)})$ ama legnagyobb közös osztóval. Ez tehát az egység osztója mod. $(P^{(k)})$ és e szerint ~ 1 (mod. $(P^{(k)})$).

Hogy e feltétel egyszersmind elegendő feltétel is, abból tünik ki, hogy a következő reductio alapján valóban megoldáshoz jutunk.

Ha az egyik együttható, pl. f_1 az x_{k+1} határozatlant egyáltalában nem tartalmazza, akkor, minthogy hiszen feltételezhetjük, hogy az együtthatók különbözők mod. $(P^{(k)})$

a zérustól, van egy könnyen meghatározható $g(x_1, \ldots, x_k)$ forma, a mely ismét különböző mod. $(P^{(k)})$ a zérustól, és a melyre nézve $f_1 g \equiv 1$. Ha g-vel szorzunk, ama congruentia a következő alakot veszi fel:

$$X_1 + \sum_{j=2}^{h} f_j g X_j \equiv g \pmod{(P^{(k)})},$$

a melynek általános megoldása

$$X_1 \equiv g - \sum_{j=2}^{h} f_j g t_j, \quad X_j = t_j, \qquad (j=2, \ldots, h)$$

a hol $t_2, \ldots, t_h$ tetszés szerinti formákat jelentenek.

(A $k=-1$ kivételes esetnek, a midőn az együtthatók egyáltalában határozatlanokat nem tartalmaznak, a congruentia «megoldott» alakja felel meg, a hol az egyik együttható már 1-gyel egyenlő.)

Ha az összes együtthatók az x_{k+1} határozatlant tartalmazzák és egyelőre a $k=-1$ esetet kizárjuk, ekkor az egyik f-nek, pl. f_1-nek x_{k+1}-re vonatkozó foka nem nagyobb, mint bármely más f_j-é. Ha azután:

$$f_j \equiv f_1 q_j + r_j \pmod{(P^{(k)})},$$

a hol q_j, ill. r_j a közönséges osztási eljárásnál fellépő hányados, ill. maradék, akkor, minthogy az osztást mod. $(P^{(k)})$ végezzük, q_j és r_j ismét raczionális és egész formák; de r_j foka legalább is egy egységgel kisebb mint az f_1-é, vagy pedig $r_j \equiv 0 \pmod{(P^{(k)})}$.

A congruentiát azonban ezután az

$$f_1(X_1 + q_2 X_2 + \cdots + q_h X_h) + \sum_{j=2}^{h} r_j X_j \equiv 1 \pmod{(P^{(k)})}$$

alakban írhatjuk, a mely e szerint az

$$f_1 Y_1 + \sum_{j=2}^{h} r_j X_j \equiv 1 \pmod{(P^{(k)})}$$

congruentiával együtt megoldottnak tekinthető. Ámde az utóbbi congruentiában az együtthatók legnagyobb közös

osztója

$$(f_1, r_2, \ldots, r_h) \sim (f_1, f_2, \ldots, f_h) \sim 1$$

és, minthogy a feltevés szerint f_1 nem $\equiv 1$, egyik r bizonyára különböző lesz a 0-tól. Ha f_1-nek x_{k+1}-re vonatkozó foka n volt, akkor e szerint a reductio e módszerének alkalmazása révén legfölebb n lépés után oly congruentiához jutunk, a melyben egyik együttható x_{k+1}-től független és így tehát annak megoldása közvetetlenül felírható.

(Az elemi kivételes esetben, midőn $k=-1$, az együtthatók raczionális és egész számok és ekkor a kifejtett eljárással ezeknek nem fokát, hanem absolut értékét redukáljuk. Ha a legkisebb együttható — az előjel mellőzésével — n volt, akkor legfölebb n lépés után oly egyenlethez jutunk, a melyben az egyik együttható ± 1 és így tehát annak megoldása ismét közvetetlenül felírható.)

7. §. Hogy az $F_1, \ldots, F_h$ formarendszer resolvens formáját mod. $(P^{(k)})$ általánosságban felállíthassuk, ismételnünk kell a III. fej. 18. §-ának fejtegetéseit. Azok érvényességüket szóról szóra megtartják, hacsak ismét «raczionális és egész szám» helyett mindenütt azt mondjuk: «az $[[1], x_1, \ldots, x_k, x_{k+1}]$ (mod. $(P^{(k)})$) tartomány raczionális és egész formája» és a congruentiák jelölésében az $(F_1, F_2, \ldots)$ modulusrendszert az $(F_1, \ldots, F_h, (P^{(k)}))$ modulusrendszerrel helyettesítjük. Végre a határozatlanok sorozata most nem $x_1, \ldots, x_m$, hanem $x_{k+2}, \ldots, x_m$.

Ily módon jutunk *az* $F_1, \ldots, F_h$ *formarendszer*

$$DD^{(1)} \ldots D^{(r)} \sum_{j_r=1}^{k_r} C_{j_r} w_{j_r} \equiv 0 \ (\text{mod. } F_1, \ldots, F_h, (P^{(k)})) \qquad (R)$$

resolvens formájához mod. $(P^{(k)})$, a hol $D^{(r)}$, C_{j_r} az

$$[[1], x_1, \ldots, x_{k+1}] \ (\text{mod. } (P^{(k)}))$$

tartományhoz tartoznak, $0 \leqq r \leqq m-k-2$ és általánosságban $D^{(s)}$ az $x_{s+k+2}, \ldots, x_m$ határozatlanoknak e tartományból

származó formája. D (vagy $D^{(0)}$) az $F_1, \ldots, F_h$ formáknak legnagyobb közös osztója mod. $(P^{(k)})$.

E mellett feltételezhetjük, hogy a D formák az $x_{k+2}, \ldots, x_m$ határozatlanokra nézve mindannyian szabályosak; mert ez elérhető, ha az $F_1, \ldots, F_h$ formarendszerre bizonyos ismeretes lineáris transformatiót alkalmazunk, a melynek együtthatói az $[[1], x_1, \ldots, x_{k+1}]$ (mod. $(P^{(k)})$) tartományhoz tartoznak. Az (R) congruentia különben megtartja érvényességét akkor is, ha ezt a transformatiót nem alkalmazzuk; csakhogy ekkor a D-k nem lesznek mindig szabályosak.

Ha az $[[1], x_1, \ldots, x_k, x_{k+1}]$ (mod. $(P^{(k)})$) tartományhoz tartozó C_{j_r} mennyiségek legnagyobb közös osztója mod. $(P^{(k)})$ a következő:

$$(\ldots, C_{j_r}, \ldots) \sim D^{(r+1)} \text{ (mod. } (P^{(k)})),$$

akkor a w_{j_r} mennyiségek úgy, a mint azt bebizonyítottuk, a

$$\sum_{j_r=1}^{k_r} C_{j_r} w_{j_r} \equiv D^{(r+1)} \text{ (mod. } (P^{(k)}))$$

feltételnek megfelelőleg meghatározhatók, és evvel *a fenforgó esetre a*

$$DD^{(1)} \ldots D^{(r)} D^{(r+1)} \equiv 0 \text{ (mod. } F_1, \ldots, F_h, (P^{(k)})), \qquad (R_k)$$

egyszerűsített resolvens formát nyerjük.

Az így előállított kifejezés alapját szolgáltatja ama P-rendszerek vizsgálatának, a melyeket az $(F_1, \ldots, F_h, (P^{(k)}))$, vagy, a mi ugyanaz, $(F_1, \ldots, F_h)$ *és* $(P^{(k)})$ tartalmaz. A nélkül, hogy ezt az elméletet egész általánosságában kifejtenők, itt csak a mi czéljainkra szükséges tételeket akarjuk levezetni.

Magától értetődik, hogy minden P-rendszer, a melyet $(P^{(k)})$ tartalmaz, úgy írható, hogy utolsó $k+1$ eleme egyenesen megegyezzék a $(P^{(k)})$ elemeivel.

Az egyszerűsített resolvensforma már mostan vagy $\simeq 1$ (mod. $(P^{(k)})$), vagy pedig felbontható mod. $(P^{(k)})$ irredu-

cibilis tényezőire; legyen azután:

$$DD^{(1)} \dots D^{(r)}D^{(r+1)} \simeq E_1^{a_1} \dots E_s^{a_s} \pmod{(P^{(k)})}.$$

A keresett P-rendszerek bármelyikét, minthogy törzsrendszer, az E formák valamelyike tartalmazza. Először is azt az esetet vizsgáljuk, midőn az E tényezők valamelyike az $x_{k+2}, \dots, x_m$ határozatlanoknak oly *igazi* formája, a melynek együtthatói az $[[1], x_1, \dots, x_{k+1}] \pmod{(P^{(k)})}$ tartományhoz tartoznak.

Ekkor először is kitünik, hogy *az*

$$E(x_{k+2}, \dots, x_m)$$

formában $x_{k+2}, \dots, x_m$ *helyébe az* $[[1], x_1, \dots, x_{k+1}] \pmod{(P^{(k)})}$ *tartomány olyan* $\xi_{k+2}, \dots, \xi_m$ *mennyiségei tehetők, hogy azután*

$$E(\xi_{k+2}, \dots, \xi_m) \equiv 0 \pmod{\pi_{k+1}, (P^{(k)})},$$

a hol π_{k+1} *az említett tartomány olyan irreducibilis formája, a mely különböző a tartomány bármiképen megadott* $\pi', \pi'', \dots, \pi^{(s)}$ *irreducibilis formáitól.*

Legyen α az E formának az $x_{k+2}, \dots, x_m$ határozatlanoktól független tagja*; és írjuk, hogy

$$x_{k+r} = \alpha\pi' \dots \pi^{(s)} z_{k+r}. \qquad (r=2, \dots, m-k)$$

Akkor

$$\frac{1}{\alpha} E(\alpha\pi' \dots \pi^{(s)} z_{k+2}, \dots, \alpha\pi' \dots \pi^{(s)} z_m)$$

a $z_{k+1}, \dots, z_m$ egyetlen értékére nézve sem mod. $(P^{(k)})$ osztható valamelyik $\pi^{(i)}$-vel; mert ama kifejezés — mint közvetetlenül látható —

$$\equiv 1 \pmod{\pi^{(i)}, (P^{(k)})}.$$

Most azonban e fejezet 4. §-a szerint a z mennyiségeket az $[[1], x_1, \dots, x_{k+1}] \pmod{(P^{(k)})}$ tartományból úgy vá-

* Az $\alpha=0$ eset, mint közvetetlenül látható, egyszerű transformatióval elkerülhető.

laszthatjuk, hogy az

$$\frac{1}{\alpha} E(\alpha\pi' \dots \pi^{(s)} z_{k+2}, \dots, \alpha\pi' \dots \pi^{(s)} z_m) - C_j$$

formák közül egyetlen egy se tünjék el mod. $(P^{(k)})$, a hol C_j egymás után az $[[1], x_1, \dots, x_k]$ (mod. $(P^{(k)})$) formái teljes maradékrendszerének minden elemét jelenti. Ebben az esetben tehát $\frac{1}{\alpha} E(\alpha\pi' \dots \pi^{(s)} z_{k+2}, \dots)$ az $x_{k+1}, \dots, x_m$ határozatlanoknak igazi formája és így oszthatónak kell lennie valamely a $\pi', \dots, \pi^{(s)}$-től különböző irreducibilis π_{k+1} formával. Állításunk értelmében ugyanez érvényes tehát E-re nézve is.

Tegyük már most fel, hogy E-t a resolvens forma $D^{(i)}$ tényezője tartalmazza úgy, hogy az az $x_{k+i+2}, \dots, x_m$ határozatlanoknak formája; továbbá a $\pi', \dots, \pi^{(s)}$ sorozat tartalmazza az összes irreducibilis formákat, a melyek (a III. fej. 18. §-ának jelölései szerint) az $F_{j_h}^{(h)}$-val jelölt formák legmagasabb tagjainak együtthatóiban előfordúlnak. Akkor az épen levezetett tétel szerint

$$E \equiv 0 (\text{mod. } x_{k+i+2} - \xi_{k+i}, \dots, x_m - \xi_m, \pi_{k+1}, (P^{(k)})).$$

Az itt álló modulusrendszer P-rendszer, a melyben, ha $i > 0$, az $x_{k+2}, \dots, x_{k+i+1}$ határozatlanok még nem találnak alkalmazást.

Ha $i = 0$, tehát E a D-nek, tehát az összes F-eknek is osztója, akkor e szerint van végtelen sok olyan $(P^{(m)})$-rendszer, a melyet az összes F-ek tartalmaznak.

Ha $i > 0$ és E a $D^{(i)}$ osztója, tehát $D^{(i)}$ (ismét a III. fej. 18. §-ának jelölése szerint) az $F_1^{(i)}, F_2^{(i)}, \dots$ formák legnagyobb közös osztója mod. $(P^{(k)})$, akkor ez a forma mind $\equiv 0 (\text{mod. } x_{k+i+2} - \xi_{k+i+2}, \dots, x_m - \xi_m, \pi_{k+1}, (P^{(k)}))$. E szerint ugyane modulusrendszerre vonatkozólag, van az $\overline{F}^{(i-1)}$ formáknak olyan legnagyobb közös osztójuk, a mely egy és csak egy új x_{k+i+1} határozatlant tartalmaz. Ha ennek egyik irreducibilis tényezőjét, pl. P_{k+i+1}-et választjuk, akkor min-

den egyes $F^{(i-1)}$-re nézve is

$$F^{(i-1)} \equiv 0 \,(\text{mod. } P_{k+i+1},\ x_{k+i+2} - \xi_{k+i+2}, \ldots, \pi_{k+1}, (P^{(k)})).$$

Minthogy ezen a módon visszafelé következtethetünk egészen az F formákig, arra a fontos eredményre jutunk, hogy *az*

$$(F_1, \ldots, F_h, (P^{(k)}))$$

formarendszer, mihelyt a resolvens formában az $x_{k+2}, \ldots, x_m$ *határozatlanok közül csak egy is valóban előfordúl, végtelen sok* $m+1$*-edfokozatú P-rendszert tartalmaz.*

Ha *másodszor* a resolvens forma, tehát minden egyes E tényező is, az egyetlen x_{k+1} határozatlannak oly formája, a melynek együtthatói — mint az magától értetődik — az $[[1], x_1, \ldots, x_k]$ $(\text{mod. } (P^{(k)}))$ tartományhoz tartoznak, akkor

$$E \simeq x_{k+1}^{n_{k+1}} + \cdots \ (\text{mod. } (P^{(k)}))$$

és egyenesen mint P_{k+1} írható. Ha tehát

$$(P^{(k+1)}) \simeq (P_{k+1}, (P^{(k)})),$$

akkor a keresett P-rendszereket az így meghatározott

$$(F_1, \ldots, F_h, (P^{(k+1)}))$$

rendszerek egyikének kell tartalmaznia és viszont minden P-rendszer, a melyet ez a rendszer tartalmaz, tartalmaztatik $(F_1, \ldots, F_h, (P^{(k)}))$-ben is. Evvel tehát meg van adva a probléma reductiója és ezt az eljárást legfölebb $m-k$-szor ismételve, azokat az $m+1$-edfokozatú P-rendszereket, a melyeket $(F_1, \ldots, F_h, (P^{(k)}))$ tartalmaz, mint azokat a P-rendszereket nyerjük, a melyeket az

$$(F_1, \ldots, F_h, (P^{(m)}))$$

rendszerek bizonyos véges sorozata tartalmaz, hacsak a redukált rendszerek közt valahol nem áll be az első eset és így tehát végtelen sok olyan P-rendszer van, a mely a felállított feltételeknek megfelel.

Ha ez egyszer sem történt meg, akkor végre minden F mint az $x_1, \ldots, x_m$ határozatlanoknak formája vagy $\equiv 0$

$(\text{mod. } (P^{(m)}))$, vagy pedig $\simeq 1 \ (\text{mod. } (P^{(m)}))$. Ha ez az utóbbi csak egy F-ről is állítható, akkor

$$(F_1, \ldots, F_h, (P^{(m)})) \simeq 1$$

és végre azokat az $m+1$-edfokozatú P-rendszereket, a melyeket $(F_1, \ldots, F_h, (P^{(k)}))$ tartalmaz, a $(P^{(m)})$ rendszereknek az a véges sorozata szolgáltatja, a melyekre nézve

$$F_j \equiv 0 \ (\text{mod. } (P^{(m)})). \qquad (j=1, \ldots, h)$$

Ha végre *minden egyes* $(P^{(m)})$-re nézve

$$(F_1, \ldots, F_h, (P^{(m)})) \simeq 1,$$

akkor, minthogy $F_1, \ldots, F_h$-nak valamely $(P^{(m-1)})$-re vett resolvens formája bizonyos $P^{(m)}$-k hatványszorzatával æquivalens, minden egyes kérdéses $(P^{(m-1)})$-re nézve

$$(F_1, \ldots, F_h, ((P^{(m-1)})) \simeq 1$$

és, ha ezen a módon tovább következtetünk visszafelé, végre azt találjuk, hogy

$$(F_1, \ldots, F_h, (P^{(k)})) \simeq 1.$$

8. §. A resolvens forma $\text{mod. } (P^{(k)})$ elmélete már az itt kifejtett igen egyszerű tételek alapján is igen fontos következtetésekre vezet. Így a megelőzőből közvetetlen bebizonyítását nyerjük annak a tételnek, a melyet már a 2. §-ban említettünk, hogy t. i. *az $m+1$-edfokozatú P-rendszerek az m határozatlan raczionális és egész formáinak tartományában létező absolut törzsrendszerek összességét és csak ezeket szolgáltatják.*

Ha ugyanis $(F_1, \ldots, F_h)$ absolut törzsrendszer (a mely e szerint nem $\simeq 1$), akkor az előadott fejtegetések szerint mindig nyerhető oly $(P^{(m)})$ rendszer, a melyet $(F_1, \ldots, F_h)$ tartalmaz. Hogy tehát az utóbbi rendszer absolut törzsrendszer lehessen, arra valóban szükséges, hogy

$$(F_1, \ldots, F_h) \simeq (P^{(m)})$$

legyen.

Az előadott tételekből továbbá közvetetlenül szárma-

zik annak a problémának is megoldása, a melyet a lineáris diophantikus egyenletek arithmetikai elméletében második alapproblémának neveztünk és már a VII. fej. 1. §-ában a következőképen fogalmaztunk:

Eldöntendő, vajjon valamely

$$\Sigma F_i X_i = 1 \tag{1}$$

alakú lineáris diophantikus egyenlet megoldható-e és ha megoldható, meghatározandó annak valamelyik megoldása.

A megvizsgálandó egyenletet a

$$\sum_{i=1}^{h} F_i X_i \equiv 1 \pmod{(P^{(k)})} \tag{2}$$

congruentia alakjában írjuk, a mely csak formálisan általánosabb és, ha $k=-1$, az előbb felírt egyenletbe megy át. Ha ennek a congruentiának van megoldása, akkor fennáll az

$$(F_1, \ldots, F_h) \simeq 1 \pmod{(P^{(k)})}$$

æquivalentia, a mely közvetetlenül annak szükséges és elegendő feltétele gyanánt tekintendő, hogy ama congruentia megoldható legyen. Ekkor mindenek előtt szükséges, hogy $F_1, \ldots, F_h$ resolvens formája mod. $(P^{(k)})$ az egyetlen x_{k+1} határozatlannak olyan formája legyen, a melynek együtthatói az $[[1], x_1, \ldots, x_k] \pmod{(P^{(k)})}$ tartományból valók. Ha ama resolvens forma x_{k+1}-et sem tartalmazza, akkor $\simeq 1 \pmod{(P^{(k)})}$ és, miután azt bizonyos közvetetlenül meghatározható mennyiséggel megszoroztuk, oly mennyiségbe megy át, a mely $\equiv 1 \pmod{(P^{(k)})}$. A resolvens formának kiszámítása a kifejtett eljárás szerint azonban annak olyan előállítását is szolgáltatja, a mely az F-eknek ismeretes együtthatókkal ellátott lineáris formája és e szerint végre a

$$\Sigma F_i \lambda_i \equiv 1 \pmod{(P^{(k)})}$$

azonos congruentiát, azaz (2)-nek egy megoldását nyerjük.

Ha a resolvens forma az x_{k+1} határozatlant tartalmazza, akkor az

$$\sim P_{k+1,1}^{a_1} \dots P_{k+1,s}^{a_s} \left(\text{mod. } (P^{(k)})\right),$$

a hol minden egyes $P_{k+1,r}$ alakja: $x_{k+1}^{\nu_r} + \cdots$ Ekkor azonban egyszersmind

$$(F_1, \dots, F_h, P_{k+1,1}^{a_1} \dots P_{k+1,s}^{a_s}) \simeq (F_1, \dots, F_h) \simeq 1 \left(\text{mod. } (P^{(k)})\right),$$

és így

$$(F_1, \dots, F_h, P_{k+1,r}) \simeq 1, \left(\text{mod. } (P^{(k)})\right);$$

mert az oly absolut törzsrendszert, a melyet ez a rendszer tartalmaz, az $(F_1, \dots, F_h)$ rendszer is tartalmazza. Ez az æquivalentia azonban az

$$(F_1, \dots, F_h) \simeq 1 \left(\text{mod. } P_{k+1,r}, (P^{(k)})\right)$$

alakban is írható és evvel a (2) alatti problemának reductióját szolgáltatja a

$$\sum_{i=1}^{h} F_i X_i \equiv 1 \left(\text{mod. } (P_{(r)}^{(k+1)})\right) \qquad (r=1, \dots, s) \qquad (3)$$

congruentia problémájára, ha az itt mint modulusrendszer szereplő P-rendszer jelölésére ezt a rövid jelképet használjuk. Ha feltételezzük, hogy ennek a congruentiának elmélete már teljesen be van fejezve, akkor evvel megvan az eredeti probléma megoldása is. A (2) alatti congruentiának ugyanis, a mint azt épen megmutattuk, csak akkor van megoldása, ha ugyanaz áll a (3) alatti congruentiákról is; másrészt pedig, ha a (3) alatt álló minden egyes congruentiának egy-egy megoldása ismeretes, akkor (2)-nek egy megoldása közvetetlenül előállítható.

A (3)-nak megoldásait jellemezzék a következő azonos congruentiák:

$$\sum_{i=1}^{h} F_i \mu_{ir} \equiv 1 \left(\text{mod. } P_{k+1,r}, (P^{(k)})\right). \qquad (r=1, \dots, s)$$

Ezeket a

$$\sum_{i=1}^{h} F_i \mu_{ir} + P_{k+1,r} \nu_r \equiv 1 \left(\text{mod. } (P^{(k)})\right) \qquad (r=1, \dots, s)$$

alakban is írhatjuk; mert, ha a μ-k adva vannak, $\sum_{i=1}^{h} F_i \mu_{ir} - 1$-nek olyan előállítását, a mely $(P_{(r)}^{(k+1)})$ elemeinek homogén lineáris formája, a közönséges osztási eljárás is szolgáltatja.

Ha már mostan ezt az azonos congruentiát az a_r-dik hatványra emeljük és kellő módon rendezzük, abból ismét bizonyos

$$\sum_{i=1}^{h} F_i \mu_{ir}' + P_{k+1,r}^{a_r} \nu_r^{a_r} \equiv 1 \pmod{(P^{(k)})} \qquad (r=1,\ldots,s)$$

alakú azonos relációt nyerünk és ha az azonos congruentiák e sorozatát egymással megszorozzuk és a szorzatot ismét kellő módon rendezzük, akkor nyerjük, hogy

$$\sum_{i=1}^{h} F_i \mu_i'' + P_{k+1,1}^{a_1} \ldots P_{k+s}^{a_s} \nu \equiv 1 \pmod{(P^{(k)})}.$$

A resolvens formának előállításából azonban még a további

$$P_{k+1}^{a_1} \ldots P_{k+1,s}^{a_s} \equiv \sum_{i=1}^{h} \lambda_i' F_i \pmod{(P^{(k)})}$$

azonos reláczio is származik és e szerint a keresett megoldást a

$$\sum_{i=1}^{h} F_i (\mu_i'' + \lambda_i' \nu) \equiv 1 \pmod{(P^{(k)})}$$

azonos congruentia szolgáltatja.

Evvel azonban az a feladat, a melyet «második alapproblémának» neveztünk, véges számú lépésben teljesen el van intézve; hisz így

$$\sum_{i=1}^{h} F_i X_i \equiv 1 \pmod{(P^{(m-1)})}$$

alakú congruentiák *egy* megoldásának meghatározására vezettük ezt vissza; azt pedig, hogy ilyen congruentiáknak nem csupán csak egy, hanem általános megoldása is hogyan határozható meg, már a 6. §-ban előadtuk.

A mi czéljainknak megfelelőleg különben elegendő az

a megjegyzés, hogy az $F_1, \ldots, F_h$ formák legnagyobb közös osztója egészen elemi úton (EUKLIDES módszere szerint) határozható meg és, ha erről kitünik, hogy $\sim 1 \pmod{(P^{(m-1)})}$, akkor ugyanaz az eljárás szolgáltat egy

$$\Sigma F_i \lambda_i \equiv 1 \pmod{(P^{(m-1)})}$$

relációt is.

Genus-tartományok mod. $(P^{(k)})$.

9. §. Ha $F(x_l, x_{l-1}, \ldots, x_1)$ olyan raczionális és egész forma, a mely x_l-t valóban tartalmazza és $l > k$, akkor az

$$F(x_l, x_{l-1}, \ldots, x_1) \equiv 0 \pmod{(P^{(k)})}$$

congruentia szóról szóra ugyanazokra a vizsgálatokra szolgáltat alkalmat, a melyeket a IV. fejezetben a $k = -1$ esetnek megfelelőleg végeztünk.

Jelesen, ha $F(x_l, x_{l-1}, \ldots, x_1)$ *irreducibilis* mod. $(P^{(k)})$ és x_l-re vonatkozólag n-edfokú, akkor teljesen úgy, mint a IV. fej. 6. §-ában a

$$\frac{G_0 + G_1\alpha + \cdots + G_{n-1}\alpha^{n-1}}{H} \pmod{(P^{(k)})}$$

pseudoorthoid tartományhoz jutunk, a hol $G_0, \ldots, G_{n-1}, H$ az $x_1, \ldots, x_{l-1}$ határozatlanoknak raczionális és egész formái «mod. $(P^{(k)})$» és H nem $\equiv 0 \pmod{(P^{(k)})}$. E tartomány két mennyisége,

$$\frac{G_0 + G_1\alpha + \cdots + G_{n-1}\alpha^{n-1}}{H} \quad \text{és} \quad \frac{G'_0 + G'_1\alpha + \cdots + G'_{n-1}\alpha^{n-1}}{H'}$$

akkor és csak akkor «egyenlő», azaz congruens mod. $(P^{(k)})$, ha

$$H'G_i \equiv HG'_i \pmod{(P^{(k)})}. \qquad (i = 0, 1, \ldots, n-1)$$

E mennyiségek összeadását és szorzását az algebra közönséges törvényei szerint hajtjuk végre, utasítva még arra, hogy α-nak n-dik és ennél magasabb hatványai az eredményből az

$$F(\alpha, x_{l-1}, \ldots, x_1) \equiv 0 \pmod{(P^{(k)})}$$

azonos reláczió segítségével eltávolítandók. Magától értetődik, hogy ennek az utasításnak értelme az, hogy az új tartományban α az $F \equiv 0 \pmod{(P^{(k)})}$ congruentia gyöke.

Az új tartomány rövid jellemzésére azt mondjuk, hogy «$(l-1) \pmod{(P^{(k)})}$-ból az $F \equiv 0 \pmod{(P^{(k)})}$ congruentia egyik gyökének adjunctiója révén származik» és jelölésére szolgáljon

$$((l-1), \alpha) \pmod{(P^{(k)})},$$

a hol az $[[1], x_1, \ldots, x_{l-1}]$ orthoid tartomány jelölésére az $(l-1)$ rövidített jelölést vezettük be; e tartomány mennyiségei absolut algebrai mennyiségek «mod. $(P^{(k)})$».

Az $((l-1), \alpha) \pmod{(P^{(k)})}$ tartomány a IV. fej. 7. §-ában kifejtett értelemben a «legkisebb» pseudoorthoid tartomány, a melyben az $F(z) \equiv 0 \pmod{(P^{(k)})}$ congruentiának van gyöke.

Teljes analogiában a IV. fej. 10. §-ának fejtegetéseivel megszerkeszthetjük azt a «Galois-féle tartományt mod. $(P^{(k)})$» is, a melyben az $F(z) \equiv 0$ congruentiának pontosan ugyanannyi gyöke van, mint a hány egységet tartalmaz x_l-re vonatkozó foka. Ép úgy (mint a IV. fej. 14. és 15. §-ában) nyerjük azután az $(l-1)$ tartományból származó genus-tartományokat mod. $(P^{(k)})$, ezeknek conjugált tartományait és az ott felsorolt ide vonatkozó egyes tételeket.

Valamely $((l-1), \alpha) \pmod{(P^{(k)})}$ genus-tartományból származó formának tényezőkre való felbontása ismét ugyanazokat a törvényeket és szabályokat követi, a melyeket a IV. fej. 16. §-ában a legegyszerűbb esetre, midőn $k = -1$, már kifejtettünk. Végre teljes analogiában a IV. fej. 19. §-ában előadottakkal belátjuk, hogy az $((l-1), \alpha) \pmod{(P^{(k)})}$ tartományból származó genus-tartományok azonosak az $(l-1) \pmod{(P^{(k)})}$ tartományból származó $((l-1), \beta) \pmod{(P^{(k)})}$ genus-tartományokkal.

Ha $l = k+1$ és $k > -1$, akkor a $((k), \alpha) \pmod{(P^{(k)})}$ tar-

tomány csak véges számmal tartalmaz mennyiségeket; az így értelmezett algebrai mennyiségek, ha $k=0$, egyszerűen azok a képzetes mennyiségek, a melyeket GALOIS vezetett be a számelméletbe. Ez az eset, a melyre nézve egyes tételek állításai módosítandók volnának, e könyv további fejtegetéseiben nem nyer alkalmazást; *a következőkben azonban mindig feltételezzük, hogy* $l \geqq k+2$.

Legyenek már most

$$\Phi_j(z_1, z_2, \ldots, z_j), \qquad (j=1, \ldots, r)$$

a $z_1, \ldots, z_r$ határozatlanoknak olyan *igazi* formái, a melyeknek együtthatói az $[[1], x_1, \ldots, x_s] \pmod{(P^{(k)})}$ tartományhoz tartoznak, z_j legmagasabb hatványának együtthatója Φ_j-ben pedig ugyane tartományhoz tartozzék és legyen $s>k+1$. Tételezzük fel továbbá, hogy Φ_1 irreducibilis $\text{mod.}(P^{(k)})$; a $\Phi_1 \equiv 0$ egyik gyökének adjunctiója révén származó genus-tartomány legyen $((s), \alpha_1) \pmod{(P^{(k)})}$ és e tartományban legyen ismét $\Phi_2(\alpha_1, z_2)$ irreducibilis $\text{mod.}(P^{(k)})$; a $\Phi_2(\alpha_1, z_2) \equiv 0$ congruentia egyik gyökének adjunctiója révén származzék az $((s), \alpha_1, \alpha_2) \pmod{(P^{(k)})}$ genus-tartomány; ezt így tovább folytatva végre $\Phi_r(\alpha_1, \ldots, \alpha_{r-1}, z_r)$-hez jutunk, a mely az $((s), \alpha_1, \ldots, \alpha_{r-1}) \pmod{(P^{(k)})}$ tartományban irreducibilisnek veendő és azután végre a $\Phi_r(\alpha_1, \ldots, \alpha_{r-1}, z_r) \equiv 0$ congruentia egyik gyökének adjunctiója révén származzék az

$$((s), \alpha_1, \ldots, \alpha_r) \pmod{(P^{(k)})}$$

tartomány.

Ha most már Ψ a $z_1, \ldots, z_r$ határozatlanoknak olyan formája, a melynek együtthatói az $[[1], x_1, \ldots, x_s]$ tartományból valók, akkor a közönséges osztási eljárás segítségével olyan

$$G\Psi \equiv \Sigma A_j \Phi_j + R \pmod{(P^{(k)})}$$

relációhoz juthatunk, a melyben G az x-eknek oly raczionális és egész formája, a mely különböző $\text{mod.}(P^{(k)})$ a 0-tól és R a

z-knek olyan formája, a melynek z_j-re vonatkozó foka legfölebb $n_j - 1$, ha Φ_j-nek z_j-re vonatkozó foka n_j. Az α mennyiségek értelmezése szerint

$$R(\alpha_1, \ldots, \alpha_r) \pmod{(P^{(k)})}$$

akkor és csak akkor zérus, ha az $R(z_1, \ldots, z_r)$ forma mod. $(P^{(k)})$ eltünik és ez csak akkor történik, ha

$$\Psi(\alpha_1, \ldots, \alpha_r) \equiv 0 \pmod{(P^{(k)})}.$$

Ebben az esetben tehát egyszersmind

$$G\Psi \equiv 0 \pmod{\Phi_1, \ldots, \Phi_r, (P^{(k)})}.$$

Ha ezt az eredményt kapcsolatba hozzuk a VII. fej. 7. §-ának eredményével végre a következő tételt nyerjük:

I. *Ha Ψ valamely olyan forma, a melyre nézve $\Psi(\alpha_1, \ldots, \alpha_r) \equiv 0 \pmod{(P^{(k)})}$, akkor van az x-eknek olyan meghatározott raczionális és egész formája K, a mely különböző* mod. $(P^{(k)})$ *a 0-tól és a melyre nézve*

$$K\Psi \equiv 0 \pmod{\Phi_1, \ldots, \Phi_r, (P^{(k)})}.$$

E mellett még teljesen úgy, mint az idézett helyen, belátható, hogy a K formát véges számú lépésben meghatározhatjuk, ha a

$$\Sigma F_i X_i \equiv 0 \pmod{(P^{(k)})}$$

homogén lineáris congruentia általános megoldása az $[[1], z_1, \ldots, z_r, x_1, \ldots, x_s]$ tartományban ismeretes.

E mellett még megjegyzendő a következő: *Ha φ_j a z_j legmagasabb hatványának együtthatója Φ_j-ben, akkor K minden esetre csak azokat az x határozatlanokat tartalmazza, a melyek $\varphi_1, \ldots, \varphi_r$-ben valóban előfordúlnak.*

Ha azonban másodszor $\Psi(\alpha_1, \ldots, \alpha_r)$ nem $\equiv 0 \pmod{(P^{(k)})}$, tehát $R(\alpha_1, \ldots, \alpha_r)$ is különböző a 0-tól, akkor meghatározhatjuk az $((s), \alpha_1, \ldots, \alpha_r)$ tartomány oly második mennyiségét, a melynek alakja ép olyan mint az R-é úgy, hogy

$$S(\alpha_1, \ldots, \alpha_r)\, R(\alpha_1, \ldots, \alpha_r) \equiv 1 \pmod{(P^{(k)})}$$

legyen és így

$$GS(\alpha_1, \ldots, \alpha_r)\ \Psi(\alpha_1, \ldots, \alpha_r) - 1 \equiv 0 \pmod{P^{(k)}}.$$

E mellett S nevezője az $x_1, \ldots, x_s$ határozatlanoknak olyan raczionális és egész formája, a mely különböző mod. $(P^{(k)})$ a 0-tól. Ha evvel a nevezővel és az előbb meghatározott K formával szorzunk, e második esetnek megfelelő következő tételt nyerjük:

II. *Ha* $\Psi(\alpha_1, \ldots, \alpha_r)$ *nem* $\equiv 0 \pmod{(P^{(k)})}$, *akkor van az x-eknek és z-knek egy másik raczionális és egész formája* X *és az x-eknek oly raczionális és egész formája* H, *hogy mind a kettő különböző* mod. $(P^{(k)})$ *a* 0*-tól, továbbá pedig olyan tulajdonságú, hogy*

$$\Psi X \equiv H \pmod{\Phi_1, \ldots, \Phi_r, (P^{(k)})}.$$

Az X és H formák meghatározása az előbb említett diophantikus problémával együtt ismét el van intézve.

A homogén lineáris diophantikus egyenlet arithmetikai megoldása. A reductio elvei.

10. §. Most már rendelkezésünkre állanak az összes segédeszközök arra, hogy a $\Sigma F_j X_j = 0$ egyenlet megoldását az $[[1], x_1, \ldots, x_m]$ tartományban teljesen elintézhessük. Ez oly általános módszer szerint történik, a melylyel az $[[1], x_1, \ldots, x_m]$ tartományban tárgyalandó problémát visszavezetjük a hasonló problémára az $[[1], x_1, \ldots, x_{m-1}]$ tartományban. Magától értetődik, hogy a feladat általánossága mellett e reductio nem lehet valami különösen egyszerű. A tárgyalásban az $m=1$ és $m=2$ esetek, a melyek bizonyos tekintetben elemieknek mondhatók, különös helyzetet foglalnak el, a melyre alkalom adtán még reámutatunk.

A problémát elejétől fogva mint a

$$\Sigma F_j X_j \equiv 0 \pmod{(P^{(k)})}$$

congruentia megoldását fogalmazhatjuk, a mely csupán

csak formálisan általánosabb a $\Sigma F_j X_j = 0$ egyenletnél; és, ha $k=-1$, egyenesen ebbe megy át.

A $k=m$ és $k=m-1$ esetek egész elemi módon intézhetők el.

Ha $k=m$, először is lehetséges, hogy az összes együtthatók $\equiv 0 \pmod{(P^{(m)})}$ és ekkor az X formák egyáltalában semmiféle további megszorításnak nincsenek alávetve. Ha pedig nem evvel az esettel van dolgunk, tehát pl. F_1 nem $\equiv 0 \pmod{(P^{(m)})}$, akkor meghatározható olyan G forma, a melyre nézve

$$GF_1 \equiv 1 \pmod{(P^{(m)})};$$

ha ezután az adott congruentiát G-vel megszorozzuk, az az

$$X_1 + \sum_{j=2}^{h} GF_j X_j \equiv 0 \pmod{(P^{(m)})},$$

congruentiába megy át, a melynek megoldása közvetetlenül felírható.

Ha $k=m-1$, ismét csak azt az esetet kell vizsgálnunk, midőn nem minden együttható $\equiv 0 \pmod{P^{(m-1)}}$. (Ha $m=0$, ez annyit jelent, hogy nem tünnek el az összes együtthatók.) Eltávolíthatjuk továbbá az F-eknek legnagyobb közös osztóját $\pmod{(P^{(m-1)})}$; ha ezután az együtthatók közül az egyik $\equiv \pm 1$, akkor nyilvánvaló, hogy a congruentia általános megoldása már is megvan. Az ellenkező esetben legyen F_1 $\pmod{(P^{(m-1)})}$ irreducibilis tényezőire felbontva:

$$F_1 \equiv \pi_1 \pi_2 \ldots \pmod{(P^{(m-1)})}.$$

Akkor az F formák közül egyik, pl. F_h nem lesz $\pmod{(P^{(m-1)})}$ osztható π_1-gyel; másrészt pedig

$$\sum_{j=2}^{h} F_j X_j \equiv 0 \pmod{\pi_1, (P^{(m-1)})}.$$

Közvetetlenül belátható, hogy az itt alkalmazott modulusrendszer $m+1$-edfokozatú P-rendszer, F_h pedig e modulusrendszerre nézve nem $\equiv 0$. Könnyen meghatározható tehát

olyan G forma, a melyre nézve

$$GF_h \equiv -1 \pmod{\pi_1, (P^{(m-1)})};$$

és így tehát

$$X_h \equiv \sum_{j=2}^{h-1} F_j G X_j \pmod{\pi_1, (P^{(m-1)})},$$

vagy pedig

$$X_h = \sum_{j=2}^{h-1} F_j G X_j + \pi_1 Y_1 \pmod{(P^{(m-1)})}.$$

Az adott congruentia tehát átmegy a következőbe:

$$F_1 X_1 + \sum_{j=2}^{h-1} F_j (F_h G + 1) X_j + F_h \pi_1 Y_1 \equiv 0 \pmod{(P^{(m-1)})}.$$

Ebben az összes együtthatók π_1-gyel oszthatók; ez az osztó tehát eltávolítható és így congruentiánk az

$$\frac{F_1}{\pi_1} X_1 + \sum_{j=2}^{h-1} F_j \frac{F_h G + 1}{\pi_1} X_j + F_h Y_1 \equiv 0 \pmod{(P^{(m-1)})}$$

congruentiával együtt megoldottnak tekinthető. Most azonban F_1 helyett X_1 együtthatója $\frac{F_1}{\pi_1}$ lett, és így tehát véges számú lépésben olyan congruentiához jutunk, a melyben X_1 együtthatója ± 1 és evvel megvan feladatunk általános megoldása.

Ha $m=0$, akkor ez egyszerűen a $\Sigma a_j x_j = 0$ diophantikus egyenlet megoldása [1]-ben.

Feladatunk tehát általánosan meg van oldva, ha azt m-ről $m-1$-re tudjuk redukálni. E mellett *minden* lineáris diophantikus rendszer megoldása az $[[1], x_1, \ldots, x_{m-1}]$ tartományban elintézettnek tekinthető, mert a második alapproblémát, t. i. $\Sigma F_j X_1 = 1$ egyik megoldásának meghatározását, ha ilyen egyáltalában létezik, előbb már teljesen elvégeztük.

11. §. Az $[[1], x_1, \ldots, x_m]$ tartományban a

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{(P^{(k)})}$$

congruentia elmélete be van fejezve, ha $k=m$, vagy $k=m-1$.

Ugyanaz áll akkor is, *ha* $k<m-1$ *és az együtthatók az* $x_{k+1}, \ldots, x_m$ *határozatlanok egyikét, pl.* x_m*-et nem tartalmazzák*

Ha ebben az esetben az X_j $(j=1, \ldots, h)$ ismeretlennek az x_m hatványai szerint rendezett alakja

$$X_j = X_{j0} + X_{j1} x_m + \cdots + X_{jr} x_m^r + \cdots,$$

akkor

$$\Sigma F_j X_{jr} \equiv 0 \pmod{(P^{(k)})}$$

és ebből — minthogy hiszen csak az $[[1], x_1, \ldots, x_{m-1}]$ tartományban megoldandó problémával van dolgunk —

$$X_{jr} \equiv \sum_{(s)} G_{js} U_{rs} \pmod{(P^{(k)})},$$

a hol a G-k az $x_1, \ldots, x_{m-1}$ határozatlanoknak adott, az r-től független, az U_{rs}-ek pedig ugyanezen határozatlanoknak tetszés szerinti raczionális és egész formái. Ez a mi esetünkben a megfelelő

$$X_j \equiv \sum_{(s)} G_{js} V_s \pmod{(P^{(k)})}$$

általános megoldást szolgáltatja, a hol tehát

$$V_s = \sum_{(r)} U_{rs} x_m^r$$

az $x_1, \ldots, x_m$ határozatlanoknak tetszés szerinti formája.

Az a specziális probléma, a mely *mindazoknak a formáknak meghatározását követeli, a melyek a*

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{(P^{(k)})}$$

congruentiát kielégítik és a melyeknek x_m*-re vonatkozó foka nem lépi túl az* n*-t*, most már szintén megoldottnak tekinthető. Ha ugyanis az F_j-ket és az X_j ismeretleneket is az x_m hatványai szerint rendezzük, akkor most szükségképen $\Sigma F_j X_j$-ben x_m minden egyes hatványának együtthatója külön $\equiv 0 \pmod{(P^{(k)})}$ és ez a homogén lineáris diophantikus egyen-

letek olyan rendszerét szolgáltatja az $[[1], x_1, \ldots, x_{m-1}]$ tartományban, a melyben az ismeretlenek az

$$X_j = \sum_{r=0}^{n} X_{jr} x_m^r$$

-ben szereplő X_{jr} formák.

Végűl mint olyan egyenletet, a melynek megoldása közvetetlenűl felírható, még megemlítjük a

$$P_{m+1} X_{m+1} + P_m X_m + \cdots + P_1 X_1 + p_0 X_0 = 0$$

egyenletet, a melynek együtthatói $m+1$-ed fokozatú P-rendszert alkotnak.

Minthogy $P_{m+1} X_{m+1} \equiv 0 \pmod{(P^{(m)})}$ és P_{m+1} nem $\equiv 0 \pmod{(P^{(m)})}$, azért

$$X_{m+1} = P_m U_m + \cdots + P_1 U_1 + p_0 U_0 \qquad (a)$$

és evvel az egyenlet átmegy a következőbe:

$$P_m (X_m + P_{m+1} U_m) + \cdots + P_1 (X_1 + P_{m+1} U_1) + p_0 (X_0 + P_{m+1} U_0) = 0,$$

a melyből ismét

$$X_m + P_{m+1} U_m = P_{m-1} U_{m-1}^{(1)} + \cdots + P_1 U_1^{(1)} + p_0 U_0^{(1)} \qquad (b)$$

származik. Ebből pedig következik, hogy

$$P_{m-1} (X_{m-1} + P_{m+1} U_{m-1} + P_m U_{m-1}^{(1)}) + \cdots + \\ + p_0 (X_0 + P_{m+1} U_0 + P_m U_0^{(1)}) = 0$$

és

$$X_{m-1} + P_{m+1} U_{m-1} + P_m U_{m-1}^{(1)} = P_{m-2} U_{m-2}^{(2)} + \cdots + p_0 U_0^{(2)} \qquad (c)$$

s í. t. Közvetetlenűl belátható, hogy az ismeretleneknek ez a szükséges alakja mindig egyszersmind elegendő is arra, hogy az adott egyenletnek megoldását szolgáltassa.

Az általános módszer kifejtésére még a következő megjegyzés is lényeges. A

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{(P^{(k)})}$$

congruentia, ha a bal oldalon álló tagokat tetszés szerinti két részre választjuk szét, még a következő módon is írható:

$$\sum_{j'=1}^{h'} F'_{j'} X'_{j'} + \sum_{j''=1}^{h''} F''_{j''} X''_{j''} \equiv 0 \left(\text{mod. } (P^{(k)})\right), \quad (h'+h''=h), \quad (1)$$

és általános megoldása természetesen a

$$\sum_{j'=1}^{h'} F'_{j'} X'_{j'} \equiv 0 \left(\text{mod. } F''_1, \ldots, F''_{h''}, (P^{(k)})\right) \quad (2)$$

congruentia általános megoldását is szolgáltatja, mert ekkor csak a X'' ismeretleneknek értékeit mellőzzük.

Ennek megfordítottja csak speciális esetekben érvényes. Minden esetre szükséges, hogy a X' ismeretlenek (1)-ben a (2)-ből származó

$$X'_{j'} = \sum_{(s)} G_{j's} U_s \left(\text{mod. } F''_1, \ldots, F''_{h''}, (P^{(k)})\right) \quad (3)$$

alakot vegyék fel és, minthogy ezek az U_s formák bármely választása mellett (2)-nek egyik megoldását szolgáltatják, ismét szükséges, hogy a (3)-ból vett értékek behelyettesítése révén származó

$$\sum_{j'=1}^{h'} F'_{j'} X'_{j'} = \sum_{(s)} H_s U_s$$

kifejezésben előforduló minden H_s-re nézve

$$H_s \equiv 0 \left(\text{mod. } F''_1, \ldots, F''_{h''}, (P^{(k)})\right)$$

legyen. Ha az ennek megfelelő

$$H_s \equiv \sum_{j''=1}^{h''} A_{j''s} F''_{j''} \left(\text{mod. } (P^{(k)})\right) \quad (4)$$

előállítások egyikét ismerjük, akkor (2)-nek megoldása után az (1) alatti congruentia a következőbe megy át:

$$\sum_{j''=1}^{h''} F''_{j''} (X''_{j''} + A_{j''1} U_1 + A_{j''2} U_2 + \cdots) \equiv 0 \left(\text{mod. } (P^{(k)})\right). \quad (5)$$

E szerint az (1) *alatti congruentia a következő két esetben teljesen pótolható a* (2)*-vel; még pedig először, ha* $\mathbf{h''=1}$ *és másodszor, ha a* F'' *formák az* $x_{k+2}, \ldots, x_m$ *határozatlanoknak egyikét, pl.* x_m*-et nem tartalmazzák.*

Az első esetben a (4)-ben és (5)-ben felállított felada-

tok megoldása közvetetlenül megvan; a második esetben pedig az $[[1], x_1, \ldots, x_{m-1}]$ tartományban megoldandó lineáris diophantikus problémákkal van dolgunk.

