AZ

ELLIPTIKAI FÜGGVÉNYEK

ALKALMAZÁSÁRÓL

A

MAGASABB FOKU EGYENLETEK

ELMÉLETÉRE.

IRTA

Dr. KÖNIG GYULA.

PEST.

EGGENBERGER-FÉLE AKAD. KÖNYVKERESKEDÉS.

(HOFFMANN ÉS MOLNÁR.)

1871.

Pest, 1871. Nyomatott az „Athenaeum“ nyomdájában.

AZ ELLIPTIKAI FÜGGVÉNYEK ALKALMAZÁSÁRÓL

a magasabb foku egyenletek elméletére.

Dr. König Gyulától.

(Előterjesztetett a III. osztály ülésén 1871. April 17).

1.

Történelmi jegyzetek.

Azon mennyiségtani feladatok története, melyekkel a következő lapok foglalkoznak, egyik legtanulságosabb szakát képezik tudományunk fejlődésének, megmutatván, mily szoros összefüggés létezik ennek minden ága között, még ott is, hol azt legkevésbé sem gyanították. Teljesen különvált utakon fejlődött az algebra — az egyenletek föloldásának tana — és az elliptikus, valamint az ezekből átalánosított Abel-féle függvények elmélete ; csak a legujabb idő deríté ki a mély összefüggést, mely e két tant egybeköti.

Az egyenletek föloldásának tana már az ó korban veszi eredetét. A görögök ismerték a másodfoku egyenletek föloldását. A XVI. században sikerült azután Scipio Ferreo és Tartaglianak a harmadfokú, valamivel később Ferrarinak a negyedfokú egyenletek föloldása. De minden további törekvés hiában volt. Lagrange felfedezte, hogy minden egyenlet megoldása egy másik egyenlettől, az ugynevezett feloldótól (resolvente) függ, mely a negyedik fokon túl magasabb az eredetileg föladottnál. Ruffini nemsokára már kifejezést

adott a valószinüségnek, hogy a magasabb mint negyedfokú egyenletek *algebraice* meg nem oldhatók és Abel ezután szigorúan be is bizonyitá e fontos tételt.

Az átalános n-edfokú egyenlet

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \cdots p_n = 0$$

meg van oldva, ha sikerült az x-nek n értékét a $p_1, \ldots p_n$ együtthatók által kifejezni; meg van oldva algebraice, ha ezen kifejezések csak algebraicus mütéteket, azaz legfelebb gyökkivonást rejtenek magukban. Abel tétele tehát azt mondja, hogy hasonló alakzatok, mint a 2, 3, és 4-edfokú egyenletek számára léteznek, magasabb foknál nem fordulhatnak elő. E ponton soká szünetelt e tan; csak 1858-ban tette közzé Hermite az ötödfokú egyenletek megoldását az elliptikus függvények segitségével, azaz, hol az ismeretlennek kifejezésében az egyenlet együtthatói által e tanból vett függvényjelek szerepelnek.

Azonban az elliptikus függvények terén is elég hosszú út kellett ezen eredmény elérésére. Miután Legendre a tan alapját megvetette az ellipticai egészletek részletes vizsgálatával (melyeket ő a mienktől eltérő terminologiával függvényeknek nevez), Abel és Jacobi egyszerre jutottak az ezekből az u. n. „megfordítás" által keletkező függvényekhez. Ezek nemcsak a változótól, hanem még egy határzatlan állandótól, az u. n. mérfok, modultól függvén, keletkezett a feladat, kutatni az összefüggést, mely különböző modullal biró elliptikus függvények közt létezik. Ez az átalakítás (transformatio) nagyhirü problemája. Ennek folyamában mintegy önként merülnek föl bizonyos magasabb fokú egyenletek, a modular-egyenletek és mások, melyek azonban végszerü helyettesités által átmennek a már említettekbe. Az egyenletek megoldása az átalakitás elméletéből foly; de fokuk mindig páros szám. A főérdek pedig az egyenletek elméletében azokat illeti, melyeknek foka törzsszám. Az oly korán elhunyt Galois mondá ki azután, hogy e modularegyenletek fokát bizonyos esetekben egygyel lejebb lehet szállítani. Hermite volt végre, ki e reductiót valóban kivitte, és kinek sikerült az igy 5. fokra hozott 6-odfokú

modularegyenletet az általános ötödfokú egyenlettel azonosítni. Ettől egészen eltérő módszert, de mely szintén az elliptikus függvények átalakításából vett egyenleteken alapszik, köszönhetünk továbbá Kroneckernek.

A föladat, melyet itt magamnak kitűztem, a modularegyenletek tulajdonait részletesen vizsgálni és ebből kiindulva átalánosan meghatározni az egyenletek azon osztályát, melyek ellipticus függvények által föloldhatók. Mielőtt azonban ehhez foghatok, szükséges lesz az átalakítási elmélet legfontosabb tételeit összeállítani.

2.

Tételek az elliptikai függvények átalakításának elméletéből.

Ismeretes, hogy a következő kifejezés

$$u = \int_0^x \frac{dx}{\sqrt{(1-x^2)\,(1-c^2x^2)}}$$

neveztetik első faju elliptikai normálegészletnek, és az ebben előforduló c határzatlan állandó az egészlet modulusának, hogy ezen egyenlet megfordítása adja az első elliptikai függvényt a sinus amplitudo-t:

$$x = sn.\,u,$$

mely kétszakaszos, és melynek szakaszai $4C$ és $2iC'$, ha

$$C = \int_0^1 \frac{dx}{\sqrt{(1-x^2)\,(1-c^2x^2)}},$$

és

$$C' = \int_0^1 \frac{dx}{\sqrt{(1-x^2)\,(1-[1-c^2]x^2)}}.$$

Megjegyzendő még a sinus ampl. kifejezése két sor hányadosa által, mely következő:

$$sn\,(u,c) = \frac{1}{\sqrt{c}} \frac{\vartheta_1\,(v,\tau)}{\vartheta_0\,(v,\tau)},$$

a hol

$$\vartheta_1(v,\tau) = 2q^{\frac{1}{4}} \sin v\pi - 2q^{\frac{9}{4}} \sin 3v\pi + \cdots$$
$$\vartheta_0(v,\tau) = 1 - 2q \cos. 2v\pi + 2q^4 \cos. 4v\pi + \cdots$$

és még

$$v = \frac{u}{2C},$$

végre

$$\tau = \frac{iC'}{C},$$

mely utolsó mennyiség τ a thetafüggvény modulusának neveztetik.

Térjünk most már át az átalakítási feladat szoros meghatározására.

Az n-edfokú átalakítás két mennyiségnek, az a együttható és k átalakított egészleti modulusnak oly meghatározásában áll, hogy

$$y = sn\left(\frac{u}{a}, k\right)$$

továbbá a cosinus ampl. és delta ampl.-nak nevezett két ell. függvény :

$$\sqrt{1-y^2} \text{ és } \sqrt{1-k^2y^2}$$

az

$$x = sn(u,c); \sqrt{1-x^2} = cn(u,c); \sqrt{1-x^2} = dn(u,c)$$

kifejezések n-edfokú végszerű függvényei legyenek.

Be van bizonyítva, — itt csak az eredményeket soroljuk elő röviden, — hogy ekkor az x és y hoz tartozó thetafüggvények modulusai, τ és τ' közt a következő összefüggés létezik :

$$\tau = \frac{b_0 + b_1\tau'}{a_0 + a_1\tau'},$$

a hol még

$$a_0 b_1 - a_1 b_0 = n,$$

az átalakítás foka. — Viszont most az átalakítás tárgyalásában ezen utolsó definitióból indulván ki, a különböző n-edfokú átalakításokat ugy osztályozhatjuk, hogy az

$$a_0,\ a_1,\ b_0,\ b_1$$
$$a_0',\ a_1',\ b_0',\ b_1'$$

számcsoportok által jelzett átalakítások ugyanazon vagy

külön osztályba tartoznak, ha az átmenet az elsőtől a másodikhoz lehetséges vagy nem oly átalakítás által, melynek

$$\alpha_0, \alpha_1, \beta_0, \beta_1$$

csoportjában

$$\alpha_0 \beta_1 - \alpha_1 \beta_0 = 1.$$

Hosszabb fejtegetések mutatják, hogy az osztályok mindig véges számmal vannak, és pedig, ha a transformatio foka

$$n = p_1^{\alpha} p_2^{\beta} \cdots p_r^{\varrho},$$

hol $p_1, p_2, \ldots p_r$ az n-ben foglalt törzsszámokat jelentik, a különböző osztályok száma

$$p_1^{\alpha-1} p_2^{\beta-1} \cdots p_r^{\varrho-1} (p_1 + 1)(p_2 + 1) \ldots (p_r + 1),$$

mely kifejezésről megjegyezzük, hogy, ha az $\alpha, \beta, \ldots \varrho$ kitevők egyenlők 0 vagy 1-gyel, ezen szám az n minden osztójának összegével egyenlő. — Ezentúl pedig csak ily n-eket fogunk a vizsgálat tárgyává tenni, melyek négyzetes osztóval nem bírnak, miután a többiek semmi ujat nem adnak. Az ily fokú átalakítás mindig átalakításra és sokszorozásra vezethető vissza.

