tanulmányok

196/1987

MTA Számítástechnikai és Automatizálási Kutató Intézet Budapest

MAGYAR TUDOMÁNYOS AKADÉMIA
SZÁMITÁSTECHNIKAI ÉS AUTOMATIZÁLÁSI KUTATÓ INTÉZETE

ALGEBRAI ALGORITMUSOK

RÓNYAI LAJOS

Tanulmányok 196/1987

A kiadásért felelős:

DR. KEVICZKY LÁSZLÓ

Főosztályvezető:

DEMETROVICS JÁNOS

ISBN 963 311 225 7

ISSN 0324-2951

Hozott anyagról sokszorosítva

8717058 MTA Sokszorosító. Budapest. F. v.: dr. Héczey Lászlóné

T A R T A L O M

old.

BEVEZETÉS

A dolgozatban véges dimenziós algebrákkal kapcsolatos algoritmikus problémákkal foglalkozunk. Kiindulópontunk a véges dimenziós asszociativ algebrák - általában Wedderburn nevével fémjelzett - struktúra elmélete. Ez az elmélet Weierstrass, Dedekind, Molien, E. Cartan, Peirce, Frobenius és Wedderburn munkássága nyomán keletkezett a múlt század hatvanas éveitől e század első évtizedéig terjedő időszakban (Andrunakievics - Rjabuhin (AR) számos a problémakör történetére vonatkozó megjegyzést tartalmaz).

Kialakult többek között a radikál (mint maximális nilpotens ideál) és a féligegyszerű algebra fogalma. Wedderburn (WE) 1908-ban bizonyitotta, hogy egy tetszőleges test feletti véges dimenziós féligegyszerű asszociativ algebra előáll teljes mátrixalgebrák direkt összegeként.

Egyik fő célunk a fenti elmélet egy algoritmikus változatának kidolgozása arra az esetre, amikor az F alaptest véges test vagy algebrai számtest. A probléma a következő: tegyük fel, hogy adott egy az F test feletti A asszociativ algebra; határozzuk meg a radikálját, majd keressük meg a radikál szerinti faktor minimális ideáljait.

Az <u>első fejezetben</u> a gyakran használt algebrai és számitáselméleti fogalmakat és eredményeket foglaljuk össze.

A <u>második fejezetben</u> a radikál meghatározásával foglalkozunk. Ez a probléma nulla karakterisztikájú testek feletti algebrák esetén

könnyen elintézhető Dickson (DI) egy tételének segitségével, ami a radikált lényegében egy lineáris egyenletrendszerrel jellemzi. A véges esetben a Dickson féle feltétel nem elégséges. A fejezetben egy új, algoritmikusan kezelhető definiciót adunk a GF(p) primtest feletti véges asszociativ algebrák radikáljára. Definiálni fogjuk az A algebra $I_{-1},I_0,\ldots,I_l$ ideáljainak egy rövid leszálló láncát melyre $I_{-1}=A$ és I_l az A radikálja úgy, hogy I_j ismeretében I_{j+1} hatékonyan megtalálható. Ezzel egy polinom idejű algoritmus adódik véges algebrák radikáljának meghatározására.

Az eredmény alkalmazható Lie algebrák nilradikáljának és feloldható radikáljának megkeresésére is. Jacobson (JA) egy tételét használva a Lie algebrák nilradikáljának meghatározása visszavezethető egy asszociativ algebra radikáljának megkeresésére. A véges esetben egy nilradikál algoritmusból könnyen kaphatunk egy módszert a feloldható radikál kiszámitására. Nulla karakterisztikájú test felett Beck, Kolman és Stewart (BKS) adtak hatékony algoritmust a feloldható radikál előállitására.

A <u>harmadik fejezetben</u> féligegyszerű asszociativ algebrákkal foglalkozunk. Célunk az ilyen algebrák minimális ideáljainak a megtalálása. Ez a probléma szoros kapcsolatban van az algebrai algoritmusok egyik centrális problémájával, a polinomok faktorizációjával. Legyen ugyanis $f\in F[x]$, $f=f_1\ldots f_k$ ahol az f_i polinomok irreducibilisek F felett és páronként relativ primek. Ekkor a kinai maradéktétel szerint az F[x]/(f) algebra előáll mint az $F[x]/(f_i)$ algebrák direkt összege. A minimális ideálok tehát f irreducibilis tényezőinek felelnek meg, vagyis a minimális ideálok megkeresésének problémája lényegében a polinom faktorizáció általánositásának tekinthető.

A véges esetre Friedl (FR) adott algoritmust. Ezt a módszert

általánositjuk algebrai számtestek feletti algebrákra. A fő nehézséget az eredmények növekedésének problémája okozza. Ennek kezelésére egy tisztán algebrai eredményt bizonyitunk, miszerint a centrális idempotensek mérete (a leirásukhoz szükséges bitek száma) polinomiális korlát alatt marad (3.4. Következmény).

A fejezet fő eredménye a 3.9. Tétel: a Q feletti féligegyszerű asszociativ algebrák minimális ideáljai polinom időben megtalálhatók.