12. §. Az eddigi fejtegetések a

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{(P^{(k)})}$$

congruentia általános megoldását szolgáltatták a $k=m$ és $k=m-1$ esetekben; az általános megoldás tehát mindig előállítható, ha a problémát ép oly congruentiára mod. $(P^{(k+1)})$ tudjuk visszavezetni. Ezt teszszük a következőkben.

A kitűzött czélt legegyszerűbben akkor érjük el, ha az együtthatók közül az egyik csak az $x_1, \ldots, x_k, x_{k+1}$ határozatlanokat tartalmazza. A congruentia ekkor a

$$\Phi^{(k+1)} Y + G_1 Z_1 + \cdots \equiv 0 \pmod{(P^{(k)})}$$

alakban írható, a hol $\Phi^{(k+1)}$ az $x_1, \ldots, x_{k+1}$ határozatlanoknak olyan raczionális és egész formája, a mely különböző mod. $(P^{(k)})$ a 0-tól.

Ha már mostan $\Phi^{(k+1)} \sim 1 \pmod{(P^{(k)})}$, tehát

$$\Psi\Phi^{(k+1)} \equiv -1 \pmod{(P^{(k)})},$$

akkor közvetetlenül találjuk, hogy

$$Y \equiv \Psi G_1 Z_1 + \cdots \pmod{(P^{(k)})}.$$

Abban az esetben, midőn $\Phi^{(k+1)}$ nem $\sim 1 \pmod{(P^{(k)})}$ $\Phi^{(k+1)}$ felbontható mod. $(P^{(k)})$ irreducibilis tényezőire. Legyen e felbontás

$$\Phi^{(k+1)} \equiv \pi_1 \pi_2 \ldots \pmod{(P^{(k)})},$$

akkor a congruentia a

$$\pi_1 (\pi_2 \ldots Y) + G_1 Z_1 + \cdots \equiv 0 \pmod{(P^{(k)})}$$

alakban írható. E szerint

$$G_1 Z_1 + \cdots \equiv 0 \pmod{\pi_1, (P^{(k)})}.$$

Az itt fellépő modulusrendszer egyenesen $k+1$-edfokozatú P-rendszer úgy, hogy ennek a congruentiának általános

megoldása ismeretesnek vehető. E megoldás a következőket szolgáltatja:

$$Z_i \equiv \sum_{(s)} H_{is} U_s + \pi_1 Y_i \ (\text{mod.}\ (P^{(k)})),$$

és

$$\pi_2 \ldots Y \equiv \sum_{(s)} K_s U_s + \sum_{(i)} G_i Y_i \ (\text{mod.}\ (P^{(k)})).$$

Ennek az utóbbi congruentiának megoldása az U-knak és Y-nak speciális alakját szolgáltatja és evvel együtt a Z-két is. A most megoldandó congruentiában azonban az Y együtthatója már csak $\frac{\Phi^{(k+1)}}{\pi_1}$, és így tehát véges számú lépésben jutunk a $\frac{\Phi^{(k+1)}}{\pi_1 \pi_2 \ldots} \equiv 1 \ (\text{mod.}\ (P^{(k)}))$ együtthatóhoz, azaz a felállított feladat végleges megoldásához.

13. §. Általánosságban legyen az adott congruentiában egy olyan együttható, a mely az $x_1, \ldots, x_k$ határozatlanokon kívül még csak az $x_{k+1}, \ldots, x_l$ határozatlanokat tartalmazza, a hol $l > k+1$. Ha ezt az esetet arra az esetre redukáljuk, midőn egyik együttható az $x_1, \ldots, x_k$ határozatlanokon kívül még csak az $x_{k+1}, \ldots, x_{l-1}$ határozatlanokat tartalmazza, akkor véges számú lépésben olyan congruentiához jutunk, a melynek megoldása már ismeretes, azaz így a felállított probléma általános megoldását nyerjük.

E mellett elegendő, ha feltételezzük, hogy ama $\Phi^{(l)}(x_1, \ldots, x_l)$ együttható mod. $(P^{(k)})$ irreducibilis. Az az eset, midőn $\Phi^{(l)}$ több mod. $(P^{(k)})$ irreducibilis tényező szorzata, teljesen elintézhető az előbbi § végén alkalmazott módszer szerint.

Feltételezhetjük továbbá, hogy az adott congruentiában, a melyet most a

$$\Phi^{(l)} Y + G_1 Z_1 + G_2 Z_2 + \cdots \equiv 0 \ (\text{mod.}\ (P^{(k)}))$$

alakban írunk, egyetlen G együttható sem osztható $\Phi^{(l)}$-vel mod. $(P^{(k)})$. Ha pl.

$$G_1 \equiv \Phi^{(l)} H_1 \pmod{(P^{(k)})}$$

volna, akkor a congruentiát a

$$\Phi^{(l)}(Y+H_1 Z_1)+G_2 Z_2+\cdots \equiv 0 \pmod{(P^{(k)})}$$

alakban írhatnók, a melynek általános megoldása az

$$Y+H_1 Z_1 = Y_1$$

helyettesítés után a

$$\Phi^{(l)} Y_1+G_2 Z_2+\cdots \equiv 0 \pmod{(P^{(k)})}$$

congruentia általános megoldásával együtt megvan. Az utóbbi congruentiából azonban az a tag, a melynek együtthatója $\Phi^{(l)}$-vel oszható, kiesett.

A tervezett reductio közvetetlenül elvégezhető, ha az adott congruentiában még egy második olyan együttható is előfordúl, a mely csupán csak az $x_1, \ldots, x_k, \ldots, x_l$ határozatlanokat tartalmazza. A congruentia ekkor a

$$\Phi^{(l)} Y_1+\Psi^{(l)} Y_2+G_1 Z_1+\cdots \equiv 0 \pmod{(P^{(k)})}$$

alakban is írható, vagy pedig (a 11. § utolsó megjegyzése szerint) a

$$\Psi^{(l)} Y_2+G_1 Z_1+\cdots \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}$$

alakban.

Minthogy $\Phi^{(l)} \bmod (P^{(k)})$ irreducibilis és $\Psi^{(l)} \bmod (P^{(k)})$ nem osztható $\Phi^{(l)}$-vel, a $\Psi^{(l)}$ és $\Phi^{(l)}$ formák x_l szerint vett resultánsa,

$$\varrho = \mu \Phi^{(l)}+\nu \Psi^{(l)}$$

nem lesz $\equiv 0 \bmod (P^{(k)})$ és magától értetődik, hogy x_l-t nem tartalmazza. Minthogy továbbá $\nu \bmod (P^{(k)})$ nem osztható $\Phi^{(l)}$-vel és $\Phi^{(l)}$ irreducibilis, ama congruentia a

$$\nu(\Psi^{(l)} Y_2+G_1 Z_1+\cdots) \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})},$$

vagy végre a

$$\varrho Y_2+\Phi^{(l)} Y_3+\nu G_1 Z_1+\cdots \equiv 0 \pmod{(P^{(k)})}$$

alakban írható, a hol a ϱ együttható már csak az $x_1, \ldots, x_{l-1}$ határozatlanokat tartalmazza. Abban az esetben, midőn $l=1$, ϱ a 0-tól különböző raczionális és egész szám.

Evvel már most a homogén lineáris diophantikus egyenlet problémája az $[[1], x_1]$ *tartományban teljesen el van intézve.*

E tartományban az ismeretleneknek együtthatói *egy* határozatlannak raczionális és egész formái. Az épen tárgyalt reductio az egyenlet megoldását olyan egyenlet megoldására vezeti vissza, a melyben az egyik együttható raczionális és egész szám. (Az $FX=0$ triviális esetet, a melyből $X=0$ következik, mellőztük.)

A 12. §. szerint a probléma megoldására már csak bizonyos

$$\Sigma G_i Z_i \equiv 0 \pmod{p}$$

congruentiáknak az $[[1], x_1]$ tartományban való megoldása szükséges, a hol p természetes törzsszámot jelent. Itt $k=0$, $m=1$; tehát olyan esettel van dolgunk, a melynek megoldását már a 10. §-ban adtuk.

14. §. A reductio további menete most már a következő. Jelenleg olyan

$$\Sigma F_j X_j \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})} \qquad \text{(I)}$$

congruentiával van dolgunk, a melyben $\Phi^{(l)}$ az $x_1, \ldots, x_l$ határozatlanoknak raczionális és egész formája, a mely mod. $(P^{(k)})$ irreducibilis, továbbá $l>k+1$ és végre egyetlen F_j együttható sem osztható $\Phi^{(l)}$-vel mod. $(P^{(k)})$.

E mellett azonban feltehető az is, hogy $l<m$. Arra az esetre, midőn $l=m$ és az x_m határozatlan az összes F_j együtthatókban valóban előfordúl, a reductiót $l=m$-ről $l=m-1$-re épen előbb végeztük el. Ha azonban pl. F_1 oly forma, a mely x_m-et nem tartalmazza, akkor ez a forma, ill. egyik irreducibilis tényezője veendő $\Phi^{(l)}$-nek és azután csakugyan ismét $l<m$.

Az az eset, midőn az x_m határozatlan egyetlen F-ben sem fordúl elő, a 11. § szerint szerint szintén elintézettnek tekinthető.

Ha egy F az x_m határozatlant tartalmazza, míg az összes többi együttható $\equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}$, akkor az

$$FX + \Phi^{(l)} Y \equiv 0 \pmod{(P^{(k)})}$$

congruentiával van dolgunk, a melyet a később külön tárgyalandó *singuláris esetek* sorozatába teszünk át.

Ha van olyan F, a mely x_m-et nem tartalmazza, a congruentia a

$$\Sigma G_j Y_j \equiv 0 \pmod{\Psi, \Phi^{(l)}, (P^{(k)})} \qquad \text{(II)}$$

alakban is írható, a hol Ψ az $x_1, \ldots, x_{m-1}$ olyan raczionális és egész formáját jelenti, a melyről magától értetődik, hogy $\bmod. (P^{(k)})$ nem osztható $\Phi^{(l)}$-vel.

Vegyük föl végre, hogy az összes F-ek tartalmazzák az x_m határozatlant és legyen pl. F_1-nek x_m-re vonatkozó foka, ν a legalacsonyabb. Akkor a közönséges osztási eljárás olyan

$$\Psi F_j \equiv Q_j F_1 + R_j \pmod{(P^{(k)})}$$

relácziókat szolgáltat, a melyekben R_j-nek x_m-re vonatkozó foka legfölebb $\nu - 1$ és Ψ az F_1-ben x_m^ν mellett álló együtthatónak valamely hatványa és így tehát különböző $\bmod. (\Phi^{(l)}, (P^{(k)}))$ a 0-tól. Az adott congruentia tehát a következőbe megy át:

$$F_1 (\Psi X_1 + Q_2 X_2 + \cdots) + R_2 X_2 + \cdots \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})},$$

a hol, ha $\Psi X_1 + Q_2 X_2 + \cdots$-t új ismeretlennek tekintjük, az F_1 együtthatónak x_m-re vonatkozó foka a legmagasabb. E reductio ismétlése azonban véges számú lépésben vagy a már előbb említett singuláris esetre vezet, vagy pedig olyan congruentiára, a melynek alakja a (II)-ével megegyező és a közben megoldandó congruentiák alakja a következő:

$$\Psi X_1 + Q_2 X_2 + \cdots \equiv \Sigma H_s U_s \pmod{\Phi^{(l)}, (P^{(k)})}.$$

E szerint *a singuláris eset kivételével az* (I) *alatti congruentia általános megoldását a* (II) *alatti congruentia általános megoldására vezettük vissza.*

Evvel azonban a homogén lineáris diophantikus egyen-

let megoldása az $[[1], x_1, x_2]$ *tartományban teljesen el van intézve.*

Ebben az esetben a jelen § elején előadott fejtegetések szerint $l>0$ és $l<2$; tehát $l=1$. A (II) alatti congruentiában Ψ és $\Phi^{(l)}$ az *egyetlen* x_1 határozatlannak formái. A 13. § szerint e probléma bizonyos homogén lineáris congruentiára (mod. p) redukálható, a mely az ott kifejtett módszer szerint teljesen megoldható. Ha az összes együtthatók *mind a két* határozatlant, x_1-et és x_2-t tartalmazzák, akkor az épen kifejtett módszer szerint vagy a singuláris esetre, vagy pedig olyan congruentiához jutunk, a melynek alakja a (II)-ével megegyező és teljes megoldása a 13. § szerint ismeretes. A singuláris eset vagy

$$FX+\Phi^{(1)}Y=0,$$

a hol feltételezhető, hogy F és $\Phi^{(1)}$-nek az 1-től különböző közös osztója nincsen; és így tehát

$$X=\Phi^{(1)}U,\quad Y=-FU$$

általános megoldása közvetetlenül felírható; vagy pedig

$$FX+\Phi^{(1)}Y\equiv 0 \pmod{p}.$$

Ez a congruentia is közvetetlenül megoldható. Megoldása nyilvánvaló, ha *vagy* F, *vagy* $\Phi^{(1)}\equiv 0 \pmod{p}$. Ha azonban e formák közül egyik sem $\equiv 0 \pmod{p}$, akkor F és $\Phi^{(1)}$ legnagyobb közös osztóját mod. p ismét eltávolíthatjuk és azután az

$$X\equiv\bar{\Phi}^{(1)}U,\quad Y\equiv -\bar{F}U \pmod{p}$$

általános megoldást nyerjük.

Az általános eset.

15. §. *A* (II) *congruentia továbbá a*

$$\Sigma G_j Y_j\equiv 0 \left(\text{mod. } \Phi^{(m-1)}, \Phi^{(l)}, (P^{(k)})\right) \qquad \text{(III)}$$

congruentiával pótolható, a hol $(\Phi^{(m-1)})_{x_l=\alpha_l}$ *oly formát jelent, a mely a* $\Phi^{(l)}\equiv 0 \left(\text{mod. } (P^{(k)})\right)$ *congruentia egyik* $x_l\equiv\alpha_l$ *gyökének*

adjunctiója révén származó $((l-1), \alpha_l) \pmod{(P^{(k)})}$ *genus-tartományban irreducibilis, az* x_{m-1} *határozatlant valóban tartalmazza és a melyben* x_{m-1} *legmagasabb hatványának együtthatója az* $x_1, \ldots, x_{l-1}$ *határozatlanoknak olyan racionális és egész formája, a mely* $\bmod. (P^{(k)})$ *a 0-tól különböző*

Hogy (II) miképen redukálható (III)-ra, most közelebbről kifejtendő. E czélból (II)-t a

$$\Psi Y + \Sigma G_j Y_j \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})} \qquad \text{(IIa)}$$

alakban írjuk. Ψ legalább is egyet tartalmaz az $x_{l+1}, \ldots, x_{m-1}$ határozatlanok közül; mert különben már megoldott problémával van dolgunk. A $\Phi^{(l)} \equiv 0 \pmod{(P^{(k)})}$ congruentia egyik $x_l \equiv \alpha_l$ gyökének adjunctiója révén származó $((l-1), \alpha_l) \pmod{(P^{(k)})}$ genus-tartományban $(\Psi)_{x_l=\alpha_l}$ nem tünhetik el, mert különben $\Psi \bmod. (P^{(k)})$ osztható volna $\Phi^{(l)}$-vel.

Ha továbbá $(\Psi)_{x_l=\alpha_l}$ valóban az $x_{l+1}, \ldots, x_{m-1}$ határozatlanok egyikét sem tartalmazza, azaz, ha

$$(\Psi)_{x_l=\alpha_l} \equiv \frac{\varphi(x_1, \ldots, x_{l-1}, \alpha_l)}{\psi(x_1, \ldots, x_{l-1}, \alpha_l)} \pmod{(P^{(k)})},$$

akkor szükségképen

$$\psi(x_1, \ldots, x_l)\, \Psi \equiv \varphi(x_1, \ldots, x_l) \pmod{\Phi^{(l)}, (P^{(k)})}$$

és az adott congruentia, ha azt ψ-vel megszorozzuk, a mi a probléma felállításán mit sem változtat, a következőbe megy át:

$$\varphi Y + \Sigma G_j (\psi Y_j) \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}.$$

Ez a congruentia azonban már teljesen megoldottnak tekinthető, mert először is vonatkozással az Y és ψY_j ismeretlenekre két együtthatója, φ és $\Phi^{(l)}$ már csak az $x_1, \ldots, x_l$ határozatlanokat tartalmazza és azután ugyanaz áll a további

$$\psi Y_j \equiv \Sigma G_s U_s + \Phi^{(l)} Z \pmod{(P^{(k)})}$$

congruentiákról is, a melyekből az Y_j-k határozandók meg.

Így tehát még csak avval az esettel kell foglalkoznunk, midőn $(\Psi)_{x_l=\alpha_l}$ az $x_{l+1}, \ldots, x_{m-1}$ határozatlanok egyikét valóban tartalmazza. Minthogy $l>k+1$, meghatározható olyan homogén lineáris transformatio, a melynek determinánsa 1, együtthatói az $x_1, \ldots, x_{l-1}$ határozatlanoknak raczionális és egész formái, a mely a $(\Psi)_{x_l=\alpha_l}$ formát az $x_{l+1}, \ldots, x_{m-1}$ határozatlanoknak szabályos formájába vezeti át és ugyanaz a transformatio átvezeti a Ψ formát az $x_{l+1}, \ldots, x_{m-1}$ határozatlanoknak olyan szabályos formájába, a melynek együtthatói az $x_1, \ldots, x_l$ határozatlanoknak raczionális és egész formái, a hol azonban ama transformatio meghatározása szerint x_{m-1} legmagasabb hatványának együtthatója mod. $(P^{(k)})$ nem lehet osztható $\Phi^{(l)}$-vel*. A transformatio alkalmazása után tehát lesz

$$\Psi = \psi x_{m-1}^{\nu} + \cdots$$

Minthogy ama transformatio alkalmazása a probléma felállításán ismét nem változtat, Ψ-t az általánosság megszorítása nélkül ebben az alakban vehetjük fel. De a ψ és $\Phi^{(l)}$ formáknak x_l szerint vett resultánsa,

$$\lambda\psi + \mu\Phi^{(l)} \equiv \Phi^{(l-1)} \pmod{(P^{(k)})},$$

olyan a 0-tól mod. $(P^{(k)})$ különböző forma, a mely már csak az $x_1, \ldots, x_{l-1}$ határozatlanokat tartalmazhatja. Ha tehát (IIα)-hoz hozzácsatoljuk a λ tényezőt, a mi a feladaton ismét nem változtat, akkor ez a

$$(\Phi^{(l-1)} x_{m-1}^{\nu} + \cdots) Y + \Sigma G_j (\lambda Y_j) \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}$$

* Tudniilik ψ-nek, mint az $x_{l+1}, \ldots, x_{m-1}$ határozatlanok formájának bármely együtthatója, valamint egyáltalában az $x_1, \ldots, x_l$ határozatlanok bármely formája az $x_l=\alpha_l$ helyettesítés után akkor és csak akkor lesz $\equiv 0 \pmod{(P^{(k)})}$, ha eredetileg is már $\equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}$ volt. Így az is világos, hogy ψ minden oly tagját, melynek együtthatója az utóbbi modulusrendszerre vonatkozólag zérus, vagyis az $x_l=\alpha_l$ helyettesítés után $\equiv 0 \pmod{(P^{(k)})}$, kezdettől fogva elhagyhatjuk.

congruentiába megy át, a melynek vonatkozással az Y és λY_j ismeretleneknek együtthatóira — kivéve az Y együtthatójának irreducibilis voltát — a (III)-ban megszabott alakja van. A végleges megoldás czéljából még tovább targyalandó

$$\lambda Y_j \equiv \Sigma G_s U_s + \Phi^{(l)} Z \pmod{(P^{(k)})}$$

congruentiák megoldása pedig elintézettnek tekinthető, minthogy λ *és* $\Phi^{(l)}$ már csak az $x_1, \ldots, x_l$ határozatlanokat tartalmazzák és $\lambda \bmod (P^{(k)})$ nem osztható $\Phi^{(l)}$-vel*.

16. §. A tárgyalt reductio-módszer teljessé válik, ha azt az *általános*

$$\Sigma F_j X_j \equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, P^{(k)}} \qquad \text{(I)}$$

congruentiára viszszük át, azaz ennek megoldását, hacsak a külön tárgyalandó «singuláris eset» nem lép fel, az $r=l+1$ esetben már ismeretes problémára, ha pedig $r>l+1$ a

$$\Sigma G_j Y_j \equiv 0 \pmod{\Psi^{(m-1)}, \ldots, \Psi^{(r)}, \Psi^{(r-1)}, \Psi^{(l)}, (P^{(k)})} \qquad \text{(II)}$$

congruentia megoldására vezetjük vissza. ($\Phi^{(l)}$-nek megvannak a 14. § elején részletezett tulajdonságai).

Itt $\Phi^{(i)}$ $(i=r, \ldots, m-1)$ mindig olyan formát jelent, a melyben az $x_{i+1}, \ldots, x_m$ határozatlanok nem fordúlnak elő, de a mely x_i-t valóban tartalmazza, a melyben továbbá az x_i legmagasabb hatványa mellett álló együtthatóban már csak az $x_1, \ldots, x_{l-1}$ határozatlanok fordúlnak elő és a mely végre az $x_l=\alpha_l$, $x_r=\alpha_r, \ldots, x_{i-1}=\alpha_{i-1}$ helyettesítés után az

$$((l-1), \alpha_l, x_{l+1}, \ldots, x_{r-1}, \alpha_r, \ldots, \alpha_{i-1}) \pmod{(P^{(k)})}$$

genus-tartományban irreducibilis. Ez a genus-tartomány $\bmod (P^{(k)})$ úgy származik, hogy a $\Phi_l \equiv 0$ congruentia $x_l \equiv \alpha_l$ gyökét, a $\Phi(x_r, \ldots, \alpha_l \ldots) \equiv 0$ congruentia $x_r \equiv \alpha_r$ gyökét stb.-t egymásután adjungáljuk.

* Ismétlés elkerülése végett itt még mellőztük, hogy Y együtthatója az $x_l=\alpha_l$ helyettesítés után az $((l-1), \alpha_l) \pmod{(P^{(k)})}$ genus-tartományban irreducibilisnek vehető fel. Ennek bebizonyítását e redukáló-eljárásnak általános tárgyalásával kapcsolatban (a 18. §-ban) fogjuk előadni.

Magától értetődik, hogy a Ψ formák követelt tulajdonságai a (II)-ben ujonnan becsatolt $\Psi^{(r-1)}$ forma miatt megfelelőleg módosítandók úgy, hogy r helyébe $r-1$ jut.

Az az eset, midőn az (I)-nek F együtthatói közűl egyik sem tartalmazza x_m-et, a 11. § szerint elintézettnek tekinthető.

Ha van olyan F, a mely az x_m határozatlant valóban tartalmazza, akkor legyen pl. F_1-nek x_m-re vonatkozó foka, μ a legalacsonyabb, a hol μ azonban 0 is lehet. Magától értetődik, hogy itt csak olyan együtthatók jönnek tekintetbe, a melyek nem tünnek el mod. $(\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)}))$. Jelesen szükséges, hogy az

$$F_1 = F_{1\mu} x_m^{\mu} + \cdots$$

kifejtésben előfordúló $F_{1\mu}$ is ilyen legyen. Mindamellett azonban

$$(F_{1\mu})_{x_l=\alpha_l,\, x_r=\alpha_r, \ldots, x_{m-1}=\alpha_{m-1}} \pmod{(P^{(k)})}$$

most el is tünhetik. De ekkor a 9. § szerint van az $x_1, \ldots, x_{l-1}$ határozatlanoknak mod. $(P^{(k)})$ el nem tünő olyan tulajdonságú $\Phi^{(l-1)}$ formája, hogy

$$\Phi^{(l-1)} F_{1\mu} \equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})},$$

a hol $\Phi^{(l-1)}$ lineáris diophantikus egyenleteknek az

$$[[1], x_1, \ldots, x_{m-1}]$$

tartományban való megoldásával teljesen meg van adva. Ha az (I) congruentiát, a mely a

$$\sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(l)} Y_l \equiv 0 \pmod{(P^{(k)})}$$

alakban is írható, $\Phi^{(l-1)}$-vel megszorozzuk, az a következő congruentiába megy át:

$$(\Phi^{(l-1)} F_1) X_1 + \sum_{j=2}^{h} F_j (\Phi^{(l-1)} X_j) + \\ + \sum_{i=r}^{m-1} \Phi^{(i)} (\Phi^{(l-1)} Y_i) + \Phi^{(l)} (\Phi^{(l-1)} Y_l) \equiv 0 \pmod{(P^{(k)})}.$$

E congruentia (I)-et teljesen pótolja; mert a $\Phi^{(l-1)} X_j, \ldots$ is-

meretleneknek meghatározása után ezekből az X_j ismeretlenek is, a melyeknek együtthatói már csak az $x_1, \ldots, x_{l-1}$ határozatlanokat tartalmazzák, meghatározhatók.

Így tehát végre olyan (I) congruentiához jutunk, a melyben, ha pl. az F_1 együtthatónak x_m-re vonatkozó foka, μ a legalacsonyabb, az

$$F_1 = F_{1\mu} x_m^{\mu} + \cdots,$$

meghatározta $F_{1\mu}$ mennyiség olyan tulajdonságú, hogy

$$(F_{1\mu})_{x_l=\alpha_l,\ x_r=\alpha_r,\ \ldots,\ x_{m-1}=\alpha_{m-1}} \pmod{(P^{(k)})}$$

nem tünik el. (Kivétel az az eset, midőn minden egyes $F \equiv 0$, és e szerint a congruentia megoldása ismét már el van intézve.)

Ekkor azonban a 9. § szerint oly második $G_{1\mu}$ formát is meghatározhatunk, hogy

$$(G_{1\mu})_{x_l=\alpha_l,\ x_r=\alpha_r,\ \ldots,\ x_{m-1}=\alpha_{m-1}} \pmod{(P^{(k)})}$$

ismét a 0-tól különböző, továbbá

$$F_{1\mu} G_{1\mu} \equiv \Phi^{(r-1)} \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})}$$

és $\Phi^{(r-1)}$ már csak az $x_1, \ldots, x_{l-1}, x_{l+1}, \ldots, x_{r-1}$ határozatlanokat tartalmazza.

A

$$G_{1\mu} \sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})} \qquad \text{(III)}$$

congruentiában tehát, ha $G_{1\mu} F_1$-et x_m hatványai szerint rendezzük, x_m^{μ}-nek együtthatója most $\Phi^{(r-1)}$ lesz és $G_{1\mu} F_1$ is az az együttható, a melynek x_m-re vonatkozó foka a legalacsonyabb.

17. §. *A* (III) *alatti congruentia megoldásának problémája azonban, mellőzve azokat az alacsonyabb rangú problémákat, a melyeknek megoldása már elintézettnek tekinthető, az* (I) *alatti congruentia megoldásának problémájával teljesen egyenlő értékü*

Az (I)-nek minden megoldása egyszersmind a (III)-nak is megoldása. A (III)-nak megoldásaiból viszont az (I)-nek megoldásait is megkapjuk a következő módon. Ha valamely X_j formarendszerre nézve

$$G_{1\mu}\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})},$$

akkor egyszersmind

$$\left(\sum_{j=1}^{h} F_j X_j\right)_{x_l=\alpha_l,\, x_r=\alpha_r, \ldots, x_{m-1}=\alpha_{m-1}} \equiv 0 \pmod{(P^{(k)})};$$

az $x_1, \ldots, x_{l-1}$ határozatlanoknak van tehát olyan a 9. § szerint ismeretes $\Phi^{(l-1)}$ formája, hogy

$$\Phi^{(l-1)}\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})},$$

vagyis

$$\Phi^{(l-1)}\sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(l)} Y_l \equiv 0 \pmod{(P^{(k)})}.$$

Hogy azonban amaz X_j formarendszer egyszersmind az (I)-nek is megoldása lehessen, még bizonyos

$$\Phi^{(l-1)}\sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)}\Phi^{(l-1)} Z_i + \Phi^{(l)}\Phi^{(l-1)} Z_l \equiv 0 \pmod{(P^{(k)})}$$

relációnak kell fennállania. Világos, hogy ennek szükséges és elegendő feltétele a

$$\sum_{i=r}^{m-1} \Phi^{(i)}(Y_i - \Phi^{(l-1)} Z_i) + \Phi^{(l)}(Y_l - \Phi^{(l-1)} Z_l) \equiv 0 \pmod{(P^{(k)})} \quad \text{(IV)}$$

congruentia, a melynek megoldása az $Y_i - \Phi^{(l-1)} Z_i$, $Y_l - \Phi^{(l-1)} Z_l$ ismeretlenek szerint már ismeretes.

A (III)-nak általános megoldása a következő congruentiát szolgáltatja:

$$X_j \equiv \Sigma G_{js} U_s \pmod{(P^{(k)})}$$

és ebből a következő további congruentiák származnak:

$$Y_i \equiv \Sigma H_{is} U_s \pmod{(P^{(k)})},$$
$$Y_l \equiv \Sigma H_{ls} U_s \pmod{(P^{(k)})}.$$

Továbbá azután

$$Y_i - \Phi^{(l-1)} Z_i \equiv \Sigma K_{it} V_t \pmod{(P^{(k)})}$$

és, minthogy itt az egyik együttható $\Phi^{(l-1)}$, evvel megvan az U_s-ek közelebbi meghatározása úgy, hogy végre

$$X_j \equiv \Sigma G_{js} U_s, \quad U_s \equiv \Sigma G'_{st} W_t \pmod{(P^{(k)})}$$

az (I) általános megoldását szolgáltatja.

Ha tehát egyik F együtthatónak x_m-re vonatkozó foka 0, akkor evvel az (I) megoldását visszavezettük a (III)-éra.

Ha egy F az x_m határozatlant tartalmazza, míg az összes többi együttható

$$\equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})},$$

akkor az

$$FX + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(l)} Y^{(l)} \equiv 0 \pmod{(P^{(k)})}$$

congruentiával van dolgunk, a mely az utoljára tárgyalandó *singuláris eset általános typusát* mutatja.

Végre az x_m határozatlant az összes F-ek tartalmazhatják, a melyeknek száma 1-nél nagyobbnak vehető. Ekkor azonban a 14. §-ban az F-ek x_m-re vonatkozó fokának reductiójára alkalmazott eljárás vagy a singuláris esetre vezet, vagy pedig olyan congruentiákra, a melyeknek alakja — a Φ-k irreducibilis voltát kivéve — megegyezik a (II)-ben megadott alakkal, és ugyanez állítható a közben megoldandó congruentiákról is.

Az az eset, midőn $\Phi^{(r-1)}$ már csak az $x_1, \ldots, x_l$ határozatlanokat tartalmazza, közvetetlenül már elintézett alacsonyabb rangú problémára vezet. Így van ez mindig, ha $r = l+1$.

Ha pedig $\Phi^{(r-1)}$ az $x_{l+1}, \ldots, x_{r-1}$ határozatlanok közül legalább egyet valóban tartalmaz, akkor még meg kell mutatnunk, hogy az a feltevés megengedhető, mely szerint az ujonnan bevezetett $\Phi^{(r-1)}$ forma az x_{r-1} határozatlant valóban tartalmazza és hogy x_{r-1} legmagasabb hatványának

együtthatója már csak az $x_1, \ldots, x_{l-1}$ határozatlanokat tartalmazza.

Minthogy $l > k+1$, (a következtetésnek a 15. § végén alkalmazott módját ismételve, belátjuk, hogy) van olyan homogén lineáris transformatio, a melynek determinánsa 1, együtthatói az $x_1, \ldots, x_{l-1}$ határozatlanoknak raczionális és egész formái és a mely a $(\Phi^{(r-1)})_{x_l=\alpha_l}$ formát az $x_{l+1}, \ldots, x_{r-1}$ határozatlanoknak szabályos formájába vezeti át; ugyanaz a transformatio átvezeti a $\Phi^{(r-1)}$ formát az $x_{l+1}, \ldots, x_{r-1}$ határozatlanoknak olyan szabályos formájába, a melynek együtthatói az $x_1, \ldots, x_l$ határozatlanoknak raczionális és egész formái, hol azonban a transformatio meghatározása szerint x_{r-1} legmagasabb hatványának együtthatója nem lehet mod. $(P^{(k)})$ osztható $\Phi^{(l)}$-vel.

Minthogy ez a transformatio sem a probléma felállításán, sem pedig a $\Phi^{(r)}, \ldots, \Phi^{(m-1)}$ formák alakján nem változtat, $\Phi^{(r-1)}$-t az általánosság megszorítása nélkül ebben az alakban vehetjük fel és ha a congruentiát a

$$\sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(r-1)} Y_{r-1} \equiv 0 \ (\text{mod. } \Phi^{(l)}, (P^{(k)}))$$

alakban írjuk, akkor teljesen úgy, mint az idézett helyen, Y_{r-1} együtthatóját a kivánt alakra hozhatjuk.

Az adott congruentia megoldása e mellett csak annyiban változik, hogy most mint «ismeretlenek» λX_j, λY_i szerepelnek, a melyekből azonban X_i, Y_i közvetetlenül meghatározhatók; mert hiszen λ az $x_1, \ldots, x_l$ határozatlanoknak és csak ezeknek oly formája, a mely $\Phi^{(l)}$-vel mod. $(P^{(k)})$ nem osztható és így tehát olyan congruentiával van dolgunk, a melyben *két* a 0-tól (mod. $(P^{(k)})$) különböző együttható van, és ezek egyedül csak az $x_1, \ldots, x_l$ határozatlanoknak formái.

18. §. A lineáris diophantikus egyenletek arithmetikai elmélete tehát — kivéve a singuláris esetet — teljes befejezést nyer avval, ha még megmutatjuk, hogy a

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})} \qquad (C)$$

congruentia olyan congruentiára vezethető vissza, a melyben a Φ-k a 16. §-ban követelt, az irreducibilitásra vonatkozó tulajdonságot mutatják. Ekkor ugyanis a bemutatott módszer végre $r=l+1$-re vezet, a mely esetben a congruentia teljesen elintézettnek tekinthető.

Legyen már most pl. $\Phi^{(s)}$ $(r \leqq s \leqq m-1)$ a $\Phi^{(r)}, \ldots, \Phi^{(m-1)}$ sorozat első olyan formája, a mely az

$$((l-1), \alpha_l, \ldots, \alpha_{s-1}) \pmod{(P^{(k)})}$$

genus-tartományban és ha $s=r$, az $((l-1), \alpha_l) \pmod{(P^{(k)})}$ genus-tartományban *nem* irreducibilis. Legyen tehát e genus-tartományban ama mennyiség irreducibilis tényezőkre való felbontása a következő:

$$(\Phi^{(s)})_{x_l=\alpha_l, \ldots, x_{s-1}=\alpha_{s-1}} = (\Phi_1)_{x_l=\alpha_l, \ldots, x_{s-1}=\alpha_{s-1}} \ldots$$

A jobb oldalon fellépő nevezők az $x_1, \ldots, x_{l-1}, x_{l+1}, \ldots, x_{r-1}$ határozatlanoknak a 0-tól különböző raczionális és egész formái mod. $(P^{(k)})$. Van tehát ugyane határozatlanoknak oly $\Psi^{(r-1)}$ formája, a melyre nézve

$$\Psi^{(r-1)} \Phi^{(s)} \equiv \Phi_1^{(s)} \Phi_2^{(s)} \ldots \pmod{\Phi^{(s-1)}, \ldots, \Phi^{(l)}, (P^{(k)})},$$

a hol $\Phi_1^{(s)}, \Phi_2^{(s)}, \ldots$ ama helyettesítés után az $x_1, \ldots, x_{l-1}, x_{l+1}, \ldots, x_{r-1}$ határozatlanoknak az

$$((l-1), \alpha_l, \ldots, \alpha_{s-1}) \pmod{(P^{(k)})}$$

genus-tartományban irreducibilis raczionális és egész formái.

A (C) minden megoldása kielégíti a következő congruentiát is:

$$\sum_{j=1}^{h} F_j (\Psi^{(r-1)} X_j) + \sum_{i=s-1}^{m-1} \Phi^{(i)} (\Psi^{(r-1)} Y_i) + \Phi_1^{(s)} \ldots Y_s \equiv$$

$$\equiv 0 \pmod{\Phi^{(s-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})}$$

és így minden megfelelő Y_s-re vonatkozólag

$$(\Phi_1^{(s)} \ldots Y_s)_{x_l=\alpha_l,\ x_r=\alpha_r,\ \ldots,\ x_{s-1}=\alpha_{s-1}}$$

osztható $\Psi^{(r-1)}$-gyel. Az első tényezők irreducibilitása folytán ilyen az $(Y_s)_{x_l=\alpha_l,\ x_r=\alpha_r,\ \ldots,\ x_{s-1}=\alpha_{s-1}}$ is. Már bebizonyított tételek szerint (e fej. 9. §-a és a VII. fej. 7. §-a) létezik, tehát az $x_1, \ldots, x_{l-1}$ határozatlanoknak olyan — már teljesen elintézett eljárásokkal meghatározott — $\overline{\Psi}^{(l-1)}$ raczionális és egész formája, hogy

$$\overline{\Psi}^{(l-1)} Y_s \equiv \Psi^{(r-1)} Z_s \ (\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})). \quad (C_1)$$

Így tehát (C) minden megoldása eleget tesz továbbá a következő congruentiának:

$$\Psi^{(r-1)} \Big(\sum_{j=1}^{h} F_j (\overline{\Psi}^{(l-1)} X_j) + \sum_{i=s+1}^{m-1} \Phi^{(i)} (\overline{\Psi}^{(l-1)} Y_i) \Big) + \Phi_1^{(s)} \ldots Z_s \equiv$$
$$\equiv 0 \ (\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(1)}, \Phi^{(l)}, (P^{(k)})),$$

honnan a használt következtetések ismételt alkalmazásával:

$$\sum_{j=1}^{h} F_j (\Psi^{(l-1)} X_j) + \sum_{i=s+1}^{m-1} \Phi^{(i)} (\Psi^{(l-1)} Y_i) + \Phi^{(s)} \ldots (\Psi_1^{(l-1)} Z_s) \equiv$$
$$\equiv 0 \ (\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(1)}, \Phi^{(l)}, (P^{(k)})) \quad (C_2)$$

és (C_1) tekintetbe vételével:

$$\sum_{j=1}^{h} F_j (\Psi^{(l-1)} X_j) + \sum_{i=s+1}^{m-1} \Phi^{(i)} (\Psi^{(l-1)} Y_i) + \Phi^{(s)} (\Psi^{(l-1)} Y_s) \equiv$$
$$\equiv 0 \ (\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(1)}, \Phi^{(l)}, (P^{(k)})). \quad (C_3)$$

A C_2 megoldása a $\Psi^{(l-1)} X_j$, $\Psi^{(l-1)} Y_i$, $\Psi^{(l-1)} Z_s$ «ismeretlenekre vonatkozólag oly congruentiák lánczolatának segítségével történhetik, melyekben az utolsó ismeretlen együtthatója rendre $\Phi_1^{(s)}$, $\Phi_2^{(s)}, \ldots$, hol most a $\Phi_1^{(s)}$, $\Phi_2^{(s)}, \ldots$ formákban is megvan az irreducibilitásra vonatkozó tulajdonság. Ezek a congruentiák azonban már teljesen elintézetteknek tekinthetők, velük együtt pedig kiadódnak a (C_3) megoldásai, ha Y_s-et ugyancsak elintézett eljárásokkal meghatározzuk (C_1)-ből.

A (C_3) megoldásai C minden megoldását magukba foglalják. Hogy fordítva, C_3 valamely megoldása C-t kielégítse,

ahhoz szükséges, hogy a (C_3)-ból kiadódó kifejezés:

$$\sum_{j=1}^{h} F_1(\Psi^{(l-1)} X_j) + \sum_{i=s+1}^{m-1} (\Psi^{(l-1)} Y_i) + \Phi_s \Psi_1^{(l-1)} Y_s \equiv$$

$$\equiv \sum_{h=1}^{s-1} \Phi^{(h)} U_h + \Phi^{(l)} U_1 \pmod{(P^{(k)})}$$

egyszersmind

$$\equiv \Psi^{(l-1)} \left(\sum_{h=r}^{s} \Phi^{(h)} U_h' + \Phi^{(l)} U_1'\right) \pmod{(P^{(k)})}$$

legyen. Ez ismert eljárás által megadja a (C_3) megoldásában még fellépő tetszőleges formák további meghatározását és végül a

$$\Psi^{(l-1)} X_j \equiv \sum_{(i)} G_{ji} W_i$$

congruentiából (C) megoldásait.

*

Mindezekkel azonban problemánk nincs még teljesen elintézve. Mert $\Phi^{(s)}$-nek irreducibilis $\Phi_1^s, \ldots$ tényezőkre való bontását elértük ugyan, de ezeknek nincs meg többé az előbb megállapított alakjuk, a mennyiben x_s legmagasabb hatványainak együtthatója tartalmazhatja nem csak $x_1, \ldots, x_{l-1}$-et, hanem $x_{l+1}, \ldots, x_{s-1}$-et is. Hogy ez beálljon, ahhoz minden esetre szükséges, hogy $r > l+1$ és $s > r$ legyen; minthogy azonban másrészt $l \geqq 1$, azért innen $s \geqq 4$; $s \leqq m-1$ folytán tehát ez csak $m \geqq 5$ esetében állhat be.

Ezek szerint *a homogén lineáris diophantikus egyenlet problémája* — a singuláris esetet a 19. §-ban tárgyaljuk — *az* $[[1], x_1, x_2, x_3]$ *és* $[[1], x_1, x_2, x_3, x_4]$ *tartományokra vonatkozólag — is teljesen el van intézve.*

Hogy most már tárgyalásainkat négynél több határozatlan esetére folytathassuk, a 9. § alapvető tételeit kell megfelelőleg általánosítanunk. Erre az $x_1, \ldots, x_{l-1}, x_{l+1}, \ldots, x_{r-1}, x_s$ határozatlanok homogén lineáris transformatiója szolgáltat

alkalmas eszközt. Mindazonáltal, hogy az így keletkező formarendszer egyáltalában nem oly egyszerű, mint a már keresztülvitt esetekben, a gondolatmenet lényegileg mégis ugyanaz marad. Tekintettel a fölötte bonyolódott részletekre mellőzöm a tárgyalást, annál inkább minthogy az eredmények tényleges alkalmazása több mint négy határozatlan esetében egyelőre úgy sem vehető kilátásba.

A singuláris eset.

19. §. A homogén lineáris diophantikus egyenlet tehát mindig véges számmal levő műveletek segítségével oldható meg, ha ugyanez történik az

$$FX+\Phi^{(m-1)}Y_{m-1}+\cdots+\Phi^{(r)}Y_r+\Phi^{(l)}Y_l\equiv 0 \pmod{(P^{(k)})} \qquad (S)$$

singuláris esetben is, a hol a Φ formák már a 16. §-ban részletezett, az irreducibilitásra vonatkozó tulajdonságot mutatják*. De akkor

$$(FX)_{x_l=\alpha_l,\ x_r=\alpha_r,\ \ldots,\ x_{m-1}=\alpha_{m-1}}\equiv 0 \pmod{(P^{(k)})}$$

és így tehát az eddigi fejtegetések szerint van az $x_1, \ldots, x_{l-1}$ határozatlanoknak a műveletek véges sorával meghatározható olyan $\Psi^{(l-1)}$ formája, hogy *vagy*

$$\Psi^{(l-1)}F\equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})}, \qquad (a)$$

vagy pedig

$$\Psi^{(l-1)}X\equiv 0 \pmod{\Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})}. \qquad (b)$$

Az első esetben azonban a

$$\Psi^{(l-1)}F\equiv G_{m-1}\Phi^{(m-1)}+\cdots+G_r\Phi^{(r)}+G_l\Phi^{(l)} \pmod{(P^{(k)})}$$

előállítás a műveletek véges sorával nyerhető és az adott congruentia a

$$\Phi^{(m-1)}(\Psi^{(l-1)}Y_{m-1}+G_{m-1}X)+\cdots+\Phi^{(r)}(\Psi^{(l-1)}Y_r+G_rX)+$$
$$+\Phi^{(l)}(\Psi^{(l-1)}Y_l+G_lX)\equiv 0 \pmod{(P^{(k)})}$$

* Itt is a szöveg explicite csakis arra az esetre vonatkozik; midőn a határozatlanok száma *négynél* nem nagyobb.

congruentiával együtt meg van oldva. Ennek megoldása azonban a $\Psi^{(l-1)}Y_{m-1}+G_{m-1}X_1,\ldots$ ismeretlenek szerint közvetetlenül nyerhető, mert együtthatói az x_m határozatlant nem tartalmazzák és a tovább fellépő

$$\Psi^{(l-1)}Y_{m-1}+G_{m-1}X\equiv\Sigma H_s^{(1)}U_s \pmod{(P^{(k)})},$$
$$\Psi^{(l-1)}Y_{m-2}+G_{m-2}X\equiv\Sigma H_s^{(2)}U_s \pmod{(P^{(k)})}$$

congruentiák ismét csak alacsonyabb rangú problémákat szolgáltatnak, a melyek már is elintézetteknek tekinthetők. Ezek közül ugyanis mindegyikben csak egy új ismeretlen fordúl elő, a melynek együtthatója már csak az $x_1,\ldots,x_{l-1}$ határozatlanokat tartalmazza.

A második esetben minden esetre a (*b*) congruentiát kell kielégítenünk. Ez azonban X-nek $\Psi^{(l-1)}$ együtthatója miatt ismét már megoldott problémát szolgáltat, azaz belőle minden esetre az X-nek következő szükséges alakja származik:

$$X\equiv\Sigma G_sU_s \pmod{(P^{(k)})};$$

és innen

$$\Psi^{(l-1)}X\equiv\Sigma G_s\Psi^{(l-1)}U_s \pmod{(P^{(k)})},$$

a hol azonban most szükségképen

$$G_s\Psi^{(l-1)}\equiv H_{s,m-1}\Phi^{(m-1)}+\cdots+H_{sr}\Phi^{(r)}+H_{sl}\Phi^{(l)} \pmod{(P^{(k)})}$$

és $G_s\Psi^{(l-1)}$ előállítása ebben az alakban ismét lineáris diophantikus egyenleteknek az $[[1], x_1,\ldots,x_{m-1}]$ tartományban való megoldása révén nyerhető.