Ezen előzmények után átmehetünk a modularegyenletek képezéséhez.

Ha ismét c az adott elliptikus egészlet modulusa, $\sqrt[4]{c}$-nek tulajdonképen 4 különböző értéke van, de a következőkben e gyök alatt mindig egy értéket akarunk gondolni, t. i.

$$\sqrt[4]{c} = \sqrt{2} \sqrt[8]{q} \{(1+q^2)(1+q^4)(1+q^6) \ldots\}^2 (1-q)(1-q^3)(1-q^5) \ldots$$

hol, mint azelőtt

$$q = e^{\pi i \tau},$$

és τ az illető thetafüggvény modulusa. Igy tehát az ellipt. egészlet modulusának egy bizonyos negyedik hatványgyöke mint a hozzátartozó thetafüggvény modulusának egyértékű függvénye határoztatott meg, a mit Hermite után következőkép jelölünk :

$$u = \sqrt[4]{c} = \varphi(\tau).$$

Legyen most már az átalakítási fok törzsszám, p. — Az előbbiek szerint akkor $p+1$ egymástól különböző osztály létezik; válaszszunk mindegyikből egy képviselőt és pedig a következő számcsoportok által jellemzetteket:

$$1,\ 0,\ 16\xi,\ p$$

hol ξ egymásután a $0, 1, \ldots p-1$ értékeket veheti föl, és

$$p,\ 0,\ 0,\ 1.$$

Az átalakítási feladat megfejtése az átalakított egészleti modulus meghatározására a következő alakzatot adja, ha ismét $v = \sqrt[4]{k}$ az átalakított thetamodulusnak

$$\tau' = \frac{b_0 + b_1 \tau}{a_0 + a_1 \tau}$$

ugyanazon egyértékű függvénye, mint $u = \sqrt[4]{c}$ a τ-nak;

$$v = (\sqrt[4]{c})^p \, snc.\frac{4C}{p}(\tau - 16\xi) \, snc.\frac{8C}{p}(\tau - 16\xi) \ldots snc.\frac{2(p-1)C}{p}(\tau - 16\xi)$$

hol

$$\xi = 0, 1, \ldots, p-1;$$

$$\left(\text{snc.} = \text{sinus coamplitudo} = \frac{cn.}{dn.}\right)$$

a mi p értéket ad, a $\overline{p+1}$-edik osztály számára pedig:

$$v = (\sqrt[4]{c})^p \, snc.\frac{4C}{p} \, snc.\frac{8C}{p} \cdots snc.\frac{2(p-1)C}{p}.$$

Ha pedig a Hermite-féle függvényjellel élünk, az

$$u = \varphi(\tau)$$

átalakítottjai,

$$v = \varphi\left(\frac{\tau - 16\xi}{p}\right),$$

hol $\xi = 0, 1, \ldots, p-1$, és

$$v = \left(\frac{2}{p}\right) \varphi(p\tau).$$

Ez utolsóban $\left(\frac{2}{p}\right)$ az ismert Legendre-féle jel, melynek értéke

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Ezek után képesek vagyunk mutatni, hogy létezik egy $\overline{p+1}$-ed fokú algebraicus egyenlet, melynek gyökei az elő-

sorolt v-értékek, és melyben a v (mint ismeretlen) egyes hatványainak együtthatói az u-nak egész függvényei. Ezen egyenlet neveztetik a p-fokú átalakításhoz tartozó modulareyenletnek. Alakja, ha például $p = 5$, a következő:

$$v^6 + 5u^2v^2(v^2 - u^2) - 4uv(1 - u^4v^4) - u^6 = 0.$$

Mi röviden így fogjuk jelölni:

$$\Theta_p(v, u) = 0.$$

Eddig csak a törzsszámú átalakításhoz tartozó modulareyenlet fogalma határoztatott meg; azonban ennek kiterjesztése könnyü. Ha

$$n = p_1 p_2 \ldots p_r$$

négyzetes osztó nélkül, létezik

$$(p_1 + 1)(p_2 + 1) \ldots (p_r + 1)$$

különböző osztály és ugyanily fokú modulareyenlet. — A gyököknek az előbbihez hasonló kifejezéseit könnyen le lehet hozni; azonban itt inkább oly elvre akarunk figyelmeztetni, mely ezek képzését az előbbiekétől teszi függővé, de épen ennél fogva a későbbi számításokban igen alkalmas.

Legyen az átalakítás foka $n = p_1 p_2$, akkor egymásután vihetjük át a p_1 és p_2-fokú átalakítást; az eredmény ugyanaz lesz. Képezzük tehát a p_1 és p_2 fokokhoz tartozó modulareyenleteket:

$$\Theta p_1(w, u) = 0$$
$$\Theta p_2(v, w) = 0$$

és helyettesítsük a másodikban w-t, e mennyiségnek az elsőből folyó értékei által. Világos, hogy így $p_1 + 1$ különböző Θp_2-egyenletet kapunk, melynek gyökei az u $p_1 p_2 = n$-edfokú átalakítottjai. Azaz, a $p_1 p_2$-fokú átalakításhoz tartozó modulareyenlet

$$\Theta p_1 p_2(v, u) = 0$$

nem más, mint a w kiküszöbölésének eredménye a

$$\Theta p_1(v, w)$$

és

$$\Theta p_2(w, u)$$

modulareyenletekből.*)

*) Hosszadalmas volna az említett tételekre mindenütt a kútforrásokat idézni, l. Königsberger kézikönyvét: „Transformation der elliptischen Functionen."

3.

A modularegyenletek gyökeinek cyclusai és kifejezései tört hatványsorok által.

Valamely többértékű függvényt magába visszatérő görbén folytatván, tudjuk, hogy visszajövén a kiindulási ponthoz, nem kell ugyanekkor a függvény eredeti értékét visszanyernünk, ha a görbe u. n. elágazási pontot rejt magában, azaz olyant, melyben a függvény több értéke összeesik. Csak többszöri körzés után tér vissza a függvény eredeti értékéhez; azon értékek pedig, melyekbe egymásután átmegy, az illető elágazási pont körül egy cyclushoz tartozóknak mondatnak.

A használandó elmélet bővebb kifejtése végett Puiseux Liouville lapjának XV-dik kötetében foglalt értekezésére utalunk.

A modularegyenletet többértékű algebraicus functió meghatározásának tekintvén, keressük ennek elágazási pontjait. Mint ilyenek ismeretesek egyelőre a 0-pont és az egységnek nyolczadgyökei, melyeket α-val akarunk jelölni. Mint a törzsszámú átalakításhoz tartozó modularegyenletek elméletéből ismeretes (l. Sohncke, Crelle's Journal, 16.), ekkor az első esetben a v-nek mind a $p+1$ értéke összeesik, ha pedig $u = \alpha$, azaz az egészleti modulus négyzete egyenlő az egységgel, akkor az egyenlet p gyöke egyenlő

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

a $p+1$-edik pedig az egység.

Első feladatunk legyen, most a nem törzsszámhoz tartozó modularegyenlet gyökeinek kifejezése a φ-függvény által. Az eredmény már ismeretes ugyan; de nem lesz talán helytelen a lehozást is közölni, miután a használandó módszer az eddig használtaknál könnyebb és rövidebb. Alapszik a már említett elven, miszerint a nem törzsszámú átalakításhoz tartozó modularegyenlet az ilyenek közt való kiküszöbölés eredményének tekinthető.

A φ-függvény definitiója volt:

$$\varphi(\tau)=\sqrt[8]{2}\sqrt[8]{q}\,\{(1+q^2)(1+q^4)..\}^2(1-q)(1-q^3)(1-q^5)...$$

hol $q=e^{\pi i\tau}$. Legyen most a tárgyalandó átalakítási fok

$$n=p_1 p_2$$

akkor a

$$\Theta p_1 (v,w)=0$$

egyenletnek gyökei:

$$\varphi\left(\frac{\tau'-16\xi'}{p_1}\right) \text{ hol } \xi'=0,1,\ldots,p-1$$

és

$$\left(\frac{2}{p_1}\right)\varphi(p_1\tau')$$

a

$$\Theta p_2 (w,u)=0$$

egyenleté hasonlókép.