A módszer egyik kulcslépése nullosztók keresése kommutativ algebrákban. Ezt a feladatot vizsgáljuk általánosabban a negyedik fejezetben. A probléma tehát az, hogy egy adott A algebrában találjunk nullosztókat (vagy bizonyitsuk, hogy A nullosztómentes). Az előző két fejezet eredményei szerint elegendő a problémát egyszerű algebrák esetén vizsgálni.

A 4. fejezetben a véges esetet vesszük szemügyre. A fő eredmény a 4.7. Tétel: a nullosztó probléma véges algebrák esetén polinomiális transzformáció erejéig ugyanabban a bonyolultsági osztályban van mint az alaptest feletti polinomok faktorizációjának problémája.

A módszer alapgondolata Wedderburn véges testekről szóló tételének egy Hersteintől ((H) 3.1.1. Tétel) származó bizonyitásából ered. Ez a bizonyitás egy az indirekt feltevés szerint létező véges ferdetestből indul ki, melyben végül kimutatja nullosztók létezését. A gondolatmenet több konstruktiv ötletet tartalmaz. Ezeket sikerül teljes mátrixalgebrákra adaptálni. A bizonyitás tisztán egzisztenciális lépéseit konstrukciókkal helyettesitjük. A lineáris algebrai jellegű lépések mellett meg kell oldanunk bizonyos norma egyenleteket is.

Az ötödik fejezetben a véges testek feletti nullosztó algoritmus alkalmazásaival foglalkozunk. A 2. és 3. fejezet eredményei szerint el tudjuk dönteni hogy az F véges test feletti A algebra

izomorf-e az $M_n(F)$ teljes mátrixalgebrával. A nullosztó algoritmust alkalmazva egy ilyen izomorfizmus explicite megadható (5.2. Tétel). Egy explicit izomorfizmus azért hasznos, mert $M_n(F)$ szokásos megadása (mint n-szer n-es mátrixok algebrája) igen jól kezelhető, például könnyen felbontható minimális balideálok direkt összegére. Igy tetszőleges véges féligegyszerű algebrát fel tudunk bontani minimális balideálok direkt összegére.

Egy szorosan kapcsolódó másik alkalmazás az invariáns altér probléma: adott egy V véges vektortér és V lineáris transzformációinak egy véges S halmaza; a feladat az, hogy találjunk nemtriviális, az S elemeinek hatására invariáns alteret V-ben. Ez a probléma is a polinom faktorizációval azonos bonyolultságú (5.4. Tétel), igy például megoldható polinom idejű Las Vegas módszerrel. Az invariáns altér problémára adott módszert kiterjesztjük tetszőleges véges féligegyszerű algebra feletti véges modulusokra: ezek hatékonyan felbonthatók egyszerű modulusok direkt összegére.

Végül egy permutációcsoportokkal kapcsolatos alkalmazással foglalkozunk. A következő problémát W. M. Kantor vetette fel. Legyen G egy n-edfokú permutációcsoport és $K \lhd H$ normálosztói G-nek úgy, hogy H/K elemi Abel p-csoport valamilyen p primre. A G,K,H csoportok egy-egy erős generátorrendszerrel (pl. Luks (LU)) vannak megadva. . A feladat az, hogy találjunk minimális, a $K \lhd L \trianglelefteq H$ feltételeknek elegettevő G-beli normálosztót.

A feladat könnyen visszavezethető a p elemű test feletti invariáns altér problémára. Mivel p szükségképpen kicsi az input méretéhez képest, a feladatra determinisztikus polinom idejű módszer adódik (5.6. Következmény).

A <u>hatodik fejezetben</u> a racionális test feletti nullosztó problémával foglalkozunk. Itt a feladat a véges esetnél jóval nehezebbnek (nagyobb bonyolultságúnak) tűnik. A fejezetben a

legkisebb nemtriviális esetet tárgyaljuk, amikor A centrális egyszerű Q felett és $\dim_Q A=4$. Ismeretes, hogy ekkor A vagy ferdetest, vagy izomorf az $M_2(Q)$ teljes mátrixalgebrával. A kvaternióalgebrák néhány tulajdonságát használva megmutatjuk, hogy a nullosztó problémának ez az esete (6.1. Probléma) ekvivalens (Karp értelemben) egy számelméleti kérdéssel: bizonyos háromváltozós kvadratikus diofantikus egyenletek nemtriviális megoldásának létezésével (6.2. Probléma).

Az ekvivalencia bizonyításához polinom idejű algoritmust adunk az A algebra egy kvaternióalgebra reprezentációjának megkeresésére (6.2. Tétel). Az ekvivalencia következményeként adódik, hogy a nullosztó problémának ez az esete az NP ∩ co-NP bonyolultsági osztályba tartozik és hogy nem nehezebb, mint az egész számok prímtényezős felbontásának feladata.