Az (S) congruentia tehát, ha ahhoz még a $\Psi^{(l-1)}$ tényezőt csatoljuk, a mi annak megoldásán mitsem változtat, átmegy a

$$\Phi^{(m-1)}(\Psi^{(l-1)}Y_{m-1}+\sum_{(s)}H_{s,m-1}FU_s)+\cdots+$$
$$+\Phi^{(l)}(\Psi^{(l-1)}Y_l+\sum_{(s)}H_{sl}FU_s)\equiv 0 \pmod{(P^{(k)})}$$

congruentiába, a melyből először is a

$$\Psi^{(l-1)} Y_{m-1} + \sum_{(s)} H_{s,m-1} FU_s, \ldots$$

«ismeretlenek» számíthatók ki és azután már elintézetteknek tekinthető alacsonyabb rangú problémák alapján $Y_{l-1}, \ldots, Y_{m-1}$, továbbá az U-knak mindinkább szűkebb meghatározása és végre X is kiadódik.

Ha az (S) congruentia csupán csak két tagból áll, akkor — mint azt már előbb említettük — ez az általános módszer természetesen felesleges és a megoldás elemi úton nyerhető.

KILENCZEDIK FEJEZET.

AZ EGÉSZ ALGEBRAI MENNYISÉGEK*.

Bevezető megállapodások.

1. §. Legyen A valamely tetszés szerinti orthoid tartomány, vagy pedig az [1] tartomány; vizsgálataink kiindulópontja pedig ismét az $[A, x_1, x_2, \ldots, x_m]$ tartomány, azaz az

* Az egész algebrai mennyiségek elméletének alapja első sorban az ideális mennyiségek fogalma, a melyet KUMMER E. E. alkotott meg. («Zur Theorie der complexen Zahlen», Journ. f. r. u. a. Mathematik XXXV. k.) Az ideális mennyiségek értelmezése, habár KUMMER azt csak a körosztás problémájából származó algebrai számoknak aránylag egyszerű, de mégis teljesen jellemző esetében adta, az arithmetika történetének korszakot alkotó fordulópontja. Az evvel megalapított tudásunk azonban csak KRONECKER-nek a «Festschrift»-ben kifejtett módszereivel vált tökéletessé, a mely módszerek lényege új határozatlan mennyiségek associatiójában rejlik. Ezeken épül fel a mi tárgyalásunk is. Hogy ez mennyiben haladja túl a «Festschrift»-et, később, a részleteknél külön lesz kimutatandó. E további kifejtésnek főpontjai a következők: A lineáris diophantikus problémáknak az előbbeniekben előadott teljes megoldása, a mely a fellépő képződmények fogalmi meghatározása helyett azoknak tényleges előállítását adja; az ideális mennyiségeknek, mint az összeadás *és* szorzás közönséges törvényének alávetett mennyiségeknek értelmezése; az ideális mennyiségek valamely «alaprendszerének» ennek alapján történő kész felállítása; KRONECKER eredményeinek kiegészítése azokra a természetes törzsszámokra nézve, a melyekre a «Festschrift» módszerei nem alkalmazhatók; és végre KRONECKER ama tételeinek helyre-

$x_1, \ldots, x_m$, számra nézve m határozatlant tartalmazó és az A tartományból származó orthoid, ill. raczionális és egész formák tartománya, a hol természetesen az x-ek új, az A tartomány értelmezésében fel nem használt határozatlanokat jelentenek. Ebből úgy, mint a megelőző fejezetekben két párhuzamos elmélet fejlődik, — egy algebrai és egy arithmetikai jellemű; és a kettőnek alapvonalai közösen adhatók elő. Ez a körülmény nemcsak megrövidíti az egész tárgyalást, hanem egyszersmind áttekinthetőbbé is teszi.

Midőn végül a két elmélet ismét elválik egymástól, az első feltevés mellett az algebrai függvényeknek az arithmetika szellemében tartott elméletét, jelesen, ha az A tartomány értelmezésében semmiféle határozatlan nem lép be, az elméletnek ama tételeit nyerjük, a melyek geometriai interpretatióra alkalmasak. A második feltevés: $A=[1]$, szolgáltatja a tiszta arithmetika legáltalánosabb fogalomképzését, KRONECKER nagy alkotását, az algebrai mennyiségek arithmetikai elméletét.

Legyen már most $F_0, F_1, \ldots, F_n$ az $[A, x_1, \ldots, x_m]$ tar

igazítása, a melyek bármely genus-tartomány egész mennyiségeinek primideálokra való felbontására vonatkoznak.

Az algebrai számok általános elméletét már sokkal előbb — a DIRICHLET-féle számelméleti előadások második kiadásában és jeles értekezéseinek további sorozatában — habár kevésbbé egyszerű, de annál nagyobb elmeéllel szerkesztett módszerek segítségével DEDEKIND alapította meg. E módszereket később ő és WEBER H. (Theorie der algebraischen Functionen einer Veränderlichen» Journ. f. r. u. a. Mathematik XCII. k.) az idézetben említett térre vitték át. Magától értetődik, hogy e munka az algebrai függvények elméletét a számbeli együtthatókra való tekintet nélkül tárgyalja. Az algebrai mennyiségeknek a szó teljes értelmében vett «arithmetikai» elmélete KRONECKER alkotása.

tomány bárhány tetszés szerinti formája* és

$$F(z)=F_0z^n+F_1z^{n-1}+\cdots+F_n=0$$

valamely az $(A, x_1, \ldots, x_m)$ tartományban irreducibilis egyenlet. Ha az $(A, x_1, \ldots, x_m)$ tartományhoz az $F(z)=0$ egyenlet egyik α gyökét adjungáljuk, bizonyos genus-tartomány származik, a melynek rövid jelölésére Γ szolgáljon. A Γ genus-tartomány az összes

$$g(\alpha)=\frac{G_0+G_1\alpha+\cdots+G_{n-1}\alpha^{n-1}}{H}$$

alakú mennyiségeket tartalmazza, a hol $G_0, G_1, \ldots, G_{n-1}, H$ a $H\neq 0$ föltétel mellett az $[A, x_1, \ldots, x_m]$ tartomány bármely formái lehetnek.

A Γ genus-tartománynak (az összeadás és szorzás révén származó kapcsolatokra vonatkozó) «tulajdonságai» az α mennyiség további interpretatiójától függetlenek. Jelesen, ha az $F(z)=0$ egyenlet Galois-féle tartományát képezzük és ebben a tartományban ennek az egyenletnek gyökei $\alpha_1, \ldots, \alpha_n$, továbbá $\Gamma_1, \ldots, \Gamma_n$ az ezeknek megfelelő conjugált genus-tartományok, akkor minden az α-ra és Γ-ra vonatkozó következtetés helyes marad bármely α_i-re és Γ_i-re nézve is és viszont mindenütt, a hol valamely α_i-ről és Γ_i-ről van szó, α és Γ írható.

A Γ genus-tartomány mennyiségei olyan «az A tartományra vonatkozólag» algebrai (vagy pedig, ha $A=[1]$, absolut algebrai) mennyiségek, a melyeknek rendszáma n, vagy n-nek valamely osztója. Jelesen a Γ tartomány *elsőrendű mennyiségei* $\frac{G_0}{H}$ alakú hányadosok, a melyek «*a Γ tartománynak az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag racionális mennyiségei*».

* Magától értetődik, hogy $m=0$ is lehet, midőn az F-ek az A tartomány mennyiségei.

A $g(\alpha)$ mennyiséggel együtt meg vannak adva egyszersmind a $g(\alpha_1), \ldots, g(\alpha_n)$ mennyiségek is. A $g(\alpha)$ mennyiség *normá*-ját

$$\text{Nm. } g(\alpha) = \prod_{i=1}^{n} g(\alpha_i)$$

értelmezi*, a hol a jobb oldalon, a mely az $\alpha_1, \ldots, \alpha_n$ mennyiségeknek symmetrikus formája, az e formák elméletének megfelelő átszámítás az

$$F_0 z^n + \cdots + F_n = F_0 \prod_{i=1}^{n} (z - \alpha_i)$$

azonosság alapján már megtörténtnek gondolandó.

A Γ genus-tartomány minden mennyiségének normája ugyane tartomány raczionális mennyisége.

Valamely a Γ genus-tartományból származó

$$\sum_{(r)} g_r(\alpha) U_r$$

forma normája (a hol az U_r-ek az $u_1, \ldots, u_m$ határozatlanoknak hatványszorzatai), megfelelő módon a következőképen értelmezendő:

$$\text{Nm.} \sum_{(r)} g_r(\alpha) U_r = \prod_{i=1}^{n} \sum_{(r)} g_r(\alpha_i) U_r ;$$

így tehát valamely a Γ genus-tartományból származó forma normája az u határozatlanoknak olyan formája, a melynek együtthatói a Γ tartomány raczionális mennyiségei.

Teljesség kedvéért itt még megemlítjük, hogy mindig Nm. $(AB) =$ Nm. A Nm. B.

A $\sum_{(r)} g_r(\alpha) U_r$ *forma*, a mely mint legegyszerűbb esetet a $g(\alpha)$ mennyiségeket is magában foglalja, *kielégíti a*

$$\text{Nm.} \left(z - \sum_{(r)} g_r(\alpha) U_r\right) = 0$$

* A norma elnevezés a complex egész számok legegyszerűbb esetének megfelelőleg már GAUSS-nál fordúl elő.

egyenletet. Ennek az egyenletnek együtthatói az u határozatlanok formái és e formák együtthatói ismét a Γ genus-tartomány raczionális mennyiségei.

A $\text{Nm.}\left(z-\sum_{(r)} g_r(\alpha)\, U_r\right)$ forma vagy az $(A, x_1, \ldots, x_m)$ tartományban irreducibilis forma, vagy pedig valamely az $(A, x_1, \ldots, x_m)$ tartományban irreducibilis formának d-dik hatványa, a hol d az n valamelyik osztóját jelenti.

Ha ugyanis

$$\text{Nm.}\left(z-\sum_{(r)} g_r(\alpha)\, U_r\right) = N_1(z)\, N_2(z) \ldots,$$

akkor feltételezhetjük, hogy z legmagasabb hatványának együtthatója az $N_1(z)$, $N_2(z)$, ... formákban az egység. Ekkor pl. az

$$N_1(z) = 0$$

egyenletnek lesz egy

$$z = \sum_{(r)} g_r(\alpha_i)\, U_r$$

alakú gyöke úgy, hogy α_i az

$$N_1\left(\sum_{(r)} g_r(z)\, U_r\right) = 0$$

és $F(z)=0$ egyenleteknek közös gyöke. Minthogy azonban az $F(z)=0$ egyenlet irreducibilis, egyszersmind

$$N_1\left(\sum_{(r)} g_r(\alpha_j)\, U_r\right)=0,$$

azaz $\sum_{(r)} g_r(\alpha_i)\, U_r$ *összes különböző conjugált értékei kielégítik az* $N_1(z)=0$ *egyenletet* és magától értetődik, hogy minden egyes ilyen érték ennek az egyenletnek csak egyszerű gyöke. Így tehát

$$N_1(z) = N_2(z) = \cdots,$$

a miből azután következik, hogy

$$\text{Nm.}\left(z-\sum_{(r)} g_r(\alpha)\, U_r\right) = \left(N_1(z)\right)^{\frac{n}{d}}.$$

Az egész algebrai mennyiségek és formák.

2. §. A Γ genus-tartomány raczionális mennyiségei, azaz a $\frac{G}{H}$ alakú forma-hányadosok kielégítik a

$$Hz - G = 0$$

elsőfokú egyenletet, a melyben a G és H legnagyobb közös osztójának eltávolítása után feltételezhető, hogy $(G, H) \sim 1$. Ha ezen egyszerűsítés után $H \sim 1$, vagy tehát $= 1$, akkor ama raczionális mennyiség *az* $[A, x_1, \ldots, x_m]$ *tartomány formája,* vagy pedig — a mint ezt még másképen is kifejezzük — *a* Γ *genus-tartománynak az* $[A, x_1, \ldots, x_m]$ *tartományra vonatkozólag raczionális és egész mennyisége.* Ha $(H, G) \sim 1$ és H nem ~ 1, akkor magától értetődik, hogy ez nincsen úgy.

Az ily módon a legegyszerűbb esetnek megfelelőleg nyert osztályozási elv közvetetlenül átvihető a Γ genus-tartomány összes mennyiségeire, valamint az ebből a genus-tartományból származó formákra is.

A $g(\alpha)$ mennyiség, valamint a $\sum_{(r)} g_r(\alpha)\, U_r$ forma is — mint láttuk — olyan $N_1(z) = 0$ irreducibilis egyenletet elégít ki, a melynek együtthatói az $[A, x_1, \ldots, x_m, u_1, \ldots]$ tartományból származó formák hányadosai. Ha ebből az egyenletből a nevezőket és azután az együtthatókként szereplő formák legnagyobb közös osztóját is eltávolítjuk, akkor az ismét irreducibilis

$$G_0 z^d + \cdots + G_d = 0$$

egyenlet származik.

Ha ebben az egyenletben $G_0 \sim 1$, *vagy tehát* $G_0 = 1$, *akkor a* $g(\alpha)$ *mennyiséget (a* Γ *genus-tartomány) egész algebrai mennyiségének, ill. a* $\sum_{(r)} g_r(\alpha)\, U_r$ *formát (a* Γ *genus-tartományból származó) egész formának nevezzük. E mellett mindig (tehát a következőkben is) «az* $[A, x_1, \ldots, x_m]$ *tarto-*

mányra vonatkozólag», mint közelebbi meghatározás hozzágondolandó.

Arra, hogy a genus-tartomány valamely mennyiségének, vagy valamely a genus-tartományból származó formának «egész» voltát felismerhessük, a következő tétel szolgál, a mely az épen adott értelmezéssel egyenlő értékű:

A $g(\alpha)$ *mennyiség, ill. a* $\sum_{(r)} g_r(\alpha)\, U_r$ *forma akkor és csak akkor egész, ha olyan*

$$z^d + G_1 z^{d-1} + \cdots + G_d = 0$$

egyenlet gyöke, a melyben $G_1, \ldots, G_d$ *az* $[A, x_1, \ldots, x_m]$, *ill. az* $[A, x_1, \ldots, x_m, u_1, \ldots]$ *tartományba tartozó formák.*

Az egész mennyiségek épen adott értelmezése szerint e feltétel okvetetlenül szükséges. Elegendő voltáról meggyőződünk, ha megjegyezzük, hogy ugyanaz a mennyiség (vagy forma) az irreducibilis

$$N_1(z) = 0$$

egyenletet is okvetetlenül kielégíti. Ha ezt az egyenletet a nevezők eltávolítása után a

$$H_0 z^r + \cdots + H_r = 0$$

alakban írjuk, a hol még feltételezhető, hogy $(H_0, \ldots, H_r) \sim 1$, akkor

$$z^d + G_1 z^{d-1} + \cdots = (H_0 z^r + \cdots + H_r)(K_0 z^s + \cdots + K_s),$$

a hol a H-k az $[A, x_1, \ldots, x_m, u_1, \ldots]$ tartomány formái. Ha már most

$$K_i = \frac{K_i'}{K},$$

akkor, ha

$$(K_0', \ldots, K_s') \sim D,$$
$$K_i' = D K_i''$$

volna, ebből következnék, hogy

$$K(z^d + G_1 z^{d-1} + \cdots) = D(H_0 z^r + \cdots)(K_0'' z^s + \cdots)$$

és, minthogy a zárójelekben álló formák kivétel nélkül primitiv formák, továbbá $K \sim D$ volna, tehát egyszersmind $H_0 K_0'' \sim 1$ és ebből végre $H_0 \sim 1$, a mi bebizonyítandó volt.

Ebből elméletünknek következő alapvető tétele következik:

Két egész algebrai forma összege, különbsége és szorzata ismét egész algebrai forma.

Magától értetődik, hogy e tétel az egész algebrai mennyiségekre is kiterjed, a melyek specziális formáknak tekinthetők. A tétel bebizonyítására feltételezhetjük, hogy mind a két forma ugyanabból a genus-tartományból származik; mert mindig alkothatunk olyan genus-tartományt, a melybe tetszés szerinti véges számmal levő algebrai mennyiségek mind beletartoznak. Ha már most γ', γ'' ama két egész algebrai forma, csak a

$$\prod_{i=1}^{n} \prod_{j=1}^{n} (z - \gamma_i' \mp \gamma_j'') = 0, \quad \prod_{i=1}^{n} \prod_{j=1}^{n} (z - \gamma_i' \gamma_j'') = 0$$

egyenleteket kell megalkotnunk, a melyekről közvetetlenül felismerhető, hogy azokban z legmagasabb hatványának együtthatója 1, míg többi együtthatóik az x és u határozatlanoknak az A tartományból származó formái. Az utóbbiak ugyanis egyrészt a γ_i'-knek, másrészt a γ_j''-knek symmetrikus formái; tehát mint az x-ek, u-k, γ_i'-k és γ_j''-k elemi symmetrikus formáinak az A-ból származó formái írhatók, a hol a feltevés szerint a γ_i'-k és γ_j''-k elemi symmetrikus formáinak az $[A, x_1, \ldots, x_m, u_1, \ldots]$ tartományhoz tartozó formáknak kell lenniök.

3. §. Az épen bebizonyított tétel értelmében minden olyan forma, a melynek együtthatói a Γ genus-tartomány egész mennyiségei, egész algebrai forma. De ennek megfordítottja is érvényes:

Minden a Γ genus-tartományból származó egész al-

gebrai formának együtthatói a Γ tartományba tartozó egész mennyiségek.

Ha ezt bebizonyítottuk, akkor teljes összhangzásban az ilyfajta melléknévi jelzők eddigi használatával az «egész algebrai formák», mint oly formák értelmezhetők, a melyeknek együtthatói egész algebrai mennyiségek.

Hogy a tételt bebizonyítsuk, írjuk az eredeti értelmezés szerint egésznek feltételezett Φ formát az egyik határozatlan hatványai szerint rendezve:

$$\Phi = \Phi_0 + \Phi_1 u_1 + \Phi_2 u_1^2 + \cdots$$

E forma kielégíti a

$$\text{Nm.}(z - \Phi) = 0$$

egyenletet, a melyben z^n-nek együtthatója 1, a többi együttható pedig a feltevés szerint az $[A, x_1, \ldots, x_m, u_1, \ldots]$ tartomány formája. Az u_1-et nem tartalmazó tagok ép ily tulajdonságúak és közvetetlenül szolgáltatják a

$$\text{Nm.}(z - \Phi_0) = 0$$

egyenlet bal oldalát, a melyet a Φ_0 mennyiség kielégít. Így tehát Φ_0 és egyszersmind

$$\Phi - \Phi_0 = u_1(\Phi_1 + \Phi_2 u_1 + \cdots)$$

is egész algebrai forma. Ez kielégíti a

$$\text{Nm.}(z - u_1(\Phi_1 + \Phi_2 u_1 + \cdots)) = 0$$

egyenletet, a mely részletesen írva legyen

$$z^n + W_1 z^{n-1} + \cdots + W_n = 0,$$

a hol közvetetlenül látható, hogy W_r az $[A, x_1, \ldots, x_m, u_1, \ldots)$ tartománynak u_1^r-vel osztható formája. Így tehát

$$\Phi_1 + \Phi_2 u_1 + \cdots$$

kielégíti a

$$t^n + \frac{W_1}{u_1} t^{n-1} + \frac{W_2}{u_1^2} t^{n-2} + \cdots + \frac{W_n}{u_1^n} = 0$$

egyenletet, és e szérint egész mennyiség. E következtetések ismétlése rendre mutatja, hogy a $\Phi_1, \Phi_2, \ldots$ formák is egész algebrai formák, a melyek azonban, ép úgy mint Φ_0, nem tartalmazzák többé az u_1 határozatlant. A tétel tehát érvényes m határozatlan formáira vonatkozólag, ha érvényes volt $m-1$ határozatlan formáira nézve. Minthogy azonban az alkalmazott következtetés egy határozatlan formái esetében az együtthatókat egyenesen mint a Γ egész algebrai mennyiségeit tünteti fel, tételünk valóban általánosan érvényes.

A Γ genus-tartomány egész mennyiségei valódi holoid tartományt alkotnak, a melyet $[\Gamma]$-val jelölünk. E tartomány ugyanis megfelel az I. fej. 4. §-a definicziójának és nem tartalmazza Γ-nak oly elsőrendű mennyiségeit, a melyek nem egyszersmind egész mennyiségek is. Kivételes csak az a triviális eset, midőn A orthoid tartomány és x határozatlanok nem lépnek fel. (L. erre vonatkozólag a 4. § végét.)

A Γ genus-tartományból származó egész algebrai formák tehát a $[\Gamma]$ tartományból származó formák; összességük valódi holoid tartományt alkot, a melyet $[\Gamma]_w$-vel jelölünk.

Primitiv egész algebrai formák.

4. §. Az épen értelmezett $[\Gamma]$ valódi holoid tartomány csak a legegyszerűbb esetekben teljes tartomány (l. a 7. §-hoz tartozó megjegyzést). Ha azonban a legnagyobb közös osztó fogalma elesik, a primitiv formákra vonatkozó, a III. fej. 9. §-ában adott értelmezés sem tartható fenn. Helyébe most a következő értelmezés lép*:

* Kronecker, Festschrift, 15. §.

Valamely a $[\Gamma]$ *tartományból származó* Φ *forma primitiv forma (vagy egységforma), ha Nm.* Φ *az* $u_1, \ldots$ *határozatlanoknak primitiv formája.* E mellett magától értetődik, — a mit egyszer mindenkorra megemlítünk, — hogy Nm. Φ az $[A, x_1, \ldots, x_m]$ tartományból származó formának tekintendő.

Magától értetődik, hogy a Nm. Φ formára nézve, a melynek együtthatói az $[A, x_1, \ldots, x_m]$ teljes holoid tartományba tartoznak, az előbbi értelmezés marad érvényben.

Ez az értelmezés, mihelyt $[\Gamma]$ teljes holoid tartomány, megegyezik az előbbivel. Ebben az esetben Nm. Φ akkor és csak akkor primitiv forma, ha ugyanilyenek a $\Phi_1, \Phi_2, \ldots, \Phi_n$ tényezői is. Ekkor azonban $\delta_1, \ldots, \delta_n$ (a $\Phi_1, \ldots, \Phi_n$ formák együtthatóinak legnagyobb közös osztói) is conjugált mennyiségek. Abból, hogy $\delta_1 \sim 1$ vagy $\delta_1 \varepsilon_1 = 1$, következik, hogy $\delta_2 \varepsilon_2 = 1$ és $\delta_2 \sim 1$ s í. t. A δ mennyiségek tehát vagy mindannyian æquivalensek 1-gyel, vagy pedig egyikük sem ~ 1. Másrészt azonban a Nm. Φ együtthatóinak legnagyobb közös osztója egyenesen $\sim \delta_1 \delta_2 \ldots \delta_n$ és így az első esetben ~ 1, a másodikban pedig nem ~ 1; mert abból, hogy $\delta_1 \ldots \delta_n \sim 1$, minthogy $\delta_2 \ldots \delta_n$ egész mennyiség és a Γ_1 tartomány mennyisége is, az következnék, hogy $\delta_1 \sim 1$.

A primitiv forma ily módon bővített értelmezésére nézve — mint közvetetlenül belátható — érvényes a következő alaptétel:

Primitiv formák szorzata ismét primitiv forma.

Itt — mint az magától értetődik — mindig a $[\Gamma]$ tartományból származó formák értendők. Fontos még a következő tétel is*:

* Kronecker, Festschrift, 15. §.

Ha Φ *az* $u_1, u_2, \ldots$ *határozatlanoknak primitiv egész algebrai formája,* Ψ *valamely tetszés szerinti egész algebrai forma, továbbá* X *olyan egész algebrai forma, a mely az* u *határozatlanokat nem tartalmazza, akkor* $\Phi\Psi$ *csak akkor osztható* X*-szel, ha már* Ψ *is osztható* X*-szel.*

Abból a feltevésből, hogy

$$\Phi\Psi = XH,$$

a hol H egész algebrai forma, következik, hogy

$$\Phi(Xz - \Psi) = X(\Phi z - H)$$

és evvel együtt, hogy

$$\text{Nm.}\,\Phi\ \text{Nm.}\,(Xz - \Psi) = \text{Nm.}\,X\ \text{Nm.}\,(\Phi z - H).$$

Ekkor azonban, minthogy Nm. Φ primitiv forma, szükséges, hogy Nm. $(Xz - \Psi)$ osztható legyen Nm. X-szel. Tehát

$$\text{Nm.}\left(z - \frac{\Psi}{X}\right)$$

olyan forma, a melynek együtthatói az $[\mathrm{A}, x_1, \ldots, x_m]$ tartományba tartoznak és z^n-nek együtthatója benne 1.

Minthogy Φ csak az $u_1, u_2, \ldots$ határozatlanokat tartalmazza, $\frac{H}{\Phi}$ okvetetlenül a Ψ-ben előfordúló további $v_1, \ldots$ határozatlanoknak formája; egyelőre azonban abban az értelemben, hogy az együtthatókban még az u-kat tartalmazó Φ mint nevező szerepelhet. Minthogy azonban ugyanarra a formára kell jutnunk, ha $\frac{\Psi}{X}$-et a közönséges osztási eljárás segítségével állítjuk elő, világos, hogy a valóban fellépő nevezők sem tartalmazhatják az u határozatlanokat. Tehát $\frac{\Psi}{X} = \frac{H}{\Phi}$ az u *és* v határozatlanoknak algebrai formája és, minthogy végre a

$$\text{Nm.}\left(z - \frac{\Psi}{X}\right) = 0$$

egyenletet is kielégíti, az ezen egyenlet bal oldaláról megállapított tulajdonságok szerint egyszersmind *egész* algebrai forma, a m. b. v.

Az a két eset, midőn A orthoid tartomány, vagy pedig az [1] tartományt jelenti, eddig teljesen egyenlő tárgyalást engedett meg. Hogy akkor, midőn e két eset szétválasztása szükségesnek mutatkozik, rövidebb kifejezésmóddal rendelkezzünk, azokat a mennyiségeket és formákat, a melyeknek értelmezése valamely orthoid A tartományból indul ki, *relativ egész* (A-ra vonatkozólag egész) *mennyiségeknek és formáknak* nevezzük és evvel ellentétben, ha A=[1], *absolut egész mennyiségekről és formákról* beszélünk.

Magától értetődik, hogy akkor, midőn A orthoid tartomány, csak avval az esettel kell foglalkoznunk, midőn az $x_1, \ldots, x_m$ határozatlanok valóban fellépnek. Ha $m=0$, akkor az A-ból származó genus-tartomány minden mennyisége egésznek nevezendő és így az egész mennyiségek elmélete elveszti tartalmát.

5. §. Legyenek

$$\alpha_0, \alpha_1, \alpha_2, \ldots$$

a $[\Gamma]$ tartomány bármilyen mennyiségei,

$$U_{k_0}, U_{k_1}, U_{k_2}, \ldots$$

az $u_1, u_2, \ldots$ határozatlanoknak bármilyen *különböző* hatványszorzatai úgy, hogy tehát $\sum_{(r)} \alpha_r U_r$ a $[\Gamma]$ tartományból származó egész algebrai forma és ennek jelölésére szolgáljon röviden az α_u jel. Nm. α_u ekkor az u határozatlanoknak az $[A, x_1, \ldots, x_m]$ tartományból származó formája. E felfogásban Nm. α_u együtthatóinak legnagyobb közös osztója az $[A, x_1, \ldots, x_m]$ tartomány mennyisége és, ha ezt a mennyiséget D-vel jelöljük, akkor $\frac{\text{Nm. } \alpha_u}{D}$ az $[A, x_1, \ldots, x_m]$ tartományból származó primitiv forma, a melyet, mint az α_u-ból teljesen meghatározott módon előállítható formát az «α_u *formájának*» nevezünk* és

* KRONECKER, Festschrift, 14. §.

$$\text{Fm.}\,\alpha_u = \frac{\text{Nm.}\,\alpha_u}{D}$$

-vel jelölünk.

A $\text{Nm.}\,\alpha_u$-nak ilyképen keletkező $\text{Nm.}\,\alpha_u = D\ \text{Fm.}\,\alpha_u$ előállításából ered az a nevezetes és az algebrai mennyiségek KRONECKER-féle elméletében alapvető tétel, hogy *csakis* $\text{Fm.}\,\alpha_u$ *függ az U hatványszorzatok választásától, míg D az összes az α együtthatókból bármily módon felépülő formákra nézve az aequivalentia értelmében változatlan (invariáns)*, azaz olyan, hogy azt az $(\alpha_0, \alpha_1, \ldots)$ mennyiség-complexus teljesen meghatározza.

Hogy e tételt bebizonyítsuk, legyenek

$$\beta_0, \beta_1, \beta_2, \ldots$$

az α együtthatók bármely tetszés szerint megváltoztatott sorrendben, továbbá

$$V_{l_0}, V_{l_1}, V_{l_2}, \ldots$$

a $v_1, v_2, \ldots$ határozatlanoknak bármilyen, ismét különböző hatványszorzatai, a hol a v-k részben vagy egészben megegyezhetnek az előbb használt u-kkal, vagy pedig ezektől teljesen különbözők is lehetnek. E mennyiségekből alkossuk a

$$\beta_v = \sum_{(s)} \beta_s V_s$$

formát és most, ha ismét

$$\text{Nm.}\,\beta_v = D'\ \text{Fm.}\,\beta_v,$$

ki kell mutatnunk, hogy $D \sim D'$.

A norma értelmezése szerint

$$\text{Nm.}\,\beta_v = \prod_{i=1}^{n} \beta_v^{(i)};$$

ha már most minden egyes $\beta_v^{(i)}$ forma együtthatói közül kiválasztunk egy-egy $\beta_{\mu_i}^{(i)}$ együtthatót és a

$$\pi_\mu = \beta_{\mu_1}^{(1)} \beta_{\mu_2}^{(2)} \ldots \beta_{\mu_n}^{(n)}$$

szorzatot alkotjuk, hol a $\mu_1, \mu_2, \ldots, \mu_n$ indexek egymástól teljesen függetlenül állapíthatók meg, akkor KRONECKER alaptétele szerint (III. fej. 7. §) minden egyes π_μ mennyiség olyan

$$\pi_\mu^\nu + A_1^{(\mu)} \pi_\mu^{\nu-1} + \cdots + A_\nu^{(\mu)} = 0$$

azonosságot elégít ki, a melyben $A_k^{(\mu)}$ a Nm. β_v-ben előfordúló együtthatóknak k-ad dimensiójú raczionális és egész homogén formája. Magától értetődik, hogy Nm. β_v itt úgy tekintendő, mint a v határozatlanoknak az $[A, x_1, \ldots, x_m]$ tartományból származó formája. Amaz együtthatóknak legnagyobb közös osztóját fent D'-vel jelöltük s így tehát $A_k^{(\mu)}$ szükségképen osztható D'^k-val. Az előbbi azonosság azonban a

$$\left(\frac{\pi_\mu}{D'}\right)^\nu + \frac{A_1^{(\mu)}}{D'}\left(\frac{\pi_\mu}{D'}\right)^{\nu-1} + \cdots + \frac{A_\nu^{(\mu)}}{D'^\nu} = 0$$

alakban is írható, a melyből kitünik, hogy $\frac{\pi_u}{D'}$ *egész mennyiség.*

Ámde Nm. α_u-ban, mint az u határozatlanoknak formájában minden egyes együttható π_μ-alakú mennyiségek összege és így szintén osztható D'-vel úgy, hogy D' a D-nek, a Nm. α_u együtthatói legnagyobb közös osztójának osztója. Pontosan ugyanazok a következtetések alkalmazhatók azonban akkor is, ha az α_u és β_v formák szerepét felcseréljük; D tehát a D'-nek is osztója és így

$$D \sim D'$$

a m. b. v.*

6. §. Az α_u formából előállított Fm. α_u primitiv formá-

* A több oldalról fölsorolt nehézségek, a melyekbe a KRONECKER-féle Festschrift 14. §-ának megértése ütközik, egész egyszerűen elesnek az itt idézett alaptétel előzetes tárgyalása és ennek most önállóan fogalmazott folyománya alapján. (L. a III. fej. 4. és 5. §-ához csatolt megjegyzéseket.)

nak még további fontos tulajdonságai vannak, a melyek a $[\Gamma]$ tartományban való oszthatóság elméletének előkészítésére itt kifejtendők. E tulajdonságokat a következő két tétel fejezi ki:

I. *Ha α_u és β_v az előbb kifejtett értelemben ugyanabból az együttható-sorozatból felépült formák, akkor $\beta_v \operatorname{Fm}.\alpha_\mu$ a $[\Gamma]_w$ tartományban osztható α_u-val, azaz van olyan a $[\Gamma]$ tartományból származó γ_w forma, a melyre nézve*

$$\beta_v \operatorname{Fm}.\alpha_u = \alpha_u \gamma_w.$$

A γ_w ugyanis, mint egész algebrai forma egyszerűen meghatározható azon megjegyzés alapján, hogy a

$$\frac{\beta_v \operatorname{Fm}.\alpha_u}{\alpha_u} = \frac{1}{D}\beta_v \frac{\operatorname{Nm}.\alpha_u}{\alpha_u}$$

formának valóban egész formának kell lennie. E hányados részletesen írva a következő:

$$\frac{1}{D}\sum_{(s)} \beta_s^{(1)} V_s \prod_{i=2}^{n} \alpha_r^{(i)} U_r ;$$

ebben pedig minden egyes $V_s U_r$ hatványszorzat együtthatója π_μ-alakú mennyiségek összege (hol π_μ-nek értelme az 5. §-ban állapíttatott meg) és így tehát valóban osztható D-vel.

II. *Ha Φ a $[\Gamma]_w$ tartomány tetszés szerinti, E pedig e tartomány primitiv formája, továbbá ΦE osztható α_u-val, akkor $\Phi \operatorname{Fm}.\alpha_u$ is osztható α_u-val.*

E tétel feltevését kifejezi bizonyos

$$\Phi E = \alpha_u \Psi$$

azonosság, a hol Ψ a $[\Gamma]_w$ tartomány formája.

Ha β_v ismét valamely az α_u együtthatóinak sorozatából felépült forma, hol azonban a v-k új, az adott formákban fellépő határozatlanoktól különböző határozatlanok legyenek, akkor I. szerint

$$\alpha_u \operatorname{Fm}.\beta_v = \beta_v \gamma_w ;$$

tehát

$$\Phi E \text{ Fm. } \beta_v = \Psi\beta_v \gamma_w$$

és, minthogy β_v oly forma, a mely az E primitiv formában fellépő határozatlanok egyikét sem tartalmazza, a 4. §-ban bebizonyított tétel szerint már Φ Fm. β_v is osztható β_v-vel, azaz

$$\Phi \text{ Fm. } \beta_v = \beta_v \gamma'_w .$$

Ha már most $\alpha_{u'}$ az a forma, a mely α_u-ból úgy származik, hogy az $u_1, u_2, \ldots$ határozatlanok helyébe az *új* $u'_1, u'_2, \ldots$ határozatlanokat teszszük, akkor ismét I. szerint

$$\beta_v \text{ Fm. } \alpha_{u'} = \alpha_{u'} \gamma''_w ;$$

tehát Φ Fm. β_v Fm. $\alpha_{u'}$ osztható $\alpha_{u'}$-val, vagy végre, minthogy a Fm. β_v forma a u' határozatlanok egyikét sem tartalmazza, ismét a 4. § szerint már Φ Fm. $\alpha_{u'}$ osztható $\alpha_{u'}$-val. Ez azonban máris az előbb kimondott tétel, csakhogy az $u_1, u_2 \ldots$ határozatlanok helyett a $u'_1, u'_2, \ldots$ jelek állanak.

Az ideális mennyiségek associatiója.

7. §. Az ebben a fejezetben értelmezett $[\Gamma]$ és $[\Gamma]_w$ valódi holoid tartományok általánosságban, azaz igen speciális esetek kivételével nem teljesek*. E körülmény alak-

* Ha pl. Γ az (1) tartományból az $x^2+5=0$ egyenlet egyik gyökének adjunctiója révén származó genus-tartományt jelenti, akkor e tartomány mennyiségei az $r+s\sqrt{-5}$ mennyiségek, hol r és s az (1)-be tartozó számok. Hogy $r+s\sqrt{-5}$ absolut egész mennyiség lehessen, ahhoz szükséges, hogy $r-s\sqrt{-5}$ is, tehát továbbá $2r$ és $2s\sqrt{-5}$, valamint $20s^2=5\,(2s)^2$ és végre $2s$ is egész legyen, azaz amaz $r+s\sqrt{-5}$ mennyiségnek $\frac{a+b\sqrt{-5}}{2}$ alakúnak kell lennie, hol a és b az [1] tartományba tartozó számok. Ekkor azonban ismét szükséges, hogy $\frac{a^2+5b^2}{4}$ és egyszersmind $\frac{a^2+b^2}{4}$ is egész számok legyenek; ez pedig csak akkor van úgy, ha a és b páros számok. Példánkban tehát a $[\Gamma]$ tartomány az a tartomány, a melyet az I. fej. 8. §-ában $[\sqrt{-5}]$-tel jelöltünk és a melyről kimutattuk ott, hogy *nem* teljes tartomány.

jában és tartalmában egyaránt igen fontos kérdéstételre vezet, a melyet már a III. fej. 13. §-ában érintettünk. *A* $[\Gamma]$ *tartomány oly módon bővítendő teljes holoid tartománynyá, hogy az alkotandó új tartományban a* $[\Gamma]$ *összes mennyiségeinek nem csupán csak az összeadás és szorzás révén nyert kapcsolatokra vonatkozó tulajdonságai, hanem az oszthatóságra vonatkozó tulajdonságai is megmaradjanak.* Ennek pontosabb kifejezése a következő: Ha α, β, γ a $[\Gamma]$ tartomány bármely mennyiségei, akkor követeljük, hogy az új bővített tartomány tartalmazzon olyan mennyiségeket, a melyeknek jelölésére az α, β, γ jelképeket úgy használhassuk, hogy az $\alpha+\beta=\gamma$, vagy $\alpha\beta=\gamma$ kapcsolatok mind a két tartományban mindig egyidőben legyenek érvényesek és ép úgy mindig mind a két tartományban egyidőben legyen α osztható, vagy nem osztható β-val.

Magától értetődik, hogy e feltételek mellett a bővített tartománynak is valódi holoid tartománynak kell lennie; pedig a $[\Gamma]$ tartomány ilyen bővítésének eddig közelebbről megvizsgált esetei, a $[\Gamma]$ mellérendelt orthoid tartománya, (Γ), valamint az ebből származó genus-tartományok e követelést *nem* elégítik ki.

A $\frac{\gamma_u}{\varepsilon_v}$ *hányadosok összessége, a hol* γ_u *a* $[\Gamma]_w$ *tartomány tetszés szerinti formáját és* ε_v *ugyanennek tetszés szerinti primitiv (egység-) formáját jelenti, a legegyszerűbb módon szolgáltat olyan tartományt, a mely az épen felállított követeléseket minden tekintetben kielégíti.* E mellett — a mi természetszerű ugyan, de nem magától értetődő — ebben a tartományban az összeadást és szorzást a következő módon értelmezzük:

$$\frac{\gamma'_{u'}}{\varepsilon'_{v'}} + \frac{\gamma''_{u''}}{\varepsilon''_{v''}} = \frac{\gamma'_{u'}\,\varepsilon''_{v''} + \gamma''_{u''}\,\varepsilon'_{v'}}{\varepsilon'_{v'}\,\varepsilon''_{v''}},$$

$$\frac{\gamma'_{u'}}{\varepsilon'_{v'}}\,\frac{\gamma''_{u''}}{\varepsilon''_{v''}} = \frac{\gamma'_{u'}\,\gamma''_{u''}}{\varepsilon'_{v'}\,\varepsilon''_{v''}};$$

úgy, hogy e műveleteket itt ugyanazon törvények szerint hajtjuk végre, a melyek a $([\Gamma]_w)$ orthoid tartományban érvényesek.

Most ki kell mutatnunk, hogy az így értelmezett tartományban valóban megvannak a felállított követeléseknek megfelelő tulajdonságok. E vizsgálatoknál, hogy rövidebb kifejezésre tegyünk szert, e tartományt [𝔊]-vel jelöljük. E tartomány értelmezése szerint mennyiségei az összes tulajdonságokat mutatják, a melyeket az elemi algebra szabályai szerint a $\frac{\gamma_u}{\varepsilon_v}$ hányadosokról kimutathatunk. Minthogy pedig primitiv formák szorzata ismét primitiv forma, azért e mennyiségek okvetetlenül holoid tartományt alkotnak. A [𝔊] tartomány továbbá valódi holoid tartomány is, mert pl. a $2x=1$ egyenletnek nincsen benne megoldása. Az ellenkező esetben valamely $2\gamma_u=\varepsilon_v$ kapcsolatnak kellene fennállania; ez pedig lehetetlen, mert különben az ε_v primitiv forma normájának oszthatónak kellene lennie 2-vel, tehát nem volna primitiv forma.

A [𝔊] *tartomány egységei a* $\frac{\varepsilon'_u}{\varepsilon_v}$ *alakú mennyiségek, a hol a* ε'_u *számláló is primitiv forma.* Minthogy $\frac{\varepsilon_v}{\varepsilon'_u}$ is a [𝔊] tartomány mennyisége, az így értelmezett mennyiségek okvetetlenül egységek; de csakis ezek a mennyiségek az egységek, mert arra, hogy $\frac{\gamma_u}{\varepsilon_v}$ egység lehessen, oly második $\frac{\gamma'_{u'}}{\varepsilon'_{v'}}$ mennyiség létezése szükséges, a melyre nézve

$$\gamma_u \gamma'_{u'} = \varepsilon_v \varepsilon_{v'}.$$

Ebből azonban következik, hogy $\mathrm{Nm}.\gamma_u \mathrm{Nm}.\gamma'_{u'}$, tehát $\mathrm{Nm}.\gamma_u$ és végre γ_u is primitiv forma.

Hogy a [𝔊] *tartomány teljes holoid tartomány,* azt egyszerűen úgy mutatjuk ki, hogy e tartomány két tetszés szerinti mennyiségének, $\frac{\alpha'_{u'}}{\varepsilon'_{v'}}$ és $\frac{\alpha''_{u''}}{\varepsilon''_{v''}}$-nek megfelelőleg valóban

alkotjuk a [𝔊] tartomány oly mennyiségét, a mely az I. fej. 6. §-a értelmében ama két mennyiség legnagyobb közös osztója.

Legyenek $\alpha'_1, \alpha'_2, \ldots$ az $\alpha'_{u'}$ forma és ép úgy $\alpha''_1, \alpha''_2, \ldots$ a $\alpha''_{u''}$ forma együtthatói; γ_w pedig jelöljön valamely oly formát, a mely $\alpha'_{u'}$ és $\alpha''_{u''}$ együtthatóiból épült fel úgy, hogy ezek az együtthatók mindannyian valóban fel is használtattak, azaz legyen

$$\gamma_w = \sum_{(r)} \alpha'_r W'_{k_r} + \sum_{(s)} \alpha''_s W''_{l_s},$$

a hol a W'-k és W''-k az $u_1, u_2, \ldots$ határozatlanoknak kivétel nélkül különböző hatványszorzatai. Akkor a legnagyobb közös osztó eredeti jelölését használva,

$$\left(\frac{\alpha'_{u'}}{\varepsilon'_{v'}}, \frac{\alpha''_{u''}}{\varepsilon''_{v''}}\right) \sim \gamma_w,$$

a hol magától értetődik, hogy γ_w helyébe minden avval æquivalens $\gamma_w \frac{\varepsilon_{w'}}{\varepsilon_{w''}}$ mennyiség is tehető *.

Ha már most az $\alpha'_{u'}$ és $\alpha''_{u''}$ formák együtthatóiból a t', t'' *új* határozatlanok segítségével a

$$\sum_{(r)} \alpha'_r t'_r + \sum_{(s)} \alpha''_s t''_s$$

lineáris formát alkotjuk, akkor a 6. § I. tétele szerint

$$\left(\sum_{(r)} \alpha'_r t'_r + \sum_{(s)} \alpha''_s t''_s\right) \mathrm{Fm}.\, \gamma_w = \gamma_w \gamma'_{w'},$$

hol $\gamma'_{w'}$ ismét a $[\Gamma]_w$ tartomány valamely formáját jelenti. Minthogy a t-k új határozatlanok, ennek az azonosságnak jobb és bal oldalán a t-knek lineáris formái állanak és a t-k együtthatóinak összehasonlítása révén minden egyes α-ra nézve egy-egy

$$\alpha\, \mathrm{Fm}.\, \gamma_w = \gamma_w \gamma''_{w''}$$

* Hogy az $\sim$ jel értelme meg ne változzék, e mellett még megjegyzendő, hogy a zárójelben álló mennyiségek még akkor sem tekintendők formáknak, ha pl. $\varepsilon'_{v'}=1$; hanem azok a [𝔊] tartományhoz tartozó mennyiségek egységes jelei.

alakú azonosságot nyerünk, a mely egyenesen kifejezése annak a ténynek, hogy α a [G] tartományban osztható γ_w-vel, mert $\frac{\gamma''_w}{\text{Fm. } \gamma_w}$ a [G] tartomány mennyisége. Ugyanez áll azután $\alpha'_{u'}$-ról és $\alpha''_{u''}$-ról is és végre az azokkal æquivalens $\frac{\alpha'_{u'}}{\varepsilon'_{v'}}$ és $\frac{\alpha''_{u''}}{\varepsilon''_{v''}}$ mennyiségekről; azaz γ_w okvetetlenül közös osztója e mennyiségeknek.

Végül γ_w a keresett legnagyobb közös osztó, ha $\alpha'_{u'}$ és $\alpha''_{u''}$ minden osztója csakugyan γ_w-nek is osztója*. Hogy ezt bebizonyíthassuk, először is megjegyezzük, hogy az épen alkalmazott következtetési módot ismételve, a 6. § szerint a

$$(\sum_{(r)} \alpha'_r t'_r) \text{ Fm. } \alpha'_{u'} = \alpha'_{u'} \beta_v$$

azonosság is érvényes, a melyből teljesen úgy mint előbb következik, hogy minden egyes α' együttható osztható $\alpha'_{u'}$-val és így $\alpha'_{u'}$ minden osztójával is. A α' és α'' együtthatók tehát $\alpha'_{u'}$ és $\alpha''_{u''}$ minden közös osztójával oszthatók és ugyanez áll a [G] tartományban a γ_w mennyiségről is. Evvel nemcsak azt bizonyítottuk be, hogy a [G] tartomány teljes tartomány, hanem egyszersmind találtunk olyan eljárást, a melynek segítségével e tartomány két mennyiségének legnagyobb közös osztója kész alakban előállítható**.

8. §. A [G] tartomány mennyiségei vagy olyanok, hogy

* Itt rövidség kedvéért csak a számlálóban álló formákat írtuk az azokkal æquivalens hányadosok helyett és ha csak el nem felejtjük, hogy itt a [G] tartományban való oszthatóságról van szó, magától értetődik, hogy ez a körülmény a kimondott tények helyességén vagy általánosságán mit sem változtat.