$$\varphi\left(\frac{\tau-16\xi}{p_2}\right) \text{ hol } \xi=0,1,\ldots p_2-1$$

és

$$\left(\frac{2}{p_2}\right)\varphi(p_2\tau).$$

Tudjuk — az említett elv szerint — hogy megkapjuk a

$$\Theta p_1 p_2 (v,u)=0$$

egyenlet gyökeit, ha a τ' helyett a Θp_2 gyökeiben a φ-jel alatt álló értékeket vezetjük be; mert evvel világos, hogy nem tettünk mást, mint a p_1 és p_2 fokú átalakítás egymásutáni kivitelét. — Csak az tehetne nehézséget, hogy a φ-jel előtt álló $\left(\frac{2}{p_2}\right)$ positiv vagy negativ egységet jelenthet. De, mint ezt az elmélet elemeiből itt ismeretesnek kell feltennünk, a modularegyenlet semmit nem változik, ha u és v fölcseréltetik $-u$ és $-v$-vel. — Ha tehát τ' az illető érték által helyettesíttetett, a végeredmény elé csak $\left(\frac{2}{p_2}\right)$ irandó, és a $\Theta p_1 p_2$ gyökét megtaláltuk. Ezen előzmények után ezeket már föl is irhatjuk; lesznek a következők:

$$\left.\begin{array}{l} \varphi\left\{\dfrac{\dfrac{\tau-16\xi}{p_2}-16\xi'}{p_1}\right\} \\ \left(\dfrac{2}{p_2}\right)\varphi\left\{\dfrac{p_2\,\tau-16\xi'}{p_1}\right\} \\ \left(\dfrac{2}{p_1}\right)\varphi\left\{p_1\,\dfrac{\tau-16\xi}{p_2}\right\} \end{array}\right\} \quad \xi'=0,1,\ldots,p_1-1 \quad \xi=0,1,\ldots,p_2-1$$

és

$$\left.\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\varphi(p_1\,p_2\,\tau)\right]$$

összesen $(p_1+1)(p_2+1)$ érték. — Rövidebb alakba öltve, lesz az első, mely az ξ és ξ' különböző csoportozásai által $p_1\,p_2$ értéket képvisel, miután a φ-jel alatt álló kifejezés

$$\frac{\tau-16(\xi+p_2\,\xi')}{p_1\,p_2}$$

és $\xi+p_2\,\xi'$, mint könnyen látható, a 0-tól a $\overline{p_1\,p_2-1}$-ig minden értéket egyszer vesz föl:

$$\varphi\left(\frac{\tau-16\,x}{p_1\,p_2}\right),\quad x=0,1,\ldots,p_1\,p_2-1 \qquad (1)$$

A második gyökcsoport megtarthatja eredeti alakját:

$$\left(\frac{2}{p_2}\right)\varphi\left(\frac{p_2\,\tau-16\,x}{p_1}\right) \qquad (2.)$$

és x egymásután $0,1,\ldots p_1-1$ értékeket vehetvén föl, p_1 gyököt képvisel. A harmadik csoport átváltoztatására nézve megjegyezzük, hogy a φ-függvény szakaszos és pedig

$$\varphi(\tau+16)=\varphi(\tau)$$

t. i. a változó csak $q=e^{\pi i\tau}$ mennyiségben fordul elő; q-nak egész hatványai tehát már 2 re nézve is szakaszosak; ekkor a q csak $e^{2\pi i}$ azaz egységgel szoroztatván; de még

$$\sqrt[8]{q}=e^{\frac{\pi i\tau}{8}}=e^{\frac{\pi i(\tau+16)}{8}}=e^{\frac{\pi i\tau}{8}}$$

is előfordul; tehát 16 lesz a szakasz. — Az eredeti alak

$$\varphi\left(\frac{p_1\,\tau-16\,x\,p_1}{p_2}\right)$$

hol $x=0,1,\ldots,p_2-1$. A magasabb számtanból most már tudjuk, hogy miután p_1 és p_2 relativ törzsszámok, az xp_1 által képviselt számok p_2 osztóra nézve a $0,1,\ldots p_2-1$ maradékokat hagyják. — A hányadost tekintetbe vennünk

nem kell, miután egész szám, és tehát 16-tal szorozva a függvénynek egy szakaszát képezi. Igy tehát a 3. csoport kifejezése :

$$\left(\frac{2}{p_1}\right) \varphi \left(\frac{p_2\, \tau - 16\, x}{p_1}\right) \qquad (3.)$$

A 4-dikre nézve csak megjegyezzük, hogy

$$\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right) = \left(\frac{2}{p_1\, p_2}\right)$$

és ez igy lesz

$$\left(\frac{2}{p_1\, p_2}\right) \varphi\, (p_1\, p_2\, \tau). \qquad (4.)$$

Az út, melyen ez eredményhez jutottunk, oly egyszerű, hogy azt még egy harmadik törzsszorzóra ismételni fölösleges volna. Az átalános eredmény a következő lesz :

Az $n = p_1\, p_2 \ldots . p_\rho$ fokú átalakításhoz tartozó modularegyenlet foka :

$$(p_1 + 1)(p_2 + 1) \cdot \cdot \cdot \cdot (p_\rho + 1)$$

(e kifejezést ezentúl $S(n)$-nel jelöljük), melynek gyökei

$$\left(\frac{2}{d}\right) \varphi \left(\frac{d\, \tau - 16\, x}{d'}\right)$$

alak által adva vannak, hol d egymásután az n minden osztóját jelöli, d' pedig egyenlő $\frac{n}{d}$-vel, végre $x = 0, 1 \ldots d' - 1$.

A használttal teljesen azonos módszer alkalmas e tétel bebizonyítására 3 vagy több törzsszorzónál ; átalánosabban ρ-ról $\rho + 1$-re is lehet következtetni ; de ezek mind oly egyszerű dolgok, hogy itt bátran mellőzhetjük.

Inauguralis iratomban : „Zur Theorie der Modulargleichungen“ a $\Theta\,(v, u)$ egyenlet gyökeit végtelen kis u számára meghatározván, ebből indultam ki a sorfejlődések és cyclusok vizsgálatában. De e meghatározás, mely csak a sor állandóinak kiszámításánál szükséges, kissé hosszadalmas ; miért is itt a gyökök kifejezését a φ-függvény által fogjuk használni.

Lássuk, mi történik $\varphi \left(\frac{d\tau - 16\, x}{d'}\right)$ gyökkel, ha az $u = 0$ körül zárt görbét ir le. Ekkor, mint az u kifejezéséből lát-

hatni, q is ezt teszi, de mig u egyszer irja le, q nyolczszor körzi a zérust azaz lesz q-ból $q.e^{16\pi i}$, de miután:

$$q = e^{\pi i \tau}$$

ez nem más, mint a τ-nak növekedése 16-tal. Azaz a

$$\varphi\left(\frac{d\tau - 16x}{d'}\right)\text{-ból}$$

lesz az első körzés után

$$\varphi\left(\frac{d\tau - 16(x+d)}{d'}\right)$$

a második után

$$\varphi\left(\frac{d\tau - 16(x+2d)}{d'}\right) \text{ stb.}$$

De ezen mennyiségek, hol x a $0, 1, \ldots d'-1$ számok bármelyikét, de mindig ugyanazt jelenti, ugyanazok, mintha az elsőben x ezen értékeket egymásután veszi föl; mert ismét tudjuk a magasabb számtan egy már használt tétele szerint, hogy az

$$x,\ x+d,\ x+2d, \ldots,\ x+(d'-1)d$$

mennyiségek d' osztóra nézve a $0, 1, \ldots . d'-1$ maradékokat adják; a hányados pedig semmi befolyással nem bir, 16-tal lévén szorzandó és igy a függvény szakaszát képezvén.

Ezek után a nyert eredmény következő:

Ha az átalakítási foknak, n-nek egy osztója d, a hozzá tartozó modulareggyenletnek gyökei közt, d egy cyclusba tartozik. Igy tehát annyi cyclus létezik, a mennyi osztója van n-nek. Legnagyobb osztója az n maga, van tehát egy n gyökből álló cyclus; a legkisebb 1, van tehát egy gyök, mely a 0-t körözvén önmagába tér vissza.

Valamint az osztók összegét $S(n)$, ugy most az osztók számát $S'(n)$-nel jelöljük; ugy hogy most röviden mondhatjuk, hogy az *n-ed fokhoz tartozó modulareggyenletnek van $S(n)$ gyöke, mely $S'(n)$ cyclusra oszlik.*

Tudjuk azonkivül a kifejtésből, hogy valóban csak d körzés után és nem talán már előbb tér vissza a gyök eredeti értékéhez. De ebből a 0 pont körül érvényes sorfejlődéseket tüstént leirhatjuk. Mint azt Puiseux a már említett értekezésben bebizonyította, ha valamely pont —a—

körül egy egyenletnek d gyöke képez egy cyclust, ugy mindegyik egy

$$(u-a)^{\frac{1}{d}}$$

hatványai szerint haladó sorba fejthető ki. A modularegyenletnek tehát minden d gyöke a 0 p. körül $u^{\frac{1}{d}}$ szerinti tört hatványsor által fejezhető ki. Határozzuk még meg, micsoda taggal kezdődik valóban a sor. Ha $u=0$, ugy a modularegyenlet minden gyöke szinte 0. Az első állandó tehát minden esetre elesik. Keressük még e zérus rendjét. Legyen

$$q'=e^{\pi i\frac{d\tau-16x}{d'}}=q^{\frac{d}{d'}}e^{-\pi i\frac{16x}{d'}}$$

akkor

$$\varphi\left(\frac{d\tau-16x}{d'}\right)=\sqrt[8]{2}\sqrt[8]{q'}\{(1+q'^2)(1+q'^4)\ldots\}^2(1-q')(1-q'^3)\ldots$$

$$=\sqrt[8]{2}\sqrt[8]{e^{-\pi i\frac{16x}{d'}}}\sqrt[8]{q^{\frac{d}{d'}}}\{(1+q'^2)(1+q'^4)\ldots\}^2(1-q')(1-q'^3)\ldots$$

míg

$$\varphi(\tau)=\sqrt[8]{2}\sqrt[8]{q}\{(1+q^2)(1+q^4)\ldots\}^2(1-q)(1-q^3)\ldots.$$

a miből látni, hogy $\varphi\left(\frac{d\tau-16x}{d'}\right)$ ugy lesz $=0$ mint

$$\{\varphi(\tau)\}^{\frac{d}{d'}}$$

vagyis hogy a modularegyenlet illető gyökének sorfejlődése $u^{\frac{d}{d'}}$ hatványnyal kezdődik; hisz $\varphi(\tau)=u$.