** Még csak az szorúl talán némi megokolásra, hogy α a β-val (α és β alatt a [Γ] mennyiségeit értve) a [G]-ben is csak akkor osztható, ha ez már [Γ]-ban is úgy van. Ha α a β-val osztható [G]-ben, akkor α Fm. β osztható β-val $[\Gamma]_w$-ben, de Fm. β=1, és így α osztható β-val $[\Gamma]_w$-ben, tehát már [Γ]-ban is.

már a $[\Gamma]$ tartományba is tartoznak, vagy pedig újak, a $[\Gamma]$ tartományhoz *associált* mennyiségek, ha *associatiónak* az eredeti tartomány oly bővítését nevezzük, a mely a most felállított feltételeknek megfelel*. (Ettől eltérőleg az előbbeniekben az adjunctio valamely adott holoid tartománynak oly bővítése volt, a melynél szintén az eredeti mennyiségeknek az összeadás és szorzás révén előálló kapcsolataira vonatkozó szabályok változatlanok maradtak, ezentúl pedig az eredeti tartományban meg nem oldható egyenletek egy sorozata vált megoldhatóvá.)

Az oly mennyiséget, a mely a $[\mathfrak{G}]$ tartományba tartozik, *a* $[\Gamma]$ *tartomány ideális mennyiségének* nevezzük. Ez nem egészen pontos ugyan, de kényelmes kifejezésmód, a milyennel a mathematika más ágaiban is találkozunk. (Így beszélünk pl. az egyenes képzetes pontjairól stb.) A $[\Gamma]$ tartománynak a szó bővebb értelmében vett ideális mennyisége olyan mennyiség is lehet, a mely «valóban» a $[\Gamma]$ tartományba tartozik (a $[\Gamma]$ tartomány valódi mennyisége); ha nem ez az eset forog fenn, akkor a szó szűkebb értelmében vett ideális mennyiséggel van dolgunk.

A $[\Gamma]$ tartománynak olyan ideális mennyiségét, a mely

* Hogy az itt associáltaknak nevezett mennyiségek a szó teljes értelmében vett «mennyiségek», a melyek megengedik úgy az összeadás, mint a szorzás műveletét és nem egyedül az utóbbi műveletet (mint Dedekind-nek az ideálokról szóló elméletében és Kronecker tárgyalásában is az erre a czélra bevezetett mennyiségek), azt nem csupán formális haladásnak tekintem az osztó fogalmának fentartására törekvő mathematikai fogalomalkotásban. (L. erre vonatkozólag a 24. §-hoz csatolt megjegyzést.) Evvel egyszersmind meg van vonva az éles határ «osztók» és «osztórendszerek» közt.

Az algebrai számok elméletének speciális esetében már Weber H. «Lehrbuch der Algebra» cz. könyvében (II. köt. 154. §.) használ ilyen mennyiségeket, a melyeket *egész functionáloknak* nevez.

csupán csak az æquivalentia-meghatározás értelmében van megadva, DEDEKIND szerint *ideálnak* nevezzük. Itt figyelembe veendő, hogy az ideál értelmezése már magában DEDEKIND elméletében is bizonyos változáson megy át. Eredetileg ebben az elméletben az «ideál» a $[\Gamma]$ tartomány mennyiségeinek minden olyan sokaságát jelenti, a mely a következő tulajdonságú: Ha α és β a sokaság két mennyisége és γ a $[\Gamma]$ tartomány valamely tetszés szerinti mennyisége, akkor $\alpha+\beta$ és $\alpha\gamma$ is a sokasághoz tartoznak. Ha már most $(\alpha_1, \alpha_2, \ldots)$ és $(\beta_1, \beta_2, \ldots)$ két ilyen sokaság vagy ideál, akkor az összes $\alpha_i \beta_j$ alakú szorzatokból és az ilyen szorzatok összegeiből álló sokaság is «ideál». Az ideálok e szorzása ugyanaz, a mit az előbbeniekben (VII. fej.) két osztórendszer compositiójának neveztünk, ha t. i. ezeket az ideálokat oly osztórendszereknek tekintjük, a melyeknek végtelen sok elemük van. DEDEKIND-nek «felette gondos és éleselméjű deductiója, a mely az ő egészen elvont fogalom-meghatározásainál ép oly szükséges, mint csodálatra méltó»*, a következőképen folytatódik. Egyrészt bebizonyítja, hogy ebben a felfogásban minden ideál æquivalens véges számú elemből álló osztórendszerrel; másrészt pedig kimutatja, hogy, ha valamely ilyen $(\alpha_1, \alpha_2, \ldots)$ osztórendszer vagy ideál egy másikat, pl. $(\beta_1, \beta_2, \ldots)$-t tartalmazza, akkor az előbbi mindig mint $(\beta_1, \beta_2, \ldots)$ és egy harmadik ideál szorzata állítható elő**.

* KRONECKER szavai a Festschrift 21. §-ának végén.

** E bizonyítás csak az algebrai számok és egy változós algebrai függvényeknek esetére terjed ki ugyan, (l. az 1. § idézetét) és nem igen látható, hogy milyen nehézségek merülnének fel az *absolut* egész mennyiségek általános esetében, ha kizárólag a DEDEKIND szerint megengedett segédeszközökre akarnánk szorítkozni. A DEDEKIND-féle ideál-elmélet különböző szerzőktől eredő «egyszerűsítései» kivétel nélkül a KRONECKER-féle alapeszmének többé-kevésbbé burkolt alkalmazásában gyökereznek.

Ha végre az ideált többé nem mennyiségek sokaságának, hanem a $[\Gamma]$ tartomány számra nézve véges mennyiségeivel értelmezett jelképnek tekintjük, a mely a szorzás jelzett szabályát követi, akkor az ideálok összessége olyan tartomány, a melyben nincsen az összeadásra vonatkozó törvény, de a szorzás törvénye a közönséges. E tartomány — a mint könnyen kimutatható — annyiban teljesnek mondható, hogy két ideál legnagyobb közös osztója ismét ideál. Ha végre α a $[\Gamma]$ tartomány meghatározott mennyisége és μ annak tetszés szerinti mennyisége, akkor az összes $\alpha\mu$ szorzatokból összeállított ideál az α jelképpel jelölhető és ezek az α jelképek minden a szorzásra és oszthatóságra vonatkozó tulajdonságukban megegyeznek az α mennyiségekkel. Ekkor a felállított probléma, de avval a megszorítással, hogy csupán csak a szorzásnak alávethető mennyiségekkel dolgozunk, meg van oldva és az ideált a $[\Gamma]$ tartomány oly ideális mennyiségének tekinthetjük, a mely csakis æquivalentia-meghatározással van megadva*. E szerint az elmélet alapjainak megvetése után — az idevágó irodalom használatánál is — közömbös, vajjon az ideált az egyik, vagy pedig a másik módon akarjuk-e értelmezni. Azokban az esetekben ugyanis, melyekre nézve Dedekind elmélete nincsen kifejtve, az eddigiek alapján szintén közvetetlenül belátható, hogy a $[\Gamma]$ tartomány ama mennyiségeinek összessége, a melyek a $[\mathfrak{G}]$ tartomány valamely meghatározott mennyiségével oszthatók, ideált alkotnak Dedekind értelmében; valamint hogy ez az ideál, a mennyiben csak æquivalentia-meghatározások jönnek tekintetbe, a $[\mathfrak{G}]$ tartomány ama mennyiségét teljesen helyettesítheti.

* Az ideális szám Kummer-féle felfogására, a mely maradandó, de ma már csak történeti jelentőségű, ép ezért nem terjeszkedünk ki.

KRONECKER azokat az ideális mennyiségeket, a melyek csupán csak æquivalentia-meghatározással vannak megadva, *algebrai osztóknak* nevezi. E kifejezés az alkalmazásban gyakran kényelmetlen és talán ezért használják oly ritkán az irodalomban. Ha ebben az egy esetben eltérünk KRONECKER terminologiájától, ez azonban nem csak az épen említett okból történik; erre késztet még a történeti fejlődés, valamint az a szembetünő analogia is, mely a képzetes és ideális mennyiségek bevezetése közt fennáll.

Hogy a tárgyalást czélszerű jelöléssel áttekinthetőbbé tegyük, a $[\Gamma]$ tartomány a szó tágabb értelmében vett ideális mennyiségeinek, azaz a $[\mathfrak{G}]$ tartomány tetszés szerinti mennyiségeinek jelölésére ezentúl az $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ kis gót betűket használjuk. Azon mennyiségek jelölésére pedig, a melyek a szó szűkebb értelmében, tehát «valóban» a $[\Gamma]$ tartományhoz tartoznak, az $\alpha, \beta, \gamma, \ldots$ kis görög betűket tartjuk fenn.

9. §. Ha a $[\Gamma]$ tartomány valamely

$$\mathfrak{a} = \frac{\Sigma \alpha_r U_r}{\Sigma \varepsilon_s V_s}$$

ideális mennyiségének előállításánál használt α, ε mennyiségek mindannyian az $[A, x_1, \ldots, x_m]$ formatartományhoz tartoznak, azaz a (Γ) genus-tartomány *elsőrendű* mennyiségei, akkor czélszerű ezt az ideális mennyiséget (az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag) *raczionális és egésznek* nevezni.

A $[\Gamma]$ tartomány bármely $\mathfrak{a}$ ideális mennyiségének normája, a melyet az előbbiek szerint a

$$\mathrm{Nm.}\,\mathfrak{a} = \prod_{i=1}^{n} \frac{\Sigma \alpha_r^{(i)} U_r}{\Sigma \varepsilon_s^{(i)} V_s}$$

képlet értelmez, e szerint mindig raczionális mennyiség, azaz az $[A, x_1, \ldots, x_m, u_1, \ldots, v_1, \ldots]$ tartományhoz tartozó

két formának hányadosa, a hol a nevező okvetetlenül primitiv forma úgy, hogy ez — a mint magától értetődik — a [𝔊] tartomány mennyisége is. *Ebben az értelemben tehát* Nm. $\mathfrak{a}$ *mindig raczionális és egész mennyiség.*

A legnagyobb közös osztó itt kifejtett általános elméletének megalapításához, még hozzátartoznak a következő megjegyzések:

Ha

$$\mathfrak{a} = \frac{\alpha_u}{\varepsilon'_{w'}}, \qquad \mathfrak{b} = \frac{\beta_v}{\varepsilon''_{w''}}$$

a [Γ] tartomány két ideális mennyisége, akkor az a genus-tartomány, a melyhez az azokban fellépő α és β együtthatók tartoznak, különböző módon állapítható meg. E mellett azonban mindig lehetséges, hogy a legnagyobb közös osztónak a

$$\mathfrak{d} \sim (\mathfrak{a}, \mathfrak{b})$$

képlet megadta értelmezését úgy alakítsuk, hogy ama genus-tartomány változásától teljesen független legyen; mert az æquivalens mennyiségek közül azokat választhatjuk, a melyeknek nevezője 1.

Jelesen az $\mathfrak{a}$ *és* $\mathfrak{b}$ *ideális mennyiségeknek az a tulajdonsága, a melyet az*

$$(\mathfrak{a}, \mathfrak{b}) \sim 1$$

jelkép ad, független a Γ *genus-tartomány választásától,* hacsak ez tartalmazza az α, β együtthatókat.

Legyen (Γ_1) és (Γ_2) két ilyen genus-tartomány és (Γ_3) oly genus-tartomány, a mely (Γ_1)-et és (Γ_2)-t tartalmazza. Most már, ha β_v-t úgy írtuk, hogy a benne föllépő V hatványszorzatok mind a α_u-ban szereplő U hatványszorzatoktól különbözők,

$$\mathfrak{d} \sim \alpha_u + \beta_v$$

és így tehát

$$\text{Nm.}\,\mathfrak{d} \sim \text{Nm.}\,(\alpha_u + \beta_v).$$

E mellett azonban Nm. $(\alpha_u+\beta_v)$ értelme különböző lesz a szerint, a mint a $(\Gamma_1), (\Gamma_2)$ vagy (Γ_3) tartományt veszszük fel alapúl. Legyen Nm. $(\alpha_u+\beta_v)$ ebben a három esetben rendre N_1, N_2 és N_3, akkor szükségképen lesz

$$N_3=N_1^{k_1}=N_2^{k_2}$$

és e szerint az N_1, N_2, N_3 formák egyidőben primitiv vagy nem primitiv formák. Ez azonban egyenesen azt jelenti, hogy a $\mathfrak{d}\sim 1$ æquivalentia a megállapított feltételt kielégítő, de egyébként tetszés szerint választott (Γ_1) és (Γ_2) tartományokra nézve mindig egyidőben helyes vagy nem.

E meggondolásokból kiindulva a következő tételt nyerjük:

Legyenek α, β és δ valamely oly genus-tartomány «valódi» egész algebrai mennyiségei, a melynek «valódi» egész mennyiségei magukban is már teljes tartományt alkotnak; legyen továbbá $\delta\sim(\alpha,\beta)$, akkor bármely más oly (Γ) genus-tartományból kiindulva, a mely α-t, β-t és δ-t tartalmazza, szintén $\delta\sim(\alpha,\beta)$, ha a megfelelőleg bővített [$\mathfrak{G}$] *tartományra megyünk át.*

Most ugyanis $\alpha=\delta\mu$, $\beta=\delta\nu$, a hol μ és ν is ama genus-tartományhoz tartoznak és e tartományra nézve $(\mu,\nu)\sim 1$. Így tehát (μ,ν) a vizsgált genus-tartományok mindegyikére nézve ~ 1, a miből az I. fej. 6. §-a és az előbb bebizonyítottak szerint valóban következik, hogy $(\alpha,\beta)\sim(\delta\mu,\delta\nu)\sim\delta(\mu,\nu)\sim\delta$.

Különös fontosságot nyer e tétel akkor, ha α-t és β-t abból az *elsőrendü* genus-tartományból választjuk, a mely minden az $(A, x_1, \ldots, x_m)$ tartományból származó genus-tartományban benne van, azaz magából az $[A, x_1, \ldots, x_m]$ tartományból, a midőn tehát α, β, valamint δ is az $[A, x_1, \ldots, x_m]$ tartomány formái. A tétel ebben az esetben a következő:

Ha a_x és b_x az $[A, x_1, \ldots, x_m]$ tartomány két oly formája,

a melynek legnagyobb közös osztója ebben a teljes tartományban d_x, *akkor, ha valamely az* $(A, x_1, \ldots, x_m)$ *tartományból származó* (Γ) *genus-tartományról áttérünk a* $[\mathfrak{G}]$ *tartományra, erre a tartományra nézve is* $d_x \sim (a_x, b_x)$.

Az ideálok oszthatósági elmélete.

10. §. A $[\mathfrak{G}]$ teljes holoid tartományból ismeretes módon származik mellérendelt orthoid tartománya, $(\mathfrak{G})$, a mely — mint közvetetlenül belátható — megegyezik a $[\Gamma]_w$ tartománynak $([\Gamma]_w)$ mellérendelt orthoid tartományával. Gyakran kényelmes lesz, ha a $(\mathfrak{G})$ tartományt «teljes» genus-tartománynak és evvel szemben (Γ)-t röviden genus-tartománynak, vagy akkor, midőn az a világosság kedvéért szükségesnek látszik, «valódi» genus-tartománynak nevezzük.

A $(\mathfrak{G})$ tartomány tartalmazza a $[\mathfrak{G}]$ teljes holoid tartományt. Összes mennyiségei «a (Γ) genus-tartomány ideális mennyiségei»; még pedig «egész ideális mennyiségek» akkor, ha már a $[\mathfrak{G}]$ tartományhoz is tartoznak, «tört ideális mennyiségek» pedig az ellenkező esetben. Az utóbbiak e könyvben ugyan már nem nyernek alkalmazást, de az algebrai mennyiségek elméletének további kifejtésénél alig lesznek nélkülözhetők. Magától értetődik, hogy ezek mindig oly alakban írhatók, hogy nevezőjük raczionális és egész mennyiség legyen.

A (Γ) genus-tartomány ideális mennyiségei, az egészek úgy mint a törtek, ismét vagy a szó szűkebb értelmében vett ideális mennyiségek, vagy pedig a (Γ) genus-tartomány valódi mennyiségei lehetnek. Az utóbbi esetben a (Γ) «valódi» genus-tartomány mennyiségei, az első esetben ez nem áll.

Most majd *az ideális mennyiségeknek az oszthatóságra vonatkozó tulajdonságaival* foglalkozunk és minthogy e mel-

lett kivétel nélkül mindig csak egy [𝔊] tartomány mennyiségeire szorítkozunk, ennek külön kijelentését mellőzhetjük.

A [𝔊] tartomány mennyiségeire nézve első sorban az I. fej. 5. §-ában adott értelmezések és tételek érvényesek, a melyek tetszés szerinti holoid tartományok oszthatósági viszonyaira vonatkoznak. Jelesen valamely ilyen $\mathfrak{p}$ mennyiség irreducibilis, ha nincsen az æquivalentia-meghatározás értelmében 1-től és $\mathfrak{p}$-től különböző osztója. Minden valódi irreducibilis egész ideális mennyiség azonban törzsmennyiség is, mert a [𝔊] tartomány teljes holoid tartomány (I. fej. 6. §). Magától értetődik, hogy minden ilyen törzsmennyiség irreducibilis egész ideális mennyiség is és ezért a két elnevezés közül többnyire a rövidebbet fogjuk használni. Mint törzsmennyiségnek, $\mathfrak{p}$-nek tudvalevőleg megvan az az alaptulajdonsága, hogy két egész mennyiség szorzata, $\mathfrak{ab}$ csak akkor osztható $\mathfrak{p}$-vel, ha $\mathfrak{p}$ már $\mathfrak{a}$-nak vagy $\mathfrak{b}$-nek osztója.

Mindenekelőtt megjegyezzük, hogy most már oly *jól értelmezett eljárással is rendelkezünk, a melylyel, ha* $\mathfrak{a}$ *és* $\mathfrak{b}$ *két egész ideális mennyiség, eldönthető, vajjon* $\mathfrak{a}$ *osztható-e* $\mathfrak{b}$*-vel.*

E tárgyalásnál $\mathfrak{a}$ és $\mathfrak{b}$ a velük æquivalens α_u és β_v formákkal helyettesíthetők; $\mathfrak{b}$ tehát akkor és csakis akkor osztója $\mathfrak{a}$-nak, ha α_u osztható β_v-vel, vagyis $\frac{\beta_v}{\text{Fm. } \beta_v}$-vel. Ámde $\frac{\alpha_u \text{ Fm. } \beta_v}{\beta_v}$ okvetetlenül az u és v határozatlanoknak formája és így tehát egész ideális mennyiség, ha egész algebrai forma, azaz, ha együtthatói egész algebrai mennyiségek, a mi a 2. §-ban kifejtett módszerekkel dönthető el. Ekkor tehát és csak ekkor $\mathfrak{b}$ az $\mathfrak{a}$-nak osztója lesz. Ha ugyanis $\alpha_u \text{ Fm. } \beta_v$ a $[\Gamma]_w$ formatartományban nem osztható β_v-vel, akkor $\frac{\alpha_u \text{ Fm. } \beta_v}{\beta_v}$ sem lehet egész ideális mennyiség, azaz nem tartozhatik a [𝔊] tartományba; mert különben léteznének két oly primitiv forma, $\varepsilon'_{u'}$ és $\varepsilon''_{u''}$, a melyre nézve

$$\frac{\alpha_u \varepsilon'_{u'} \text{ Fm. } \beta_v}{\beta_v \varepsilon''_{u''}}$$

egész algebrai forma volna. De akkor a 6. § II. tétele szerint, minthogy ε'_u Fm. β_v is primitiv forma, a $[\Gamma]_w$ tartományban $\alpha_u \varepsilon'_u$ Fm. β_v-vel együtt már α_u Fm. β_v-nek is oszthatónak kellene lennie β_v-vel, a mi a mostani feltevésnek épen ellenkezője.

Közvetetlenül belátható továbbá, hogy $\mathfrak{b}$ *akkor és csak akkor* ~ 1, *midőn a* $\mathfrak{b}$*-vel aequivalens* β_v *formából képezett raczionális és egész forma*, Nm. β_v (ha ezt — mint magától értetődik — az $[A, x_1, \ldots, x_m]$ tartományból származó formának tekintjük) *primitiv forma.*

Annak eldöntésére, vajjon $\mathfrak{b}$ az $\mathfrak{a}$-nak valódi osztója-e, még a következő tétel szolgál:

Az $\mathfrak{a}$*-nak valamely* $\mathfrak{b}$ *osztója* $\mathfrak{a}$*-nak akkor és csak akkor valódi osztója, ha* Nm. $\mathfrak{b}$ *a* Nm. $\mathfrak{a}$*-nak valódi osztója.*

Ha ugyanis $\mathfrak{a}=\mathfrak{b}\mathfrak{c}$, akkor egyszersmind

$$\text{Nm. } \mathfrak{a} = \text{Nm. } \mathfrak{b} \text{ Nm. } \mathfrak{c},$$

és $\mathfrak{b}$ vagy $\mathfrak{c}$ akkor és csak akkor ~ 1, ha Nm. $\mathfrak{b}$ vagy Nm. $\mathfrak{c} \sim 1$. Ez a fölötte egyszerű tétel azért fontos, mert a felállított kérdés eldöntését az $[A, x_1, \ldots, x_m]$ tartományra vezeti vissza. Ugyanis

$$\text{Nm. } \mathfrak{a} = \frac{\bar{A}\varepsilon_1}{\varepsilon}, \quad \text{Nm. } \mathfrak{b} = \frac{\bar{B}\varepsilon_2}{\varepsilon}, \quad \text{Nm. } \mathfrak{c} = \frac{\bar{C}\varepsilon_3}{\varepsilon},$$

hol $\bar{A}, \bar{B}, \bar{C}$ az $[A, x_1, \ldots, x_m]$ tartomány formái es $\varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3$ e tartományból származó primitiv formák. Így tehát továbbá $\mathfrak{b}$ vagy $\mathfrak{c}$ akkor és csak akkor ~ 1, ha vonatkozással erre a tartományra $\bar{B}$ vagy $\bar{C} \sim 1$; azaz $\mathfrak{b}$ *akkor valódi osztója* $\mathfrak{a}$*-nak, ha a* $\bar{B}$ *forma valódi osztója az* $\bar{A}$ *formának.*

Látjuk továbbá, hogy minden egész ideális mennyiség normája a $[\mathfrak{G}]$ tartomány valamely raczionális és egész valódi mennyiségével, azaz az $[A, x_1, \ldots, x_m]$ tartomány valamely formájával æquivalens. Ezt a gyakori alkalmazás miatt külön kiemeljük.

11. §. Az ideális mennyiségek associatiója után a genustartomány egész mennyiségeire nézve az oszthatóság törvényei ép oly egyszerűek és világosak, mint a raczionális és egész számok tartományában. Jelesen érvényes — és ez tulajdonképen a bevezetett módszerek fontosságának és termékenységének alapja — a következő alaptétel:

A 0 és az egységek kivételével minden egész ideális mennyiség mint véges számú törzsmennyiség szorzata állítható elő; még pedig úgy, hogy ez az előállítás az aequivalentia értelmében egyértelműen meg van határozva.

Ha $\mathfrak{a}$ ilyen egész ideális mennyiség, a mely tehát sem nem $=0$, sem pedig nem ~ 1, akkor az vagy törzsmennyiség, vagy pedig van egy valódi osztója, $\mathfrak{b}$. Ekkor azonban $\mathfrak{b}$ nem $=0$, sem pedig nem ~ 1; $\mathfrak{b}$ tehát vagy törzsmennyiség, vagy pedig van egy valódi osztója, c s í. t. Ebben az $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ sorozatban azonban véges számú lépés után törzsmennyiségre kell jutnunk, a mely — mint az magától értetődik — az $\mathfrak{a}$-nak osztója. Ugyanis a Nm. $\mathfrak{a}$, Nm. $\mathfrak{b}$, Nm. $\mathfrak{c}, \ldots$ sorozatban is minden egyes mennyiség a megelőzőnek valódi osztója és ugyanaz áll az $\bar{A}, \bar{B}, \bar{C}, \ldots$ sorozatról is, ha ezek a mennyiségek az $[A, x_1, \ldots, x_m]$ tartománynak ama normákkal æquivalens formái és az oszthatóság kérdését erre a tartományra vonatkoztatjuk. Minthogy azonban az $\bar{A}$ formának csak véges számmal vannak osztói, szükséges, ha az $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ sorozat nem szakad meg már előbb, hogy véges számú lépés után oly $\mathfrak{h}$ mennyiségre jussunk, a melynek normája az $[A, x_1, \ldots, x_m]$ tartomány valamely irreducibilis formájával, $\bar{H}$-val æquivalens. Ez a $\mathfrak{h}$ mennyiség azonban ekkor a 10. § utolsó tétele szerint szükségképen törzsmennyiség.

Az $\mathfrak{a}$-val jelölt mennyiség tehát okvetetlenül osztható valamely $\mathfrak{p}_1$ törzsmennyiséggel; $\mathfrak{a}$ akkor vagy maga is a

$\mathfrak{p}_1$-gyel æquivalens törzsmennyiség, vagy pedig $\mathfrak{a}=\mathfrak{p}_1\mathfrak{a}_1$ és $\mathfrak{a}_1$ sem nem $=0$, sem pedig nem ~ 1. Az $\mathfrak{a}_1$ akkor ismét osztható valamely $\mathfrak{p}_2$ törzsmennyiséggel s í. t. Az így származó $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2, \ldots$ sorozat minden mennyisége ismét valódi osztója a megelőzőnek és így tehát e sorozatnak ismét meg kell szakadnia a végesben. Ezek szerint

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_\varrho,$$

hol $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\varrho$ egyenlő vagy különböző törzsmennyiségeket jelentenek, vagy pedig, ha az æquivalens törzsmennyiségeket egyesítjük,

$$\mathfrak{a} \sim \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \ldots \mathfrak{p}_r^{a_r}.$$

Hogy $\mathfrak{a}$-nak nincsen az æquivalentia értelmében ettől különböző

$$\mathfrak{a} \sim \mathfrak{q}_1^{b_1} \mathfrak{q}_2^{b_2} \ldots \mathfrak{q}_s^{b_s}$$

előállítása, azt ismeretes módon mutatjuk. (L. pl. a IV. fej. 2. §-át.) Ép úgy belátható, hogy *minden a 0-tól különböző $\mathfrak{a}$ mennyiség nem aequivalens osztóinak száma csak véges lehet* és azok mindannyian a

$$\mathfrak{d} \sim \mathfrak{p}_1^{c_1} \mathfrak{p}_2^{c_2} \ldots \mathfrak{p}_r^{c_r} \qquad (c_h = 0, 1, \ldots, a_h)$$

alakban írhatók.

Még megjegyzendő, hogy az épen kifejtett gondolatmenet *a jelzett előállításnak csak existentia-bizonyítására* vezetett és így tulajdonképen egészen hasznavehetetlen, midőn későbbi vizsgálatainkban ezt az előállítást ismeretesnek kell feltételeznünk. Ezt a hézagot majd csak a folytatólagos fejtegetések egész sora után tölthetjük be és ehhez képest $\mathfrak{a}$-nak tényleges előállítása, mint törzsmennyiségek szorzata bizonyos meghatározott véges eljárás alapján csak később (a 26. §-ban) lesz bemutatható.

12. §. Az oszthatóság elmélete az [1] tartományban, vagy pedig általánosabban az $[A, x_1, \ldots, x_m]$ tartományban egyrészt és a $[\mathfrak{G}]$ tartományban másrészt az épen tárgyalt

alaptétel közös volta mellett is igen lényeges pontban különbözik azért, mert a [𝔊] tartomány oly egész mennyiségeket is tartalmaz, a melyek nem raczionálisak. Ez megtörténik, mihelyt (Γ) nem esik egybe az $(A, x_1, \ldots, x_m)$ tartománynyal, tehát igazi genus-tartomány (azaz az elsőnél magasabbrendű). Az erre vonatkozó főtételeket soroljuk föl most.

I. *Minden* $\mathfrak{a}$ *egész ideális mennyiségnek megfelel az* $[A, x_1, \ldots, x_m]$ *tartomány bizonyos* A *formája úgy, hogy e tartomány valamely formája, midőn azt a* [𝔊] *tartomány mennyiségének tekintjük, akkor és csak akkor osztható* $\mathfrak{a}$*-val, ha* A*-val osztható, hol az utóbbi oszthatóság az* $[A, x_1, \ldots, x_m]$ *formatartományban értendő.*

Nm. $\mathfrak{a}$ és az $[A, x_1, \ldots, x_m]$ tartománynak a Nm. $\mathfrak{a}$-val æquivalens $\bar{A}$ formája okvetetlenül osztható $\mathfrak{a}$-val és így tehát e tartománynak minden $\bar{A}$-val osztható formája is osztható $\mathfrak{a}$-val. Ha ugyanez áll valamely az $\bar{A}$-val nem osztható B formáról is, akkor $\bar{A}$-nak és B-nek a formatartományban alkotott legnagyobb közös osztója, A_1 (a 9. § végén tárgyalt tétel szerint) szükségképen osztható lesz $\mathfrak{a}$-val. Ha B_1 osztható ugyan $\mathfrak{a}$-val, de nem A_1-gyel, akkor ismét az A_1 és B_1 legnagyobb közös osztója, A_2 osztható lesz $\mathfrak{a}$-val s í. t. Az $\bar{A}, A_1, A_2, \ldots$ forma-sorozatban azonban A_r az A_{r-1} osztója, de sohasem lesz $A_r \sim A_{r-1}$; mert A_r az A_{r-1} és valamely az A_{r-1}-gyel nem osztható B_{r-1} forma legnagyobb közös osztója és e szerint A_r vagy ~ 1, vagy pedig az A_{r-1} valódi osztója. A sorozat tehát megszakad, mert annak egyik tagja végre ~ 1 lesz; azaz végül nincsen olyan B_s forma, a mely A_s-sel nem osztható, de osztható $\mathfrak{a}$-val. Így valóban olyan A formára jutottunk, a mely a tételben jellemzett tulajdonságot mutatja és — mint az magától értetődik — akkor és csak akkor ~ 1, ha $\mathfrak{a} \sim 1$.

II. *Az a P forma, a mely a jellemzett módon valamely* $\mathfrak{p}$ *törzsmennyiségnek felel meg, törzsforma és a Nm.* $\mathfrak{p}$*-vel aequivalens* $\overline{P}$ *forma* $\sim P^k$.

Ha ugyanis $P=P_1 P_2$ volna, akkor épen, minthogy $\mathfrak{p}$ törzsmennyiség, már P_1-nek vagy P_2-nek oszthatónak kellene lennie $\mathfrak{p}$-vel; tehát a P-re nézve megállapított tulajdonság miatt P_1 *vagy* $P_2 \sim 1$ volna.

Ámde továbbá $P=\mathfrak{p}\mathfrak{a}$, tehát

$$\text{Nm.}\, P = P^n = \text{Nm.}\, \mathfrak{p}\ \text{Nm.}\, \mathfrak{a}$$

és így a Nm. $\mathfrak{p}$-vel æquivalens $\overline{P}$ a P^n-nek osztója és nem 1, hanem $\sim P^k$ $(k=1, \ldots, n)$.

A $\mathfrak{p}$ mennyiség *k-adfokú törzsmennyiség (törzsideál)*, ha Nm. $\mathfrak{p} \sim P^k$.

Azon különböző törzsideálokat, melyek ugyanazon törzsformának osztói, KRONECKER szerint *összetartozó* (verbundene) törzsideáloknak nevezzük.

III. *Ha a vizsgálat alapjául szolgáló* (Γ) *genus-tartomány Galois-féle tartomány, akkor a* $[\mathfrak{G}]$ *tartomány minden raczionális és egész mennyisége az összetartozó törzsosztókat egyenlő gyakran tartalmazza.*

Minthogy az $[A, x_1, \ldots, x_m]$ tartomány nem æquivalens irreducibilis formái a $[\mathfrak{G}]$ tartományban is relativ törzsformák, a tételt csak irreducibilis formákra nézve kell bebizonyítanunk. Legyen valamely P irreducibilis formára nézve

$$P \sim \mathfrak{p}^a \mathfrak{q}^b \mathfrak{r}^c \ldots,$$

akkor ez a felbontás a conjugált tartományok mindegyikében is érvényes. Ha tehát $\mathfrak{p}$ conjugált értékei $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ s ú. t., akkor

$$P \sim \mathfrak{p}_i^a \mathfrak{q}_i^b \mathfrak{r}_i^c \ldots, \qquad (i=1, \ldots, n).$$

Minthogy azonban a conjugált genus-tartományok most egybeesnek, ezek az előállítások nem lehetnek különbözők; ebből pedig közvetetlenül világos, hogy a conjugált törzs-

mennyiségek most összetartozók is. De megfordítva, az összetartozó törzsmennyiségek conjugáltak is, mert pl. Nm. $\mathfrak{p}_i$ osztható P-vel, tehát $\mathfrak{q}_i$-vel is, a mi csak úgy lehetséges, ha valamely $\mathfrak{p}_j \sim \mathfrak{q}_i$. Ha már most pl. $a < b$ volna, akkor, minthogy $\mathfrak{q}_i$ conjugált értékeinek egyike, pl. $\mathfrak{q}_j$ szükségképen $\sim \mathfrak{p}_i$, ebből következnék, hogy

$$P \sim \mathfrak{p}_j^a \mathfrak{q}_j^b \ldots,$$

azaz, hogy P osztható $\mathfrak{p}_i^b$-vel. Ép így lehetetlen a $b < a$ föltevés is.

Ha tehát $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots$ a P forma törzsosztói, akkor most

$$P \sim (\mathfrak{pqr} \ldots)^a.$$

13. §. Az olyan ideált, a mely a $[I]$ tartomány valamely valódi mennyiségével æquivalens, DEDEKIND szerint *főideálnak* nevezzük.

Könnyen felismerhető a következő tény:

Ha $\mathfrak{a}$ *bármely ideál,* $\mathfrak{p}$ *pedig bármely törzsideál, akkor mindig van olyan főideál, a mely osztható ugyan* $\mathfrak{a}$*-val, de* $\mathfrak{ap}$*-vel nem osztható.*

Ezt a főideált közvetetlenül az $\mathfrak{a}$-val æquivalens α_u forma együtthatói szolgáltatják. Ezen együtthatóknak kivétel nélkül oszthatóknak kell lenniök $\mathfrak{a}$-val (7. §), de $\mathfrak{ap}$-vel legalább egy közülük nem osztható. Hisz az ellenkező esetben $\mathfrak{a}$-nak is oszhatónak kellene lennie $\mathfrak{ap}$-vel, a mi lehetetlen. Az így meghatározott együttható az æquivalentia értelmében meghatározza a keresett főideált.

Ebből a következő általánosabb tételt is nyerjük:

Ha $\mathfrak{a}$ *bármely ideál, míg* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ *tetszés szerinti törzsideálok, akkor mindig van oly főideál, a mely osztható ugyan* $\mathfrak{a}$*-val, de az* $\mathfrak{ap}_1, \mathfrak{ap}_2, \ldots, \mathfrak{ap}_r$ *ideálok egyikével sem osztható.*

Legyen $\mathfrak{m}_i$ a $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tényezőkből a $\mathfrak{p}_i$ kizárásával

alkotott szorzat. Ekkor — a mint fentebb megmutattuk — van a $[\Gamma]$ tartományban olyan valódi mennyiség, β_i, a mely osztható ugyan $\mathfrak{am}_i$-vel, de $\mathfrak{am}_i\mathfrak{p}_i$-vel nem osztható; a

$$\beta_1+\beta_2+\cdots+\beta_r$$

meghatározta főideál pedig az, a mely a keresett tulajdonságot mutatja. Ez a főideál ugyanis okvetetlenül osztható $\mathfrak{a}$-val. De minthogy a β_i kivételével minden egyes β bizonyára osztható $\mathfrak{ap}_i$-vel, csak akkor volna osztható $\mathfrak{ap}_i$-vel, ha β_i is osztható volna $\mathfrak{ap}_i$-vel. Ámde $\mathfrak{am}_i\mathfrak{p}_i$ a $\mathfrak{p}_i$ kivételével az egyes törzsmennyiségeket ugyanannyiszor tartalmazza mint osztót, a hányszor $\mathfrak{am}_i$; a $\mathfrak{p}_i$ törzsmennyiségeket pedig ugyanannyiszor, a hányszor $\mathfrak{ap}_i$; a feltevés ellenére tehát β_i-nek oszthatónak kellene lennie $\mathfrak{am}_i\mathfrak{p}_i$-vel.

Felismerjük továbbá, hogy *van végtelen sok* (az æquivalentia értelmében) *különböző főideál, a mely a felállított feltételnek megfelel.* Ha a feladatnak megfelelőleg pl. az

$$\alpha_1, \alpha_2, \ldots, \alpha_s$$

valódi mennyiségek által megadott főideálokat előállítottuk és most $\mathfrak{q}$ olyan törzsideál, mely relativ törzsideál az $\alpha_1, \alpha_2, \ldots, \alpha_s, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideálokhoz, akkor meghatározható oly α_{s+1} főideál, a mely osztható ugyan $\mathfrak{aq}$-val, de az $\mathfrak{aqp}_1, \ldots, \mathfrak{aqp}_r$ mennyiségek egyikével sem osztható; így tehát ez a főideál nyilván ismét megoldása a feladatnak és az $\alpha_1, \ldots, \alpha_s$ főideáloktól különböző. Világos, hogy ily módon az α mennyiségek határtalan sorozatát nyerjük; mert az $[A, x_1, \ldots, x_m]$ tartomány végtelen sok irreducibilis formát tartalmaz és így a törzsideálok száma is végtelen nagy.

Ez végre a DEDEKIND-től származó és az ő elméletében különösen fontos szép tételhez vezet:

Minden $\mathfrak{a}$ *ideál két főideál legnagyobb közös osztója; még pedig minden ideál végtelen sokféleképen állítható elő ezen a módon.*

Ha $\mathfrak{a}$ valamely α főideál, akkor ezeket az előállításokat — mint az magától értetődik — $(\alpha\mu, \alpha\nu)$ szolgáltatja, hol $(\mu, \nu)\sim 1$; ha azonban $\mathfrak{a}$ nem főideál és α valamely az $\mathfrak{a}$-val osztható főideál, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ továbbá az α törzsosztói, akkor az összes végtelen sok β főideálra nézve, a mely osztható ugyan $\mathfrak{a}$-val, de az $\alpha\mathfrak{p}_1, \alpha\mathfrak{p}_2, \ldots, \alpha\mathfrak{p}_r$ ideálok egyikével sem osztható, $(\alpha, \beta)\sim\mathfrak{a}^*$.

* Az épen kifejtett elmélethez csatlakozik a további problémák egész sorozata, a melyek, habár további kifejtések nélkül, itt mégis megemlítendők.

Az ideális mennyiségeknek a szövegben használt æquivalentiája az I. fej. 5. §-a értelmében «absolut æquivalentiának» tekintendő. Evvel szemben a $\gamma\mathfrak{e}$ mennyiségek összessége, hol γ a genustartomány valamely valódi mennyisége, $\mathfrak{e}$ pedig a $[\mathfrak{G}]$ tartomány valamely ideális egysége, azaz a $[\mathfrak{G}]$ tartomány ama mennyiségeinek összessége, a melyek valódi egész mennyiséggel absolute æquivalensek, oly æquivalentiatartományt alkotnak, a mely (az I. fej. 12. §-a szerint) ismét relativ æquivalentiának, — Kronecker javaslata szerint — ú. n. Kummer-féle æquivalentiának szolgál alapjául. Ez a relativ æquivalentia szolgáltatja az ideális mennyiségek, vagy ideálok osztályokba való sorozását, a melyet eddig csak az algebrai számok elméletében dolgoztak ki részletesebben. Ebben a legegyszerűbb esetben az így származó osztályok száma véges és ezen osztályok számának meghatározása (l. pl. Dedekind többször idézett könyvét) alkotja az ú. n. *analitikai számelmélet* egyik alapproblémáját.

Kronecker-től kezdeményezett egyik további fogalomalkotás (Festschrift 22. §), a melyet azonban eddig bővebben nem fejtegettek, épen az ellenkező irányban mozog, a mennyiben az eredeti æquivalentia-fogalom szigorításán alapszik. Csatlakozva e fejezet 7. §-ának fejtegetéséhez, ezek a vizsgálatok úgy jellemezhetők, hogy az ott bevezetett $\frac{\gamma_u}{\varepsilon_v}$ hányadosban az ε_v nevezőnek most *tulajdonképeni primitiv* formának kell lennie. Tulajdonképeni primitiv forma az olyan $\Sigma\varepsilon_r U_r$ forma, a melynek együtthatói, ha azokat osztórendszer elemeinek veszszük, kielégílik a szűkebb értelemben vett

$$(\varepsilon_1, \varepsilon_2, \ldots) \simeq 1$$

æquivalentiát (VII. fej. 2. §).

A genus-tartomány valódi mennyiségeinek alaprendszere.

14. §. Ha a Γ genus-tartomány az $(A, x_1, \ldots, x_m)$ tartományból az

$$F_0 z^n + F_1 z^{n-1} + \cdots + F_n = 0$$

egyenlet egyik α gyökének adjunctiója révén származik, akkor α — mint az magától értetődik — általánosságban nem egész mennyiség, de $F_0\alpha$ mindig ilyen; mert ez a mennyiség kielégíti a

$$t^n + F_1 t^{n-1} + F_2 F_0 t^{n-2} + \cdots + F_n F_0^{n-1} = 0$$

egyenletet, a mely az előbbiből úgy származik, hogy F_0^{n-1}-vel szorzunk és azután $F_0 z$ helyébe t-t helyettesítjük. E mellett közvetetlenül belátható, hogy α-val egyidőben $F_0\alpha$ is n-edrendű algebrai mennyiség.

A Γ genus-tartománynak, valamint az abban foglalt $[\Gamma]$ tartománynak értelmezésére e szerint mindig a tartománynak valamely közvetetlenül ismeretes γ egész mennyisége használható, a mihez a következőben mindig alkalmazkodunk.

Ha a Γ genus-tartomány ama mennyisége γ, akkor a genus-tartomány minden mennyisége ismét a

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{H}$$

alakban állítható elő, a hol $G_0, G_1, \ldots, G_{n-1}$ és H (a mely $\neq 0$) az $[A, x_1, \ldots, x_m]$ tartomány formái. Ha $H=1$, akkor az így előállított mennyiség bizonyára egész mennyiség; de azért egyáltalában nem szükséges, hogy minden egész mennyiség előállításában $H=1$ legyen.

Ez a körülmény már ama genus-tartomány legegysze-

rűbb példájában is mutatkozik, a mely az (1) tartományból az $x^2+3=0$ egyenlet egyik gyökének adjunctiója révén származik. Ekkor ugyanis közvetetlenűl látni, hogy a

$$\frac{-1+\sqrt{-3}}{2}$$

mennyiség egész mennyiség, mert kielégíti az $x^2+x+1=0$ egyenletet. E mellett nem is lehetséges, hogy

$$\frac{-1+\sqrt{-3}}{2} = a + b\sqrt{-3}$$

legyen, a hol a, b közönséges egész számokat jelentenek. Ebből ugyanis

$$(2a+1) + (2b-1)\sqrt{-3}=0,$$

azaz

$$2a+1=0,\ 2b-1=0$$

származnék, a miből a feltevés ellenére $a=-\frac{1}{2}$, $b=\frac{1}{2}$ volna.

Hogy már most a Γ genus-tartomány egész mennyiségeinek általános alakját megállapíthassuk, legyen μ valamely tetszés szerinti ilyen mennyiség; akkor μ okvetetlenűl a

$$\mu=R_0+R_1\gamma+\cdots+R_{n-1}\gamma^{n-1}$$

alakban írható, hol az R-ek a Γ genus-tartomány elsőrendű mennyiségei, azaz az $[A, x_1, \ldots, x_m]$ tartomány két formájának hányadosai. Ugyanez történhetik azonban az összes conjugált genus-tartományokban is és így az R-ek meghatározására a következő egyenletrendszert nyerjük:

$$\mu_i=R_0+R_1\gamma_i+\cdots+R_{n-1}\gamma_i^{n-1}. \quad (i=1, \ldots, n)$$

Ha meggondoljuk, hogy az ismeretlenek mellett álló együtthatókból alkotott determináns négyzete az előjel mellőzésével egyenesen a γ mennyiség meghatározására szolgáló n-edfokú irreducibilis egyenlet discriminánsa, a melynek

jelölésére D vagy $D(\gamma)$ szolgáljon (és a melyet röviden a γ discriminánsának is nevezünk), akkor belátjuk, hogy

$$DR_i$$

szükségképen egész mennyiség; a $\frac{G_i}{H}$ kifejezésben tehát a G_i és H legnagyobb közös osztójának eltávolítása után H okvetetlenül D-nek osztója úgy, hogy

$$R_i = \frac{G_i'}{D}.$$

A Γ genus-tartomány minden valódi egész mennyisége tehát a

$$\mu = \frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D}$$

alakban állítható elő, hol D a γ discriminánsa és így tehát D, valamint $G_0, \ldots, G_{n-1}$ is az $[A, x_1, \ldots, x_{m-1}]$ tartomány formái.

Ebből az előállításból most már a Γ genus-tartomány egész mennyiségeinek egész formák alakjában való alapvető jelentőségű előállítása származik.

A $(G_0, G_1, \ldots, G_{n-1})$ formarendszerekből ugyanis, a melyek az összes egész mennyiségek előállításánál előfordúlnak, a VII. fej. 5. §-a szerint* kiválaszthatók véges számmal levő

$$G_0^{(i)}, G_1^{(i)}, \ldots, G_{n-1}^{(i)} \qquad (i=1, \ldots, r)$$

formarendszerek úgy, hogy minden további

$$G_0, G_1, \ldots, G_{n-1}$$

rendszerre nézve

* Ha ugyanis teljesen úgy, mint a VII. fej. 6. §-ában a $G_0^{(i)}, G_1^{(i)}, \ldots$ formákat az új $u_0, u_1, \ldots$ határozatlanok segítségével a következőben foglaljuk össze:

$$G^{(i)} = G_0^{(i)} u_0 + G_1^{(i)} u_1 + \cdots.$$

$$G_j = \sum_{i=1}^{r} H_i G_j^{(i)}$$

alakú kapcsolatok állanak fenn.

Ha tehát

$$\mu_i = \frac{G_0^{(i)} + G_1^{(i)}\gamma + \cdots + G_{n-1}^{(i)}\gamma^{n-1}}{D}$$

$$(i=1, \ldots, r)$$

a Γ genus-tartománynak bizonyos r meghatározott egész mennyisége, akkor a Γ genus-tartomány minden további valódi mennyisége a

$$\mu = \sum_{i=1}^{r} H_i \mu_i$$

alakban írható, hol a H_i-k az $[A, x_1, \ldots, x_m]$ tartomány mennyiségei. Világos, hogy minden ilyen alakban írható mennyiség valóban a genus-tartomány egész mennyisége.

Minden ilyen $\mu_1, \ldots, \mu_r$ rendszert *a genus alaprendszerének* nevezzük. E mellett ez a rendszer szükséges elemeire szorítható annyiban, hogy pl. oly μ_r, a melyet a többi μ-höz valamely

$$\mu_r = \sum_{i=1}^{r-1} H_i' \mu_i$$

alakú kapcsolat fűz, egyszerűen elhagyható. Vajjon valamely μ ezen a módon elhagyható-e, azt — mint közvetetlenül látjuk — bizonyos lineáris egyenletrendszer megoldásával dönthetjük el.

Más, sokkal mélyebb eredetű kérdés, a melyet azonban ilyen általánosságban eddig nem vizsgáltak, azon elemek legkisebb számára vonatkozik, melyek minden alaprendszerben feltétlenül föllépnek.

Az alaprendszer elemeinek száma, r semmi esetre sem lehet kisebb n-nél, a genus rendszámánál.

Az ellenkező esetben ugyanis abból, hogy

$$\gamma^j = \sum_{i=1}^{r} H_{ij}\,\mu_i, \qquad (j=1,\ldots,r)$$

a γ meghatározására olyan legfölebb $n-1$-edfokú egyenlet származnék, a melynek együtthatói nem tünnek el mindannyian; ez pedig lehetetlen, mert hisz γ n-edrendű algebrai mennyiség.

15. §. *Hogy valamely az* $(A, x_1, \ldots, x_m)$ *tartományból származó genus-tartomány az* A *orthoid tartományra vonatkozólag relativ egész mennyiségeinek egy alaprendszerét felállíthassuk,* ismét a genus-tartománynak (a genus-tartomány értelmezésével közvetetlenül megadott) γ egész mennyiségéből indulunk ki. Legyen γ discriminánsa D, a mely — mint tudjuk — az $[A, x_1, \ldots, x_m]$ tartomány formája.

A genus-tartomány minden (relativ) egész mennyisége a

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D} \qquad (1)$$

alakban állítható elő; ha tehát $D \sim 1$, ebből közvetetlenül kitünik, hogy $1, \gamma, \ldots, \gamma^{n-1}$ alaprendszer. Így tehát csak azt az esetet kell közelebbről megvizsgálnunk, midőn D az x határozatlanokat valóban tartalmazza.

A dolog azon fordúl meg, hogy a G formákat, mint az $[A, x_1, \ldots, x_m]$ tartomány formáit a legáltalánosabb módon úgy határozzuk meg, hogy ama mennyiség egész mennyiség legyen. De akkor szükséges, hogy a $\Gamma_i (i=1, \ldots, n)$ tartomány

$$\frac{G_0 + G_1\gamma_i + \cdots + G_{n-1}\gamma_i^{n-1}}{D} \qquad (i=1,\ldots,n)$$

mennyiségei egészek legyenek, valamint e mennyiségek elemi symmetrikus formái is. Ezek az

$$\frac{S_1}{D}, \frac{S_2}{D^2}, \ldots, \frac{S_n}{D^n}$$

alakban írhatók, a hol S_j a $G_0, G_1, \ldots, G_{n-1}$ mennyiségeknek az $[A, x_1, \ldots, x_m]$ tartományba tartozó együtthatókkal ellátott j-ed dimensiójú homogén formája. A megszabott feltétel — mint közvetetlenül belátható — nemcsak szükséges, hanem elegendő is; mert azon egésznek bizonyítandó mennyiség ekkor valóban megfelelő alkatú egyenlet gyöke.

Problémánk tehát úgy fogalmazható, hogy az S_j $(j=1, \ldots, n)$ j-ed dimensiójú formában az «ismeretlen» G formák úgy határozandók meg, hogy S_j osztható legyen D^j-vel. Magától értetődik, hogy ez az oszthatóság az $[A, x_1, \ldots, x_m]$ tartományra vonatkozik.

Az x határozatlanoknak bizonyos oly lineáris transformatiója, a melynek determinánsa az egység, együtthatói pedig raczionális és egész számok és a melynek alkalmazása — mint közvetetlenül belátható — a probléma felállításán mit sem változtat, átviszi D-t az x határozatlanoknak szabályos formájába, a melynek dimensiója legyen r. E mellett fölvehető, hogy $r>0$, mert a $D \sim 1$ eset már elintézettnek tekinthető.

E lineáris transformatio alkalmazása után

$$G_i = DQ_i + G_i',$$

$$G_i' = \sum_{h=0}^{r-1} G_{ih} x_m^h$$

írható, hol a G_{ih}-k már csak az $[A, x_1, \ldots, x_{m-1}]$ tartomány formái, (ha $m=1$, az A tartomány mennyiségei). A $G_0, \ldots, G_{n-1}$ formák az (1) alatti kifejezésben akkor és csak akkor szolgáltatnak egész mennyiségeket, ha ugyanaz történik a $G_0', \ldots, G_{n-1}'$ formák használata mellett. A probléma ezen új fogalmazásában tehát az ismeretlen formákat egyenesen az

x_m határozatlanra vonatkozólag $r-1$-edfokú formáknak vehetjük fel és a D^j-vel való oszthatóság tényét e szerint az $[A, x_1, \ldots, x_{m-1}]$ tartományban képezett diophantikus egyenletek rendszere fejezi ki, a melyben az egyenletek foka azonban felemelkedik n-ig. Mint «ismeretlenek» ezekben az egyenletekben a G_{ih} formák és csak ezek szerepelnek; nem pedig a létezőknek föltételezett hányadosok ismeretlen együtthatói is. Ezt közvetetlenül felismerjük, ha a kérdéses oszthatóság feltételeit a III. fej. 1. és 2. §-a szerint közönséges osztási eljárással állapítjuk meg.

Ugyanezek az oszthatósági feltételek azonban még egészen másképen is magyarázhatók. Ha A helyett az $(A, x_1, \ldots, x_{m-1})$ tartományból származó algebrai mennyiségek országát választjuk alapúl, — ezt úgy, mint már előbb, $\{A, x_1, \ldots, x_{m-1}\}$-gyel jelölve — akkor az a követelés, hogy a

$$\frac{G'_0+G'_1\gamma_i+\cdots+G'_{n-1}\gamma_i^{n-1}}{D} \qquad (i=1,\ldots,n)$$

mennyiségek az $\{A, x_1, \ldots, x_{m-1}\}$ tartományra vonatkozólag relativ egész mennyiségek legyenek, most azonban a G_{ih}-k alatt e tartomány tetszés szerinti mennyiségeit értve, ismét pontosan ugyanazokra az egyenletekre vezet, melyeket az imént fejtegettünk.

Ennek az egyenletrendszernek azonban az a szembetünő tulajdonsága van, hogy a $G_{ih}^{(1)}$ és $G_{ih}^{(2)}$ rendszerekkel együtt egyszersmind az $uG_{ih}^{(1)}+vG_{ih}^{(2)}$ rendszer is megoldása; még pedig u-nak és v-nek, mint az $\{A, x_1, \ldots, x_{m-1}\}$ tartomány mennyiségeinek bármely választásánál. Erre az egyenletrendszerre tehát alkalmazhatók az V. fej. 12. és 13. §-ának eredményei; ezek szerint pedig minimális resolvense a G_{ih} ismeretlenekre vonatkozólag lineáris. Ez a minimális resolvens azonban az adott egyenletekből raczionális műveletek segítségével állítható elő és így végre a vizsgált egyenletrendszer

tartalma megegyezik oly egyenletrendszer tartalmával, a mely a G'_{ih} ismeretlenekre vonatkozólag lineáris és a melynek együtthatói az $[A, x_1, \ldots, x_{m-1}]$ tartomány formái. Arra, hogy az $[A, x_1, \ldots, x_{m-1}]$ tartomány formái amaz egyenleteket kielégítsék, szükséges, hogy kielégítsék ezeket a lineáris egyenleteket is és viszont.

A G_{ih} mennyiségek meghatározását e szerint egyszerűen az $[A, x_1, \ldots, x_{m-1}]$ tartományból származó lineáris diophantikus egyenletek rendszere szolgáltatja; a Γ genus-tartománynak az A-ra vonatkozólag relativ egész mennyiségeit pedig összességükben a

$$H_1\mu_1+H_2\mu_2+\cdots$$

lineáris forma állítja elő, hol $H_1, H_2, \ldots$ az $[A, x_1, \ldots, x_m]$ tartomány tetszés szerinti formái.

Az alaprendszert úgy nyerjük, hogy a

$$\frac{G_0+G_1\gamma+\cdots+G_{n-1}\gamma^{n-1}}{D}$$

kifejezésben beteszszük a $G_0, G_1, \ldots$ számára nyert általános megoldást és az ebben előfordúló határozatlan formák szerint rendezünk; az alaprendszer ezután e formák együtthatóinak rendszere. Ezek egész mennyiségek, mert megfelelnek a $H_i=1$ választásnak, ha az összes többi H-t egyenlővé teszszük zérussal.

Az épen kifejtett módszert Kronecker a Festschrift-ben (6. §) csak röviden jelzi. Az ott hozzácsatolt megjegyzés szerint e módszer «akkor is alkalmazandó», ha absolut egész mennyiségek alaprendszeréről van szó. A módszer ezen alkalmazására azonban. a mely feltétlenül végrehajtható, új elméleti segédeszközök volnának szükségesek, különösen a congruentiarendszerek általános eliminácziő-elméletének (felette bonyolódott) kifejtése. E kifejtésre itt nem terjeszkedünk ki, mert evvel az eliminácziő-módszerrel ide-

gen és minden esetre felesleges elem lép be a tárgyalásba; még pedig nemcsak az alaprendszer elméletébe, hanem annak gyakorlati előállításába is. E helyett a felállított probléma megoldásának más, lényegesen egyszerűbb módszerét mutatjuk be, a mely azonkívül még a relativ és absolut egész mennyiségekre nézve teljesen azonos. Ez a módszer csak a legegyszerűbb határesetre nem alkalmazható, midőn a genus-tartomány algebrai számokból áll; ezért ezt a szélső esetet először külön kell elintéznünk.

16. §. *A γ egész algebrai szám meghatározta (γ) genus-tartomány* minden mennyisége relativ egész mennyiség az (1) tartományra vonatkozólag és, ha γ n-edrendű algebrai szám, akkor a tartomány minden mennyisége bizonyára előállítható az

$$r_0+r_1\gamma+\cdots+r_{n-1}\gamma^{n-1}$$

alakban, ha az r-ek megfelelően választott raczionális számok.

A (γ) tartományhoz tartozó (absolut*) egész algebrai számok valamely alaprendszerének előállítására igen egyszerű eljárás szolgál, a mely minden az algebrai számok elméletét tárgyaló munkában feltalálható ugyan, de mindamellett itt mégis van helye; mert a később tárgyalandó általános módszer épen ebben a legegyszerűbb esetben megtagadhatja a szolgálatot.

Ha a γ discriminánsa d, akkor a tartomány minden egész száma bizonyára előállítható a

$$\frac{g_0+g_1\gamma+\cdots+g_{n-1}\gamma^{n-1}}{d}$$

alakban és így tehát úgy, mint előbb, az ilyen alakú szá-

* Ez a hozzátétel, hogy «absolut», ebben az esetben, mint magától értetődő elhagyandó, mert hiszen minden algebrai szám «relativ» egész mennyiség.

mok közül választandók ki az egész számok. Magától értetődik, hogy a g-k, valamint d is, raczionális és egész számok. Ha már most k_i a g_i legkisebb nem negativ maradéka (mod. d), akkor ama számok legáltalánosabb alakja

$$a_0+a_1\gamma+\cdots+a_{n-1}\gamma^{n-1}+\frac{k_0+k_1\gamma+\cdots+k_{n-1}\gamma^{n-1}}{d},$$

hol az a-k tetszés szerinti raczionális és egész számokat jelentenek, míg $k_0, k_1, \ldots, k_{n-1}$ csak a $0, 1, \ldots, d-1$ értékeket vehetik fel.

Szembetünő, hogy az $1, \gamma, \ldots, \gamma^{n-1}$ számok a véges számmal levő

$$\frac{k_0+k_1\gamma+\cdots+k_{n-1}\gamma^{n-1}}{d}$$

alakú *egész* számokkal együtt alaprendszert alkotnak.

Hogy ebből mindig igen egyszerű módon nyerhető egy pontosan n elemet tartalmazó alaprendszer, az már az algebrai számok specziális elméletébe tartozó tétel, a melynek további fejtegetésébe ép ezért itt nem bocsátkozunk*.

A formák æquivalentia-modulus szerint való oszthatósága.

17. §. Hogy az algebrai mennyiségek arithmetikai elméletébe tartozó és még ezután elintézendő általános alapproblémák végleges megoldását lehetőleg egyszerűen fogalmazhassuk, még egy új (utolsó) fogalom-meghatározást kell bevezetnünk, a melynek megbeszélésére most térünk át.

* Evvel a következtetés-sorozattal teljesen analog eljárás alkalmazható még akkor is, ha az (A, x) tartományból származó genus-tartományokkal van dolgunk, hol A orthoid tartomány; különösen tehát az egy változós algebrai függvények elméletében, ha a számbeli együtthatókat mellőzzük. (L. Kronecker, Festschrift 7. §)

Valamely teljes holoid tartomány amaz e mennyiségeinek összessége, a melyeknek legnagyobb közös osztójuk valamely adott $\mathfrak{m}$ mennyiséggel az egység, az I. fej. 12. §-a értelmében æquivalentiatartományt határoz meg, a melyről azt mondhatjuk, hogy az $\mathfrak{m}$ mennyiség mellé van rendelve. Ezt az $\mathfrak{m}$ mennyiséget, a mely most majd egyidőben congruentiatartományt és æquivalentiatartományt határoz meg, ezentúl *aequivalentia-modulusnak* nevezzük. Ama teljes holoid tartományból származó két forma $\mathfrak{A}_1$ és $\mathfrak{A}_2$ az $\mathfrak{m}$ æquivalentia-modulus szerint — (æqu. mod. $\mathfrak{m}$) — æquivalens, ha abban az æquivalentiatartományban van két olyan e_1 és e_2 mennyiség, hogy

$$e_1\mathfrak{A}_1 \equiv e_2\mathfrak{A}_2 \text{ (mod. } \mathfrak{m}),$$

Ezt a vonatkozást, ha az e_1 és e_2 mennyiségek kiírására nem helyezünk súlyt, a következő módon jelezzük:

$$\mathfrak{A}_1 \sim \mathfrak{A}_2 \text{ (æqu. mod. } \mathfrak{m}).$$

Továbbá azt mondjuk, hogy $\mathfrak{A}_1$ osztható $\mathfrak{A}_2$-vel æqu. mod. $\mathfrak{m}$, ha abban az æquivalentiatartományban van két oly e_1 és e_2 mennyiség, hogy

$$e_1\mathfrak{A}_1 \equiv e_2\mathfrak{A}_2\mathfrak{A}_3 \text{ (mod. } \mathfrak{m}),$$

hol $\mathfrak{A}_3$ is valamely ama teljes holoid tartományból származó forma.

Magától értetődik, hogy az oszthatóság az $\mathfrak{m}$ æquivalentia-modulus szerint jól megkülönböztetendő az $\mathfrak{m}$ modulus (congruentia-modulus) szerint való oszthatóságtól. Tudniillik — úgy mint előbb — $\mathfrak{A}_1$ osztható $\mathfrak{A}_2$-vel mod. $\mathfrak{m}$, ha van olyan harmadik $\mathfrak{A}_3$ forma, hogy

$$\mathfrak{A}_1 \equiv \mathfrak{A}_2\mathfrak{A}_3 \text{ (mod. } \mathfrak{m}),$$

míg az oszthatóságot æqu. mod. $\mathfrak{m}$ az ujonnan bevezetett jelölés szerint

$$\mathfrak{A}_1 \sim \mathfrak{A}_2\mathfrak{A}_3 \text{ (æqu. mod. } \mathfrak{m})$$

fejezi ki.

Könnyen belátható, hogy az æquivalentiákkal való számolásnak az I. fej. 5. §-ában felsorolt három alaptörvénye megtartja érvényességét most is, avval az egyetlen módosítással, hogy a harmadikban nemcsak a zérus zárandó ki, hanem minden oly $\mathfrak{L}$ mennyiség, melyre nézve $(\mathfrak{L}, \mathfrak{m})$ *nem* ~ 1; irreducibilis $\mathfrak{m}$ esetében tehát minden $\mathfrak{L}$, mely $\equiv 0 (\mathrm{mod.}\, \mathfrak{m})$.

Ezeket a fogalom-meghatározásokat most arra az esetre alkalmazzuk, midőn az adott holoid tartomány $[A, x_1, \ldots, x_m]$, és A úgy, mint mindig vagy orthoid tartományt, vagy pedig az [1] tartományt jelenti. Így tehát a $z_1, z_2, \ldots$ új határozatlanoknak e tartományból származó formáival lesz dolgunk. *A P modulus azonban most az* $[A, x_1, \ldots, x_m]$ *tartománynak valódi irreducibilis mennyisége legyen.*

A $z_1, z_2, \ldots$ új határozatlanoknak valamely az $[A, x_1, \ldots, x_m]$ tartományból származó G formájáról ezután azt mondjuk, hogy F-nek valódi osztója æqu. mod. P, ha F osztható G-vel æqu. mod. P, de G a P æquivalentia-modulus szerint sem az egységgel, sem magával az F formával nem æquivalens.

Ha valamely G forma ~ 1 (æqu. mod. P) úgy, hogy

$$e_1 G \equiv e_2 (\mathrm{mod.}\, P),$$

a hol e_1 és e_2 az $[A, x_1, \ldots, x_m]$ tartomány oly mennyiségei, a melyek a P-hez relativ törzsmennyiségek, akkor nyilván G-nek magának is a P modulus szerint congruensnek kell lennie oly mennyiséggel, a melynek legnagyobb közös osztója P-vel ~ 1. Ha tehát

$$G \sim G_1 G_2 \quad \text{és} \quad G_1 \sim 1 \text{ (æqu. mod. } P),$$

akkor szükségképen

$$G_2 \sim G \text{ (æqu. mod. } P),$$

a mi különben az æquivalentiákra vonatkozó III. alaptörvénynek is közvetetlen folyománya.

Olyan G formát, a melynek a P æquivalentia-modulus

szerint nincsen valódi osztója, ismét æqu. mod. *P irreducibilis formának* nevezzük. Akkor áll a következő tétel:

Valamely G forma a P aequivalentia-modulus szerint bizonyára nem irreducibilis, ha a P modulus szerint mint két a z határozatlanokat valóban tartalmazó forma szorzata állítható elő.*

Magától értetődik, hogy a

$$G \equiv G_1 G_2 \pmod{P}$$

congruentiából, hol G_1 és G_2 a z határozatlanokat tartalmazó formák, következik:

$$G \sim G_1 G_2 \text{ (æqu. mod. } P)$$

és a G_1 és G_2-re vonatkozó most érvényes feltevés szerint sem G_1, sem pedig G_2 nem ~ 1.

18. §. A formáknak a P æquivalentia-modulusra vonatkozó oszthatósági elméletében, hol P az $[A, x_1, \ldots, x_m]$ tartomány valódi irreducibilis mennyisége, most már azt az alapvető tételt kell bebizonyítanunk, hogy *minden* æqu. mod. P *valódi irreducibilis forma egyszersmind törzsforma is,* azaz, hogy valamely ilyen G formával bármely $F_1 F_2$ szorzat csak akkor lehet osztható æqu. mod. P, ha már az F_1 vagy F_2 tényezők valamelyike osztható G-vel æqu. mod. P.

E mellett az az eset, midőn P valamely p közönséges törzsszámot jelent, külön lesz tárgyalandó. Magától értetődik, hogy ekkor $A=[1]$; mert orthoid tartományban minden raczionális szám, tehát p is æquivalens 1-gyel.

Ebben az (első) esetben az

$$F_1 F_2 \sim GH \text{ (æqu. mod. } p)$$

æquivalentiából az

* Ez természetesen úgy értendő, hogy az illető formában a z-k valamely az egytől különböző hatványszorzata a 0-tól mod. P különböző együtthatóval lép föl.

$$e_1 F_1 F_2 \equiv e_2 GH \text{ (mod. } p)$$

congruentia következik.

Ámde G, a mely a z határozatlanokat valóban tartalmazza, a p modulus szerint okvetetlenül az $e_3 G_1$ alakban állítható elő, hol G_1 a z határozatlanoknak mod. p primitiv formája és a z határozatlanokat ismét valóban tartalmazza. De ekkor G_1-nek továbbá mod. p irreducibilis formának és így tehát mod. p törzsformának* is kell lennie, míg e_1, a mely a z-ket nem tartalmazza, bizonyára nem osztható G_1-gyel. Tehát $F_1 F_2$-nek és így végre F_1-nek *vagy* F_2-nek kell mod. p oszthatónak lennie G_1-gyel. Ha tehát pl.

$$F_1 \equiv G_1 H_1, \quad e_3 F_1 \equiv GH_1 \text{ (mod. } p),$$

akkor egyszersmind

$$F_1 \sim GH_1 \text{ (æqu. mod. } p).$$

Ezekből a fejtegetésekből még a következő tétel is származik:

Ha az aequivalentia-modulus valamely p közönséges törzsszám, a G forma akkor és csak akkor irreducibilis æqu. mod. *p, ha irreducibilis* mod. *p.*

Hogy a forma irreducibilis volta mod. p, a p æquivalentia-modulus szerinti megfelelő tulajdonságnak következménye, azt már előbb (a 17. §-ban) kimutattuk; ha pedig viszont G irreducibilis mod. p, ebből könnyen következtethető, hogy a p æquivalentia-modulus szerint lehetetlen G-t oly szorzat alakjában előállítani, a melynek tényezői a z határozatlanokat valóban tartalmazó formák, azaz, hogy a

$$G \sim G_1 G_2 \text{ (æqu. mod. } p)$$

æquivalentia lehetetlen. A G, G_1, G_2 formákat szorzatok alak-

* A formák oszthatósága valamely p törzsszám-modulus szerint egészen elemi természetű, a melyet a P-rendszereknek az előbbi fejezetben tárgyalt elmélete természetesen már magában foglal.

jában írhatjuk, a melyeknek egyik tényezője az $[A, x_1, \ldots, x_m]$ tartomány oly mennyisége, a melynek legnagyobb közös osztója p-vel ~ 1, a másik pedig a z határozatlanoknak mod. p primitiv formája. Legyenek az utóbbi formák G', G'_1, G'_2, a melyek — mint az magától értetődik — æqu. mod. p æquivalensek G-vel, ill. G_1-gyel és G_2-vel; akkor, ha amaz æquivalentia fennáll,

$$e_1 G' \equiv e_2 G'_1 G'_2 \text{ (mod. } p);$$

minthogy pedig G' és $G'_1 G'_2$ primitiv formák, azért végre

$$G' \equiv \pm G'_1 G'_2 \text{ (mod. } p)$$

úgy, hogy G' és evvel együtt G sem volna mod. p irreducibilis.

Minden olyan forma tehát, a mely nem ~ 0 *vagy* 1 (æqu. mod. p), *a* p *aequivalentia-modulus szerint mint* æqu. mod. p *irreducibilis formák szorzata állítható elő és ez az előállítás az aequivalentia-meghatározás értelmében egyértelműleg van meghatározva.*

Az utóbbi állítás helyessége abból a körülményből következik, hogy az aequ. mod. p irreducibilis formák egyszersmind törzsformák is. Magát az előállítást közvetetlenül a p modulus szerint való felbontás szolgáltatja; csakhogy a z határozatlanokat nem tartalmazó osztók, a melyek most ~ 1, elhagyhatók úgy, hogy minden æqu. mod. p valódi osztó most egy mod. p primitiv forma *kanonikus* alakjában írható.

19. §. Egészen másképen kell eljárnunk, ha *a* P *irreducibilis formában legalább egy* x *határozatlan*, pl. x_1 *valóban előfordúl.* Ekkor a hasonlóképen irreducibilis

$$P(x_1, \ldots, x_m) = 0$$

egyenletben x_1-et ismeretlennek, a többi x-et pedig határozatlannak tekinthetjük. Ez az egyenlet ekkor bizonyos az $(A, x_1, \ldots, x_m)$ tartományból származó (ξ) genus-tartományt értelmez, hol ξ e genus-tartomány oly mennyisége, a melyre nézve $P(\xi, \ldots) = 0$.

Ekkor minden $A \equiv B \pmod{P}$ congruentia bizonyos $[A]_\xi = [B]_\xi$ azonosságra vezet, hol a $[\cdots]_\xi$ jelölés arra utal, hogy x_1 helyébe ξ teendő.

Magától értetődik, hogy a (ξ) genus-tartomány minden mennyisége az $\frac{[A]_\xi}{E}$ alakban írható, hol A és E az $[A, x_1, \ldots, x_m]$ tartomány oly formái, a melyek közül az elsőnek x_1-re vonatkozó foka nem magasabb $n-1$-nél, míg a második x_1-et egyáltalában nem tartalmazza. Ha tehát F a z határozatlanoknak az $[A, x_1, \ldots, x_m]$ tartományból származó formája, akkor F számára valamely

$$E[F]_\xi - [\Psi]_\xi = 0$$

alakú kapcsolat származik, hol E az $[A, x_2, \ldots, x_m]$ tartomány formája és Ψ az x és z határozatlanoknak oly formája, a melynek x_1-re vonatkozó foka az $n-1$-et nem lépi túl. $EF - \Psi$ tehát okvetetlenül osztható P-vel abban az értelemben, hogy még az $x_2, \ldots$ határozatlanokat tartalmazó nevezők léphetnek fel. Minthogy azonban nemcsak a $P=0$ egyenlet, hanem már a P forma is irreducibilis, azaz e formának nincsen x_1-től független osztója, azért

$$EF - \Psi \equiv 0 \pmod{P}.$$

Ha továbbá Ψ, mint a z-k formája nem primitiv, tehát $\Psi = E_1 \Phi$, akkor végül

$$F \sim \Phi \text{ (æqu. mod. } P).$$

Evvel F számára egy avval æqu. mod. P æquivalens oly *kanonikus* alakú Φ formát találtunk, a mely a z határozatlanoknak primitiv formája és az x_1-re vonatkozólag legfölebb $n-1$-edfokú. Ezek után *két forma* F_1 *és* F_2 *akkor és csak akkor aequivalens* (æqu. mod. P), *ha* $[\Phi_1]_\xi$ *és* $[\Phi_2]_\xi$ *a* (ξ) *genus-tartományban aequivalensek.*

Abból, hogy $F_1 \sim F_2$ (æqu. mod. P), következik, hogy $\Phi_1 \sim \Phi_2$ (æqu. mod. P), vagyis, hogy

$$A_1 \Phi_1 \equiv A_2 \Phi_2 \text{ (mod. } P\text{)};$$

így tehát lesz

$$[A_1]_\xi [\Phi_1]_\xi = [A_2]_\xi [\Phi_2]_\xi,$$

azaz $[\Phi_1]_\xi$ és $[\Phi_2]_\xi$ csakis a (ξ) tartományból származó, a 0-tól különböző tényezőkben különböznek egymástól és így æquivalensek. Minthogy szembetünő, hogy ez a következtetés a megfordított sorrendben is végezhető, evvel a felállított tételt már be is bizonyítottuk.

Valamely a 0-tól különböző Φ forma, a mely egyetlen z-t sem tartalmaz — mint az magától értetődik — ~ 1 (æqu. mod. P), mert Φ foka legfölebb $n-1$ és így P-hez relativ törzsmennyiség.

Ha már most visszatérünk a 18. § elején kimondott tétel bebizonyítására és a feltevés szerint

$$F_1 F_2 \sim GH \text{ (æqu. mod. } P\text{)},$$

akkor az összes formákat a fentebb jellemzett, velök æquivalens alakban gondolhatjuk írva és ekkor a következő azonosság érvényes:

$$[e_1 F_1 F_2]_\xi = [e_2 GH]_\xi.$$

Ha azonban G irreducibilis æqu. mod. P, akkor bizonyára $[G]_\xi$ is irreducibilis a (ξ) genus-tartományban. Hisz ennek valamely valódi felbontása a G-t a P æquivalentia-modulus szerint mint két a z-ket valóban tartalmazó forma szorzatát szolgáltatná. Így tehát $[F_1]_\xi$ vagy $[F_2]_\xi$ osztható lesz $[G]_\xi$-vel. Ha pl. $[F_1]_\xi = [G]_\xi \bar{H}$, akkor a $\bar{H}$ forma úgy írható, hogy a nevezők már csak az $x_2, \ldots, x_m$ határozatlanokat tartalmazzák és ha a számlálót $[H]_\xi$-vel jelöljük, végre — a mint be kellett bizonyítanunk — nyerjük, hogy

$$F \sim GH \text{ (æqu. mod. } P\text{)}.$$

E fejtegetésekből már most továbbá a következő tétel ered:

A P aequivalentia-modulus a határozatlanok oly for-

mája lévén, a mely pl. x_1-et valóban tartalmazza, a G forma akkor és csak akkor irreducibilis æqu. mod. *P, ha $[G]_\xi$ irreducibilis a (ξ) genus-tartományban, a melyet a $P=0$ egyenletnek (x_1 lévén az ismeretlen) egyik gyöke értelmez*.*

* Tehát semmiképen sem akkor, ha a G forma irreducibilis mod. P. Ezt a fontos különbséget az æquivalentia-modulusra nézve különválasztott két eset közt, a melyre még visszatérünk, itt külön kiemeljük. *Általánosságban a P modulus szerint történő szétbontásnál irreducibiliseknek mutatkozó formák semmiképen sem mindig törzsformák.* Ez csak az algebrai számoknak és az egy határozatlan algebrai függvényeinek elméletében van úgy, ha még az utóbbiaknál a számbeli együtthatókat mellőzzük. Itt azután a forma irreducibilis volta mod. P és æqu. mod. P is ugyanaz.

Így pl.

$$F=z_1^2-2z_1z_2+z_2^2-xz_1z_3+xz_2z_3+tz_3^2$$

reducibilis az x^2-4t æquivalentia-modulus szerint, hol x és t határozatlanokat jelentenek. Ugyanis

$$F\sim(2z_1-2z_2-z_3x)^2 \text{ (æqu. mod. } x^2-4t),$$

mert

$$4F\equiv(2z_1-2z_2-z_3x)^2 \text{ (mod. } x^2-4t);$$

ellenben F irreducibilis mod. x^2-4t abban az értelemben, hogy mod. x^2-4t nem állítható elő mint két raczionális és egész forma szorzata. Ekkor ugyanis az x és t határozatlanok oly raczionális és egész X formáit kellene találhatnunk, a melyekre nézve

$$4(X_1z_1+X_2z_2+X_3z_3)(X_1'z_1+X_2'z_2+X_3'z_3)\equiv(2z_1-2z_2-z_3x)^2 \text{ (mod. } x^2-4t)$$

volna. Ha az e congruentiának megfelelő azonosságba a következőket helyettesítjük:

$$t=u^2,\quad x=2u,$$

a következő újabb azonosságot nyerjük:

$$(\overline{X}_1z_1+\overline{X}_2z_2+\overline{X}_3z_3)(\overline{X}_1'z_1+\overline{X}_2'z_2+\overline{X}_3'z_3)=(z_1-z_2-uz_3)^2,$$

hol $\overline{X}$ mindig azt a raczionális és egész formát jelenti, a mely a megfelelő X-ből az adott helyettesítés alkalmazásával származik. Minthogy azonban már az X-ek együtthatói raczionális és egész számok voltak, közvetetlenül belátható, hogy minden egyes $\overline{X}$-ben az u első hatványának együtthatója szükségképen páros szám.

Másrészt azonban abból, hogy $(z_1-z_2-uz_3)^2$ csak egyértelműleg

Már előbb említettük, hogy G-nek a P æquivalentia-modulus szerint való irreducibilis voltából $[G]_\xi$-nek irreducibilis volta a (ξ) tartományban is következik. Ha viszont $[G]_\xi$ a (ξ) tartományban irreducibilis, a

$$G \sim G_1 G_2 \text{ (æqu. mod. } P)$$

feltevés, hol G_1 és G_2 a z határozatlanokat valóban tartalmazó formák, ellenmondásra vezet. Ekkor ugyanis

$$EG \equiv E_1 G_1 G_2 \text{ (mod. } P),$$

volna, hol E, E_1 az $[A, x_1, \ldots, x_m]$ tartománynak P-vel nem osztható formái; továbbá

$$[G]_\xi = \eta [G_1]_\xi [G_2]_\xi,$$

volna, hol η a (ξ) genus-tartománynak a 0-tól különböző mennyisége; ez pedig $[G]_\xi$-nek valódi szétbontását adná.

Minden oly forma tehát, a mely nem ~ 0 *vagy* 1 (æqu. mod. P) — *ép úgy mint előbb, valamely közönséges törzsszám esetében — a* P *aequivalentia-modulus szerint mint* æqu. mod. P *irreducibilis formák szorzata állítható elő és ez az előállítás az aequivalentia-meghatározás értelmében egyértelműleg van meghatározva.*

Az utóbbi állítás annak a ténynek következménye, hogy az æqu. mod. P irreducibilis formák mindig törzsformák is. Magát az előállítást közvetetlenül a $[G]_\xi$ formának a (ξ) genus-tartományban történő felbontása szolgáltatja, a melyből csak a nevezőkként szereplő és x_1-től független formák szorzás útján eltávolítandók úgy, hogy tehát a tényezők az előbb taglalt kanonikus alakban írhatók.

20. §. A mint a forma felbontásának most befejezett elmélete mutatja, az «æquivalentia-modulus» bevezetése elvi

bontható fel raczionális és egész törzsformákra, ellentétben a most megállapított tulajdonsággal, következnék, hogy

$$\overline{X}_3 = \pm u.$$

A feltételezett felbontás tehát valóban lehetetlen.

szempontból nem föltétlenül szükséges; mert az illető fogalom-meghatározások végre e kifejezésmód használata nélkül is megállapíthatók. De ugyanez történik a mathematikai symbolika minden bővítésénél és minden egyes esetben megfontolandó, hogy az új symbolum bevezetése mennyiben czélszerű. Az æquivalentia-modulus bevezetése valóban nagy mértékben ilyennek mutatkozik. A nélkül, hogy a formáknak itt kérdéses tulajdonságaira kiterjeszkednénk, az algebrai mennyiségek arithmetikai elméletének kifejtése egyáltalában nem lehetséges; ha azonban mind e mellett mégis kerülni akarnók az új æquivalentia-meghatározásnak megfelelő jelölések bevezetését, akkor az egész tárgyalás nemcsak nehézkessé válnék és nélkülözné az áttekinthetőséget, hanem az eddig megkülönböztetett két esetet mindig külön kellene tárgyalnunk. Egységes elmélet tehát nem mellőzheti ezt az új kifejezésmódot.

Használatával az épen bebizonyított alapvető tények mellett még a következő, az alkalmazásban fontos tételeket nyerjük:

Legyen G a $z, z_1, z_2, \ldots$ *határozatlanoknak az* $[A, x_1, \ldots, x_m]$ *tartományból származó olyan formája, a mely z-re nézve szabályos* mod. *P. Legyen továbbá G felbontása a P aequivalentia-modulus szerint:*

$$G \sim G_1^{a_1} G_2^{a_2} \ldots G_r^{a_r} \text{ (æqu. mod. } P),$$

a hol a most használt írásmódnál $G_1, G_2, \ldots$ *már nem aequivalens formák* æqu. mod. *P. E feltevés mellett G-nek felbontása akkor és csakis akkor tartalmaz valamely törzsformát többszörösen, ha G-nek (z szerint vett) discriminánsa zéras* mod. *P. Ekkor továbbá a* $G_1, G_2, \ldots$ *törzsformáknak (z szerint vett) discriminánsai, valamint e törzsformák közül bármely két különbözőnek (z szerint vett) resultánsa kivétel nélkül különbözik a* 0*-tól* mod. *P.*

A felsorolt tények nyilvánvalók, ha az æquivalentia-modulus természetes törzsszám, mert ekkor csakis a G formának a p modulus szerint való felbontásával van dolgunk.

Akkor pedig, midőn az æquivalentia-modulus határozatlanokat tartalmaz, a következőket kell meggondolnunk. Többszörös törzsténye zők akkor fordúlnak elő G-ben, ha ilyenek fellépnek a $[G]_\xi$ formának a (ξ) genus-tartományban történő felbontásánál. A $[G]_\xi$ forma a z-re nézve szintén szabályos forma és így osztói ismét a z-re nézve szabályos formák lesznek. Többszörös ilyen osztók akkor és csak akkor léphetnek fel, ha a $[G]_\xi$ formának z szerint vett discriminánsa eltünik. Ez pedig $[\mathrm{Dscr.}\, G]_\xi$ és így tehát csak akkor zérus, ha $\mathrm{Dscr.}\, G \equiv 0 \,(\mathrm{mod.}\, P)$.

Ha továbbá $\mathrm{Dscr.}\, G_1 \equiv 0 \,(\mathrm{mod.}\, P)$ volna, ebből következnék, hogy $\mathrm{Dscr.}\, [G_1]_\xi = 0$, azaz $[G_1]_\xi$ nem volna törzsforma, és így G_1 sem. Ép úgy abból, hogy $\mathrm{Res.}\,(G_1, G_2) \equiv 0 \,(\mathrm{mod.}\, P)$, következnék, hogy $\mathrm{Res.}\,([G_1]_\xi, [G_2]_\xi) = 0$; minthogy azonban $[G_1]_\xi$ és $[G_2]_\xi$ irreducibilis formák, a $[G_1]_\xi$ és $[G_2]_\xi$ formáknak akkor æquivalenseknek kellene lenniök és ekkor a feltevés ellenére $G_1 \sim G_2 \,(\mathrm{æqu.\ mod.}\, P)$ volna.

Az alaprendszerek felállítására szolgáló általános módszer.

21. §. A mostan megoldandó probléma a következő módon fogalmazható:

Legyen ismét A valamely orthoid tartomány, vagy pedig az [1] tartomány, P az $[\mathrm{A}, x_1, \ldots, x_m]$ tartomány irreducibilis mennyisége és γ ismét valamely e tartományból származó n-edrendű egész algebrai mennyiség; legyenek továbbá $\varphi_1, \varphi_2, \ldots, \varphi_k$ a γ értelmezte (Γ) genus-tartomány valódi egész mennyiségei. Akkor az $[\mathrm{A}, x_1, \ldots, x_m]$ tartományhoz

tartozó $X_1, \ldots, X_k$ mennyiségek úgy határozandók meg, hogy

$$\frac{X_1\varphi_1 + X_2\varphi_2 + \cdots + X_k\varphi_k}{P}$$

egész mennyiség legyen és e mellett még kimutatandó, hogy ez csak akkor történik, ha

$$X_i = H_{i1}Y_1 + \cdots + H_{is}Y_s,$$

hol a H-k az $[A, x_1, \ldots, x_m]$ tartomány meghatározott formái, az Y-ok pedig ugyanennek a tartománynak tetszés szerinti formái.

Hogy e probléma megoldása után a (I') genus-tartomány valódi mennyiségeinek alaprendszere véges számú lépésben felállítható, igen könnyen belátható.

Legyen γ discriminánsa az $[A, x_1, \ldots, x_m]$ tartományban irreducibilis tényezőkre felbontva:

$$D = P_1 P_2 P_3 \ldots,$$

akkor a 14. § jelöléseit használva,

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D}$$

csak úgy lehet egész mennyiség, ha a

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{P_1}$$

mennyiség is ilyen. A feltevés szerint ez a G-knek bizonyos fentebb jellemzett alakja mellett áll be; és ekkor minden esetre

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{P_1} = \sum_{j=1}^{s} Y_j \frac{H_{0j} + H_{1j}\gamma + \cdots + H_{n-1,j}\gamma^{n-1}}{P_1}.$$

Az épen felírt összegben tehát az Y_j-k együtthatói egész mennyiségek és, ha ezeket röviden φ_j-vel jelöljük, lesz

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D} = \frac{\sum_{j=1}^{s} \varphi_j Y_j}{P_2 P_3 \ldots}.$$

Ekkor ismét a

$$\frac{\sum_{j=1}^{s} \varphi_j Y_j}{P_2}$$

mennyiségnek egész mennyiségnek kell lennie. Ez a helyesnek felvett tétel szerint az Y-ok hasonló meghatározását szolgáltatja, mint a milyen a G-ké volt. Ha így folytatjuk, míg D összes irreducibilis tényezőit (a melyek közt — mint az magától értetődik — egyenlők is lehetnek) eltávolítottuk, végre a genus-tartomány összes valódi mennyiségeit a

$$\Sigma \psi_j Y_j^{(r)}$$

alakban nyerjük, hol a ψ-k meghatározott egész mennyiségek, az $Y_j^{(r)}$-k pedig az $[A, x_1, \ldots, x_m]$ tartomány tetszés szerinti formái. Más szóval: *A ψ_j mennyiségek alaprendszert alkotnak.*

Ismétlések elkerülése végett az ehhez képest megoldandó problémát mindjárt még általánosabban fogalmazzuk:

Legyenek $\varphi_1, \varphi_2, \ldots, \varphi_k$ a (Γ) genus-tartományhoz tartozó Galois-féle tartomány valódi egész mennyiségei, P az $[A, x_1, \ldots, x_m]$ tartomány valódi irreducibilis formája, továbbá (a 12. § III. tétele szerint) e Galois-féle tartományban

$$P = (\mathfrak{pqr} \ldots)^a,$$

akkor szintén az $[A, x_1, \ldots, x_m]$ tartományhoz tartozó $X_1, \ldots, X_k$ formák a legállalánosabb módon meghatározandók úgy, hogy

$$X_1 \varphi_1 + \cdots + X_k \varphi_k \equiv 0 \pmod{\mathfrak{p}^c \mathfrak{q}^c \mathfrak{r}^c \ldots} \qquad (C)$$

legyen, hol c fölveszi az $1, 2, \ldots,$ a értékeket.

E mellett mindenekelőtt kitünik, hogy a $c=1$ esettel együtt a többi eset is el van intézve, t. i. midőn $c>1$. Ha ugyanis — a mint azt majd később kimutatjuk — az

$$X_1 \varphi_1 + \cdots + X_k \varphi_k \equiv 0 \pmod{\mathfrak{pqr} \ldots}$$

congruentia általános megoldása az

$$X_i = H_{i1} Y_1 + \cdots + H_{il} Y_l$$

alakot ölti, akkor természetesen a (C) congruentia megoldásainak is ilyen alakúaknak kell lenniök és ezek bizonyára kielégítik a (C) congruentiát is, ha még továbbá

$$Y_1 \sum_{i=1}^{k} H_{i1} \varphi_i + \cdots + Y_l \sum_{i=1}^{k} H_{il} \varphi_i \equiv 0 \pmod{\mathfrak{p}^c \mathfrak{q}^c \mathfrak{r}^c \ldots}. \qquad (C')$$

Ámde származása szerint minden egyes $\sum_{i=1}^{k} H_{ij} \varphi_i$ mennyiség osztható $\mathfrak{pqr}\ldots$-vel és ezeknek a mennyiségeknek, összes conjugáltjaiknak és P-nek legnagyobb közös osztója a $\mathfrak{pqr}\ldots$-nek hatványa. Ha ugyanis e mennyiségek valamelyikére nézve

$$\left(\sum_{i=1}^{k} H_{ij} \varphi_i^{(e)}, P\right) \sim \mathfrak{p}^r \mathfrak{q}^s \ldots$$

volna, akkor, minthogy a Galois-féle tartományban az összetartozó törzsideálok egyszersmind conjugált ideálok is, valamely conjugált mennyiségre nézve is

$$\left(\sum_{i=1}^{k} H_{ij} \varphi_i^{(f)}, P\right) \sim \mathfrak{p}^s \mathfrak{q}^t \ldots$$

lenne; és az összes ily mennyiségek legnagyobb közös osztójában a $\mathfrak{p}$ törzsideál kitevője szükségképen a legkisebb mindazon számok közt, a melyek itt mint kitevők egyáltalában szerepelnek.

Így tehát

$$\mathfrak{d} \sim \left(\sum_{i=1}^{k} H_{i1} \varphi_i^{(1)}, \ldots, \sum_{i=1}^{k} H_i \varphi_i^{(N)}, \ldots, P\right) \sim \mathfrak{p}^g \mathfrak{q}^g \ldots,$$

a hol magától értetődik, hogy $g \leqq a$.

A (C') congruentia tehát, ha a $\mathfrak{d}$ osztót eltávolítjuk, az

$$Y_1 \frac{\sum_{i=1}^{k} H_{i1}\varphi_i}{\mathfrak{d}} + \cdots + Y_l \frac{\sum_{i=1}^{k} H_{il}\varphi_i}{\mathfrak{d}} \equiv 0 \pmod{\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots} \quad (C'')$$

alakban írható *.

E mellett mindjárt arra a fontos körülményre is figyelmeztetünk, hogy *a* $\mathfrak{d}$ *mennyiség meghatározása nem követeli, hogy P-nek törzsideáljaira való felbontását már ismerjük;* valamint, hogy, *ha a* (C') *congruentia modulusa e felbontás nélkül ismeretes, akkor ismeretes egyuttal a* (C'') *congruentia modulusa is, mert hisz csak a* $\mathfrak{d}$ *osztót kell elávolítanunk* $(\mathfrak{pqr}\ldots)^c$*-ből.*

A (C'') congruentia bal oldala, ha a $\mathfrak{d}$-vel való osztást az ideális mennyiségekre nézve megállapított számolási szabályok szerint valóban elvégezzük, két forma hányadosába megy át, a melyben mindenekelőtt a $\mathfrak{d}$ tényleges képezésénél fellépő új határozatlanok tekintendők határozatlanoknak. A nevezőben fellépő forma primitiv forma és mint ilyen a congruentiából elhagyható, mert evvel csak æquivalens ideális mennyiségre térünk át. A számláló végre akkor és csak akkor osztható $\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots$-vel, ha az új határozatlanok hatványszorzatai szerint rendezett forma minden együtthatója osztható $\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots$-vel. Így tehát az Y-ok meghatározására a (C') vagy (C'') congruentiával egyenlő

* Hogy itt a congruentiában, habár nem pusztán æquivalentia-meghatározással van dolgunk, mégis oszthatunk $\mathfrak{d}$-vel, az annak következménye, hogy $\mathfrak{d}$ nem csupán ideálnak tekinthető az æquivalentia-meghatározás értelmében, hanem mint holoid tartomány mennyisége szerepel. Ez sem DEDEKIND, sem pedig KRONECKER elméletében nem történhetik. Ebből áll az ideális mennyiségek elméletének amaz — épen ezen és más alkalmazásainál fogva lényeges — bővítése, a mely — e munkában legelőször — megengedi az ide tartozó arithmetikai alapproblémák végleges elintézését, és a melyre már a 8. §-ban reámutattunk.

értékű

$$Y_1\psi_{1r}+Y_2\psi_{2r}+\cdots+Y_s\psi_{sr}\equiv 0 \pmod{\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots} \quad (r=1,2,\ldots) \qquad (C''')$$

congruentiarendszert nyerjük, a mely *a probléma keresett reductióját* adja; a modulus ugyanis most $\mathfrak{pq}\ldots$-nak alacsonyabb hatványa, mint előbb. Hogy e mellett *egy* congruentia helyett az ilyen congruentiák rendszere lép fel, nem lényeges körülmény. Ha t. i. az egyik ilyen congruentia általános megoldása ismeretes és — a mint feltételeztük — véges sereg alakjában van megadva, akkor ezt a megoldást a többi congruentiába helyettesítve, evvel a feladatot oly rendszerre redukáljuk, a melyben a congruentiák száma egygyel kisebbedett, sőt esetleg többel is, ha a származó congruentiák közt vannak olyanok, a melyek azonosan elégíttetnek ki.

A reductio e módszere véges számú lépésben a congruentiák oly rendszerére vezet, a mely azonosan kielégített congruentiákból áll, a hol t. i. minden egyes együttható osztható $\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots$-vel úgy, hogy azokból az Y-ok mint semmi további feltételnek alá nem vetett tetszés szerinti formák adódnak ki. Minthogy ugyanis ezen eljárás minden egyes lépésénél a $\mathfrak{p}, \mathfrak{q}, \ldots$ törzsideálok közös kitevője legalább is egygyel száll alább, annak, ha nem előbb, minden esetre c lépés után meg kell történnie, a midőn a modulus már ~ 1 lett. Hogy ez megtörtént-e és hogy mikor történt meg, kiderül közvetetlenül a

$$\mathrm{Nm}.\frac{\mathfrak{p}^c\mathfrak{q}^c\ldots}{\mathfrak{d}}$$

mennyiség képezése révén, a mely ekkor primitiv formák hányadosa lesz.