Vezessük be most már a modularegyenlet gyökeinek megkülönböztetésére a következő jeleket. Legyen a mod.-egyenlet gyöke v; lássuk el a betűt két jelzővel; az első jelentse a cyclust, melyhez tartozik, azaz a gyökök számát, mely ebben foglaltatik; a második jelző pedig a gyök sorszámát a cyclusban. Ebben még némi önkény rejlik; ez eltünik, ha megállapítjuk, hogy a második jelző akkor legyen 0, ha a gyöknek a φ általi kifejezésében $x=0$. E szerint lesznek a gyökök $v_{d,\,i}$, hol d az n minden osztóját, és i minden számot jelöl, mely $<d$. — Az előbbiek szerint tudjuk most, hogy p. o.

$$v_{d,0} = c_d^{(d')}\, u^{\frac{d'}{d}} + c_d^{(d'+1)}\, u^{\frac{d'+1}{d}} + \cdots$$

sorfejlődéssel bir. Ha már most az $u = 0$ pontot egyszer körözzük, lesz $v_{d,0}$-ból $v_{d,1}$, u-ból pedig $u.\, e^{2\pi i}$ azaz $u^{\frac{1}{d}}$-ből $u^{\frac{1}{d}} e^{\frac{2\pi i}{d}}$, vagyis ha Ed az egység egy d-ed gyökét jelenti, $Ed\, u^{\frac{1}{d}}$; ezek után

$$v_{d,1} = c_d^{(d')}\, (Ed)^{d'}\, u^{\frac{d'}{d}} + c_d^{(d'+1)}\, (Ed)^{d'+1}\, u^{\frac{d'+1}{d}} + \cdots$$

és u. t. $vd, 2' \ldots vd, d-1$ számára. Megjegyzendő, hogy egy gyök sora az u-nak csak egész hatványait tartalmazza; ha t. i. $d = 1$, lesz

$$d' = \frac{n}{d} = n$$

tehát

$$v_{1,0} = c_1^{(n)}\, u^n + c_1^{(n+1)}\, u^{n+1} + \cdots$$

ez természetesen az, mely a zéruspont körzése után magába tér vissza.

Evvel a gyököknek viszonyait a 0 közelében teljesen ismerjük; menjünk át most már azon pontok megvizsgálására, a hol u az egységnek bármelyik nyolczadgyökét képviseli. Jelöljük ezt rövidség kedveért α-val. Feladatunk nagyon megkönnyíttetik a következő tétel által:

A modulareggyenlet nem változik, ha u és v helyett mindenütt $\sqrt[8]{\alpha - u^8}$ *és* $\sqrt[8]{\alpha - v^8}$ *irunk.* De e helyettesítés által a föntebbiekből oly sorokat nyertünk, melyek $u = \alpha$ pont körüli körben lesznek összetartók, melyek tehát a szükséges adatokat tüstént szolgáltatják.

Miután itt nem lehet feladatom ismert fejtegetéseket ismételni, az említett tétel bebizonyítására, valamint a következőknél, melyek annak bővebb fogalmazását képezik, Königsberger már említett kézikönyvére utalok. (l. 32. és 180. lapon).

Ha c az elliptikus egészlet modulusa, ugy a

$$c^2 + c'^2 = 1$$

által meghatározott c' mennyiség kiegészítő (complementaris) modulusnak neveztetik. Valamint mi amazt

$$\sqrt[4]{c} = \varphi(\tau)$$

a theta-modulus függvénye gyanánt tekintettük, ugy ezt c'-vel is tehetjük:

$$\sqrt[4]{c'} = \psi(\tau).$$

Akkor φ és ψ közt a következő két alapviszony létezik:

$$\varphi^8(\tau) + \psi^8(\tau) = 1$$

és

$$\varphi\left(-\frac{1}{\tau}\right) = \psi(\tau);$$

továbbá $\psi(\tau)$-nak következő kifejezése:

$$\psi(\tau) = (1+q^2)(1+q^4)\ldots\{(1-q)(1-q^3)\ldots\}^2,$$

a melyben

$$q = e^{\pi i \tau},$$

mutatja, hogy

$$\psi(\tau+2) = \psi(\tau);$$

tehát ψ is szakaszos függvény; szakasza kettő.

Az említett helyettesítés most már (l. e. h. 182 l.) a

$$\left(\frac{2}{d}\right)\varphi\left(\frac{d\tau - 16\xi}{d'}\right)$$

gyököt a következő alakba viszi át:

$$\left(\frac{2}{u'}\right)\psi\left(\frac{u\tau - 16x}{u'}\right)$$

hol u a 16ξ és d' legnagyobb közös osztója, továbbá

$$u' = \frac{n}{u}$$

és az x ismét 0 és $u'-1$ közt való egész szám.

Igy tehát ismerjük a kifejezést, melybe a modularegyenletnek egy gyöke az említett helyettesítés által átmegy; de a φ-hez teljesen hasonló ψ függvény által levén advatudjuk egyszersmind, hogy a 0 pontra nézve micsoda cyclus, hoz tartozik, mert hogy ismét a modularegyenlet gyöke, az említett tételből világos. — De helyettesítsük most az illető sorkifejezésben az u és v-t az illető gyökkifejezések $\sqrt[8]{\alpha - u^8}$ és $\sqrt[8]{\alpha - v^8}$ által, és ismét a helyettesítés ugyanaz levén, ugyanazon uj gyököt kapjuk meg. Legyen p. o.

$$vd', \xi = c\,u\,\frac{d}{d'} + \cdots \qquad (1)$$

lesz 8-dik hatványra emelve

$$v^8_{d',\xi} = c\, u^{8\frac{d}{d'}} + \cdots \qquad (2.)$$

(hol nem irunk c helyett c^8-at; mert evvel csak állandót akarunk jelölni, tekintet nélkül értékére.) Irjunk most v^8 és u^8 helyett $\alpha - v^8$ és $\alpha - u^8$, lesz :

$$\alpha - v^8_{d',\xi} = c\,(\alpha - u^8)^{\frac{d}{d'}} + \cdots \qquad (3.)$$

Tekintsük most már e sort $u = \alpha$ pont közelében, ugy hogy $u - \alpha$ igen kicsiny legyen. Lesz akkor

$$\alpha - u^8 = \alpha - (\alpha + u - \alpha)^8 = \gamma_1 + \gamma_2 (u - \alpha) + \cdots \qquad (4.)$$

végtelen sor, melynek többi tagjait elhanyagolhatjuk; mert $u - \alpha$ igen kicsiny. Hasonlókép, ha a $v_{d',\xi} = \beta$ megfelel $u - \alpha$-nak,

$$\alpha - v^8_{d',\xi} = \alpha - (\beta + v - \beta)^8 = \delta_1 + \delta_2 (v - \beta) + \cdots \qquad (5.)$$

és mindezeket a (3.)-ba bevezetvén, a következő egyenletet nyerjük, mely érvényes az $u = \alpha$ legközelebb szomszédságában :

$$\delta_1 + \delta_2 (v_{d',\xi} - \beta) = c\,\{\gamma_1 + \gamma_2 (u - \alpha)\}^{\frac{d}{d'}} \qquad (6.)$$

vagyis

$$v_{d',\xi} = \eta_1 + \eta_2 (u - \alpha)^{\frac{d}{d'}}. \qquad (7.)$$

Ebből tüstént következtethetjük, hogy v az $u = \alpha$ pont körül oly sorba fejthető ki, mely az $(u - \alpha)^{\frac{1}{d'}}$ hatványai szerint halad, és melynek két első tagja a följegyzett. De ha valamely egyenletnek gyöke bizonyos α pont körül $(u - \alpha)^{\frac{1}{d'}}$ hatványai szerint haladó sorba fejthető, ugy e gyök e pontra nézve egy d' gyökből álló cyclusnak tagja. De most tudjuk azt is, hogy a 0 pontra nézve micsoda cyclushoz tartozik a gyök. Ugyanezen gyöknek következő is kifejezése :

$$\left(\frac{2}{u'}\right) \psi \left(\frac{u\tau - 16x}{u'}\right).$$

De a 0-pontnak körzése azonos a τ-nak 16-tal való szaporításával, ismételhetjük tehát előbbi következtetéseinket, melynél fogva e gyök a 0-p.-ra nézve egy u' tagból álló cyclushoz tartozik.

Mielőtt e fejtegetést folytatnók, különösen arra kívánunk figyelmeztetni, hogy az $\alpha^8 = 1$ által meghatározott 8 pontra nézve a gyökök ugyanazon cyclusokat képezik. Az

α-ról csak is az volt föltételezve, hogy az egység nyolczadgyöke; az eredmény az α különértékétől független maradt. Az összefüggés is meg van határozva, mely a 0 és α pontok körüli cyclusok közt létezik; ezt azonban, a következőkre nézve igen fontos lévén, még részleteznünk kell.

Mindenekelőtt látjuk, hogy *a 0 és α pontok körül egészen hasonló cyclusok léteznek.* Minden az u hatványai szerint haladó sorfejlődésnek itt ugyanolyan felel meg az $u-\alpha$ szerint. Tehát a kilencz pont mindegyike körül lesz egy legnagyobb cyclus n gyökből, következnek azután cyclusok, melyeknek tagszáma megfelel az n minden osztójának, és létezik végre egy gyök, mely önmaga képez cyclust, azaz az illető pont körzése után önmagába tér vissza. Használjuk most a már kifejtett jelzési módszert az α pontokra vonatkoztatott gyököknél, megkülönböztetés kedveért a v-t vonással látván el. Lesz akkor az illető jelek közt a következő összefüggés:

$$v_{d'_1\xi} = v'_{u'_1 x},$$

hol u a d' és ξ ϱ legnagyobb közös osztója (tulajdonképen d' és 16 ξ közt; de ez ugyanaz, miután n és tehát d' is mindig páratlannak tétetik föl). Lesz azután:

$$u' = \frac{n}{u}.$$

Most már könnyen bizonyíthatjuk be a következő érdekes viszonyokat:

A 0 pontra vonatkoztatott n gyökből álló cyclus tartalmaz gyököket minden cyclusból az α pontot illetőleg és pedig $\varphi(d)$ gyököt a d tagú cyclusból, ha $\eta(d)$ az ismert jel a magasabb számtanból, és a a d-hez relativ törzsszámok számát jelenti, melyek kisebbek a d-nél. Ép ugy van az n-tagú cyclus egy α pont körül, összehasonlítva a 0 pont cyclusaival.

Hogy ez valóban ugy van, könnyen beláthatjuk. Tekintsük a $v_{d_1 x}$ gyököket; a hányszor d és x relativ primek lesz az $u = 1$; tehát u' egyenlő n-nel; ez a $\eta(d)$ definitiója szerint $\varphi(d)$-szer történik. Ha pedig $u' = n$, a cyclus, melyhez a gyök tartozik, n taggal bír. — De ilyformán láthatjuk azt is, hogy ez által az n tagú cyclus ki van merítve, mert ha d és x nem relativ törzsszámok, az u nem lesz az egység; és a cyclus

tagszámát jelző u' kisebb az n-nél. Ebből tehát a következő tétel is folyik:

$$\Sigma\varphi(d) = n,$$

ha a Σ jel által az n minden osztója utáni összeadást jelöljük. A magasabb számtannak ismert alakzata, mely itt fölmerül.

4.

A foklehozás (reductio) feladata.

Valamely egyenlet megoldásának föladata nem követelhet mást, mint az adott egyenletet visszavezetni más, már ismert egyenletekre. Így, a legegyszerűbb esetben, a másodfokú egyenlet meg van oldva, ha azt bármi helyettesítés által a binomicus alakra, $x^2 = a$ hoztuk vissza. — A $\sqrt{}$ jelét ismeretes müveleti jelnek tesszük fel ekkor, daczára annak, hogy ez által jelzett mennyiség értéke, ritka esetek kivételével, csak megközelitőleg fejezhető ki.

Átalánosan tehát azon egyenletet mondjuk algebraice oldhatónak, mely a helyettesitések bizonyos sora által föloldásában csak is $x^n = a$ forma egyenletek feloldásától függ.

Ezekután világos lesz, mit értünk ellipticus függvények által megoldható egyenletek alatt. Ezek oly egyenletek, melyek ismét végszerű helyettesítések által a modular egyenletekre vezethetők vissza.

Feladatunk, most már keresni, vajjon léteznek-e ily egyenletek, és ha léteznek, ezeket felsorolni és osztályozni. — A legközelebbi teendő volna azután, az egyenletek e tulajdonára nézve hasonló gyakorlati kriteriumokat találni, valamint ezek Abel és Galois által az algebraicus oldhatóságra nézve állíttattak fel, és végre a kifejtett módszerek oly átalakítása, mely azokat egyszersmind gyakorlati érvényre emelheti.

Az első kérdést a következő alakba öntjük át: Léteznek-e egyenletek, melyeknek gyökei a modularegyenlet gyökeinek végszerű függvényei, és melyeknek együtthatói, valamint a moduláregyenletekéi, az u-nak egész függvényei?

Tüstént látjuk, hogy ha a moduláregyenlet foka $S(n)$, csak ennél alacsonyabb fokú egyenletek forognak kérdésben. Hisz magasabb fokú egyenlet, melynek föloldása a modular egyenletére vezethető vissza, nem lehetne irreductibilis; azaz az egész függvény, mely baloldalát képezi, két önálló szorzóra esik szét, és csak ezekkel egyenként kell foglalkoznunk. — Ugy szintén maga $S(n)$-foku egyenleteket nem kell tekintenünk, ilyenek természetesen mindig léteznek, de ismert elméletük itt nem ad ujat.

További egyszerüsítést ad a magasabb abgebrának következő tétele:

Valamely egyenlet gyökeinek végszerü függvénye mint ugyanezeknek egész függvénye állítható elő.

Tehát csak oly egyenleteket kell tekintenünk, melyeknek gyökei a modularegyenletek gyökeinek egész függvényei. Ha nem egész, könnyen átvezethető ezen alakba.

Továbbá szabad lesz föltennünk, hogy az ujonnan képzendő egyenlet gyökei nem symmetricus függvényei a modularegyenlet gyökeinek. Mint ilyenek ők maguk, tehát az uj egyenlet együtthatói is az u-nak egész függvényei volnának ugyan, de ezen eset semmi érdekkel nem bír, az uj egyenlet baloldala első fokú szorzókba esvén szét.

Az uj egyenletnek gyöke tehát a modularegyenlet gyökeinek egész függvénye; mint ilyen a 0 és α pontok körül az ezek számára érvényes sorokból állítható össze. Miután e kifejezések mindegyik tagjában a kitevőknek nevezője az n-nek egy osztója, ez az uj gyök sorkifejezésében is úgy lesz. Miután pedig ezek adják a cyclusok tagszámát, melyekhez a gyök az illető pontok körül tartozik, látjuk ebből, hogy az uj, u. n. reducált-egyenlet, bár birhat kevesebb cyclussal, mint az adott modularegyenlet, de *a cyclusok tagszáma ismét csak is az n-nek osztója lehet.*

Forduljon elő most már az egész függvényben, mely az uj egyenlet gyökét képezi, bizonyos sora a modularegyenlet gyökeinek, melyek a

$$d', d'', d''' \ldots .$$

tagu cyclusokhoz tartoznak. Az uj egyenletnek gyöke ugyan-

ezen pontra nézve oly cyclushoz tartozik, melynek tagszáma a d', d'' .... számok legkisebb közös többese.

Hogy e cyclus valóban az eredeti értékhez vezeti vissza a függvényt, könnyen belátható. Az első gyökkel ez megtörténik d', $2d'$,.... stb. körzés után, a másodikkal d'', $2dt'$,... körzés után stb., tehát mindegyikkel történt ez, ha oly számot választunk, mely mindezeknek többese. De előbb ez meg nem történhetik. Mint már kimutattuk, a cyclus tagszáma mindenesetre az n-nek osztója. Vegyük tehát az n-nek egy osztóját, mely az illető legkisebb közös többesnél kisebb. Akkor ez a d', d''.... szorzókból néhányat tartalmaz, néhányat nem. Az első nemnek megfelelő cyclussal biró gyökök tehát visszatérnek eredeti értékükhöz, de nem a többiek. Tehát az egész függvénynek, az uj egyenlet gyökének értéke is változott.

Még egy kivételre szükség figyelmeztetni. — Ha t. i. az illető uj egyenletnek gyöke a modularegyenlet bizonyos cyclusához tartozó gyököknek symmetricus függvénye, az illető osztó a legkisebb közös többes kiszámításánál tekintetbe nem veendő, miután mint az illető mennyiségekből symmetrice összeállított kifejezés, semmi elcserélésnél értékét nem változtatja.