Mint már kiemeltük, ez az eljárás nem kívánja meg, hogy P-nek törzsideálokra való felbontása ismeretes legyen; csak a $\mathfrak{p}^c\mathfrak{q}^c\ldots$ modulust kell valahogyan megadnunk. P-nek

ama felbontását csak az eljárás megokolásánál mint elméleti segédeszközt használtuk, a mely azonban a gyakorlati kivitelben *nem* nyer alkalmazást. Ezért elegendőnek mutatkozik az e felbontásra vonatkozólag előbb adott existentia-bizonyítás és megfordítva a most kifejtett módszer avval, hogy az alaprendszer előállítását szolgáltatta, lehetségessé teszi majd azt is, hogy P-t tényleg felbontsuk törzsideálokra.

Az e § elején felállított probléma egyenesen az

$$X_1\varphi_1+\cdots+X_k\varphi_k\equiv 0 \pmod{P}$$

congruentia megoldását követeli; e mellett P okvetetlenül a $\mathfrak{pq}\ldots$-nek hatványa és az előbb kiemelt további feltevés is megvalósul, hogy t. i. a congruentia modulusa valamely tényleg megadott mennyiség. E szerint az egész eljárás, a melyre valamely genus-tartomány alaprendszerének felállításánál szükségünk van, az

$$X_1\varphi_1+\cdots+X_k\varphi_k\equiv 0 \pmod{\mathfrak{pq}\ldots}$$

congruentia megoldására van visszavezetve, hol $\mathfrak{p}, \mathfrak{q}, \ldots$ a P-ben foglalt *különböző* törzsmennyiségeket jelentik; az eljárás azonban, a mely e congruentia megoldását szolgáltatja, ismét úgy állapítandó meg, hogy a P felbontásának ismeretétől független legyen.

22. §. Hogy most ezt a már legegyszerűbb alakjára hozott problémát megoldhassuk, képezzük az

$$F=\Pi(z-\varphi_1^{(i)}z_1-\cdots-\varphi_k^{(i)}z_k)$$

kifejezést, hol a szorzás a $z-\varphi_1 z_1-\cdots-\varphi_k z_k$ különböző conjugált értékeire terjesztendő ki és F e szerint az új $z, z_1, \ldots, z_k$ határozatlanoknak az $[A, x_1, \ldots, x_m]$ tartományból származó formája. A P æquivalentia-modulus szerint felbontva legyen

$$F\sim F_1^{a_1}F_2^{a_2}\ldots \text{ (æqu. mod. } P).$$

Ez az æquivalentia — mint tudjuk — ugyanazt a tényt fejezi ki, mint egy bizonyos

$$Q'F \equiv Q''F_1^{a_1} F_2^{a_2} \ldots \pmod{P}$$

congruentia, hol Q' és Q'' olyan az $[A, x_1, \ldots, x_m]$ tartományhoz tartozó mennyiségek, a melyeknek legnagyobb közös osztója P-vel ~ 1. Az alapúl szolgáló GALOIS-féle tartomány legyen most már az, mely az eddig használtból az

$$F_1 F_2 \ldots = 0$$

egyenlet összes gyökeinek adjunctiójával keletkezik, a mely egyenletben z-t ismeretlennek, $z_1, \ldots, z_k$-t pedig továbbra is határozatlanoknak tekintjük. Magától értetődik, hogy az $F=0$ egyenlet gyökei akkor a $\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k$ conjugált mennyiségek. Végre az $F_1=0$, $F_2=0$ egyenletek gyökeinek jelölésére szolgáljanak

$$\alpha_1, \ldots, \alpha_{l_1}; \beta_1, \ldots, \beta_{l_2}; \ldots,$$

hol e szerint $l_1, l_2, \ldots$ az $F_1, F_2, \ldots$ formáknak z-re vonatkozó fokát jelentik. Ha tehát az F formának z-re vonatkozó foka l, akkor e szerint még lesz

$$l = a_1 l_1 + a_2 l_2 + \cdots .$$

Ha már most $\mathfrak{p}$ a P-ben foglalt valamelyik törzsideál, akkor fennáll a

$$Q'F \equiv Q''F_1^{a_1} F_2^{a_2} \ldots \pmod{\mathfrak{p}}$$

congruentia is és egyrészt a

$$\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k$$

mennyiségeknek, másrészt az

$$\alpha_1, \ldots, \alpha_{l_1}; \beta_1, \ldots, \beta_{l_2}; \ldots$$

mennyiségeknek, ha minden egyes α-t a_1-szer, minden egyes β-t a_2-ször s í. t. számlálunk, a sorrend mellőzésével mod. $\mathfrak{p}$ meg kell egyezniök*. E mellett az $\alpha_1, \ldots, \alpha_{l_1}; \beta_1, \ldots, \beta_{l_2}; \ldots$

* Ha ugyanis

$$Q'(z-\mu_1)(z-\mu_2)\ldots \equiv Q''(z-\nu_1)(z-\nu_2)\ldots \pmod{\mathfrak{p}},$$

akkor

$$Q'(\nu_1-\mu_1)(\nu_1-\mu_2)\ldots \equiv 0 \pmod{\mathfrak{p}}.$$

Minthogy továbbá (Q', P) és így egyszersmind $(Q', \mathfrak{p}) \sim 1$, a többi tényező

mennyiségek mindannyian különbözők mod. $\mathfrak{p}$; mert ellenkezőleg valamely F_i forma discriminánsának, vagy pedig két ilyen F_i, F_j forma resultánsának el kellene tünnie mod. $\mathfrak{p}$; vagyis, minthogy ezek a z határozatlanoknak az $[A, x_1, \ldots, x_m]$ tartományból származó formái, a P modulus szerint is el kellene tünniök. Ez azonban képezésüknél fogva és a 20. § tétele alapján ki van zárva.

Első pillanatra úgy látszik ugyan, mintha e fejtegetések, valamint a jegyzetben alkalmazott következtetésmód is ahhoz a föltételhez volna kötve, hogy az $\alpha, \beta, \ldots$ mennyiségek egész mennyiségek. Általánosságban azonban ezek semmiképp sem ilyenek; jelesen akkor nem, ha a P æquivalentia-modulus az $x_1, \ldots$ határozatlanokat tartalmazza. Ekkor z legmagasabb hatványának együtthatója $F_1 F_2 \ldots$-ben épen nem 1, hanem mivel F a z-kre nézve szabályos forma, az $[A, x_1, \ldots, x_m]$ tartomány valamely formája, a melyre nézve csak azt tudjuk, hogy e forma és P közös osztója ~ 1.

E szerint tehát, ha z legmagasabb hatványának együtthatója F-ben A, akkor α nem egész mennyiség, hanem csak $A\alpha = \alpha'$. Lehet azonban úgy, mint az gyakran a számelmélet elemeiben is történik, a $\mathfrak{p}$ modulus szerint vett congruentiákban akadály nélkül oly törteknek helyt adni, a melyeknek nevezői $\mathfrak{p}$-vel nem osztható mennyiségek, ha a

$$\frac{\mu}{A} \equiv \frac{\nu}{B} \pmod{\mathfrak{p}}$$

congruentiával kifejezett

közül valamelyiknek oszthatónak kell lennie $\mathfrak{p}$-vel, minthogy $\mathfrak{p}$ törzsideál. Ha pl. $\nu_1 - \mu_1$ osztható $\mathfrak{p}$-vel, tehát $\nu_1 \equiv \mu_1 \pmod{\mathfrak{p}}$, akkor a $z - \mu_1 \equiv z - \nu_1$ tényezőt mind a két oldalon eltávolíthatjuk és így tehát ismét nyerjük, hogy $\nu_2 \equiv \mu_2 \pmod{\mathfrak{p}}$ stb. E következtetésnél csak azt kell figyelembe vennünk, hogy a valamely törzsmodulus szerint történő közönséges osztási eljárás egyértelműleg meghatározott művelet.

vonatkozást egyszerűen a

$$B\mu_1 \equiv A\nu \pmod{\mathfrak{p}}$$

vonatkozás más írásmódjának tekintjük. Így akkor az

$$\alpha \equiv \varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k \pmod{\mathfrak{p}}$$

congruentia jelentése ugyanaz, mint a következőé:

$$A\alpha \equiv \alpha' \equiv A(\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k) \pmod{\mathfrak{p}}.$$

Az előbbi megjegyzésben alkalmazott következtetésmód most már könnyen átvihető arra az esetre, midőn $\mu_1, \ldots, \mu_2, \nu_1, \ldots, \nu_2$ nem egészek. Ekkor ugyanis

$$A_1\mu_1, A_2\mu_2, \ldots, B_1\nu_1, B_2\nu_2, \ldots$$

egészek, hol $A_1, A_2, \ldots, B_1, B_2, \ldots$ a $\mathfrak{p}$-vel *nem* osztható mennyiségek. E mellett még megjegyzendő, hogy ekkor az A és B mennyiségek a P-hez relativ törzsmennyiségek és így tehát az összetartozó vagy conjugált $\mathfrak{q}, \mathfrak{r}, \ldots$ törzsideálokkal sem oszthatók. Így tehát csakis $A_1 A_2 \ldots B_1 B_2 \ldots$ megfelelő hatványával szorozva, $A_1 A_2 \ldots B_1 B_2 \ldots z = z'$ vezetendő be.

23. §. Ha e további megállapodások után az előbbi § elején kifejtett congruentiához visszatérünk, akkor végre

$$F_1 F_2 \ldots \equiv 0 \pmod{\mathfrak{p}}$$

olyan congruentia, a melynek gyökei a $\mathfrak{p}$ modulus szerint különböző

$$\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k$$

alakú mennyiségek, a melyeknek száma megegyezik a congruentia fokával, $l_1 + l_2 + \cdots$-vel. Ha e congruentiában z legmagasabb hatványának együtthatója Q, akkor magától értetődik, hogy Q az $[A, x_1, \ldots, x_m]$ tartomány oly formája, a melynek és P-nek közös osztója ~ 1; és ha még rövidség kedvéért a

$$\Phi = F_1 F_2 \ldots$$

jelölést vezetjük be, végre (hasonlóan, mint a VI. fej. 15. §-ában) a következő congruentiához jutunk:

$$\left[\frac{\partial \Phi}{\partial z}\right]_{z=\Sigma \varphi_r^{(i)} z_r} \varphi_r^{(i)} + \left[\frac{\partial \Phi}{\partial z_r}\right]_{z=\Sigma \varphi_r^{(i)} z_r} \equiv 0 \ (\text{mod. } \mathfrak{p}).$$

Ámde Φ-nek z szerint vett discriminánsa az

$$[\mathrm{A}, x_1, \ldots, x_m, z_1, z_2, \ldots]$$

tartomány oly mennyisége, a mely különböző mod. P a 0-tól és e tulajdonságát megtartja akkor is, ha $z_1, z_2, \ldots$ helyébe az $[\mathrm{A}, x_1, \ldots, x_m]$ tartomány megfelelően választott, $Z_1, Z_2, \ldots$ mennyiségeit teszszük*.

Ha annak jelölésére, hogy a $z=\Sigma \varphi_r^{(i)} Z_r$, $z_r = Z_r$ helyettesítés megtörtént, röviden a $[\ldots]_{Z^{(i)}}$ jelt használjuk, akkor

$$\left[\frac{\partial \Phi}{\partial z}\right]_{Z^{(i)}}$$

különböző mod. $\mathfrak{p}$ a 0-tól és a $\mathfrak{p}$ modulus szerint különböző $\varphi_1^{(i)}, \ldots, \varphi_k^{(i)}$, számra nézve $l_1+l_2+\cdots$ értékrendszerre kiterjesztett

$$\Pi \left[\frac{\partial \Phi}{\partial z}\right]_{Z^{(j)}}$$

szorzat is különböző mod. $\mathfrak{p}$ a zérustól. Ez úgy származik

$$\Pi \left[\frac{\partial \Phi}{\partial z}\right]_{z=\Sigma \varphi_r^{(j)} z_r}$$

* Hogy igy következtethessünk, ismét (úgy, mint a VIII. fej. 4. §-ában) csak az szükséges, hogy az $[\mathrm{A}, x_1, \ldots, x_m]$ tartomány végtelen sok a P modulus szerint különböző mennyiséget tartalmazzon. Ez mindig megtörténik, ha a tartomány határozatlanokat tartalmaz. Ha P közönséges törzsszám, akkor $1, x_1, x_1^2, \ldots$ ilyen mennyiségek; ha pedig P legalább is egy határozatlant tartalmaz, $1, 2, 3, \ldots$ a megszabott föltételnek megfelelő mennyiségek. Kizárva marad e szerint az algebrai számok esete, hol az $[\mathrm{A}, x_1, \ldots, x_m]$ tartomány helyébe az $[1]$ tartomány lép. Ekkor az alkalmazandó következtetés esetleg valóban helytelen lehet és ezért az itt általánosan megoldandó problémát épen erre a legegyszerűbb határesetre nézve külön kellett tárgyalnunk.

-ből, hogy erre a $z_r = Z_r$ helyettesítést alkalmazzuk; ez az utóbbi mennyiség pedig a $\Phi \equiv 0 \pmod{\mathfrak{p}}$ congruentia gyökeinek symmetrikus formája és így tehát, ha Q elég magas hatványával megszorozzuk, a $\mathfrak{p}$ modulus szerint mint az $[A, x_1, \ldots, x_m, z_1, z_2, \ldots]$ tartomány S formája állítható elő, a mely mod. P a zérustól különböző.

Egészen hasonló módon belátható, hogy a

$$\Pi^{(i)} \left[\frac{\partial \Phi}{\partial z}\right]_{Z^{(j)}}$$

szorzat, a hol a $\left[\frac{\partial \Phi}{\partial z}\right]_{Z^{(i)}}$ tényező kizárandó, a $z_r = Z_r$ helyettesítés révén származik

$$\Pi^{(i)} \left[\frac{\partial \Phi}{\partial z}\right]_{z = \Sigma \varphi_r^{(j)} z_r}$$

-ből. Ez az utóbbi mennyiség a $\Sigma \varphi_r^{(i)} z_r$ kizárása után a $\Sigma \varphi_r^{(j)} z_r$ mennyiségek symmetrikus formája és így tehát, ha Q elég magas hatványával szorozzuk, a p modulus szerint a

$$[\Psi(z, z_1, z_2, \ldots)]_{z = \Sigma \varphi_r^{(i)} z_r}$$

alakban állítható elő úgy, hogy végre

$$S\varphi_r^{(i)} \equiv \left[-\Psi \frac{\partial \Phi}{\partial z_r}\right]_{Z^{(i)}} \pmod{\mathfrak{p}},$$

vagyis

$$S\varphi_r^{(i)} \equiv \psi_r(\zeta_i, Z_1, Z_2, \ldots) \pmod{\mathfrak{p}},$$

hol most $\zeta_1, \zeta_2, \ldots$ rendre az

$$[F_1 F_2 \ldots]_{z_r = Z_r} \equiv 0 \pmod{\mathfrak{p}}$$

congruentia gyökeit, azaz a $\varphi_1^{(i)} Z_1 + \cdots + \varphi_k^{(i)} Z_k$ mennyiségeket jelentik. Minthogy a Z_r-eket megfelelőleg választottuk, e congruentiának most is annyi a p modulus szerint különböző gyöke van, mint a hány egységet tartalmaz foka és minden egyes ζ_i gyökének egy-egy $\varphi_1^{(i)}, \varphi_2^{(i)}, \ldots$ mennyiségrendszer

felel meg. E mellett a $\varphi_r^{(i)}$ mennyiségek e meghatározása a P-ben foglalt törzsideál bármely választásánál *ugyanaz* marad és ha a számítást $\mathfrak{p}$ helyett $\mathfrak{q}$-ra vonatkoztatva végezzük el, ez csak annyiban okozhat különbséget, hogy a conjugált $\varphi_r^{(i)}$ mennyiségek *más sorrendben* lépnek fel.

Az

$$X_1\varphi_1+\cdots+X_k\varphi_k\equiv 0 \pmod{\mathfrak{p}\mathfrak{q}\ldots}$$

congruentiával most már azonos jelentésű az

$$X_1\varphi_1^{(i)}+\cdots+X_k\varphi_k^{(i)}\equiv 0 \pmod{\mathfrak{p}\mathfrak{q}\ldots} \quad (i=1,2,\ldots)$$

congruentiarendszer; ez pedig ismét az

$$X_1\varphi_1^{(i)}+\cdots+X_k\varphi_k^{(i)}\equiv 0 \pmod{\mathfrak{p}}, \quad (i=1,2,\ldots)$$

$$X_1\varphi_1^{(i)}+\cdots+X_k\varphi_k^{(i)}\equiv 0 \pmod{\mathfrak{q}}, \quad (i=1,2,\ldots)$$

. . . . . .

rendszerekkel helyettesíthető; mert hisz $\mathfrak{p}, \mathfrak{q}, \ldots$ *különböző* törzsideálok.

E rendszerek bármelyike, pl. az első $\overline{S}$-sel való szorzás révén átmegy a következőbe:

$$X_1\psi_1(\zeta_i)+\cdots+X_k\psi_k(\zeta_i)\equiv 0 \pmod{\mathfrak{p}} \quad (i=1,2,\ldots)$$

és ez a rendszer ismét a teljesen azonos jelentésű

$$\sum_{(i)}\zeta_i^r\left(X_1\psi_1(\zeta_i)+\cdots+X_k\psi_k(\zeta_i)\right)\equiv 0 \pmod{\mathfrak{p}} \quad (r=1,2,\ldots)$$

rendszerrel helyettesíthető. (Alig szükséges ujból kiemelnünk, hogy itt is csak a $Q\zeta_i$ mennyiségek egész mennyiségek és így ismét a Q valamely hatványával kell szoroznunk, hogy a szó szorosabb értelmében vett congruentiát nyerjünk, azaz hogy egész mennyiségek tulajdonságait fejezzük ki.) Az utolsó rendszer teljesen pótolja a megelőzőt; mert hiszen, ha $|\zeta_i^r|^2$-et ismét Q bizonyos hatványával megszorozzuk, oly egész mennyiség származik, a melynek legnagyobb közös osztója $\mathfrak{p}$-vel ~ 1.

Ámde az utolsó rendszer minden egyes congruentiájának bal oldala a ζ_i-k symmetrikus formája; e rendszer tehát a következő raczionális és egész alakban írható:

$$A_{1r} X_1 + \cdots + A_{kr} X_k \equiv 0 \pmod{P}; \qquad (r=1, 2, \ldots)$$

mert — a mint az magától értetődik — az $[A, x_1, \ldots, x_m]$ tartomány bármely $\mathfrak{p}$-vel osztható formája osztható P-vel is és viszont. Ez azonban lineáris diophantikus egyenletek rendszere az $[A, x_1, \ldots, x_m]$ tartományban és általános megoldása ismeretes módon állítható elő, még pedig — a mint állítottuk — véges sereg alakjában.

Minthogy végre $\mathfrak{p}$-ről csakis azt teszszük fel, hogy ez valamely a P-ben tartalmazott törzsideál, a nyert megoldás ép úgy vonatkozik a $\mathfrak{q}, \mathfrak{r}, \ldots$ ideálokra is és így tehát ez az

$$X_1 \varphi_1 + \cdots + X_k \varphi_k \equiv 0 \pmod{\mathfrak{p}\mathfrak{q} \ldots}$$

congruentiának is általános megoldása.

Evvel azonban most már rendelkezésünkre állanak az összes segédeszközök, a melyek szükségesek, hogy valamely tetszés szerinti genus-tartomány valódi mennyiségeinek alaprendszerét véges számú ismeretes művelet segítségével valóban kiszámíthassuk.

Hogy az ily általános, a mathematika legkülönbözőbb ágait érintő probléma tényleges megoldásánál föllépő számítások hosszadalmasak, az bizonyára előre látható volt. Azonban az algebrai mennyiségek általános arithmetikájának teljes áttekintése mutatja majd, hogy az itt adott módszer, épen azért, mert bizonyos raczionális és egész mennyiségeknek törzsideálokra való felbontásával párhuzamosan halad, az egyetlen természetes módszer, a mely idegen, a dolog lényegéhez nem tartozó segédeszközök alkalmazása nélkül a megvizsgálandó arithmetikai-algebrai képződmények jellemző tulajdonságait elvi alapon kidomborítja.

A genus-tartomány ideális mennyiségeinek alaprendszere.

24. §. Ha $\mu_1, \mu_2, \ldots, \mu_r$ a (Γ) genus-tartomány valódi egész mennyiségeinek alaprendszere, akkor az bizonyos értelemben ugyanazon genus-tartomány ideális mennyiségeire nézve is alaprendszernek tekinthető. Minden ilyen ideális mennyiség, ha azt mint a genus-tartományból származó két egész algebrai forma hányadosát értelmezzük, közvetetlenül úgy írható, hogy nevezője «az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag» egyszersmind raczionális és egész forma, azaz úgy, hogy nevezője valamely az $[A, x_1, \ldots, x_m]$ tartományból származó és — a mint az magától értetődik — primitiv forma legyen. Ha az egész ideális mennyiség ebben az alakban írva a következő:

$$\mathfrak{a} = \frac{\alpha_0 U_{k_0} + \alpha_1 U_{k_1} + \cdots}{E},$$

akkor minden egyes α együttható, mint a $[\Gamma]$ tartományhoz tartozó valódi egész mennyiség az alaprendszer segítségével az

$$\alpha_i = a_{i1}\mu_1 + a_{i2}\mu_2 + \cdots + a_{ir}\mu_r$$

alakra hozható, hol az a mennyiségek az $[A, x_1, \ldots, x_m]$ tartomány formái; ha tehát a μ mennyiségek szerint rendezünk,

$$\mathfrak{a} = \mathfrak{k}_1\mu_1 + \mathfrak{k}_2\mu_2 + \cdots + \mathfrak{k}_r\mu_r,$$

hol a $\mathfrak{k}$-k raczionális és egész ideális mennyiségek, azaz mint az $[A, x_1, \ldots, x_m]$ tartományból származó két formának hányadosai állíthatók elő, a melyekben a nevező primitiv forma.

Valamely genus-tartomány egész ideális mennyiségeinek ezen előállítása azonban még lényegesen egyszerűsíthető és ez ismét egészen új szempontból mutatja, hogy az

ideális mennyiségek associatiója valamely genus-tartomány vizsgálatában mennyire természetes és czélszerű segédeszköz.

A míg ugyanis azon elemek száma, a melyek a genus-tartomány valódi mennyiségeinek valamely alaprendszerébe felveendők, általánosságban nagyobb a genus-tartomány rendszámánál, addig az ideális mennyiségek associatiója után mindig vannak oly alaprendszerek, a melyekben az elemek száma épen n, ha n a genus rendszámát jelenti; legalább is akkor, ha az alaprendszer elnevezést az eddiginél valamivel általánosabb értelemben használjuk. Részletesebben fogalmazva, *mindig van n oly tulajdonságú* $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ *ideális egész mennyiség, hogy a genus-tartomány minden egész ideális mennyisége, mint az* $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ *mennyiségek homogén és lineáris formája állítható elő; még pedig úgy, hogy az együtthatók mindenesetre a genus-tartomány racionális és egész ideális mennyiségei lesznek, ha azokat bizonyos meghatározott — később teljesen kiszámítandó — racionális és egész számmal, d-vel megszorozzuk.*

Az ideális egész mennyiségeknek ez az alaprendszere minden számítás nélkül előállítható a valódi egész mennyiségek alaprendszeréből. Ha ugyanis az utóbbi alaprendszer $\mu_1, \ldots, \mu_r$, továbbá $u_1, \ldots, u_r$ új határozatlanok és végre

$$\mathfrak{g} = \mu_1 u_1 + \cdots + \mu_r u_r,$$

akkor egyszerűen

$$1, \mathfrak{g}, \mathfrak{g}^2, \ldots, \mathfrak{g}^{n-1}$$

a genus-tartomány ideális egész mennyiségeinek az épen megadott értelemben vett alaprendszere.*

* Az itt használt és az összeadás közönséges törvényének is alávetett ideális mennyiségek bevezetésével a felállított tétel fogal-

Mielőtt azonban az általános arithmetika e leglényegesebb alaptételének bebizonyítására áttérnénk, még néhány egyszerű megjegyzést kell előre bocsátanunk.

A $\mathfrak{g}$ mennyiséget a következőkben *a genus-tartomány alapmennyiségének* vagy *alapformájának* nevezzük. Képezésénél fogva, ha benne $u_1, \ldots, u_r$ helyébe az $[A, x_1, \ldots, x_m]$ tartomány tetszés szerinti mennyiségeit teszszük és csakis ilyeneket, akkor a genus-tartomány összes valódi mennyiségeit szolgáltatja. Közvetetlenül belátható, hogy $\mathfrak{g}$ egység. A $\mathfrak{g}$ mennyiség ugyanis az $\mu_1, \ldots, \mu_r$ mennyiségek legnagyobb közös osztója és minthogy az

$$1 = \mu_1 c_1 + \cdots + \mu_r c_r$$

egyenletnek is fenn kell állania, e legnagyobb közös osztó szükségképen osztója lesz az 1-nek.

A $\mathfrak{g}$ mennyiség n-edrendű mennyiség, mert a

$$\mathrm{Nm.}(z - \mathfrak{g}) = 0$$

egyenlet, a melyet kielégít, irreducibilis egyenlet tartozik lenni; mert irreducibilis még akkor is, ha az u-kat úgy választjuk, hogy $\mathfrak{g}$ n-edrendű valódi egész mennyiség legyen. A $\mathfrak{g}_1, \ldots, \mathfrak{g}_n$, számra nézve n conjugált mennyiség e szerint mind különböző.

mazása és bebizonyítása különösen egyszerűen alakúl; a KRONECKER-féle Festschrift megfelelő fejtegetései a 25. §-ban találhatók.

Magától értetődik, hogy a d szám hozzácsatolásának kérdése csakis az absolut egész mennyiségek vizsgálatára vonatkozik; mert relativ egész mennyiségek esetében minden közönséges raczionális szám az egységgel æquivalensnek tekintendő.

Az $[A; x_1, \ldots, x_m] = [1]$ esetre, azaz az algebrai számok elméletére vonatkozólag ezt a kérdést elegáns speciális módszerek segítségével HENSEL K. intézte el. (Untersuchung der Fundamentalgleichung einer Gattung stb. Journal f. r. u. a. Math. CXIII. k.). Ekkor az $1, \mathfrak{g}, \ldots, \mathfrak{g}^{n-1}$ a szó szorosabb értelmében is alaprendszer; azaz *d egy*-nek vehető.

A

$$\mathrm{Nm.}(z-\mathfrak{g})=0$$

egyenlet, a mely bizonyos tekintetben a genus-tartomány összes mennyiségeit — a valódiakat és a szükebb értelemben vett ideálisokat is — magában foglalja, *a genus alapegyenlete.*

Az alapegyenlet discriminánsa, $\mathfrak{D}$ közvetetlenül ismeretes és magától értetődik, hogy ez a

$$\mathfrak{D}=P_1 \dots P_r E$$

alakban írható, a hol $P_1, \dots, P_r$ az $[A, x_1, \dots, x_m]$ tartomány egyenlő vagy különböző törzsformái és E az u határozatlanoknak e tartományból származó primitiv formája. Így tehát

$$\mathfrak{D} \sim P_1 \dots P_r$$

Hogy valamely $\mathfrak{a}$ ideális egész mennyiségre nézve oly

$$\mathfrak{a}=\mathfrak{r}_0 \mathfrak{g}^{n-1}+\mathfrak{r}_1 \mathfrak{g}^{n-2}+\dots+\mathfrak{r}_{n-1}$$

azonosság állhasson fenn, melyben az $\mathfrak{r}$-ek raczionális ideális mennyiségeket jelentenek, szükséges, hogy ez az azonosság az n conjugált genus-tartományban egyaránt érvényes legyen. Ha tehát $\mathfrak{a}$-nak n conjugált értéke rendre $\mathfrak{a}_1, \dots, \mathfrak{a}_n$, akkor az $\mathfrak{r}$ mennyiségek meghatározására az

$$\mathfrak{a}_i=\mathfrak{r}_0 \mathfrak{g}_i^{n-1}+\mathfrak{r}_1 \mathfrak{g}_i^{n-2}+\dots+\mathfrak{r}_{n-1} \quad (i=1, 2, \dots, n)$$

feltételi egyenletek szolgálnak, a melyekből az $\mathfrak{r}$ mennyiségeknek

$$\mathfrak{r}_j=\frac{\mathfrak{k}_j}{\mathfrak{D}}$$

egyértelmű meghatározása származik, hol a $\mathfrak{k}_j$ mennyiségek, minthogy az $\mathfrak{a}_i$-k egészek, raczionális és egész ideális mennyiségek.

A bebizonyítandó tétel már most azt mondja, hogy az így meghatározott $\mathfrak{k}_j$ mennyiségek d-vel megszorozva az $\mathfrak{a}$ mennyiségek bármely választása mellett mindig $\mathfrak{D}$-vel oszt-

hatók. Tételünk tehát a következő módon is kimondható: Valamely

$$\mathfrak{k}_0 \mathfrak{g}^{n-1} + \mathfrak{k}_1 \mathfrak{g}^{n-2} + \cdots + \mathfrak{k}_{n-1}$$

alakú mennyiség csak akkor osztható $\mathfrak{D}$-vel, ha a $d\mathfrak{k}_0, d\mathfrak{k}_1, \ldots$ raczionális és egész ideális mennyiségek mindegyike osztható $\mathfrak{D}$-vel.

25. §. A most kimondott tételt, mint közvetetlenül látszik, magában foglalja a következő egyrészt egyszerűbb, másrészt általánosabb tétel:

Ha $\mathfrak{k}_0, \ldots, \mathfrak{k}_{n-1}$ *raczionális és egész ideális mennyiségek és* $\mathfrak{g}$ *a genus-tartomány alapmennyisége, akkor*

$$\mathfrak{k}_0 \mathfrak{g}^{n-1} + \mathfrak{k}_1 \mathfrak{g}^{n-2} + \cdots + \mathfrak{k}_{n-1}$$

csak akkor lehet az $[A, x_1, \ldots, x_m]$ *tartomány valamely P törzsformájával osztható, ha a* $d_P\mathfrak{k}_0, d_P\mathfrak{k}_1, \ldots$ *mennyiségek mindegyike ily tulajdonságú.*

Relativ egész mennyiségek esetére $d=1$*-nek veendő; ép így az absolut egész mennyiségek elméletében minden valódi törzsforma, valamint minden oly természetes törzsszám esetére is, a melyet nem tartalmaz egy időben mint osztót* $(n-2)!$ *és az alapegyenlet discriminánsa. Ha az utóbbi esetben* $\mathfrak{D}$ *pontosan* p^a*-val osztható, akkor elegendő felvenni, hogy* $d_p = p^{e(\frac{a}{2})}$*, hol* $e(\frac{a}{2})$ *a legnagyobb* $\frac{a}{2}$*-ben tartalmazott egész számot jelenti.*

E bizonyítás elve Kronecker-től* származik.

A tartomány bármely egész ideális mennyisége, $\mathfrak{a}$ ily alakban írható: $\mathfrak{h}_1\mu_1 + \mathfrak{h}_2\mu_2 + \cdots + \mathfrak{h}_r\mu_r$. Két konjugált $\mathfrak{a}_i$ és $\mathfrak{a}_j$ mennyiség különbségére vonatkozólag akkor

$$\mathfrak{a}_i - \mathfrak{a}_j = \mathfrak{h}_1(\mu_{1i} - \mu_{1j}) + \cdots + \mathfrak{h}_r(\mu_{ri} - \mu_{rj}).$$

A megfelelő konjugált alapmennyiségek különbsége,

$$\mathfrak{g}_i - \mathfrak{g}_j = (\mu_{1i} - \mu_{ij})u_1 + \cdots + (\mu_{ri} - \mu_{rj})u_r,$$

* Festschrift, 25. §.

tehát nem egyéb, mint a $\mu_{1i}-\mu_{1j}, \ldots, \mu_{ri}-\mu_{rj}$ mennyiségek legnagyobb közös osztója. Innen következik, hogy $\alpha_i-\alpha_j$ *mindig osztható* $\vartheta_i-\vartheta_j$*-vel**.

Ha már most $\mathfrak{f}(\vartheta)=\mathfrak{f}_0\vartheta^s+\mathfrak{f}_1\vartheta^{s-1}+\cdots+\mathfrak{f}_s$ osztható P-vel, akkor az utolsó segédtétel szerint

$$\frac{\mathfrak{f}(\vartheta_i)-\mathfrak{f}(\vartheta_j)}{P(\vartheta_i-\vartheta_j)}$$

egész mennyiség, vagy, részletesen kiírva:

$$\sum_{h=0}^{s-2}\mathfrak{f}_h(\vartheta_i^{s-h-1}+\vartheta_j\vartheta_i^{s-h-2}+\cdots+\vartheta_j^{s-h-1})+\mathfrak{f}_{s-1} \qquad (1)$$

osztható P-vel. Itt j helyébe rendre minden szám tehető 1-től n-ig, az i kivételével

Tekintetbe véve, hogy

$$\Sigma\vartheta_j^k=S_k-\vartheta_i^k,$$

hol $S_1, \ldots, S_k$ az $[A, x_1, \ldots, x_m]$ tartományból származó formák, ez az összeg, mely természetesen egész és P-vel osztható, a következő:

$$\sum_{h=0}^{s-2}\mathfrak{f}_h((n-s+h)\vartheta_i^{s-h-1}+S_1\vartheta_i^{s-h-2}+\cdots+S_{s-h+1})+(n-1)\mathfrak{f}_{s-1}.$$

Ez a kifejezés pedig nem más, mint

$$(n-s)\mathfrak{f}_0\vartheta_i^{s-1}+\mathfrak{f}_1'\vartheta_i^{s-2}+\cdots \qquad (2)$$

Ha ezt az eljárást ismételten alkalmazzuk, végül azon eredményhez jutunk, hogy $(n-s)\ldots(n-2)\mathfrak{f}_0$ szintén osztható P-vel. Ha tehát a *relativ egész mennyiségek* elméletében maradunk, hol minden szám ~ 1, végül $\mathfrak{f}_0$-nak is P-vel oszthatónak kell lennie.

Az *absolut egész* algebrai mennyiségek arithmetikai elméletében végeredményünk megtagadja a szolgálatot, ha P az $(n-2)!$-ban osztóként szereplő természetes törzsszám, p.

* Evvel a tárgyalás át van téve a $[\Gamma]$ tartományból a megfelelő GALOIS-féle tartományba, a mi azonban annak eldöntésére, hogy valamely mennyiség egész-e, teljesen közömbös.

Ez esetben jegyezzük meg, hogy, ha

$$\mathfrak{k}_0 \mathfrak{g}_i^s + \mathfrak{k}_1 \mathfrak{g}_i^{s-1} + \cdots + \mathfrak{k}_s$$

osztható $p^{e(\frac{a}{2})+1}$-nel és $\mathfrak{D}$ pontosan p^a-t tartalmazza, akkor a determinánsokra vonatkozó elemi tételek szerint $\mathfrak{k}_i^2 \mathfrak{D}$-nek oszthatónak kell lennie $p^{2e(\frac{a}{2})+2}$ és így $a < 2e(\frac{a}{2})+2$ folytán $\mathfrak{k}_i^2$, tehát $\mathfrak{k}_i$ is osztható p-vel.

Evvel még nincs kizárva, hogy ily törzsszámra vonatkozólag is elegendő már $d=1$. Ha nem elegendő, akkor azt mondjuk, hogy ezen törzsszám *nem szabályos*. Az elmélet felépítésére rendkívül fontos volna annak eldöntése, hogy léteznek-e egyáltalában bizonyos genus-tartományokban ilyen nem szabályos törzsszámok. Hogy ezen hiány mellett is teljesen bebizonyíthassuk később a *kritikus törzsformákra* vonatkozó alaptételt, hozzácsatoljuk még ezekhez a következő fejtegetéseket.

Legyen ismét $\mathfrak{k}(z)$ (fokszáma: $s \leqq n-1$) oly tulajdonságú forma, hogy $\mathfrak{k}(\mathfrak{g}_i)$ osztható a nem szabályos p törzsszámmal, a nélkül, hogy a $\mathfrak{k}_0, \mathfrak{k}_1, \ldots$ együtthatókra ez beállana. Legyen az alapegyenlet $F(z)=0$ és bontsuk fel $F(z)$-t æqu. mod. p, vagy a mi itt ugyanazt jelenti, mod. p irreducibilis tényezőire:

$$F(z) \equiv F_1(z)^{a_1} \ldots F_r(z)^{a_r} \pmod{p}.$$

Legyen hasonlóképen

$$\mathfrak{k}(z) \equiv F_1(z)^{b_1} \ldots F_r(z)^{b_r} G_1(z)^{c_1} \ldots \pmod{p},$$

hol azon esetre, midőn $\mathfrak{k}(z)$ nem osztható $F_1(z)$-vel mod. p, $b_1 = 0$ teendő.

Ha most $z = \mathfrak{g}_i$-t helyettesítünk, akkor, minthogy a feltétel szerint $\mathfrak{k}(\mathfrak{g}_i) \equiv 0 \pmod{p}$,

$$F_1(\mathfrak{g}_i)^{a_1} \ldots F_r(\mathfrak{g}_i)^{a_r} \equiv 0 \pmod{p},$$

$$F_1(\mathfrak{g}_i)^{b_1} \ldots F_r(\mathfrak{g}_i)^{b_r} G_1(\mathfrak{g}_i)^{c_1} \ldots \equiv 0 \pmod{p}.$$

A p minden törzsideáljának elő kell tehát mint osztónak fordúlnia az $F_1(\mathfrak{g}_i) \ldots F_r(\mathfrak{g}_i)$ mennyiségek valamelyikében; és e szerint $G_1(\mathfrak{g}_i), \ldots$ nem lehet osztható e törzsideálok egyi-

kével sem, különben G_1 és pl. F_j resultánsának is p-vel oszthatónak kellene lennie. Minthogy azonban F_j és G_1 mod. p irreducibilis és nem æquivalens formák, azért e resultáns p-vel nem osztható mennyiség. És így már:

$$F_1(\mathfrak{g}_i)^{b_1} \dots F_r(\mathfrak{g}_i)^{b_r} \equiv 0 \pmod{p}.$$

Ha tehát oly $\mathfrak{k}(z)$ formát választunk, melynek megvan a kivánt tulajdonsága és a mellett z-ben a lehető legalacsonyabb fokú, akkor ez egy G_1 tényezőt sem tartalmazhat. Evvel azon fontos eredményhez jutottunk, hogy, *ha p nem szabályos törzsszám, akkor ennek oly* $\mathfrak{k}(z)$ *forma felel meg, mely* mod. p *az* $F(z)$ *osztója*

Ha ezek után

$$F(z) \equiv \mathfrak{k}(z) K(z) \pmod{p},$$

jelöljük továbbá a $\mathfrak{k}(z)=0$ egyenlet gyökeit $\alpha_1, \dots, \alpha_s$-sel, $K(z)=0$ gyökeit $\beta_1, \dots, \beta_{n-s}$-sel. Törzsszám-modulussal biró congruentiákra vonatkozó és már e fejezet 22. §-ában említett tételek szerint a

$$\mathfrak{g}_1, \mathfrak{g}_2, \dots, \mathfrak{g}_n$$

és

$$\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_{n-s}$$

sorozatok mod. $\mathfrak{p}$ megegyeznek, ha $\mathfrak{p}$ a p valamely törzsideálját jelenti. Visszatérve ismét (1)-re, nyerjük, hogy

$$\sum_{h=0}^{s-2} \mathfrak{k}_h (\beta_1^{s-h-1} + \alpha_1 \beta_1^{s-h-2} + \dots + \alpha_i^{s-h-1}) + \mathfrak{k}_{s-1} \equiv 0 \pmod{\mathfrak{p}}.$$

Ha az $i=1,\dots,s$ helyettesítésével keletkező congruentiákat összeadjuk és tekintetbe veszszük a

$$\sum_{i=1}^{s} \alpha_i^r = S_r$$

jelöléssel

$$k_0 S_r + \mathfrak{k}_1 S_{r-1} + \dots + r\mathfrak{k}_r = 0 \quad (r=1,\dots,s-1)$$

alakban írható Newton-Girard-féle formulákat, akkor nyerjük, hogy

$s\mathfrak{k}_0\beta_1^{s-1}+(s-1)\mathfrak{k}_1\beta_1^{s-2}+(s-2)\mathfrak{k}_2\beta_1^{s-3}+\cdots\equiv 0 \pmod{\mathfrak{p}}$,

a mely congruentia a $\mathfrak{k}(\beta_1)\equiv 0 \pmod{\mathfrak{p}}$ congruentiával összekapcsolva közvetetlenül mutatja, hogy $\mathfrak{k}(z)$ *discriminánsa osztható p-vel.*

Jegyezzük meg végre még, hogy *raczionális müveletek véges sorából álló oly eljárással rendelkezünk, mely egy adott genus-tartomány nem szabályos törzsszámainak meghatározására képesit*, ha egyáltalában léteznek ilyenek. Csak $F(z)$ osztóinak sorozatát kell felírnunk mod. p és megvizsgálnunk, hogy van-e ezek közt olyan $\mathfrak{k}(z)$ osztó, melyre vonatkozólag

$$\frac{\mathfrak{k}(\mathfrak{g})}{p}$$

egész mennyiség.

Az egész mennyiségek felbontása törzsideálokra.

26. §. Az épen bebizonyított alaptétel megadja most már az összes segédeszközöket arra, hogy az adott genus-tartomány bármely a 0-tól különböző egész mennyiségét, a mennyiben nem egység, jól értelmezett eljárás segítségével valóban mint törzsmennyiségek szorzatát állítsuk elő. Ez az eljárás egyszersmind pontosabb betekintést enged a kérdéses arithmetikai képződmények szerkezetébe, a mennyiben ezt a felbontást bizonyos tekintetben az $[A, x_1, \ldots, x_m]$ tartományból származó formák tartományában leképezi.

Minthogy minden egész mennyiség osztja normáját, e norma pedig az $[A, x_1, \ldots, x_m]$ tartomány valamely formájával æquivalens és végre minden ilyen forma mint ugyanilyen törzsformák szorzata írható; magától értetődik, hogy elegendő, ha csakis az $[A, x_1, \ldots, x_m]$ tartomány P törzsformáinak felbontását végezzük el valóban. Az erre vonat-

kozó tények oly egyszerűek, hogy legjobb lesz, ha a végleges tételt végérvényes fogalmazásában előrebocsátjuk*.

Legyen $F(z)=0$ *a genus-tartomány alapegyenlete,* P *az* $[A, x_1, \ldots, x_m]$ *tartomány valamely törzsmennyisége az esetleg létező nem szabályos törzsszámok kivételével***; *bontsuk fel azután* $F(z)$*-t a* P *aequivalentia-modulusra vonatkozólag irreducibilis tényezőire*:

$$F(z)\sim F_1(z)^{a_1} F_2(z)^{a_2} \ldots F_r(z)^{a_r} \text{ (æqu. mod. } P),$$

hol tehát $a_1 l_1+a_2 l_2+\cdots+a_r l_r=n$, *ha* l_i *az* $F_i(z)$ *forma* z*-re vonatkozó foka.*

Akkor $F_i(\mathfrak{g})$ *és* P *legnagyobb közös osztója törzsideál (nem is* ~ 1*) és, minthogy* $F_i(\mathfrak{g})$ *az* u *határozatlanoknak homogén formája, egyenesen a* $P+F_i(\mathfrak{g})$ *alakban írható. A* P *törzsideálokra való felbontását ezután a*

$$P\sim(P+F_1(\mathfrak{g}))^{a_1}(P+F_2(\mathfrak{g}))^{a_2}\ldots(P+F_r(\mathfrak{g}))^{a_r} \qquad (1)$$

aequivalentia szolgáltatja.

Végül (l. a 27. §-t) $P+F_i(\mathfrak{g})$ l_i*-edfokú törzsideál, azaz*

$$\text{Nm.}(P+F_i(\mathfrak{g}))\sim P^{l_i}.$$

Az e tételben összefoglalt tények helyességének kimutatásánál mindenekelőtt vegyük figyelembe azt a körülményt, hogy $F(z)$-nek a P æquivalentia-modulus szerint történt felbontásából közvetetlenül a

$$\overline{Q}F(z)=QF_1(z)^{a_1} F_2(z)^{a_2}\ldots F_r(z)^{a_r}-PH(z)$$

* Hogy mily helyet foglal el az itt kimondott tétel az irodalomban — különösen KRONECKER tárgyalásával szemben — az még részletesebb fejtegetést igényel; erre nézve l. a 29. §-t.

** A nem szabályos törzsszámok fölbontását utólag a 28. §-ban végezzük. Lehetett volna ugyan, a két esetet egységes tárgyalásban egyesíteni; de tekintettel a geometriai és függvénytani alkalmazásokra, — a mikor a második eset egyáltalában elő sem fordúl — czélszerűnek mutatkozott, ezen egyszerűbb meggondolásokat előre bocsátani, a mennyiben ezek kevesebb segédeszközt igényelnek.

azonosság* következik, hol Q és $\overline{Q}$ az $[A, x_1, \ldots, x_m]$ tartomány oly formái, a melyeknek legnagyobb közös osztójuk P-vel ~ 1, és H e tartományból származó olyan forma, a melynek z-re vonatkozó foka nem éri el n-t. Ha ebben az azonosságban z helyébe a $\mathfrak{g}$-t teszszük, végre

$$QF_1(\mathfrak{g})^{a_1} F_2(\mathfrak{g})^{a_2} \ldots F_r(\mathfrak{g})^{a_r} = PH(\mathfrak{g}). \qquad (2)$$

Először is látjuk, hogy $P+F_i(\mathfrak{g})$ *és* $P+F_j(\mathfrak{g})$ *legnagyobb közös osztója szükségképen* ~ 1, *ha* $i \neq j$. E legnagyobb közös osztó ugyanis $F_i(\mathfrak{g})$, $F_j(\mathfrak{g})$ és P közös osztója volna és ha R az $F_i(z)$ és $F_j(z)$ formák z szerint vett resultánsát jelenti, egyszersmind az R és P közös osztója is. Ámde P irreducibilis forma és R a 20. §. szerint nem osztható P-vel, tehát $(R, P) \sim 1$ és, a mint állítottuk, $(P+F_i(\mathfrak{g}), P+F_j(\mathfrak{g})) \sim 1$.