Előbb a modularegyenlet gyökeire nézve bebizonyítottuk azon tételt, hogy azon gyökök közt, melyek a 0 pont körül egy bizonyos cyclushoz tartoznak, mindig vannak, melyek az α pontok körül, az n-edrendü cyclusnak tagjai. — Ha most már adva van a reducált egyenletnek gyöke, ugy tehát a zéruspontnak néhányszor ismételt körzése után oly kifejezést nyerünk, mely az α körül n tagu cyclust képez. Mert vegyük föl bármely gyökét a modularegyenletnek; ugy ez vagy már maga tagja az n-edrendü cyclusnak α körül, vagy pedig a 0 körzése által ilyenbe átmegy. De akkor az egész kifejezés is, mely a reducalt egyenlet gyökét képezi, n-edrendü cyclushoz tartozik; mert ha a

$$d', d'', d''', \ldots .$$

mennyiségek közt egy $d = n$, ugy természetesen e számok legkisebb közös többese is n. De e következtetésben, mint már azelőtt, a 0 és α pontot egymással fölcserélni is szabad. Tehát a következő eredményt nyerjük:

Bármily cyclusból az egyik pont körül mindig egy n-edrendü cyclus léte következik a másik pontra nézve. És ebből:

A reducált egyenlet legalább n-edfokú.

Legyen a reducált egyenlet foka : v, ugy

$$n \leqq v < S(n).$$

Jelöljük továbbá gyökeit

$$y_1, y_2, \cdots y_{v-1}, y_v$$

jelekkel; legyen végre a reducált egyenlet maga:

$$y^v + P_1 y^{v-1} + P_2 y^{v-2} + \cdots + P_v = O.$$

Feladatunk ekkor azt kivánja, hogy a $P_1, P_2 \cdots P_v$ mennyiségek az u-nak egész függvényei legyenek. Ismeretesek ezen együtthatóknak kifejezései az egyenlet gyökei által:

$$P_1 = y_1 + y_2 + \cdots + y_v$$
$$P_2 = y_1 y_2 + y_1 y_3 + \cdots + y_{v-1}, y_v$$
$$\cdots\cdots\cdots\cdots$$
$$P_v = y_1 y_2 \cdots y_v$$

Mielőtt fejtegetéseinket folytatnók, szükséges, a magasabb abgebrának néhány tételét idézni, melyeknek bővebb tárgyalását Serret munkájában : Cours d'algèbre supèrieure találhatni.

Legyen adva a $v_1, \cdots v_r$ mennyiségek két függvénye, t. i.

$$V = f_1(v_1, \cdots, v_r)$$

és

$$P = f_2(v_1, \cdots, v_r);$$

létezik bizonyos elcserélési csoport, mely a v mennyiségekre alkalmazva a V függvény értékét nem változtatja; ha most már P sem változik ezen elcserélési csoport alkalmazása által, ugy P mint a V-nek végszerű függvénye fejezhető ki, melynek együtthatói a v mennyiségek symmetricus függvényei.

Továbbá:

Ha valamely egyenlet gyökeinek egész függvénye bizonyos elcserélési csoport alkalmazásánál értékét nem változtatja, ugy e függvény mint az egyenlet együtthatóinak és bizonyos „adjungált" mennyiségek egész függvénye is fejezhető ki. És megfordítva, ha ez megtörténhetik, ugy létezik

bizonyos elcserélési csoport, mely a függvény értékén nem változtat.

Tegyük fel most, hogy az igényelt tulajdonokkal biró egyenlet valóban létezzék és pedig úgy, hogy annak utolsó tagja

$$P_\nu = y_1 y_2 \cdots y_\nu = V$$

a modularegyenlet gyökeinek oly függvénye legyen, mely csakis az utolsó helyen idézett elcserélési csoport alkalmazásánál marad meg változatlanul. Akkor a gyökök minden más egész függvénye, mely egyszersmind az u-nak egész függvénye, és tehát az illető elcserélési csoport alkalmazásánál nem változik, a V-nek végszerű függvénye lesz, melyet $R(V)$-vel jelölünk.

Ha létezett reducált egyenlet, melynek utolsó tagja V volt, úgy létezik — mint ezt most akarjuk bizonyítani, — *hasonfokú reducált egyenlet, melynek utolsó tagja $R(V)$.*

Jelöljön $r(y)$ az y-nak egy együtthatóiban még határozatlan végszerü függvényét. — Ha a föltett egyenletnek gyökei voltak y , $y_2, \ldots y_\nu$, úgy az ismert Tschirnhausen-féle módszer szerint mindig képezhetni uj egyenletet, melynek gyökei $r(y_1), r(y_2), \ldots r(y_\nu)$. Ez mindig lehetséges, hacsak r végszerü függvényt jelent. Ekkor uj egyenletet kaptunk tehát, mely a szükségelt tulajdonokkal bír és melynek utolsó tagja a gyökök szorzata $r(y_1)\, r(y_2) \ldots r(y_\nu)$. Más részt V függvény nem levén egyéb mint az eredeti gyökök szorzata $y_1 y_2 \ldots y_\nu$, lesz

$$R(V) = R(y_1 \ldots y_\nu)$$

és most, ha még

$$r(y_1)\, r(y_2) \ldots r(y_\nu) = R(y_1 \ldots y_\nu)$$

tettük, az $r(y)$ átalakitás által nyert egyenlet a kivánt utolsó taggal is bir. Hogy pedig az utolsó egyenletnek eleget lehet tenni, világos, miután az r függvény együtthatói még határzatlanok. A mindkét oldali együtthatók összehasonlitása tiszta numericus egyenleteket ad, hol legfölebb egyes számbeli irrationalitást adjungálni szükséges.

Ha most már eredetileg oly egyenlet nem vala képezhető, melynek együtthatói az u egész függvényei és melynek utolsó tagja V, úgy más hasonfokú reducált egyenlet sem létezhetik.

Képezzük az illető $y_1, y_2, \ldots, y_\nu$ gyökökből a $P_1, P_2, \ldots P_\nu$ mennyiséget, úgy hogy algebraicus egyenlet ne létezzék, melynek az y-ok gyökei lehetnek, szükségkép a P-k közt néhányan az u-nak túllépő vagy sokértékü függvényei lesznek. Ha most már, épen úgy, mint azelőtt, a Tschirnhausen-féle átalakítás által más utolsó taggal biró egyenletre megyünk át, úgy ez az átalánosság megőrzésével mindig úgy történhetik, (l. Hermite : Sur quelques théorèmes d'algèbre et l'équation du 4-ième degré, Comptes rendus, 1859.) hogy az új egyenlet P_i' együtthatója a régi P mennyiségek i-foku egész függvénye legyen. Ha volt tehát a $P_1, \ldots P_\nu$ közt túllépő vagy többértékü függvénye az u-nak, úgy most a $P'_1, \ldots P'_\nu$ közt is lesz, s az uj egyenlet sem felel meg a kivántaknak.

Az eddig nyert eredmény röviden az, hogy vizsgálatunkat sokkal szükebb körre szorítván, egy tetszés szerinti utolsó taggal biró egyenletet kell csak felvennünk, de daczára ennek, az illető egyenlet lehetségét átalánosan biráljuk meg.

Mint ily utolsó tagot a következőkben a modulareg yenlet gyökeinek minden különbségét egymással szorozzuk; tudva levő, hogy az így képzett kifejezés nem más, mint a modulareg yenlet discriminánsának négyzetgyöke. E discriminánsnak tulajdonait előbb idézett iratomban bővebben fejtegettem bármi átalakítási fok számára. Itt ily átalánosságban csak a következő tételre lesz szükségünk:

A moduláregyenletek discriminánsa az u egy egész függvényének teljes négyzete.

Először Hermite mondá ki e tételt törzsszámfokú átalakításhoz tartozó modulareg yenletek számára.

A discrimináns e tulajdonára azért kell itt utalnunk, mert csak ebből tünik ki, hogy azon mennyiség, melyet mint a képzendő egyenlet utolsó tagját akarjuk használni, valóban is az u-nak egész függvénye. Ez most világos, mert a discrimináns maga ilyennek négyzete, tehát négyzetgyöke is az lesz.

5.

A foklehozás lehetetlensége, ha az átalakítási fok összetett szám.

Legyen az átalakitási fok:

$$n = p_1 p_2 \ldots p_r;$$

akkor a hozzá tartozó modularegyenlet foka:

$$S(n) = p_1 + 1)\,(p_2 + 1) \ldots (p_r + 1)$$

és a gyökök, a mint jelölni szoktuk:

$$v_{n_1 o}, \ldots, v_{n_1 n-1}, \ldots, v_{d_1 i}, \ldots v_{1_1 o}.$$

A gyökök különbségeinek szorzata az

$$(v_{d_1 i} - v_{d'_1 i'})$$

alakú szorzókból áll, e szorzók száma pedig nem lesz más mint $S(n)$ elemnek kettős combinatiója, azaz

$$\frac{S(n)(S(n)-1)}{2}$$

Föltevésünk szerint, melynek igazolásával az előbbi fejezetben foglalkoztunk, e szorzat egyszersmind a reducált egyenlet gyökeinek szorzata legyen. Föladatunk tehát e szorzatot, ha lehetséges, úgy szétválasztani egyes szorzókra, hogy ezek az egyenlet gyökei lehessenek.