Ha továbbá

$$\mathfrak{k}(\mathfrak{g}) = \mathfrak{k}_0 \mathfrak{g}^s + \cdots + \mathfrak{k}_s,$$

hol $\mathfrak{k}_0, \ldots, \mathfrak{k}_s$ *ismét az* $[A, x_1, \ldots, x_m]$ *tartományból származó formákat jelentenek és* $s < l_i$, *akkor* $\mathfrak{k}(\mathfrak{g})$ *csak akkor lehet osztható* $P+F_i(\mathfrak{g})$*-vel, ha* $\mathfrak{k}(\mathfrak{g})$ *osztható* P*-vel; tehát, ha az egyes* $\mathfrak{k}_0, \ldots, \mathfrak{k}_s$ *együtthatók osztható* P*-vel.*

Ha ugyanis $\mathfrak{k}(\mathfrak{g})$ osztható $P+F_i(\mathfrak{g})$-vel, akkor a P-vel osztható $F_1(\mathfrak{g})^{a_1} \ldots F_r(\mathfrak{g})^{a_r}$ szorzatban $F_i(\mathfrak{g})$ helyettesíthető $\mathfrak{k}(\mathfrak{g})$-vel a nélkül, hogy a P-vel való oszthatósága megszünnék. Ekkor azonban ez a szorzat oly $\mathfrak{K}(\mathfrak{g})$ kifejezést szolgáltat, a melynek $\mathfrak{g}$-re vonatkozó foka nem éri el n-t és így tehát csak akkor lehet osztható P-vel, ha $\mathfrak{g}$ minden egyes hatványának együtthatója is P-vel osztható. Ámde $\mathfrak{g}$ legmagasabb hatványának kérdéses együtthatója $\mathfrak{k}_0^{a_i}$ és oly mennyiségek szorzata, a melyeknek legnagyobb közös osztójuk P-vel ~ 1. E szerint tehát $\mathfrak{k}_0$ osztható P-vel. Ekkor azonban

$$\mathfrak{k}_1 \mathfrak{g}^{s-1} + \cdots + \mathfrak{k}_s$$

* Mellesleg megjegyezzük, hogy $Q=1$.

is osztható $P+F_i(\mathfrak{g})$-vel; tehát ismételve az épen részletezett következtetést, azt találjuk, hogy $\mathfrak{k}_1$ osztható P-vel s í. t.

Ebből továbbá következik, hogy $P+F_i(\mathfrak{g})$ *valódi irreducibilis mennyiség (törzsmennyiség).* Az semmi esetre sem lehetséges, hogy $P+F_i(\mathfrak{g}) \sim 1$; mert hisz különben az $F_1(\mathfrak{g})^{a_1} \ldots F_r(\mathfrak{g})^{a_r}$ szorzat az $F_i(\mathfrak{g})^{a_i}$ tényező elhagyása után is osztható volna P-vel, pedig ha ez úgy van, olyan kifejezéssel van dolgunk, a melynek $\mathfrak{g}$-re vonatkozó foka nem éri el n-t és a melyben $\mathfrak{g}$ legmagasabb hatványának együtthatója nem osztható P-vel.

Ha már most $P+F_i(\mathfrak{g})$ több törzsmennyiség szorzata, pl.

$$P+F_i(\mathfrak{g}) \sim \mathfrak{p}\mathfrak{q},$$

hol $\mathfrak{p}$ *és* $\mathfrak{q}$ az æquivalentia értelmében az 1-től különbözők és $\mathfrak{p}$ törzsideál. De ekkor, minthogy minden egész ideális mennyiség ilyen módon előállítható,

$$dE\mathfrak{p} = \mathfrak{k}_0 \mathfrak{g}^{n-1} + \mathfrak{k}_{n-1} \mathfrak{g}^{n-2} + \cdots + \mathfrak{k}_{n-2}$$

volna, hol E, $\mathfrak{k}_0, \ldots, \mathfrak{k}_{n-1}$ az $[A, x_1, \ldots, x_m]$ tartományból származó formák és E azonfelül még primitiv forma. Ha $F_i(z)$-ben z legmagasabb hatványának együtthatója Q_i, és így tehát Q_i az $[A, x_1, \ldots, x_m]$ tartomány olyan formája, a melynek legnagyobb közös osztója P-vel ~ 1, akkor a közönséges osztási eljárást alkalmazva, azt találjuk, hogy

$$dQ_i^{k'} E\mathfrak{p} = F_i(\mathfrak{g})\,\mathfrak{K}'(\mathfrak{g}) + \mathfrak{k}'_0 \mathfrak{g}^{l_i-1} + \cdots + \mathfrak{k}'_{l-1}.$$

E szerint $\mathfrak{k}'_0 \mathfrak{g}^{l_i-1} + \cdots$ osztható $\mathfrak{p}$-vel. Az $F_i(z)$ és $\mathfrak{k}'_0 z^{l_i-1} + \cdots$ formák resultánsa mod. P e szerint eltünik, és e szerint, minthogy $F_i(z)$ irreducibilis æqu. mod. P már a $\mathfrak{k}'_0$, $\mathfrak{k}'_1$ együtthatók is $\equiv 0$ (mod. P) lesznek. Ebből következik, hogy

$$Q_i^{k'} E\mathfrak{p} \equiv F_i(\mathfrak{g})\,\mathfrak{K}'(\mathfrak{g}) \text{ (mod. } P).$$

Ez azt jelentené, hogy $\mathfrak{p}$ osztható $\mathfrak{p}\mathfrak{q}$-val, a mi ismét csak akkor lehetséges, ha a feltevés ellenére $\mathfrak{q} \sim 1$. Így tehát $P+F_i(\mathfrak{g})$ valóban irreducibilis mennyiség.

Magától értetődik továbbá, hogy $F_i(\mathfrak{g})$ osztható a

$P+F_i(\mathfrak{g})$ törzsideállal; ámde, *ha* $a_i>1$, $F_i(\mathfrak{g})$ *sohasem lehet osztható* $(P+F_i(\mathfrak{g}))^2$*-tel.* $F_i(\mathfrak{g})$ semmi esetre sem osztható valamely a P-ben tartalmazott és a $P+F_i(\mathfrak{g})$-től különböző törzsideállal; mert hisz különben $P+F_i(\mathfrak{g})$ e két különböző törzsideállal volna osztható és így tehát nem lehetne törzsideál. Ha azonban $F_i(\mathfrak{g})$ a $(P+F_i(\mathfrak{g}))^2$-tel volna osztható, akkor P nem lehetne osztható $(P+F_i(\mathfrak{g}))^2$-tel, mert különben P és $F_i(\mathfrak{g})$ legnagyobb közös osztójának, azaz a $P+F_i(\mathfrak{g})$ törzsideálnak is oszthatónak kellene lennie $(P+F_i(\mathfrak{g}))^2$-tel. Ebben az esetben tehát

$$F_i(\mathfrak{g})\sim(P+F_i(\mathfrak{g}))^e\mathfrak{q}_1,$$
$$P\sim(P+F_i(\mathfrak{g}))\mathfrak{q}_2$$

és $(\mathfrak{q}_1, P)\sim 1$, a hol még ki kell mutatnunk, hogy e szükségképen 1. Ebben az esetben ugyanis nem csupán

$$F_1(\mathfrak{g})^{a_1}\ldots F_i(\mathfrak{g})^{a_i}\ldots F_r(\mathfrak{g})^{a_r},$$

hanem, ha a_i helyébe az 1-et teszszük, már

$$F_1(\mathfrak{g})^{a_1}\ldots F_i(\mathfrak{g})\ldots F_r(\mathfrak{g})^{a_r}$$

is osztható lesz P-vel. A P-ben tartalmazott és $P+F_i(\mathfrak{g})$-től különböző törzsideálokat ez nem érinti, minthogy nincsen az 1-től különböző közös osztójuk $F_i(\mathfrak{g})$-vel; a $P+F_i(\mathfrak{g})$ törzsideál azonban, a melyet P csak egyszer tartalmaz, már az $F_i(\mathfrak{g})$ osztója. *Ekkor végre szükségképen* $a_i=1$. Ellenkezőleg, habár a fentebbi második szorzat osztható P-vel, $\mathfrak{g}$-re vonatkozó foka kisebb volna n-nél, míg benne a $\mathfrak{g}$ legmagasabb hatványának együtthatója nem osztható P-vel.

A P mennyiségnek az e § elején említett felbontása most már az épen tárgyalt részlet-tételeknek egyszerű következménye.

Az $F(z)$-nek a P æquivalentia-modulus szerint történő felbontásából eredő azonosság közvetetlenül mutatja, hogy P az

$$F_1(\mathfrak{g})^{a_1}\ldots F_i(\mathfrak{g})^{a_i}\ldots F_r(\mathfrak{g})^{a_r}$$

osztója; a miből rögtön látni, hogy P a

$$P+F_1(\mathfrak{g}), \ldots, P+F_i(\mathfrak{g}), \ldots, P+F_r(\mathfrak{g})$$

törzsideálok valamely hatványszorzatával æquivalens. Ha $a_i=1$, akkor $F_i(\mathfrak{g})$ lehet ugyan esetleg a $P+F_i(\mathfrak{g})$ valamely magasabb hatványával osztható; de P ekkor csakis $P+F_i(\mathfrak{g})$-vel osztható, és nem osztható $(P+F_i(\mathfrak{g}))^2$-tel. Ebben az esetben tehát P megfelelő osztója valóban $(P+F_i(\mathfrak{g}))^{a_i}$.

Ha pedig $a_i>1$, akkor P megfelelő osztója okvetetlenül $(P+F_i(\mathfrak{g}))^{b_i}$ alakú és $b_i \leqq a_i$. Ha azonban $b_i<a_i$ volna, akkor már az

$$F_1(\mathfrak{g})^{a_1} \ldots F_i(\mathfrak{g})^{b_i} \ldots F_r(\mathfrak{g})^{a_r}$$

kifejezésnek is oszthatónak kellene lennie P-vel. Ez azonban lehetetlen; mert az épen felírt szorzat olyan kifejezés, a melynek $\mathfrak{g}$-re vonatkozó foka nem éri el n-t és a melyben a $\mathfrak{g}$ legmagasabb hatványának együtthatója nem osztható P-vel.

Evvel tehát kimutattuk, hogy P-nek az (1) alatt felállított törzsideálokra való felbontása helyes.

27. §. Csatlakozva az algebrai számok elméletében használatos kifejezésmódhoz, *az* $[A, x_1, \ldots, x_m]$ *tartomány oly törzsformáját, a mely az adott genus-tartomány valamely törzsideáljának négyzetével osztható, a genus kritikus törzsformájának nevezzük*

Könnyen igazolható akkor, hogy az $[A, x_1, \ldots, x_m]$ *tartománynak az alapegyenlet discriminánsában tartalmazott törzsformái és csak ezek a genus kritikus törzsformái*.*

* Az algebrai számok esetére Dedekind R. bizonyította be először ezt a tételt egyik nagy dolgozatában. («Über die Discriminanten endlicher Körper». Abhandl. d. Göttinger Ges. d. Wiss. XXIX. köt.). Ezen értekezés mélyreható, nehéz módszerei alig nélkülözhetők, ha úgy — mint az ott történik — a határozatlan mennyiségek bevezetését elvileg mellőzni akarjuk.

Kronecker módszereinek segítségével fentebb idézett értéke-

A tétel akkor is érvényes, ha P nem szabályos törzsszám. Az ezen esetre vonatkozó bizonyítást a § végén pótoljuk. Minden más esetben az, hogy P kritikus törzsforma-e, közvetetlenül kitünik, mihelyt $F(z)$-t a P æquivalentia-modulus szerint felbontjuk. P ugyanis akkor és csak akkor kritikus törzsforma, ha e felbontásnál többszörös tényezők lépnek fel, vagyis akkor, ha az alapegyenlet discriminánsa osztható P-vel. Ha P természetes törzsszám, akkor a keresett feltételnek ez az utóbbi fogalmazása közvetetlenül világos; de könnyen belátható ennek helyes volta akkor is, ha P határozatlanokat tartalmaz, pl. x_1-et. Hiszen e felbontás az $[F(z)]_\xi$ felbontásából adódik ki, a hol ξ a $P(x_1)=0$ egyenlet gyökét jelenti. Többszörös tényezők akkor és csak akkor fordúlnak elő, ha $[\text{Dscr. } F(z)]_\xi=0$, vagyis, ha Dscr. $F(z)$ osztható P-vel.

Az az eset, midőn P csupán $P+F_i(\mathfrak{g})$ első hatványával osztható, e szerint az *általános* esetnek tekintendő; erre az esetre vonatkozik a következő fontos megjegyzés. Épen akkor, midőn $a_i=1$, lehetne $F_i(\mathfrak{g})$ még $(P+F_i(\mathfrak{g}))^2$-tel is osztható; ámde az $F(z)$ forma felbontásában előfordúló $F_i(z)$ forma a nélkül, hogy ez a nyert eredmények érvényességét érintené, felcserélhető bármely oly $\overline{F}_i(z)$ formával, a mely $\equiv F_i(z) (\text{mod. } P)$. Ha tehát $F_i(\mathfrak{g})$ valóban osztható $(P+F_i(\mathfrak{g}))^2$-tel, most $F_i(z)$ helyébe csak az $F_i(z)+Pu_1^n$ formát kell bevezetnünk és evvel oly formát nyerünk, a mely már csak $P+F_i(\mathfrak{g})$-vel osztható, de nem $(P+F_i(\mathfrak{g}))^2$-vel.

A következő vizsgálatokban, a mennyiben ez szükségesnek mutatkoznék, feltételezzük, hogy $F_i(z)$-t már ezen a

zésében HENSEL K. bizonyította be először a teljes tételt ugyancsak az algebrai számok esetére; KRONECKER-nél ugyanis az $(n-2)!$-ben tartalmazott természetes törzsszámok viselkedése még kérdéses maradt.

módon megváltoztattuk, tehát hogy $F_i(\mathfrak{g})$ *nem* osztható $(P+F_i(\mathfrak{g}))^2$-vel.

Visszatérünk már most a

$$\bar{Q}F(z)=QF_1(z)^{a_1}\dots F_i(z)^{a_i}\dots -PH(z)$$

azonosságra. Legyenek

$$\zeta_1, \zeta_2, \dots, \zeta_{l_i}$$

az $F_i(z)=0$ egyenlet gyökei. Ha az épen felírt azonosságban ezeket az értékeket teszszük z helyébe és szorzunk, a következőt nyerjük:

$$\bar{Q}^{l_i}\prod_{j=1}^{l_i}F(\zeta_j)=(-1)^{l_i}P^{l_i}\prod_{j=1}^{l_i}H(\zeta_j).$$

Ámde (a III. fej. 24. §-a szerint) $F(z)$ és $F_i(z)$-nek z szerint vett resultánsára nézve, ha Q_i ismét a z legmagasabb hatványának együtthatója $F_i(z)$-ben,

$$\text{Res.}\,(F(z), F_i(z))=(-1)^{nl_i}Q_i^n\prod_{j=1}^{l_i}F(\zeta_j)=\prod_{j=1}^{n}F_i(z_j),$$

a hol $z_1, \dots, z_n$ az $F(z)=0$ egyenlet gyökeit jelentik és így tehát továbbá

$$=\text{Nm.}\,F_i(\mathfrak{g})$$

úgy, hogy végre Nm. $F_i(\mathfrak{g})$ *oszlható* P^{l_i}*-vel.* Minthogy továbbá $F_i(\mathfrak{g})$ a P-nek csak ezt az egy $P+F_i(\mathfrak{g})$ törzsideálját tartalmazza és csakis $P+F_i(\mathfrak{g})$-vel, de $(P+F_i(\mathfrak{g}))^2$-tel már nem osztható, végre nyerjük, hogy

$$\text{Nm.}\,F_i(\mathfrak{g})\sim\text{Nm.}\,(P+F_i(\mathfrak{g}))\,Q,$$

hol $(P, Q)\sim 1$, és így tehát

$$\text{Nm.}\,(P+F_i(\mathfrak{g}))\sim P^{l_i+e_i},$$

a hol még csak azt kell kimutatnunk, hogy $e_i=0$.

Ez kitünik a 26. §. (2) alatti

$$QF_1(\mathfrak{g})^{a_1}F_2(\mathfrak{g})^{a_2}\dots F_r(\mathfrak{g})^{a_r}=PH(\mathfrak{g})$$

azonosságából. Itt $H(\mathfrak{g})$ P egy törzsideáljával sem osztható; mert a bal oldali szorzat és P a P törzsideáljainak egyenlő hatványait tartalmazzák. Arra az esetre, midőn $a_i>1$, ezt

már előbb bebizonyítottuk; midőn pedig $a_i=1$, épen az F_i-vel congruens formák közül egy megfelelőt választottunk. E szerint $(\text{Nm.}\, H(\mathfrak{g}), P)\sim 1$. Ha csak egyetlen e_i is különböző a 0-tól és — mint az magától értetődik — nem negativ egész szám, akkor a bal oldalon álló kifejezés normája P-nek az n-diknél magasabb hatványával volna osztható. Ez azonban lehetetlen, mert ugyanazt a normát közvetetlenül a $P^n \text{Nm.}\, H(\mathfrak{g})$ kifejezés szolgáltatja.

Így tehát — a mint be kellett bizonyítanunk — $P+F_i(\mathfrak{g})$ *l_i-edfokú törzsideál,* azaz $\text{Nm.}\,(P+F_i(\mathfrak{g}))\sim P^{l_i}$, ha l_i az $F_i(z)$ forma z-re vonatkozó foka.

Végre még bebizonyítandó, hogy, a mennyiben ilyenek léteznek, *a nem szabályos törzsszámok is kritikus törzsszámok.*

Ez esetben van egy legalacsonyabb, s-ed fokú forma $(s\leqq n-1)$, mely oly tulajdonságú, hogy $\mathfrak{f}(\mathfrak{g})$ osztható p-vel. Ez a forma valamelyik $F_i(z)$-nek, — a mint ezt a 25. § végén bebizonyítottuk — legalább négyzetét tartalmazza æqu. mod. p mint tényezőt. De most is $\text{Nm.}\, F_i(\mathfrak{g})$ osztható p^{l_i}-vel; az erre vonatkozó fejtegetések ugyanis függetlenek minden e tárgyalásnál különben használt föltevéstől. E szerint $F_i(\mathfrak{g})$ osztható bizonyos a p-ben foglalt $\mathfrak{p}$, $\mathfrak{q}$, ... törzsideálokkal. De akkor kell, hogy p osztható legyen $\mathfrak{p}^2$, $\mathfrak{q}^2$, ...-tel is; mert különben a

$$F_i(z)\overline{\mathfrak{f}}(z) \equiv \mathfrak{f}(z) \pmod{p}$$

meghatározta $\overline{\mathfrak{f}}(z)$ forma, melynek foka csak $s-l_i$, szintén oly tulajdonságú volna, mint $\mathfrak{f}(z)$; pedig ezt már az illető formák közt legalacsonyabb fokúnak tételeztük föl*.

* Az algebrai számok elméletében $\text{Nm.}\,\mathfrak{p}$ egyszersmind megadja a mod. $\mathfrak{p}$ nem congruens számok számát. Ebből kiindúlva, bebizonyítható, hogy $\text{Nm.}\,(p+F_i(\mathfrak{g}))$ pontosan $\sim p^{l_i}$, tekintet nélkül arra, vajjon p szabályos törzsszám-e, vagy sem. Ebből azután könnyen

28. §. *A genus-tartomány nem szabályos törzsszámainak felbontása* — ha ilyenek léteznek — ugyanezen elvek szerint történhetik, bár a végeredményben nincs meg az az elegáns egyszerűség, melylyel a szabályos törzsszámok felbontási törvényénél találkozunk.

Az

$$F_1(\mathfrak{g})^{a_1} \ldots F_r(\mathfrak{g})^{a_r} \equiv 0 \pmod{p}$$

congruentiából ez esetben is következik, hogy

$$p+F(\mathfrak{g}), \ldots, p+F_r(\mathfrak{g})$$

a p valódi osztói; mert azon észrevétel, hogy $\mathrm{Nm.}(p+F_i(\mathfrak{g})) \sim p^l$ a p-re vonatkozó szűkebb megszorító feltételtől független. Épen így most is

$$(p+F_i(\mathfrak{g}),\ p+F_j(\mathfrak{g})) \sim 1,$$

mert $F_i(z)$ és $F_j(z)$ mod. p irreducibilis és nem æquivalens formák. Végűl szükséges, hogy minden p-ben foglalt törzsideál a $p+F_1(\mathfrak{g}), \ldots$ mennyiségek egyikének osztója legyen. Azt kell tehát már csak bebizonyítanunk, hogy e mennyiségek törzsideálok. Ekkor p-nek felbontása a következő:

$$p \sim (p+F_1(\mathfrak{g}))^{b_1} \ldots (p+F_r(\mathfrak{g}))^{b_r},$$

hol $b_1 \leqq a_1$, s í. t. A $b_1, \ldots, b_r$ kitevők pontos meghatározása véges kisérletsorral történhetik. Csakis azt kell e czélból megvizsgálnunk, hogy a

$$\frac{p}{p_1+F_1(\mathfrak{g})}, \quad \frac{p}{(p+F_1(\mathfrak{g}))^2}, \ldots$$

mennyiségek közül hány egész?

Teljesen elintézzük tehát problémánkat, ha bebizonyítjuk, hogy $p+F_i(\mathfrak{g})$ *törzsideál.* (E bizonyításnál használandó eljárás HENSEL K. egy gondolatát is felhasználja).

következik, hogy ez esetben nem szabályos törzsszámok egyáltalában nem léteznek. (L. erre vonatkozólag K. HENSEL már előbb idézett értekezését, valamint a tárgy részletes kifejtését H. WEBER «Lehrbuch der Algebra» cz. művében.)

Ha nem volna törzsideál és így

$$p+F_i(\mathfrak{g})\sim\mathfrak{pq},$$

hol $\mathfrak{q}$ az æquivalentia értelmében 1-től különböző, akkor régebben bebizonyított tételek alapján meghatározható a genustartománynak oly

$$\alpha\sim\mathfrak{p}\alpha$$

valódi egész mennyisége, hogy $(\alpha, \mathfrak{q})\sim 1$ legyen. Legyen ez az α mennyiség az alaprendszer segítségével a következőképen kifejezve:

$$\alpha=a_1\mu_1+\cdots+a_r\mu_r.$$

Így tehát a $\mathfrak{g}$ alapmennyiség α-ba megy át, ha $u_1, \ldots, u_r$ helyébe $a_1, \ldots, a_r$-et teszünk.

Azon tény, hogy $F_i(\mathfrak{g})$ osztható $\mathfrak{pq}$-val, igaz marad akkor is, ha az $u_1, \ldots, u_r$ határozatlanok helyébe bármily egész mennyiségeket teszünk. Ha $F_i(\mathfrak{g})$-t részletesebben $F_i(\mathfrak{g}, u_1, \ldots, u_r)$-nek írjuk és $u_1, \ldots, u_r$ helyébe $u_1+a_1, \ldots, u_r+a_r$-et teszünk, akkor

$$F_i(\mathfrak{g}+\alpha, u_1+a_1, \ldots, u_r+a_r)\equiv 0 \pmod{\mathfrak{pq}}. \qquad (1)$$

Minthogy azonban $\alpha\equiv 0 \pmod{\mathfrak{p}}$, azért az

$$F_i(z, u_1, \ldots, u_r)\equiv 0 \pmod{\mathfrak{p}},$$
$$F_i(z, u_1+a_1, \ldots, u_r+a_r)\equiv 0 \pmod{\mathfrak{p}}$$

congruentiáknak van közös gyökük. Resultánsuknak tehát mod. $\mathfrak{p}$ és így mod. p is el kell tűnnie. Minthogy azonban $F_i(z)$ irreducibilis mod. p, továbbá a két forma egyenlő fokszámú és végül z^{l_i} együtthatója a második formában is 1, azért világos, hogy

$$F_i(z, u_1+a_1, \ldots, u_r+a_r)\equiv F_i(z, u_1, \ldots, u_r) \pmod{p}. \qquad (2)$$

(1) szerint tehát

$$F_i(\mathfrak{g}+\alpha, u_1, \ldots, u_r)\equiv 0 \pmod{\mathfrak{pq}}, \qquad (3)$$

oly oszthatóság meghatározás, melynek fenn kell maradnia, ha az u-k helyébe tetszőleges egész mennyiségeket teszünk, tehát pl. akkor, ha $u_1=0, \ldots, u_r=0$. Ekkor tehát

$$\alpha^{l_i} \equiv 0 \pmod{\mathfrak{p}\mathfrak{q}}$$

volna, a mi a feltétel szerint lehetetlen, ha $\mathfrak{q}$ az æquivalentia értelmében egy $\mathfrak{p}$-től különböző törzsideált tartalmaz.

E szerint már csak azon eset vizsgálata van hátra, midőn $\mathfrak{q}$ a $\mathfrak{p}$ törzsideál hatványa. Ekkor azonban a feltétel szerint α csak $\mathfrak{p}$-vel osztható és $\mathfrak{p}^2$-tel nem. Így (3) szerint

$$F_i(\mathfrak{g}+\alpha, u_1, \ldots, u_r) \equiv 0 \pmod{\mathfrak{p}^2}.$$

Ha a bal oldali kifejezést most α hatványai szerínt kifejtjük, akkor

$$F_i(\mathfrak{g}) + F_i'(\mathfrak{g})\,\alpha + \frac{1}{2} F_i''(\mathfrak{g})\,\alpha^2 + \cdots \equiv 0 \pmod{\mathfrak{p}^2}.$$

Itt azonban $F_i(\mathfrak{g})$, α^2, α^3, . , . osztható $\mathfrak{p}^2$-tel. Ugyanennek kellene tehát $F_i'(\mathfrak{g})\,\alpha$-ra is beállania, és így végűl

$$F_i'(\mathfrak{g}) \equiv 0 \pmod{\mathfrak{p}}$$

volna. Minthogy azonban $F_i(\mathfrak{g}) \equiv 0 \pmod{\mathfrak{p}}$, azért $F_i(z)$ és $F_i'(z)$ (mod. p) resultánsának el kellene tűnnie és ez $F_i(z)$ irreducibilis volta miatt lehetetlen. Evvel a kérdéses tétel minden részében be van bizonyítva.

29. §. Az e tétel nyújtotta mély belátást, a mely új vizsgálatoknak majdnem kimeríthetetlen forrása, KRONECKER bámulatra méltó intuitiójának köszönjük. Ezen intuitiv fölfödözés érdekét még csak növeli, hogy KRONECKER *tételei leglényegesebb pontjukban helyreigazításra szorúlnak.* KRONECKER eredményei feltétlenűl csak az algebrai számok elméletében érvényesek és az egy változós algebrai függvények elméletében akkor, midőn a számbeli együtthatókat mellőzzük; az általános esetben azonban csak akkor érvényesek, ha valamely természetes törzsszám felbontásáról van szó. Ámde, ha P határozatlanokat tartalmaz, akkor a KRONECKER kijelölte, a P felbontására szolgáló módszer bizonyos esetekben egyenesen *hamis eredményekre vezet.*

KRONECKER-nek ezen érdekes tévedése, úgy látszik,

onnan ered, hogy valamely formának a P modulus szerint történő felbontásánál fellépő irreducibilis formákat a P modulus szerint törzsformáknak tekinti; ez pedig — mint a 19. §-ban kifejtettük — általánosságban *nem* helyes.

Pontosabban fogalmazva, KRONECKER az $F(z)$ formának nem a P æquivalentia-modulus, hanem a P congruentia-modulus szerint való felbontását követeli. Hogy itt tényleges tévedéssel van dolgunk, világosan kitünik a tárgyalás részleteiből, annál is inkább, mert az æquivalentia-modulus bonyolódott fogalom-alkotása a Festschrift-ben egyáltalában nem fordúl elő.

Minthogy itt az algebrai mennyiségek arithmetikai elméletének tulajdonképeni alapja — tehát kiváló fontosságú tárgy — forog szóban, a tényállást egy egyszerű példán még részletesebben is megmagyarázzuk.

A

$$z^2 = x^2 - 4t$$

egyenlet, hol x és t határozatlanok, oly $(\sqrt{x^2-4t})$ genus-tartományt értelmez, a mely az $([1], x, t)$, tartományból származik. Az egyenlet discriminánsa $4(x^2-4t)$; a $(\sqrt{x^2-4t})$ genus-tartomány valódi absolut egész mennyiségei pedig a következő alakúak:

$$\frac{X_1 + X_2\sqrt{x^2-4t}}{4(x^2-4t)},$$

hol X_1 és X_2 a jellemzett formatartományhoz tartoznak. Valamely alaprendszer meghatározása itt majdnem triviálisan egyszerű úgy, hogy nem érdemes ebben az esetben az általános módszereket betű szerint alkalmazni. Arra, hogy $X_1 + X_2\sqrt{x^2-4t}$ osztható legyen $4(x^2-4t)$-vel, szükéges, hogy $X_1 - X_2\sqrt{x^2-4t}$, tehát $2X_1$ is osztható legyen $4(x^2-4t)$-vel úgy, hogy végre X_1-nek oszthatónak kell lennie $2(x^2-4t)$-vel. Továbbá még $2X_2\sqrt{x^2-4t}$-nek $4(x^2-4t)$-vel; tehát

$4X_2^2(x^2-4t)$-nek $16(x^2-4t)^2$-vel és X_2^2-nek $4(x^2-4t)$-vel, vagyis végre X_2-nek $2(x^2-4t)$-vel kell oszthatónak lennie. A $(\sqrt{x^2-4t})$ genus-tartomány absolut egész mennyiségei tehát okvetetlenül

$$\frac{X_1+X_2\sqrt{x^2-4t}}{2}$$

alakúak és viszont ezek a mennyiségek valóban absolut egész mennyiségek, ha $X_1^2-X_2^2(x^2-4t)$ osztható 4-gyel, vagyis, ha fönnáll az

$$X_1^2-X_2^2\,x^2\equiv 0 \pmod 4$$

congruentia. Ekkor azonban az

$$X_1+X_2\,x\equiv 0,\quad X_1-X_2\,x\equiv 0 \pmod 2$$

congruentiák közül legalább az *egyiknek* fenn kell állania. E congruentiák bármelyike a másiknak következménye; tehát pl. azt írhatjuk, hogy $X_1=X_2x+2X_3$. És így látni, hogy a $(\sqrt{x^2-4t})$ genus-tartomány absolut egész mennyiségeinek szükséges alakja:

$$X_3+X_2\frac{x+\sqrt{x^2-4t}}{2};$$

végre pedig, minthogy $\frac{x+\sqrt{x^2-4t}}{2}$ valóban a genus-tartomány absolut egész mennyisége,

$$1,\ \frac{x+\sqrt{x^2-4t}}{2}$$

a *keresett alaprendszer*

A genus-tartomány alapmennyisége tehát

$$u_1+\frac{x+\sqrt{x^2-4t}}{2}u_2$$

és alapegyenlete

$$\left(z-u_1-\frac{x+\sqrt{x^2-4t}}{2}u_2\right)\left(z-u_1-\frac{x-\sqrt{x^2-4t}}{2}u_2\right)=0;$$

ez pedig kiszámítva:

$$z^2-z(2u_1+u_2x)+u_1^2+u_1u_2x+u_2^2t=0.$$

Ha már most $P=x^2-4t$-t KRONECKER *utasítása szerint* bontanók fel törzsideálokra, akkor — a 19. §-hoz csatolt jegyzetben elvégzett számítások értelmében, hol most z_1, z_2, z_3 helyébe z, u_1, u_2 teendő — az alapegyenlet bal oldala irreducibilis volna mod. (x^2-4t) úgy, hogy x^2-4t-nek törzsideálnak kellene lennie, a mi nyilvánvalóan helytelen, mert $x^2-4t=(\sqrt{x^2-4t})^2$ és Nm. $\sqrt{x^2-4t}=x^2-4t$ nem ~ 1.

Ha *az itt adott utasításnak megfelelőleg* a P æquivalentia-modulus szerint végezzük a felbontást, akkor nyerjük, hogy

$$P\sim(2u_1+(x+\sqrt{x^2-4t})\,u_2-2u_1-xu_2)^2,$$

vagyis, hogy

$$P\sim(\sqrt{x^2-4t})^2$$

és ez a helyes eredmény.

A genus discriminánsa.

30. §. Az alapegyenlet discriminánsa mindig a

$$\mathfrak{D}=D\mathfrak{E}$$

alakban írható, hol $\mathfrak{E}$ valamely az $[A, x_1, \ldots, x_m]$ tartományból származó primitiv forma, D pedig az $[A, x_1, \ldots, x_m]$ tartomány formája; még pedig a kritikus törzsformák hatványszorzata.

Az alapegyenlet discriminánsa a tulajdonságoknak oly sorozatát értelmezi, a melyek a genusnak, mint ilyennek sajátos tulajdonságai, azaz függetlenek maradnak attól, hogy a genust eredetileg hogyan értelmeztük. Ennek megfelelőleg a D forma bizonyos æquivalentia értelmében egyértelműleg meghatározott és — KRONECKER kifejezésmódja szerint — «*a genus invariánsa*» *e szó magasabb értelmében.* Pontosabban kifejezve, ez a következőt jelenti: Ha a genus különböző értelmezéseiből kiindulva és tetszés szerinti alaprend-

szereket használva, egyik esetben D'-t, más esetben pedig D''-t nyerjük az alapegyenlet discriminánsául, akkor D' és D'' az $[A, x_1, \ldots, x_m]$ formatartományban æquivalensek, ha A orthoid tartomány. Ha pedig $A=[1]$, akkor esetleg csak a D'-ben és D''-ben foglalt nem szabályos törzsszámoknak, mint tényezőknek kihagyása után áll fönn ezen æquivalentia.

Hogy ezt bebizonyítsuk, vegyük fel, hogy ugyanannak a genusnak kétféle értelmezése mellett két különböző alaprendszerre,

$$\lambda_1, \lambda_2, \ldots, \lambda_s \quad \text{és} \quad \mu_1, \mu_2, \ldots, \mu_r$$

-re jutottunk, a melyeknek tehát az

$$\mathfrak{f}=\sum_{i=1}^{s} \lambda_i u_i, \quad \mathfrak{g}=\sum_{j=1}^{r} \mu_j v_j$$

alapmennyiségek felelnek meg. Ezen alapmennyiségek conjugált értékei legyenek $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ ill. $\mathfrak{g}_1, \ldots, \mathfrak{g}_n$.

Minthogy $\mathfrak{f}$ és $\mathfrak{g}$ ugyanannak a genusnak két ideális egész mennyisége és egyszersmind alapmennyiségek is, közvetetlenül a következő azonosságokhoz jutunk:

$$d\mathfrak{f}_i^k = \mathfrak{a}_{k0} + \mathfrak{a}_{k1}\mathfrak{g}_i + \cdots + \mathfrak{a}_{k,n-1}\mathfrak{g}_i^{n-1},$$
$$d\mathfrak{g}_i^k = \mathfrak{b}_{k0} + \mathfrak{b}_{k1}\mathfrak{f}_i + \cdots + \mathfrak{b}_{k,n-1}\mathfrak{f}_i^{n-1},$$
$$(i=1, \ldots, n;\ k=0, \ldots, n-1)$$

hol az $\mathfrak{a}$-k és $\mathfrak{b}$-k a tartomány raczionális és egész ideális mennyiségei; tehát továbbá

$$d^N |\mathfrak{f}_i^k|^2 = \mathfrak{A} |\mathfrak{g}_i^k|^2,$$
$$d^N |\mathfrak{g}_i^k|^2 = \mathfrak{B} |\mathfrak{f}_i^k|^2$$

és

$$\mathfrak{A}\mathfrak{B} = d^{2N}.$$

E szerint az $\mathfrak{A}$ és $\mathfrak{B}$ raczionális és egész ideális mennyiségek a bennök előforduló nem szabályos törzsszámok kihagyása után egységek, azaz az $[A, x_1, \ldots, x_m]$ tartományból származó primitiv formáknak hányadosai. Továbbá pedig

amaz $|\mathfrak{f}_i^k|^2$ és $|\mathfrak{g}_i^k|^2$ determináns-négyzetek egyszerűen a genus alapegyenleteinek discriminánsai, $\mathfrak{D}'$ és $\mathfrak{D}''$, a mint azok a genus két különböző értelmezéséből kiadódnak. Így tehát az $[A, x_1, \ldots, x_m]$ tartománynak $\mathfrak{D}'$-ben és $\mathfrak{D}''$-ben együtthatókként szereplő formáinak a nem szabályos törzsszámok kihagyása után legnagyobb közös osztója ugyanaz a mennyiség, a mi épen bebizonyítandó volt.

Végre még megadjuk a *genus discriminánsa* értelmezését, a melynek különösen az algebrai alkalmazásokban nagy elvi jelentősége van.

Ha $\alpha_1, \alpha_2, \ldots, \alpha_n$ a genus-tartomány bármely valódi egész mennyiségei és $\alpha_{i1}, \ldots, \alpha_{in}$ az α_i conjugált értékei, akkor az $|\alpha_{ij}|^2$ determináns-négyzetet az $\alpha_1, \ldots, \alpha_n$ mennyiségek discriminánsának nevezzük. Ha már most $\mu_1, \ldots, \mu_r$ $(r \geqq n)$ a genus valódi egész mennyiségeinek egyik alaprendszere, akkor abból $\binom{r}{n}$ különböző módon választható ki n mennyiség:

$$\mu_{s_1}, \mu_{s_2}, \ldots, \mu_{s_n}$$

és minden egyes választásnak megfelelőleg azután képezhető e mennyiségek discriminánsa, Δ_s.

E számra nézve $\binom{r}{n}$ discrimináns: $\Delta_1, \Delta_2, \ldots$ — Kronecker szerint — *a discriminánsok egy alaprendszerét* alkotja. Végre pedig *a genus discriminánsa a discriminánsok egy alaprendszerében foglalt mennyiségeknek (az $[A, x_1, \ldots, x_m]$ tartományban vett) legnagyobb közös osztója.*

Ha $\mathfrak{f}$ az alapmennyiséget jelenti, akkor közvetetlenül lesz

$$d\mu_{s_j i} = c_{j0} + c_{j1}\mathfrak{f}_i + \cdots + c_{j,n-1}\mathfrak{f}_i^{n-1}$$

és így

$$d^a|\mu_{s_j i}| = \mathfrak{C}|\mathfrak{f}_i^k|;$$

e szerint tehát a $d^a|\mu_{s_j i}|$ mennyiségek mindegyike osztható $|\mathfrak{f}_i^k|$-val, hol az oszthatóság az ideális egész mennyiségek tartományában értendő.

Továbbá még

$$\mathfrak{f}_i^k = \mathfrak{h}_{k1}\mu_1 + \cdots + \mathfrak{h}_{kr}\mu_r \qquad (k=0, 1, \ldots, n-1)$$

és így

$$|\mathfrak{f}_i^k| = \sum_{s=1}^{\binom{r}{n}} \mathfrak{H}_s |\mu_{s_j i}| .$$

E szerint tehát végre $|\mathfrak{f}_i^k|^2$, azaz az alapegyenlet discriminánsa a $|\mu_{s_j i}|^2$ discriminánsok legnagyobb közös osztójából származik, ha a nem szabályos törzsszámok egy bizonyos hatványszorzatát ehhez mint tényezőt hozzácsatoljuk. E mellett az oszthatóság az ideális mennyiségek tartományában értendő.

31. §. A mint közvetetlenül belátható, bármely két $|\mu_{s_j i}|$ determináns szorzata is az $[A, x_1, \ldots, x_m]$ tartomány formája és e szorzatok legnagyobb közös osztója ismét a genus discriminánsa. E szerint végre közvetetlenül felírhatjuk azon (a genus discriminánsával æquivalens) mennyiséget, a melyet KRONECKER *a genus discrimináns-formájának* nevezett. A genusnak ez a discrimináns-formája a

$$|\mu_{ij}|^2 \qquad (i, j=1, \ldots, r)$$

determináns-négyzet, hol $r \geqq n$ és $\mu_{i1}, \ldots, \mu_{in}$ az alaprendszer μ_i elemének n conjugált értékét jelentik, míg a μ_{ij}-k, ha $j > n$, kivétel nélkül különböző új határozatlanok. Közvetetlenül belátható ezután, hogy a genus discriminánsformája az $[A, x_1, \ldots, x_m]$ tartományból származó forma, a melyben az együtthatók legnagyobb közös osztója egyenesen a genus discriminánsa.

A genus discrimináns-formája, vagy még pontosabban kifejezve a genus discriminánsainak alaprendszere ismét *a genus invariánsa,* a mely a tulajdonságok oly sorozatát fejezi ki, a melyek a genusnak, mint ilyennek sajátos tulajdonságai. Ugyanis, *ha* $D_1, D_2, \ldots$ *a genus discriminánsainak*

egy alaprendszere, akkor a

$$(D_1, D_2, \ldots)$$

osztórendszer a genus absolut invariánsa. Azaz, ha a genust két különböző módon értelmezve és két különböző alaprendszert $\lambda_1, \ldots, \lambda_s$-t és $\mu_1, \ldots, \mu_r$-t használva, a discriminánsok különböző alaprendszerei, $D'_1, D'_2, \ldots$ és $D_1, D_2, \ldots$ származnak, akkor az ezeknek megfelelő osztórendszerek a szó szűkebb értelmében æquivalensek; vagyis

$$(D'_1, D'_2, \ldots) \simeq (D_1, D_2, \ldots).$$

Jelesen, ha van olyan alaprendszer, a melyben az elemek száma pontosan n és D ennek discriminánsa, akkor egyszersmind lesz

$$D \simeq (D_1, D_2, \ldots).$$

Mind e tények helyessége abból a megjegyzésből következik, hogy, ha úgy $\lambda_1, \ldots, \lambda_s$ mint $\mu_1, \ldots, \mu_r$ alaprendszerek, akkor mindig

$$\lambda_{ij} = a_{i1}\mu_{1j} + \cdots + a_{ir}\mu_{rj}$$

alakú azonosságoknak kell fennállaniok, hol az $a_{ij}^{(k)}$-k az $[A, x_1, \ldots, x_m]$ tartomány formái. Ebből közvetetlenül kitünik, hogy a $|\lambda_{ij}|$ determinánsok a $|\mu_{ij}|$ determinánsoknak oly homogén és lineáris formái, a melyekben az együtthatók az $[A, x_1, \ldots, x_m]$ tartomány formái. Teljesen azonos módon bármely két $|\lambda_{ij}|$ determináns szorzata mint két-két $|\mu_{ij}|$ determinánsból alkotott szorzatok homogén és lineáris formája áll elő. A $(D'_1, D'_2, \ldots)$ osztórendszer tehát tartalmazza a $(D_1, D_2, \ldots)$ osztórendszert és ép úgy tartalmazza a $(D_1, D_2, \ldots)$ osztórendszer a $(D'_1, D'_2, \ldots)$ osztórendszert. E két osztórendszer tehát valóban *a szó szükebb értelmében aequivalens.*

Így tehát a discriminánsforma, vagyis az ennek együtthatóiból alkotott osztórendszer raczionális és egész alakban szolgáltatja a genus és egyszersmind a benne tartalmazott

algebrai mennyiségek lényeges tulajdonságait. E tulajdonságok — ha a geometriában szokásos kifejezésmódot használjuk természetszerű általánosításban — *a genus singulárításai.* E kifejezés magyarázatául még fölhozzuk, hogy bármely alapegyenlet discriminánsa és a genus discriminánsa az $[A, x_1, \ldots, x_m]$ tartomány *ugyanazon* törzsformáival osztható. Általánosságban sokszorosságuk is ugyanaz; csak a nem szabályos törzsszámok, ha ilyenek vannak, az alapegyenlet discriminánsaiban magasabb hatványon fordúlhatnak elő, mint a genus discriminánsában. Megfelelő felfogásban ugyanis az alapegyenlet discriminánsa nem egyéb, mint a

$$\mu_{1i}-\mu_{1j}, \ldots, \mu_{ri}-\mu_{rj}$$

mennyiségek legnagyobb közös osztóiból alkotott négyzetek szorzata. Minden ilyen legnagyobb közös osztó azonban, mint közvetetlenül látni, a genus discriminánsának is osztója.

Evvel megvan az alap bármely specziális algebrai képződmény vizsgálatára. Eddig még csak a legegyszerűbb esetek kifejtése ismeretes. Ilyennek tekintendő az algebrai számok elmélete egyrészt és az egy változós algebrai függvények elmélete, azaz az algebrai síkgörbék geometriája másrészt.

Úgy algebrai (geometriai), mint arithmetikai tekintetben megmérhetetlen a kilátás, a melyet az algebrai mennyiségek elmélete nyújt. És bizonyára nem utolsó érdeme ennek az egyszerű és általános voltában eddig aligha felül mult fogalomalkotásnak, hogy megszünteti az arithmetika és geometria ellentétét és a kettőt mintegy magasabb egységben foglalja össze.

NÉV- ÉS TÁRGYMUTATÓ.

(A római számjelek a fejezeteket, az arabs számjelek pedig a paragrafusokat jelentik.)

Absolut:
A. æquivalentia I. 5, IX. 13; a. algebrai mennyiség IV. 7, IX. 1; a. egész algebrai számok alaprendszere IX. 16; a. egész forma IX. 4; a. egész mennyiség IX. 4; a. egész mennyiségek alaprendszere IX. 15; a. egység I. 3, IV. 6; a. raczionális tartomány IV. 20; a. törzsrendszer VII. 4; a. törzsrendszer $[[1], x_1, \ldots, x_k]$-ban VIII. 1—4, 8.

Absolute æquivalens I. 5, IX. 13.

Adjunctio I. 4, IV. 5, 7, 21, VIII. 9.

Adjungált mennyiség IV. 5.

Aequivalens I. 5:
Ae. modulus- vagy osztórendszerek VII. 2; absolute æ. I. 5, IX. 13; relative æ. I. 5, 12, IX. 13.

Aequivalentia I. 5:
Ae. mod. (S) VIII. 1; absolut æ. I. 5, IX. 13; bővebb æ. VII. 2; bővebb æ. mod. $(P^{(k)})$ VIII. 5; KUMMER-féle æ. IX. 13; raczionális és egész formák æquivalentiája IV. 1; raczionális és egész számok æquivalentiája IV. 1; relativ æ. I. 5, 12, IX. 13; szűkebb æ. VII. 2; szűkebb æ. mod. $(P^{(k)})$ VIII. 5.

æqu. mod. P irreducibilis forma IX. 17.

æqu. mod. P törzsforma IX. 18.

Aequivalentia-modulus IX. 17:
Ae. szerint æquivalens mennyiségek IX. 17; æ. szerint való oszthatóság IX. 17.

Aequivalentiatartomány I. 12:
Ae. egységei I. 12; holoid tartományból ([A]-ból) származó legkisebb æ. I. 12; valódi æ. I. 12.

Affinitás III. 18.

Alapegyenlet:
Genus alapegyenlete IX. 24.

Alapforma:
Genus-tartomány alapformája IX. 24.

Alapmennyiség:
Genus-tartomány alapmennyisége IX. 24.
Alapműveletek I. 1.
Alapprobléma:
Eliminácció-elmélet alapproblémája V. 1; lineáris diophantikus egyenletek rendszere teljes megoldásának alapproblémái diophantikus tartományban VII. 1.
Alaprendszer VIII. 2, IX. 1:
A. elemeinek száma IX. 14; absolut egész algebrai számok alaprendszere IX. 16; absolut egész mennyiségek alaprendszere IX. 15; discriminánsok alaprendszere IX. 30; egész ideális mennyiségek alaprendszere IX. 24, 25; egy változós algebrai függvények alaprendszere IX. 16; genus alaprendszere IX. 14; orthoid tartományból származó genus-tartomány az orthoid tartományra vonatkozólag relativ egész mennyiségeinek alaprendszere IX. 15; valódi egész mennyiségek alaprendszere IX. 21—23.
Alaptétel:
Algebra alaptétele IV. 27, 28; Gauss alaptétele IV. 27; Kronecker alaptétele III. 5—7; leképezés elméletének alaptétele V. 10; teljes tartományokból származó formákra vonatkozó a. III. 8.
Algebra I. 1, IV. 8, VII. 1:
A. alaptétele IV. 27, 28.
Algebrai:
A. egyenletek Galois-féle elmélete IV. 26; a. függvény IV. 7; a. mennyiség I. 1, IV. 7; a. mennyiségek arithmetikai elmélete IX. 1; a. módszer IV. 8; a. osztó IX. 8; a. sokaság V. 6; a. szám I. 1, III. 21, IV. 7; a. számok országa IV. 19; a. számok összessége IV. 22.
Algebrai elmélet:
Lineáris diophantikus rendszerek a. elmélete VII. 8, 9.
Algebrai forma:
Genus-tartományból származó egész a. f. IX. 2, 3.
Algebrai mennyiség I. 1, IV. 7:
Absolut a. m. IV. 7, IX, 1; mod. $(P^{(k)})$ absolut a. m. VIII. 9; orthoid tartományra vonatkozólag a. m. IV. 7, IX. 1.
Általános:
Á. forma IV. 1, VI. 1; á. formarendszer VI. 1; á. formarendszer discriminánsa VI. 21; á. formarendszer discriminánsának alaptulajdonságai VI. 23, 25, 26; á. formarendszer resultánsa VI. 3; á. formarendszer resultánsának alaptulajdonságai VI. 5; á. (homogén) lineáris transformatio II. 19; á. lineáris congruentia VIII. 16; á. lineáris formák

resultánsa VI. 11; á. másodfokú egyenlet V. 6; á. n-edfokú egyenlet IV. 26.

Általánosítás:

KRONECKER alaptételének általánosítása VIII. 5; NOETHER tételének általánosítása VII. 13.

Analitikai:

A. függvény VII. 8; a. számelmélet IX. 13.

Analizis I. 1; IV. 7:

A. határértékei IV. 21.

Arithmetika I. 1, IV. 8, VII. 1.

Arithmetikai elmélet:

Algebrai mennyiségek a. elmélete IX. 1; lineáris diophantikus rendszerek a. elmélete VII. 8.

Arithmetikai megoldás:

Homogén lineáris diophantikus egyenlet a. megoldása VIII. 10—18.

Arithmetikai módszer IV. 8.

Associált mennyiségek IX. 8.

Associatio IX. 8.

Associativ I. 2, 3.

Azonos substitutio IV. 24.

BALTZER V. 15.

Basis:

Raczionális tartomány basisa IV. 22.

BÉZOUT-féle tétel VI. 16.

Bővebb:

B. æquivalentia VII. 2; b. æquivalentia mod. $(P^{(k)})$ VIII. 5; b. értelemben vett ideális mennyiség IX. 8.

BRILL VII. 13.

Charakteristika:

Gyökrendszer charakteristikája VII. 13—15.

Charakteristikus:

Egyenlet ch. csoportja IV. 24, 25.

Collineatio VI. 13.

Combinatio IV. 27.

Commutativ I. 2, 3.

C. elv VII. 3.

Complementáris osztó III. 1.

Complex számok III. 21, IV. 5, 6:

C. sz. összessége IV. 22.

Componált osztórendszer VII. 3.

Compositio:

C. tényezői VII. 3; osztórendszerek compositiója VII. 3.

Congruens mennyiségek:

Modulusrendszerre vonatkozólag c. m. I. 10.

Congruentia:

C. gyöke VIII. 4, 9; általános lineáris c. VIII. 16; n-edfokú c. egy ismeretlennel VIII. 4.

Congruentiarendszerek általános elimináczió-elmélete IX. 15.

Congruentiatartomány I. 10:

Valódi c. I. 10.

Conjugált:

C. formák IV. 16; c. genustartományok IV. 14; c. gyö-

kök IV. 14; c. megoldások V. 8; c. mennyiségek IV. 14.

Csoport:

Cs. rendszáma IV. 24; egyenlet charakteristikus csoportja IV. 24, 25; permutációk csoportja IV. 23; substitutiók csoportja IV. 23.

DEDEKIND I. 2, 8, III. 4, 5, IV. 22, IX. 1, 8, 13, 27:

D. segédtétele III. 4.

Derivált:

Első d. II. 5; magasabb d. II. 5, 6.

Derivatio alaptörvényei II. 5.

Determináns:

D.-matrix III. 4; d. rangja V. 15; $|f_{rs}|$ d. II. 15; függvényd. V. 14; lineáris transformatio determinánsa. II. 18. SYLVESTER-féle determináns III. 14, VI. 4; $|x_{i_1}^{j_1} x_{i_2}^{j_2} \ldots x_{i_e}^{j_e}|$ d. II. 12; $|x_{k+i}^{m-k-j}|$ d. II. 11.

Differenciálszámolás II. 5, V. 14.

Dimensio:

Egyenlet dimensiója III. 19; forma dimensiója II. 2.

Diophantikus:

D. egyenlet III. 19; d. tartomány VII. 1.

DIRICHLET I. 2.

Discriminánsok:

D. invariáns-tulajdonsága VI. 27; d. mint symmetrikus forma III. 25; általános formarendszer discriminánsa VI. 21; általános formarendszer discriminánsának alaptulajdonságai VI. 23, 25, 26; egyenlet discriminánsa IV. 13; egy forma discriminánsa III. 22; egy forma discriminánsának alaptulajdonságai III. 23; formarendszer discriminánsa, a melynek minden formája általános lineáris formák szorzata VI. 24; genus discriminánsa IX. 30; genus-tartomány mennyiségének discriminánsa IX. 14; genus-tartomány n valódi mennyiségének discriminánsa IX. 30; homogén formák rendszerének discriminánsa VI. 26.

Discriminánsok alaprendszere IX. 30.

Distributiv I. 3.

Egész:

E. functionál IX. 8; e. függvény II. 2, 16, 17; e. ideális mennyiség IX. 10; e. ideális mennyiségek alaprendszere IX. 24, 25; e. mennyiségek felbontása törzsideálokra IX. 11, 21, 26—28.

Egész algebrai forma:

Genus-tartományból származó e. a. f. IX. 2, 3.

Egész algebrai mennyiség:

Genus-tartomány e. a. mennyisége IX. 2.

Egész forma:
Absolut e. f. IX. 4; relativ e. f. IX. 4.
Egész mennyiség:
Absolut e. m. IX. 4; relativ e. m. IX. 4.
Egyenesnek képzetes pontja IX. 8.
Egyenlet:
E. charakteristikus csoportja IV. 24, 25; e. dimensiója III. 19; e. discriminánsa IV. 13; e. foka III. 19; e. gyöke III. 19, IV. 6; e. gyökeinek raczionális függvénye IV. 15; e. megoldása III. 19; e. raczionális gyöke III. 12; e. rendszáma IV. 12; e. többszörös gyöke IV. 13; egyenletek elméletének problémája III. 19; algebrai egyenletek GALOIS-féle elmélete IV. 26; általános másodfokú e. V. 6; általános n-edfokú e. IV. 26; diophantikus e. III. 19; genus alapegyenlete IX. 24; lineáris e. V. 6; orthoid tartományban ((A)-ban) irreducibilis e. IV. 5; orthoid tartományból ((A)-ból) származó egy ismeretlent tartalmazó n-edfokú e. IV. 5; $x^2=2$ e. IV. 7.
Egyenletrendszer V. 1:
E. értelmezte sokaság fokozata vagy rangja V. 6; e. fokozata vagy rangja V. 6; e. gyökrendszere III. 19; e. megoldása III. 19, 20; e. tartalma V. 5; egyenletrendszerek elméletének problémája III. 19; egyenletrendszernek a végtelenben fekvő megoldása VI. 13; határozatlan e. VI. 14, 15, 30; határozott e. VI. 14, 15; közönséges e. VI. 14, 15; orthoid tartományban irreducibilis e. V. 7; singularis e. VI. 30; tiszta $h+1$-edfokozatú e. V. 6; transformált e. V. 2; vegyes $h+1$-edfokozatú e. V. 6.
Egymástól független:
E. f. formák V. 14; E. f. gyökrendszerek V. 13.
Egymástól függő:
E. f. formák V. 14.
Egység I. 5:
Absolut e. I. 3, IV. 6; æquivalentiatartomány egységei I. 12; [$\mathfrak{G}$] tartomány egységei IX. 7.
Egység-forma III. 9, IX. 4.
Egytagú modulusrendszer I. 11.
Együttható II. 1, 2:
Transformatio együtthatói II. 18.
EISENSTEIN IV. 4.
Elem:
Modulusrendszer eleme I. 10; raczionális tartomány eleme IV. 21; sokaság eleme III. 21, V. 6; sokaság kétszeres eleme V. 6; sokaság singuláris eleme V. 6; sokaság többszörös eleme V. 6; sokaság végtelen eleme V. 6.

Elemi symmetrikus forma II. 11, VI. 18.

Eliminácziό-elmélet:
E. alapproblémája V. 1; congruentiarendszerek általános eliminácziό-elmélete IX. 15.

Eliminácziό-elv:
KRONECKER-féle e. III. 18, V. 2.

Eliminácziό-módszer:
KRONECKER-féle e. V. 2.

Eliminácziό probléma IV. 21.

Eliminánс VI. 15.

Elmélet:
Algebrai egyenletek GALOIS-féle elmélete IV. 26; algebrai mennyiségek arithmetikai elmélete IX. 1; egy változós algebrai függvények elmélete IX. 1; lineáris diophantikus rendszerek algebrai elmélete VII. 8, 9; lineáris diophantikus rendszerek arithmetikai elmélete VII. 8.

Elsőrendű:
E. infinitesimális tartomány V. 8; e. végtelen kis mennyiség V. 8.

Elv:
Commutativ e. VII. 3; GALOIS-féle e. IV. 24; GAUSS-féle e. II. 14; KRONECKER-féle eliminácziό-e. III. 18, V. 2.

Esetleges körülmény III. 18; V. 2, 3.

e **szám** IV. 21.

EUKLIDES-féle algorithmus III. 11.

EULER III. 14.
EULER-féle képletek II. 16; EULER-nek a homogén formákra nézve fennálló képletsorozata II. 9.

Felbontás:
Egész mennyiségek felbontása törzsideálokra IX. 11, 21, 26—28; nem szabályos törzsszám felbontása IX. 28; orthoid forma felbontása törzsformákra IV. 3; raczionális és egész forma felbontása törzsformákra IV. 2; raczionális és egész szám felbontása törzstényezőkre IV. 1; raczionális forma felbontása törzsformákra IV. 3.

Felbonthatatlan osztórendszer VII. 4.

Felület V. 6:
F., mely valamely egyenest teljesen tartalmaz V. 6.

Fok:
Egyenlet foka III. 19; forma foka II. 2; orthoid tartományra vonatkozólag algebrai mennyiségek országából ({A}-ból) származó *m*—*h*—1-szeres sokaság foka V. 6; törzsideál foka IX. 12.

Fokozat:
Egyenletrendszer fokozata V. 6; egyenletrendszer értelmezte sokaság fokozata V. 6; orthoid formarendszer fokozata

V. 6; osztórendszer fokozata VII. 10; teljes részletresolvens fokozata V. 4.

Forma II. 2:

F. dimensiója II. 2; f. foka II. 2; f. tagjának magassága II. 3; f. többszörös osztója III. 22; formák oszthatósága III. 2; absolut egész f. IX. 4; æqu. mod. P irreducibilis f. IX. 17; æqu. mod. P törzsf. IX. 18; a_u formája IX. 5; általános f. IV. 1, VI. 1; conjugált formák IV. 16; egy határozatlan formája, mely n határozatlan formájának megfelel II. 4; $[[1], x_1, \ldots, x_{k+1}]$ (mod. $(P^{(k)})$) tartomány raczionális és egész formája VIII. 7; egymástól független formák V. 14; egymástól függő formák V. 14; egységf. III. 9, IX. 4; elemi symmetrikus f. II. 11, VI. 18; föltétlenül irreducibilis f. IV. 18; genus discrimináns-formája IX. 31; genus-tartományból származó egész algebrai f. IX. 2, 3; holoid f. III. 12; homogén f. II. 8; kritikus törzsf. IX. 27; lineáris f. IV. 3, 18; mod. $(P^{(k)})$ szabályos f. VIII. 4; mod. (S) irreducibilis f. VIII. 1; orthoid f. III. 12; primitiv f. III. 9, IX. 4; $P^{(k)}(z)$ f. II. 11; redukált f. II. 13; relativ egész f. IX. 4; resolvens f. III. 18; resolvens f. mod. $(P^{(k)})$ VIII. 6, 7; symmetrikus f. II. 10, 14; szabályos f. II. 19; több mennyiség-rendszer symmetrikus formája VI. 18; törzsf. IV. 2; törzsf. orthoid formatartományban IV. 3; törzsf. a raczionális formák tartományában IV. 3; törzsf. a raczionális és egész formák tartományában IV. 2; transformált f. II. 18; tulajdonképeni primitiv f. IX. 13; typikus symmetrikus f. VI. 18; x_i-re nézve szabályos f. II. 19.

Formarendszer:

F. discriminánsa, a melynek minden formája lineáris formák szorzata VI. 24. általános f. VI. 1.

Főelőállítás:

m-edfokozatú sokaság főelőállítása V. 10; tiszta algebrai térgörbe főelőállítása V. 9; tiszta elsőfokozatú sokaság főelőállítása V. 10; tiszta sokaság főelőállítása V. 9, 10.

Főideál IX. 13.

Föltétlenül irreducibilis:

F. i. forma IV. 18; f. i. képződmény V. 7; f. i. sokaság V. 7.

Főmegoldás V. 8.

Főosztályhoz tartozó osztórendszer VII. 10.

Frobenius V. 15.

Functionál:
Egész f. IX. 8.
Függvény:
Algebrai f. IV. 7; analitikai f. VII. 8; egész f. II. 2, 16, 17; egyenlet gyökeinek racionális függvénye IV. 15; racionális f. IV. 20; transcendens f. IV. 21.
Függvénydeterminánsok V. 14:
F. irreducibilis volta VI. 22.

Galois IV. 11, 21, 24.
Galois-féle:
G. elv IV. 24; G. genus-tartomány IV. 14; G. képzetes mennyiségek VIII. 9; G. resolvens IV. 11, 13; G. tartomány IV. 13; G. tartomány mod. $(P^{(k)})$ VIII. 9; algebrai egyenletek G. elmélete. IV. 26.
Gauss I. 4, 11, II. 3, III. 12, IV. 27, VIII. 2, IX. 1:
G. alaptétele IV. 27; G. elve II. 14; Gauss-nak a racionális és egész formák felbontására vonatkozó tétele III. 12.
Genus IV. 15:
G. absolut invariánsa IX. 31; g. alapegyenlete IX. 24; g. alaprendszere IX. 14; g. discriminánsa IX. 30; g. discriminánsformája IX. 31; g. invariánsa IX. 30; g., mely más g. alá van foglalva IV. 15; g. rendszáma IV. 15; g. singularitásai IX. 31.
Genus-tartomány:
G. alapformája IX. 24; g. alapmennyisége IX. 24; g. egész mennyiségeinek tartománya, $[\Gamma]$ IX. 3; g., melynek törzstartománya is már g. IV. 16; g. mennyiségének discriminánsa IX. 14; g. mennyiségének rendszáma IV. 15; g. n valódi mennyiségének discriminánsa IX. 30; g. törzstartománya IV. 14; genus-tartományból származó egész algebrai forma IX. 2, 3; g.-tartományból származó egész formák tartománya, $[\Gamma]_w$ IX. 3; genus-tartománynak az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag racionális mennyisége IX. 1; g.-tartománynak az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag racionális és egész mennyisége IX. 2; genus-tartománynak az összeadás és szorzás révén származó kapcsolatokra vonatkozó tulajdonságai IX. 1. genus-tartománynak egész algebrai mennyisége IX. 2; conjugált genus-tartományok IV. 14; Galois-féle g. IV. 14; orthoid tartományból származó g. IV. 14; pseudoorthoid tartományból származó g. mod. $(P^{(k)})$ VIII. 9; teljes g. IX. 10; valódi g. IX. 10.
Gordan VII. 6.

Gyök:
Congruentia gyöke VIII. 4, 9; conjugált gyökök IV. 14; egyenlet gyöke III. 19, IV. 6; egyenlet raczionális gyöke III. 12; egyenlet többszörös gyöke IV. 13.
Gyökrendszer:
Gy. charakteristikája VII. 13—15; gy. sokszorossága V. 5, VI. 15, 28—30; egyenletrendszer gyökrendszere III. 19; egymástól független gyökrendszerek V. 13.

HANCOCK VII. 8.
Hányados III. 1.
Határérték IV. 7:
Analizis határértékei IV. 21.
Határozatlan II. 1, 2, V. 1:
H. egyenletrendszer VI. 14, 15, 30; h. szám I. 1.
Határozott egyenletrendszer VI. 14, 15.
HENSEL VII, 8, IX. 24, 27, 28.
HERMITE IV. 21.
HESSE III. 14.
HILBERT VII. 6, 16:
H. tétele VII. 6, 16.
Holoid:
H. forma III. 12; h. mennyiség III. 12; h. tartomány I. 4; h. tartományból ([A]-ból) származó legkisebb æquivalentiatartomány I. 12; h. tartományból ([A]-ból) származó m—k-szoros sokaság III. 21.
Holoid tartomány I. 4:
Nem valódi h. t. I. 4; teljes h. t. I. 6; valódi h. t. I. 4.
Homogén:
H. egyenletek rendszere VI. 13; h. egyenletek rendszerének valódi megoldása VI. 13; h. forma II. 8; h. formák rendszerének discriminánsa VI. 26; h. formák rendszerének resultánsa VI. 12; h. lineáris congruentia megoldásai VII. 6; h. lineáris diophantikus egyenlet arithmetikai megoldása VIII. 10—18; h. lineáris diophantikus egyenlet megoldásának reductiója VIII. 10—18; h. lineáris diophantikus egyenlet megoldásának singuláris esetei VIII. 14, 16, 17, 19.
HURWITZ III. 5.
Hyperorthoid tartomány IV. 9.

Ideál IX. 8:
Fői. IX. 13.
Ideális:
I. mennyiség IX. 1; i. mennyiségek osztályokba sorozása IX. 13; i. mennyiségek osztályainak száma IX. 13; i. mennyiségeknek az oszthatóságra vonatkozó tulajdonságai IX. 10.
Ideális mennyiség IX. 1:
Bővebb értelemben vett i. m. IX. 8; [Γ] tartomány i. mennyisége IX. 8; (Γ) genus-tar-

tomány i. mennyisége IX. 10. egész i. m. IX. 10; raczionális és egész i. m. IX. 9; szűkebb értelemben vett i. m. IX. 8; tört i. m. IX. 10.

Infinitesimális:
Elsőrendű i. tartomány V. 8.

Invariáns III. 9, IX. 5:
Genus invariánsa IX. 30; genus absolut invariánsa IX. 31.

Invariáns-tulajdonság:
Discrimináns invariáns-tulajdonsága VI. 27; resultáns invariáns tulajdonsága VI. 12.

Invers substitutio IV. 24.

Irraczionalitás:
Valós quadratikus i. IV. 5.

Irreducibilis egyenlet:
Orthoid tartományban i. e. IV. 5.

Irreducibilis egyenletrendszer:
Orthoid tartományban i. e. V. 7.

Irreducibilis forma:
æqu. mod. *P* i. f. IX. 17; föltétlenül i. f. IV. 18; mod. (*S*) i. f. VIII. 1.

Irreducibilis $h+1$-edfokozatú részlet-resolvens:
Orthoid-tartományra vonatkozólag i. $h+1$-edf. r. V. 7.

Irreducibilis képződmény:
Föltétlenül i. k. V. 7.

Irreducibilis mennyiség I. 5, IX. 10:
Valódi i. m. I. 5.

Irreducibilis osztórendszer VII. 4.

Irreducibilis sokaság:
Föltétlenül i. s. V. 7; orthoid tartományban i. s. V. 7.

Irreducibilitásra vonatkozó tételek V. 7.

Ismeretlen III. 19.

Isobarikus VI. 5.

JACOBI V. 14.

Jól értelmezett:
J. é. tartomány III. 1, IV. 3, 16; j. é. teljes tartomány III. 8.

JUNKER VI. 18.

Kapcsolat I. 1.

Képzetes mennyiségek:
GALOIS-féle k. m. VIII. 9.

Képződmény:
Föltétlenül irreducibilis k. V. 7; különböző kiterjedésű képződmények V. 6.

Kétszeres elem:
Sokaság k. eleme V. 6.

Kivonás I. 1, 2.

KLEIN IV. 26.

Koordináta V. 6:
K.-transformatio V. 3.

Korlátlanul változó mennyiség:
Orthoid tartományra vonatkozólag algebrai mennyiségek országában ({A}-ban) k. v. m. V. 1.

Közönséges:
K. egyenletrendszer VI. 14, 15; k. osztási eljárás III. 1; összeadás k. törvénye I. 2; szorzás k. törvénye I. 3.

Kritikus törzsforma IX. 25, 27.

KRONECKER I. 1, 4, 11, II. 2, 4, 13, III. 5, 18, 23, IV. 1, 14, 16, 20, 21, 24, V. 2, 10, 11, VI. 1, 25, 26, VII, 2, 4, IX. 1, 4, 5, 8, 13, 15, 24, 25, 27, 28, 29:
K. alaptétele III. 5—7; K. alaptételének általánosítása VIII. 5; K. eliminácziό-elve III. 18, V. 2; K. eliminácziό-módszere V. 2; K. relácziói II. 16.
KUMMER IX. 1, 8.
KUMMER-féle:
K. æquivalentia IX. 13.
Kúpszelet:
Szét nem eső k. V. 6.
Különbségek szorzata II. 11.

LAGRANGE-féle interpoláczió-képlet II. 17, IV. 1.
Legkisebb:
L. orthoid tartomány, mely valamely irreducibilis egyenlet gyökét tartalmazza IV. 7.; l. pseudoorthoid tartomány, a melyben valamely congruentiának gyöke van VIII. 9.
Legnagyobb közös osztó I. 6, IX. 7. 9:
Két forma l. k. osztója III. 11, 17; két főideál l. k. osztója IX. 13.
Legnagyobb közös tartalom:
Két osztórendszer l. k. tartalma VII. 2; két osztórendszer l. k. tartalma mod. $(P^{(k)})$ VIII. 5.
Leképezés elméletének alaptétele V. 10.
LINDEMANN IV. 21.
Lineáris:
L. diophantikus egyenletek rendszere VII. 1; l. diophantikus rendszerek algebrai elmélete VII. 8, 9; l. diophantikus egyenletek arithmetikai elmélete VII. 8; l. diophantikus egyenletek rendszere teljes megoldásának alapproblémái diophantikus tartományban VII. 1; l. egyenlet V. 6; l. forma IV. 3, 18; l. sokaság V. 12; l. substitutio II. 18; l. transformatio II. 18; l. transformatio determinánsa II. 18; $AX \equiv B \pmod{(S)}$ l. congruentia megoldása VIII. 1; reczíprok l. transformatio II. 18; $\Sigma F_i X_i = 1$ alakú l. diophantikus egyenlet megoldása VIII. 8.

Magasság:
Forma tagjának magassága II. 3.
Maradék III. 1.
Maradékrendszer:
Teljes m. VII. 8, VIII. 1.
Másodfokú:
Általános m. egyenlet V. 6.
Mathematikai mennyiség I. 1.
Matrix:
M. rangja V. 15; determináns-m. III. 4.

m-dimensiós tér V. 6.

m-edfokozatú sokaság főelőállítása V. 10.

Megoldás sokszorossága V. 5, VI. 28—30.

Megoldás:

$AX \equiv B$ (mod. (S)) lineáris congruentia megoldása VIII. 1; conjugált megoldások V. 8; egyenlet megoldása III. 19; egyenletrendszer megoldása III. 19, 20; egyenletrendszernek a végtelenben fekvő megoldása VI. 13; főm. V. 8; homogén egyenletek rendszerének valódi megoldása VI. 13; homogén lineáris congruentia megoldásai VII. 6; homogén lineáris diophantikus egyenlet arithmetikai megoldása VIII. 10—18; orthoid tartományból ((A)-ból) származó egy ismeretlent tartalmazó egyenlet megoldása ugyanabban az orthoid tartományban ((A)-ban) IV. 5; $\Sigma F_i X_i = 1$ alakú lineáris diophantikus egyenlet megoldása VIII. 8.

Megoldhatóság:

$\sum_{j=1}^{h} f_j X_j \equiv 1$ congruentia megoldhatósága VIII. 6; $\sum_{i=1}^{h} F_i X_i = 1$ egyenlet megoldhatósága VIII. 8.

Mellérendelt:

M. orthoid tartomány I. 4, III. 12; m. pseudoorthoid tartomány VIII. 2.

Mennyiség:

Absolut algebrai m. IV. 7, IX. 1; absolut egész m. IX. 4; adjungált m. IV. 5; æquivalentia-modulus szerint æquivalens mennyiségek IX. 17; algebrai m. I. 1, IV, 7; associált m. IX. 8; bővebb értelemben vett ideális m. IX. 8; conjugált mennyiségek IV. 14; egész ideális m. IX. 10; elsőrendű végtelen kis m. V. 8; Galois-féle képzetes m. VIII. 9; (Γ) genus-tartomány ideális mennyisége IX. 10; $[\Gamma]$ tartomány ideális mennyisége IX. 8; genus-tartomány alapmennyisége IX. 24; genus-tartománynak az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag racionális mennyisége IX. 1; genus-tartománynak az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag racionális és egész mennyisége IX. 2; genus-tartománynak egész algebrai mennyisége IX. 2; holoid m. III. 12; ideális m. IX. 1; irreducibilis m. I. 5, IX. 10; mathematikai m. I. 1; mérő m. IV. 7; mod. $(P^{(k)})$ absolut algebrai m. VIII. 9; modulusrendszerre vonatkozólag congruens mennyiségek I. 10; orthoid m. III. 12; orthoid tar-

tományra ((A)-ra) vonatkozólag algebrai m. IV. 7, IX. 1; orthoid tartományra vonatkozólag algebrai mennyiségek országában ({A}-ban) korlátlanúl változó m. V. 1; raczionális és egész ideális m. IX. 9; relativ egész m. IX. 4; singuláris m. I. 3, IV. 9; szűkebb értelemben vett ideális m. IX. 8; tört ideális m. IX. 10; törzsm. I. 5, IX. 10; transcendens m. IV. 21; valódi irreducibilis m. I. 5; végtelen kicsiny m. IV. 9; végtelen nagy m. IV. 9.

Mérő mennyiség IV. 7.

MERTENS VI. 4, 5, 9.

Minimális resolvens V. 11.

Módszer:

Algebrai m. IV. 8; arithmetikai m. IV. 8.

mod. ($P^{(k)}$) absolut algebrai mennyiség VIII. 9.

mod. ($P^{(k)}$) æquivalens osztórendszerek VIII. 5.

mod. ($P^{(k)}$) relativ törzs-osztórendszerek VIII. 5.

mod. ($P^{(k)}$) szabályos forma VIII. 4.

mod. (S) irreducibilis forma VIII. 1.

Modulus I. 11.

Modulusrendszer I. 10:

M. elemei I. 10; modulusrendszerre vonatkozólag congruens mennyiségek I. 10; æquivalens modulusrendszerek VII. 2; egytagú m. I. 11; többtagú m. I. 10, VII. 2; törzs-m. VII. 4; valódi m. I. 10, VII. 2.

MOLK III. 5, IV. 16, V. 5, 10.

Művelet:

Alapm. I. 1; raczionális m. V. 1.

***n* határozatlan algebrai függvényeinek országa** IV. 19.

Nem szabályos törzsszám IX. 25:

N. sz. t. felbontása IX. 28.

Nem valódi holoid tartomány I. 4.

NETTO V. 5.

NEWTON-GIRARD-féle formulák IX. 25.

NŒTHER VII. 13, 14:

N. tétele VII. 8; N. tételének általánosítása VII. 13.

Norma IX. 1.

Ország:

Algebrai számok országa IV. 19; *n* határozatlan algebrai függvényeinek országa IV. 19; orthoid tartományra vonatkozólag algebrai mennyiségek országa V. 1.

Orthoid:

O. forma III. 12; o. forma felbontása törzsformákra IV. 3; o. formarendszer fokozata vagy rangja V. 6; o. mennyiség III. 12; o. tartomány I. 4, IV. 9, 22; o. tartományban irreducibilis

egyenlet IV. 5; o. tartományban irreducibilis egyenletrendszer V. 7; o. tartományban irreducibilis sokaság V. 7; o. tartományból származó egy ismeretlent tartalmazó n-edfokú egyenlet IV. 5; o. tartományból származó egy ismeretlent tartalmazó n-edfokú egyenlet megoldása ugyanabban az o. tartományban IV. 5; o. tartományból származó genus-tartomány az o. tartományra vonatkozólag egész mennyiségeinek alaprendszere IX. 15; o. tartomány az oszthatóságra vonatkozó tulajdonságainak megmaradása III. 13, IX. 7; o. tartományra vonatkozólag algebrai mennyiség IV. 7, IX. 1; o. tartományra vonatkozólag algebrai mennyiségek országa V. 1; o. tartományra vonatkozólag algebrai mennyiségek országában korlátlanúl változó mennyiség V. 1; o. tartományra vonatkozólag algebrai mennyiségek országából származó m—h—1-szeres sokaság foka V. 6; o. tartományra vonatkozólag irreducibilis $h+1$-edfokozatú részletresolvens V. 7; legkisebb o. tartomány, mely valamely irreducibilis egyenlet gyökét tartalmazza IV. 7; mellérendelt o. tartomány I. 4, III. 12.

Osztás I. 1, 4.

Osztási eljárás:

Közönséges o. e. III. 1.

Oszthatóság:

O. elemi törvényei I. 5; o. elmélete az $[[1], x_1, \ldots, x_m]$ (mod. $(P^{(k)})$) tartományban VIII. 2; o. fogalmának bővítése VII. 2; o. mod. (S) VIII. 1; o. törvényei az [1] tartományban IV. 1; o. törvényei a raczionális és egész formák tartományában ($[[1], x_1, \ldots, x_m]$-ben) IV. 1; æquivalentia-modulus szerint való o. IX. 17; formák oszthatósága III. 2; ideális mennyiségeknek az oszthatóságra vonatkozó tulajdonságai IX. 10; orthoid tartomány az oszthatóságra vonatkozó tulajdonságainak megmaradása III. 13, IX. 7.

Osztó I. 5.

Algebrai o. IX. 8; complementáris o. III. 1; forma többszörös osztója III. 22; legnagyobb közös o. I. 6, IX. 7, 9; raczionális és egész forma osztója IV. 1; raczionális és egész szám osztója IV. 1; törzso. IV. 2; valódi o. I, 5. IX. 10; zérus osztója IV. 9; zérus valódi osztója IV. 8, 9.

Osztó-láncz VII. 5:

Véges o. VII. 5.

Osztórendszer VII. 2:

O. fokozatszáma VII. 10; o.,

melynek teljes maradékrendszer megfelel VIII. 1; osztórendszerek compositiója VII. 3; osztórendszerek szorzata VII. 3; æquivalens osztórendszerek VII. 2; componált o. VII. 3; felbonthatatlan o. VII. 4; főosztályhoz tartozó o. VII. 10; irreducibilis o. VII. 4; mod. ($P^{(k)}$) æquivalens osztórendszerek VIII. 5; mod. ($P^{(k)}$) relativ törzs-osztórendszerek VIII. 5; relativ törzs-osztórendszerek VII. 2; törzs-o. VII. 4.

Osztótartomány VII. 3.

Összeadás I. 1.

Ö. közönséges törvénye I. 2.

Összeg I. 2, II. 1, IV. 6.

Összesség:

Algebrai számok összessége IV. 22; complex számok összessége IV. 22; valós számok összessége IV. 22.

Összetartozó törzsideálok IX. 12.

Összresolvens V. 4.

Permutáczió II. 14, IV. 10, 14, 23.

Permutácziók csoportja IV. 23.

π-szám IV. 21.

Poisson VI. 17.

Poisson-féle:

Resultáns P. előállítása VI. 17.

Polynomialis tétel II. 7.

Pont V. 6.

Egyenesnek képzetes pontja IX. 8.

***P*-rendszer:**

$k+1$-edfokozatú *P*-rendszer VIII. 2.

Primitiv forma III. 9, IX. 4:

Tulajdonképeni p. f. IX, 13.

Pseudoholoid tartomány VIII. 2:

Teljes p. t. VIII. 2.

Pseudoorthoid:

P. tartomány VIII. 2; p. tartományból származó genus-tartomány mod. ($P^{(k)}$) VIII. 9; legkisebb p. tartomány, melyben valamely congruentiának van gyöke VIII. 9; mellérendelt p. tartomány VIII. 2.

Quadratikus irraczionalitás:

Valós qu. i. IV. 5.

Raczionális:

R. forma felbontása törzsformákra IV. 3; r. függvény IV. 20; r. műveletek V. 1; r. számok tartománya I. 1, IV. 20; r. tartomány IV. 20.

Raczionális és egész:

R. és e. forma felbontása törzsformákra IV. 2; r. és e. forma osztója IV. 1; r. és e. formák æquivalentiája IV. 1; r. és e. ideális mennyiség IX. 9; r. és e. szám felbontása törzsténye-

zőkre IV. 1; r. és e. szám osztója IV. 1; r. és e. számok æquivalentiája IV. 1; $[[1], x_1, \ldots, x_{k+1}]$ (mod. $P^{(k)}$)) tartomány r. és e. formája VIII. 7; genus-tartománynak az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag r. és e. mennyisége IX. 2.

Raczionális függvény:
Egyenlet gyökeinek r. függvénye IV. 15.

Raczionális gyök:
Egyentet r. gyöke III. 12.

Raczionális mennyiség:
Genus-tartománynak az $[A, x_1, \ldots, x_m]$ tartományra vonatkozólag r. mennyisége IX. 1.

Raczionális tartomány IV. 20:
R. t. basisa IV. 22; r. t. eleme IV. 21; r. t. rendszáma IV. 22; absolut r. t. IV. 20; természetes r. t. IV. 20.

Rados II. 12.

Rang:
Determináns rangja V. 15; egyenletrendszer rangja V. 6; egyenletrendszer értelmezte sokaság rangja V. 6; matrix rangja V. 15; orthoid formarendszer rangja V. 6.

Recziprok lineáris transformatio II. 18.

Reductio:
Homogén lineáris diophantikus egyenlet megoldásának reductiója VIII. 10—18.

Redukált:
R. forma II. 13; r. resolvens V. 5.

Relativ:
R. æquivalentia I. 5, 12, IX. 13; r. egész forma IX. 4; r. egész mennyiség IX. 4; r. törzs-osztórendszerek VII. 2; mod. $(P^{(k)})$ r. törzs-osztórendszerek VIII. 5.

Relative æquivalens I. 5, 12, IX, 13.

Rendszám:
Csoport rendszáma IV. 24; egyenlet rendszáma IV. 12; genus rendszáma IV. 15; genus-tartomány rendszáma IV. 15; genus-tartomány mennyiségének rendszáma IV. 15; raczionális tartomány rendszáma IV. 22.

Rendszer:
Alapr. VIII. 2, IX. 1; általános formar. VI. 1; congruentiar. IX. 15; egyenletr. V. 1; modulusr. I. 10, VII. 2; homogén egyenletek rendszere VI. 13; lineáris diophantikus egyenletek rendszere VII. 1; osztór. VII. 2.

Resolvens:
R. forma III. 18; r. forma mod. $(P^{(k)})$ VIII. 6. 7; Galois-féle r. IV. 11, 13; minimális r. V. 11; orthoid tartományra vonatkozólag irreducibilis $h+1$-edfokozatú részlet-r. V. 7;

összr. V. 4; redukált r. V. 5; részlet-r. V. 4; teljes $h+1$-edfokozatú részlet-r. V. 4.

Resultáns:
R. invariáns-tulajdonsága VI. 12; r. képezési törvénye VI. 10; r. mint symmetrikus forma III. 24; r. Poisson-féle előállítása VI. 17; resultánsok szorzás-tétele VI. 11; általános formarendszer resultánsa VI. 3; általános formarendszer resultánsának alaptulajdonságai VI. 5; általános lineáris formák resultánsa VI. 11; homogén formák rendszerének resultánsa VI. 12; két forma resultánsa III. 15; két forma resultánsának alaptulajdonságai III. 15, 16; speciális formák resultánsa VI. 3.

Részlet-resolvens V. 4:
Orthoid tartományra vonatkozólag irreducibilis $h+1$-edfokozatú r. V. 7; teljes $h+1$-edfokozatú r. V. 4.

Richelot III. 14.

Runge IV. 1.

Schläfli VI. 18.

Schönemann VIII. 2.

Sereg V. 13:
k-tagú s. V. 13.

Singuláris:
S. egyenletrendszer VI. 30; s. mennyiség I. 3, IV. 9; homogén lineáris diophantikus egyenlet megoldásának s. esetei VIII. 14, 16, 17, 19; sokaság s. eleme V. 6.

Singularitás:
Genus singularitásai IX. 31.

Sokaság:
S. eleme III. 21, V. 6; s. kétszeres eleme V. 6; s. singuláris eleme V. 6; s. többszörös eleme V. 6; s. végtelen eleme V. 6; algebrai s. V. 6; föltétlenül irreducibilis s. V. 7; holoid tartományból ([A]-ból) származó m—k-szoros s. III. 21; lineáris s. V. 12; m-edfokozatú s. főelőállítása V. 10; orthoid tartományban irreducibilis s. V. 7; tiszta elsőfokozatú s. főelőállítása V. 10; tiszta $h+1$-edfokozatú s. V. 6; tiszta s. főelőállítása V. 9, 10; transcendens s. V. 6; vegyes $h+1$-edfokozatú s. V. 6.

Sokaság foka:
Orthoid tartományra vonatkozólag algebrai mennyiségek országából ({A}-ból) származó m—h—1-szeres s. f. V. 6.

Sokaság fokozata:
Egyenletrendszer értelmezte s. f. V. 6.

Sokaság rangja:
Egyenletrendszer értelmezte s. r. V. 6.

Sokszorosság:
Gyökrendszer vagy megoldás sokszorosságaV.5,VII.52,8—30.

Speciális formák resultánsa VI. 3.
Substitutio II. 10, IV. 23.
Substitutiók csoportja IV. 23; substitutiók egymásutánja IV. 23; substitutiók szorzata IV. 23; azonos s. IV. 24; invers s. IV. 24; lineáris s. II. 18.
Súly VI. 5.
SYLVESTER III. 14.
SYLVESTER-féle determináns III. 14, VI. 4.
Symmetrikus forma II. 10, 14: Discrimináns, mint s. f. III. 25; elemi s. II. 11, VI. 18; resultáns, mint s. f. III. 24; több mennyiség-rendszer s. formája VI. 18; typikus s. f. VI. 18.
Szabályos forma II. 19: mod. $(P^{(k)})$ sz. f. VIII. 4; x_i-re nézve sz. f. II. 19.
Szám I. 1: Alaprendszer elemeinek száma IX. 14; algebrai sz. I. 1, III. 21, IV. 7; complex sz. III. 21, IV. 5, 6; e szám IV. 21. határozatlan sz. I. 1; ideális mennyiségek osztályainak száma IX. 13; π szám IV. 21; nem szabályos törzssz. IX. 25; természetes törzsszám I. 5; transcendens sz. IV. 21.
Számelmélet: Analitikai sz. IX. 13.
Szét nem eső kúpszelet V. 6.
Szorzás I. 1: Sz. közönséges törvénye I. 3.
Szorzástétel: Resultánsok szorzástétele VI. 11.
Szorzat I. 3, II. 1, IV. 6: Különbségek szorzata II. 11; osztórendszerek szorzata VII. 3; substitutiók szorzata IV. 23.
Szűkebb: Sz. æquivalentia VII. 2; sz. æquivalentia mod. $(P^{(k)})$ VIII. 5; sz. értelemben vett ideális mennyiség IX. 8.

Tartalmazás: T. fogalma VII. 2, 4; t. mod. $(P^{(k)})$ fogalma VIII. 5.
Tartalom: Egyenletrendszer tartalma V. 5; két osztórendszer legnagyobb közös tartalma VII. 2; két osztórendszer legnagyobb közös tartalma mod. $(P^{(k)})$ VIII. 5.
Tartomány: Absolut raczionális t. IV. 20; æquivalentiat. I. 12; $[A, x]$ t. II. 1; $[A, x_1, \ldots, x_m]$ t. II. 2; congruentiat. I. 10; diophantikus t. VII. 1; $[1]$ t. I. 4; (1) t. I. 4; $[[1], x_1, \ldots, x_k]$ (mod. $(P^{(k)})$) t. VIII. 2; $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m]$ (mod. $(P^{(k)})$) t. VIII. 2; $(1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m)$ (mod. $(P^{(k)})$) t. VIII. 2; elsőrendű infinitesimális t. V. 8; $[\mathfrak{G}]$ t. IX. 7; $(\mathfrak{G})$ t. IX. 10;

Galois-féle t. IV. 13; Galois-féle tart. mod. ($P^{(k)}$) VIII. 9; genus-tartomány egész mennyiségeinek tartománya, [Γ] IX. 3; genus-tartomány törzstartománya IV. 14; genus-tartományból származó egész algebrai formák tartománya, $[\Gamma]_w$ IX. 3; holoid t. I. 4; hyperorthoid t. IV. 9; jól értelmezett t. III. 1, IV. 3, 16; jól értelmezett teljes t. III. 8; legkisebb orthoid t., mely valamely irreducibilis egyenlet gyökét tartalmazza IV. 7; legkisebb pseudoorthoid t., melyben valamely congruentiának gyöke van VIII. 9; mellérendelt orthoid t. I. 4, III. 12; mellérendelt pseudoorthoid t. VIII. 2; $\sqrt{-k}$ t. I. 7; $\sqrt{-5}$ t. I. 8, IX. 7; nem valódi holoid t. I. 4; orthoid t. I. 4, IV. 9, 22; orthoid tartományból származó genus-t. IV. 14; osztó-t. VII. 3; pseudoholoid t. VIII. 2; pseudoorthoid t. VIII. 2; pseudoorthoid tartományból származó genus-t. mod. ($P^{(k)}$) VIII. 9; raczionális t. IV. 20; raczionális számok tartománya I. 1, IV. 20; teljes genus-t. IX. 10; teljes holoid t. I. 6; teljes pseudoholoid t. VIII. 2; természetes raczionális t. IV. 20; valódi congruentiat. I. 10; valódi genus-t. IX. 10; valódi holoid t. I. 4.

Teljes:

T. genus-tartomány IX. 10; t. $h+1$-edfokozatú részlet-resolvens V. 4; t. holoid tartomány I. 6; t. maradékrendszer VII. 8, VIII. 1; t. pseudoholoid tartomány VIII. 2; t. részlet-resolvens fokozata V. 4; t. tartományokból származó formákra vonatkozó alaptétel III. 8.

Teljes tartomány:

Jól értelmezett t. t. III. 8.

Tényező:

Compositio tényezői VII. 3.

Tér:

m-dimensiós t. V. 6.

Térgörbe főelőállítása:

Tiszta algebrai t. f. V. 9.

Természetes:

T. raczionális tartomány IV. 20; t. törzsszám I. 5.

Test IV. 22.

Tiszta:

T. algebrai térgörbe főelőállítása V. 9; t. elsőfokozatú sokaság főelőállítása V. 10; t. $h+1$-edfokozatú egyenletrendszer V. 6; t. $h+1$-edfokozatú sokaság V. 6; t. sokaság főelőállítása V. 9, 10.

Több mennyiségrendszer symmetrikus formája VI. 18.

Többszörös I. 5.

Többszörös elem:
Sokaság t. eleme V. 6.
Többszörös gyök:
Egyenlet t. gyöke IV. 13.
Többszörös osztó:
Forma t. osztója III. 22.
Többtagú modulusrendszer I. 10, VII. 2.
Tört ideális mennyiség IX. 10.
Törzsforma IV. 2:
T. orthoid formatartományban IV. 3; t. a raczionális formák tartományában IV. 3; t. a raczionális és egész formák tartományában IV. 2; æqu. mod. P t. IX. 18; kritikus t. IX. 27.
Törzsideál IX. 12.
T. foka IX. 12; összetartozó törzsideálok IX. 12.
Törzsmennyiség I. 5, IX. 10.
Törzs-modulusrendszer VII. 4.
Törzsosztó IV. 2.
Törzs-osztórendszer VII. 4:
mod. $(P^{(k)})$ relativ törzsosztórendszerek VIII. 5; relativ törzs-osztórendszerek VII. 2.
Törzsrendszer VII. 4:
Absolut t. VII. 4; absolut t. $[[1], x_1, \ldots, x_k]$-ban VIII. 1—4, 8.
Törzsszám:
Nem szabályos t. IX. 25; természetes t. I. 5.
Törzstartomány:
Genus-tartomány törzstartománya IV. 14.
Transcendens:
T. függvény IV. 21; t. mennyiség IV. 21; t. sokaság V. 6; t. szám IV. 21.
Transformált:
T. egyenletrendszer V. 2; t. forma II. 18.
Transformatio:
T. együtthatói II. 18; általános (homogén) lineáris t. II. 19; koordináta-t. V. 3; lineáris t. II. 18; recziprok lineáris t. II. 18.
Transformatio determinánsa:
Lineáris t. d. II. 18.
Tulajdonképeni primitiv forma IX. 13.
Tulajdonságok:
Genus-tartománynak az összeadás és szorzás révén származó kapcsolatokra vonatkozó tulajdonságai IX. 1; ideális mennyiségeknek az oszthatóságra vonatkozó tulajdonságai IX. 10.
Tulajdonságok megmaradása:
Orthoid tartomány az oszthatóságra vonatkozó tulajdonságainak m. III. 13, IX. 7.
Typikus symmetrikus forma VI. 18.
Typus VI. 18.
Egyformájú t. VI. 19; k-formájú t. VI. 19.

VAHLEN VI. 11.

Valódi:
V. æquivalentiatartomány I. 12; v. congruentiatartomány I. 10; v. egész mennyiségek alaprendszere IX. 21—23; v. genus-tartomány IX. 10; v. holoid tartomány I. 4; v. irreducibilis mennyiség I. 5; v. modulusrendszer I. 10, VII. 2; v. osztó I. 5, IX. 10.
Valódi megoldás:
Homogén egyenletek rendszerének v. megoldása VI. 13.
Valódi osztó:
Zérus v. osztója IV. 8, 9.
Valós:
V. quadratikus irraczionalitás IV. 5; v. számok összessége IV. 22.
Változó mennyiség:
Orthoid tartományra vonatkozólag algebrai mennyiségek országában ({A}-ban) korlátlanul v. m. V. 1.
Variáczió II. 12.
Varietás V. 6.
Véges osztóláncz VII. 5.
Végtelenben fekvő megoldások:
Egyenletrendszernek a v. f. megoldásai VI. 13.
Végtelen elemek:
Sokaságnak v. elemei V. 6.
Végtelen kis mennyiség IV. 9:
Elsőrendű v. k. m. V. 8.
Végtelen nagy mennyiség IV. 9.
Vegyes:
V. $h+1$-edfokozatú egyenletrendszer V. 6; v. $h+1$-edfokozatú sokaság V. 6.
Vonal V. 6.

WARING VI. 18.
WEBER IX. 1, 8.
WEIERSTRASS IV. 8.

Zérus I. 2, 3. IV. 6, VIII. 2:
Z. osztója IV. 9; z. valódi osztója IV. 8, 9.
Zérushely III. 19.

BUDAPEST