Mindenekelőtt könnyen beláthatni, hogy a O és α pontok körzése által minden gyöktől minden gyökhöz lehet jutni, épen úgy valamint maga a modularegyenletnél. Ez abból következik, hogy minden cyclusban az egyik pont körül van oly gyök, mely a másik pont körül az n-edrendü cyclushoz tartozik. — Ebben tehát eszközölhető az átmenet az egyik cyclusból a másikba, p. az α körzése által, mig azután ismét a o-t körözve, az illető cyclus minden gyökét nyerjük. Ezek után világos, hogy minden gyöknek a föntebb idézett alakkal biró szorzók egyenlő számából kell állania. A körzés csakis a jelzőket változtatja, a gyököknek alakja különben tehát ugyanaz marad.

Lássuk most már, melyek és hányan e szorzók közöl tartoznak n-edrendű cyclushoz. Tudjuk előbbi fejtegetéseinkből, hogy

$$v_{d_1 i} - v_{d'_1 i'}$$

alaku szorzó a o pontra nézve oly cyclushoz tartozik, melynek tagszáma a d és d' legkisebb közös többese. Ki kell keresnünk azon combinatiokat, hol ez n lesz. Könnyen látni, hogy ezek a következők:

$$v_{1_1 o} - v_{n_1 i},$$

összesen n, továbbá

$$v_{n_1 i} - v_{n_1 i'},$$

a melyeknek száma $\frac{n(n-1)}{2}$, végre a következők

$$v_{p_1 i} - v_{\frac{n}{p_1} i'}$$

amely alak nr szorzót képvisel.

Azon gyökök, melyek e szorzókból csoportosúlnak, semmi más szorzót nem tartalmazhatnak, miután ennek cyclusa az n-nek már csak osztója levén, ugyanazon szorzó többször jelennék meg, mig amazok n-edrendü cyclusukat végezik be. Így tehát a gyökök szorzatában e szorzó az egységnél magasabb kitevővel foglalna helyet, a mi első föltevésünkkel ellenkezik.

Ezen n-edrendü cyclushoz tartozó szorzók, melyeknek száma

$$n + \frac{n(n-1)}{2} + nr = n\left(r + 1 + \frac{n-1}{2}\right)$$

most már maguk közt oszlanak fel a gyökök bizonyos számára. Ez, miután mindegyiknek cyclusa n, csak is n maga, vagy ennek többese, σn, lehet. — Lesz tehát az egy gyökben tartalmazott gyökök száma

$$\frac{r + 1 + \frac{n-1}{2}}{\sigma}$$

Ha most már v a reducált egyenlet foka, vagyis a gyökök száma, miután láttuk, hogy minden gyöknek hasonszámú szorzókból kell állania, és a szorzók száma összesen

$$\frac{S(n)\,(S(n)-1)}{2}$$

lesz

$$\nu\,\frac{r + 1 + \frac{n-1}{2}}{\sigma} = \frac{S(n)\,(S(n)-1)}{2}$$

De, hogy reducált egyenletet kapjunk, ν legfölebb

$S(n)-1$ lehet; mert már $S(n)$ maga a modularegyenlet foka. Ha tehát r helyett e legmagasabb értékét helyettesitjük, lesz:

$$\{S(n)-1\}\frac{r+1+\frac{n-1}{2}}{\sigma} \geqq \frac{S(n)\,(S(n)-1)}{2},$$

vagy:

$$\sigma\, S(n) \leqq 2\left(r+1+\frac{n-1}{2}\right)$$

Ha $S(n)$ és n értékeit kiirjuk:

$$\sigma(p_1+1)\,(p_2+1)\ldots(p_r+1) \leqq 2\left(r+1+\frac{p_1p_2\ldots p_r-1}{2}\right)$$

amely nem egyenletet még következő alakra hozhatni:

$$\sigma(p_1+1)\,(p_2+1)\ldots(p_r+1)-p_1p_2\ldots p_r \leqq 2r+1.$$

De jegyezzük meg, hogy a $p_1,\ldots,p_r$ számok az n-nek törzsszorzói, mig r ezeknek számát jelenti. E nemegyenlet lehetetlenség. Csak egy kivételi eset létezik és ez az, mikor az n már törzsszám; akkor a p szorzók száma

$$r=1$$

a σ pedig, miután a reducalt egyenlet foka legfölebb n, szinte

$$\sigma=1$$

a miután valóban a nemegyenlet

$$1<3$$

lesz. De minden más esetben már

$$\sigma(p_1+p_2+\cdots p_r) > 2r+1$$

miután mindig $p>2$. —

Evvel tehát a következő fontos tételt nyertük:

A modularegyenlet reductioja lehetetlen, mihelyt az átalakitási fok nem törzsszám.

6.

A foklehozás feladata, ha az átalakítási fok törzsszám.

Lássuk mindenekelőtt, minő kifejezése lesz az eddig nyert eredménynek, midőn az átalakítási fok törzsszám, p. — Ekkor a gyökkülönbségek mindegyike p-edrendü cyclushoz

tartozik. Ismerjük azonkivül a reducált egyenlet fokát. Előbb bizonyitottuk be, hogy ez nem lehet kisebb p-nél; de $p+1$ már maga a modularegyenlet foka; *ha tehát létezik reducált egyenlet, úgy foka p lesz.*

Világos most már továbbá, hogy az egyenlet gyökei mindnyájan úgy a o, mint az α pontok körül egy (p-tagú) cyclust képeznek.

A modularegyenletnek gyökei e pontok körül 2 cyclusba, — egy n-tagú és egy egytagúba — csoportosúlnak; jelöljük őket ismét a o-pontra nézve, következőképen:

$$v_{p1o},\ v_{p1},\ \ldots\ v_{p1p-1},\ v_{1_1o};$$

az α pontokra nézve pedig:

$$v'_{p1o},\ v'_{p1},\ \ldots\ v'_{p_1p-1},\ v'_{1_1o}$$

mely utolsó sor, a gyökök rendjétől eltekintve, az előbbivel azonos. A $p+1$ gyökből

$$\frac{p(p+1)}{2}$$

különböző különbség képezhető; tegyük fel egyelőre a reducált egyenlet lehetségét és keressük ezen esetben egyes gyökeinek kifejezését. Jelöljük ezeket a o pontot illetőleg

$$y_1,\ y_2,\ \ldots\ y_n$$

jelekkel, az α pontokra nézve pedig ekkép

$$y'_1,\ y'_2,\ \ldots\ y'_n$$

hol ismét a két sor a rendtől eltekintve azonos; a jelzők pedig, ha sonlóan mint a modularegyenlet gyökeinél, a cyclusbeli sorozatszámot adják.

Minden gyök, mint ez szinte előbb átalánosságban bizonyíttatott be, a gyökkülönbségek egyenlő számának szorzata; tehát minden gyök $\frac{p+1}{2}$ szorzóból áll, melynek mindegyike ismét

$$v_{1_1o} - v_{p_1i}$$

vagy

$$v_{p_1i} - v_{p_1i'}$$

alakkal bír. De a gyökök azon tulajdona, hogy a o és α pontok körül p tagu cyclust képeznek, elegendő ezeknek teljes meghatározására, és most az egyenletek lehetségének fejtegetését későbbre halasztván, e módszerrel akarunk foglalkozni.

Ismerünk mindenekelőtt $\frac{p+1}{2}$ szorzót, mely a o pont körzésénél egymásba átmegy. Ezek az

$$v_{1_0} - v_{p_1 i}$$

alakkal birók. Ebből következtetni, hogy a reducált egyenlet gyökei mindenesetre a következő alakkal birnak

$$y_1 = (v_{1_0} - v_{p_1 o}) \cdots\cdots$$
$$y_2 = (v_{1_0} - v_{p_1 1}) \cdots\cdots$$
$$\cdots\cdots\cdots$$
$$y_n = (v_{1_0} - v_{p_1 p-1}) \cdots$$

Ismét létezik $\frac{p+1}{2}$ szorzó, mely az α pontok körzésénél egymásba átmegy; ezek a következők:

$$v'_{1_0} - v'_{p_1 i}$$

Tehát a reducált egyenlet gyökei ezek is lesznek:

$$y'_1 = (v'_{1_0} - v'_{p_1 o}) \cdots\cdots$$
$$y'_2 = (v'_{1_0} - v'_{p_1 1}) \cdots\cdots$$
$$\cdots\cdots\cdots$$
$$y'_n = (v'_{1_0} - v'_{p_1 p-1}) \cdots$$

A v és v' jelek, hogy felelnek meg egymásnak, azt tudjuk, az illető számítás részletei Königsberger kézikönyvében (l. 176. lapot) találhatók. Legyen e szerint:

$$v_{1_0} = v'_{p_1 \rho}$$

és

$$v_{p_1 \sigma} = v'_{1_0};$$

akkor

$$y_\sigma = (v_{1_0} - v_{p\sigma}) \cdots\cdots = (v'_{1_0} - v'_{p_1 \rho}) \cdots\cdots$$

azaz

$$y_\sigma = y'_\rho$$

Hasonlókép legyen

$$v'_{1_0} = v_{p_1 \sigma}$$
$$v'_{p_1 o} = v_{p_1 \varkappa}$$
$$v'_{p_1 1} = v_{p_1 \lambda}$$
$$\cdots\cdots$$
$$v'_{p_1 \rho} = v_{1_0}$$
$$\cdots\cdots$$
$$v'_{p_1 p-1} = v_{p_1 \tau}$$

Helyettesitsük e kifejezések az y'-okban; úgy uj p kifejezést kapunk a gyökök számára:

$$y'_1 = (v_{p_1\sigma} - v_{p_1\varkappa})$$
$$y'_2 = (v_{p_1\sigma} - v_{p_1\lambda})$$
$$\cdots\cdots\cdots$$
$$y'_\rho = (v_{1_1 o} - v_{p_1\sigma})$$
$$\cdots\cdots\cdots$$
$$y'_p = (v_{p_1\sigma} - v_{p_1\tau})$$

Most a gyökök a o pontra vonatkoztatott jelekben fejezvék ki; de, rendjük még az α pontok cyclusának sorozata. Vizsgáljuk most, vajjon a jobboldalon nyert szorzók a o pontra nézve egy vagy különböző cyclushoz tartoznak-e. Mindenesetre az y'_ρ szorzója

$$(v_{1_1 o} - v_{p_1\sigma})$$

külön cyclust képez. Két más szorzó p.

$$v_{p_1\sigma} - v_{p_1\mu} \qquad (\alpha)$$

és

$$v_{p_1\sigma} - v_{p_1\nu}$$

ily alakban egy cyclushoz nem tartozik; de változtassuk a második előjelét, úgy hogy

$$v_{p_1\nu} - v_{p_1\sigma} \qquad (\beta)$$

legyen (a mit tehetünk, mert a jelváltozást a kifejezés folytában ismét pótolva gondoljuk). Hogy most már (α) és (β) szorzók egy cyclushoz tartozzanak, azaz a körzések bizonyos száma után egyik a másikba menjen át, szükséges, hogy:

$$\nu - \sigma \equiv \sigma - \mu, \text{ mod. } p,$$

mert a jelző szaporítása egygyel egy körzést jelent. De e congruentia, mely jobban irva

$$2\sigma \equiv \nu - \mu, \text{ mod. } p$$

minden ν-hez egy és csak egy μ-t ad. — Tudjuk továbbá, hogy a o pontra vonatkoztatva, ha az első gyök volt y_γ, lesz a második $y_{\gamma+\nu-\sigma}$. Ha most az y'-okat a o pontra vonatkoztatott sorrendüket illetőleg $[y']$ által jelöljük, (hol tehát $[y']$ nem más mint a megfelelő y jelzője) eddig $\frac{p-1}{2}$ meghatározást kaptunk, melyeknek alakja

$$[y'_\alpha] - [y'_\beta] \equiv m \equiv [y_m]$$

és azonkivül tudjuk, hogy

$$[y_\rho]' \equiv \sigma \equiv [y_\sigma].$$

De hogy így az $[y']$-okat mindnyájan meghatározhassuk, még $\frac{p-1}{2}$ egyenletre van szükségünk, melyeket következőképen nyerünk. Hasonlóan, mint azelőtt, lesz:

$$y_1 = (v'_{p_1\rho} - v'_{p_1\varkappa'}) \cdot \cdot \cdot \cdot \cdot$$
$$y_2 = (v'_{p_1\rho} - v'_{p_1\lambda'}) \cdot \cdot \cdot \cdot \cdot$$
$$\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot$$
$$y_\sigma = (v'_{1_1\rho} - v'_{p_1\rho}) \cdot \cdot \cdot \cdot \cdot$$
$$\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot$$
$$y_p = (v'_{p_1\rho} - v'_{p_1\tau'}) \cdot \cdot \cdot \cdot \cdot$$

Ismét hogy kettő e szorzóból az α körzésénél egymásba átmenjen, szükség, hogy

$$\nu' - \varrho \equiv \varrho - \mu' \text{ mod. } p;$$

továbbá, ha az első gyök (y'_γ) volt, lesz a második $y'_{\gamma + \nu' - \rho}$, ez ismét $\frac{p-1}{2}$ meghatározást ad, melyeknek alakja:

$$[y_{\varkappa - l}] = K - l = [y'_\gamma]$$

Így tehát meghatároztatott, az y és y', hogy felelnek meg egymásnak, a o pontra nézve a gyökök sorozatában $\frac{p+1}{2}$ önálló szorzó fordul elő, azaz olyan, mely e pont körzésénél egymásba át nem megy. Ha tehát most y, körzi a o-t, tudjuk hogy átmegy y_2-be; de a máris ismert szorzóból így az y_2-nek egy uj szorzóját ismerjük meg és úgy tovább y_n-ig; hasonlóan tehetjük ezt $\frac{p+1}{2}$ gyökkel, és így minden gyöknek $\frac{p+1}{2}$ szorzóját ismertük meg. Akkor azonban már teljesen ismerjük ezeket, miután a p gyök szorzata $\frac{p(p+1)}{2}$ szorzóból áll.

A numericus számítás természetesen csak adott p-nél történhetik meg; és alig áll másból, mint oly táblának elkészitéséből, mely mutatja, mikép felelnek meg egymásnak a v és v'-k, az y és y'-ok.

Így találni $p = 5, 7, 11$ számára a következő eredményt:

$$p = 5$$
$$y_i = (v_{1,0} - v_{5,i})\ (v_{5,i+1} - v_{5,i+4})\ (v_{5,i+2} - v_{5,i+3})$$

$$p=7$$

$$y_i=(v_{1,0}-v_{7,i})\,(v_{7,i+1}-v_{7,i+5})\,(v_{7,i+2}-v_{7,i+3})\,(v_{7,i+4}-v_{7,i+6})$$

$$p=11$$

$$y_i=(v_{1,0}-v_{11,i})\,(v_{11,i+1}-v_{11,i+2})\,(v_{11,i+4}-v_{11,i+8})\,(v_{11,i+3}-v_{11,i+6})\times$$
$$\times(v_{11,i+9}-v_{11,i+7})\,(v_{11,i+5}-v_{11,i+10})$$

hol i egymásután $=1, 2, \ldots, p-1, p$. Hol a jelzőkben a $p-1$-nél nagyobb szám fordul elő, ebből a p-nek többesei elvetendők. Könnyü belátni, hogy v_i és v_{i+p} ugyanazt jelentik. Hisz p körzés után a gyök önmagába tér vissza; azaz $v_i=v_{i+p}$.

A reducált egyenletek gyökeinek ezen alakját már Hermite találta meg inductio utján, azokat az illető egyenletek kiszámitása által igazolván. Épen e három esetet közöltük, mivel további fejtegetések végre még a következő tételt adják:

A modularegyenlet reductiója akkor is lehetetlen, ha az átalakítási fok törzsszám, de ez nagyobb 12-nél.

E tétel, mint ez értekezés elején megjegyeztük — Galoistól származik. Mihelyt ily esetben a kivitelt megkisértjük, kell, hogy ellentétre találjunk, mely az egyenletek képzését lehetlenné teszi. Ilyen volna például hogyha az előbb fölállitott p ismeretlennel biró p első fokú egyenletben ezek nem veszik föl külön-külön minden értéket az 1-től p-ig. Ily ellentét kimutatásával a tétel be lesz bizonyítva.

Camille Jordan legujabb müvében „Traité des substitutions et des équations algébriques“ először adta e tétel általános bebizonyitását, — Galois algebraicus elméleteiből indulván ki.

Egészen más úton, a reducált egyenlet discriminánsának vizsgálatánál, a tétel bebizonyitása mintegy önkényt tünik föl. Léteznek t. i. az u-nak 16-jával csoportosuló értékei, hol a reducált egyenletnek ugyanazon két gyöke lesz egyenlővé. Ily u-érték, miután n gyök létezik, ha ezeknek mindaz $\frac{n(n-1)}{2}$ combinatióit kimeritjük, legfölebb

$$8n(n-1)$$

lehet. De az értékek számára az n-nek más numericus függvényét kapjuk: $\chi(n)$. A nemegyenlet

$$\chi(n) < 8(n-1)n$$

melynek azután állania kell, adja a megszorítást azon esetekre, hol

$$n < 12.$$

E vizsgálatokat más alkalommal remélem közölhetni

Itt eljutottunk azon pontig, hol 5, 7 és 11 fokú typicus egyenletek állittattak fel, melyek ellipticus függvények által oldhatók. Az 5. fokú egyenletek ezeknek segítségével általánosan oldhatók; a többi fokokból csak bizonyos osztályok választatnak ki.

Miután így a modulareqyenletekben és az ezekből képzett reducált egyenletekben, az ellipticus függvények által oldható egyenletek teljes mintasorozatát megkaptuk, a további vizsgálódásnak csakis az algebra terén kell történnie. Ezen oldalról a tárgyra nemsokára visszatérni szándékom.