A fejezet hátralevő részében a probléma nehézségét szeretnénk illusztrálni azzal, hogy a 6.1. Problémára redukálunk egy a szakmai közvélemény által nehéznek tekintett másik feladatot, a kvadratikus maradék problémát (6.11. Tétel). Ez az eredmény feltételes. Feltesszük, hogy a Riemann sejtés igaz az algebrai számtestek Dedekind féle dzetafüggvényeire. Ezzel a feltétellel Lagarias és Odlyzko (LO) bizonyították a Csebotarjev Sűrűségi Tétel egy igen erős változatát. A Lagarias – Odlyzko tételt alkalmas testre alkalmazva adódik, hogy egy viszonylag rövid intervallumban is sok olyan 4k+1 alakú r prím van mely a modulo n kvadratikus maradékok csoportja szerint egy előre megadott mellékosztályba esik (6.9. Következmény). Ezt a (feltételes) eredményt használva egy randomizált redukciót adunk.

A redukció (feltételes) következménye, hogy a nullosztó probléma Q felett legalább olyan nehéz mint a négyzetmentes egész számok prímtényezőinek megkeresése.

A hetedik fejezetben visszatérünk az alapokhoz. A terület talán

legfontosabb nyitott kérdésével, a véges testek feletti polinomfaktorizációval kapcsolatban bizonyitunk néhány eredményt. A fejezet fő eredménye a következő:

7.1. Tétel Legyen $f \in GF(p)[x]$ egy polinom, melynek gyökei a primtesteben vannak. Legyen r az n=deg(f)>1 egy primosztója. Tegyük fel továbbá, hogy a GF(p) feletti r-edik körosztási test és ebből egy r-edik nemmaradék adottak. Ekkor f felbontható két nem állandó tényező szorzatára egy determinisztikus algoritmussal, melynek a futási ideje polinomiális az n^r és log p paraméterekben.

A fenti eredményből következik például, hogy ha p 4k+3 alakú prim és f egy a tétel feltételének eleget tevő páros fokú polinom, akkor polinom időben találhatunk f-nek egy nemtriviális osztóját. A Riemann sejtés egy általánositását feltételezve Huang (H2) determinisztikus polinom idejű algoritmust adott a körosztási testek konstrukciójára és bennük r-edik nemmaradék keresésére. Huang eredményét használva polinom idejű algoritmust adunk a korlátos sok irreducibilis tényezőre bomló polinomok faktorizálására (7.3. Következmény).
A 7.1. Tétel bizonyitása és a mögötte levő algoritmus multilineáris algebrai jellegű.

Köszönetnyilvánitás

Szeretnék köszönetet mondani Dr. Babai Lászlónak, aki számos értékes tanáccsal, útmutatással segitette munkámat. Ő irányitotta a figyelmemet az algebrákkal kapcsolatos algoritmikus kérdésekre és az általa vezetett szemináriumon tanultam meg a számitáselmélet alapjait.
Köszönettel tartozom Dr. Demetrovics Jánosnak és az általa vezetett kollektivának, akiknek támogatása és segitőkészsége

számomra lehetőséget biztositott a kutatómunkához.

Végül szeretném megköszönni feleségemnek, Mártinak azt az áldozatkészséget, bátoritást és támogatást, amit munkám során nyújtott.

1. FOGALMAK, ELŐKÉSZÜLETEK

A fejezetben röviden ismertetjük a gyakran használt fogalmakat, jelöléseket, eredményeket.

1.1. Véges dimenziós algebrák

Legyen A egy az F test feletti vektortér. Tegyük fel, hogy az A alaphalmazán (amit szintén A-val jelölünk) értelmezett egy bináris F-bilineáris operáció *. Ekkor a vektortér műveletekkel és a fenti "szorzással" ellátott A-t az F test feletti algebrának nevezzük.

A szokásos módon értelmezhetjük a részalgebra, ideál, homomorfizmus, faktoralgebra fogalmakat. Az A algebra F test feletti dimenziója $\dim_F A$ az A-nak mint F feletti vektortérnek a dimenziója. A disszertációban kizárólag véges dimenziós algebrákkal foglalkozunk.

Ha a * szorzás asszociatív, vagyis $x*(y*z)=(x*y)*z$ teljesül minden A-beli x,y,z elemhármasra, akkor A egy asszociatív algebra.

Az alábbiakban néhány asszociatív algebrákkal (röviden: algebrákkal) kapcsolatos fogalmat, eredményt tekintünk át. A részleteket illetően Jacobson (JAC), Herstein (H), Drozd - Kirivenko (DK) és Pierce (P) munkáira hivatkozunk. Az egyszerűség kedvéért két elem szorzatára x*y helyett az xy jelölést alkalmazzuk. Az A asszociatív algebra egyszerű, ha csak triviális ideáljai vannak (ezek (0) és A maga) és AA=A teljesül.

Reprezentáció Tétel bizonyitásához elég az A egységelemes bővitésének, illetve A-nak magának a reguláris reprezentációját venni (utóbbit akkor ha A egységelemes).

Az A algebra nullától különböző x eleme nullosztó, ha van olyan nullától különböző y eleme A-nak, hogy xy=0. Ebben az esetben x,y egy nullosztópár.

Az A algebra x eleme nilpotens, ha $x^m=0$ teljesül alkalmas m természetes számra. Az x elem erősen nilpotens eleme A-nak, ha xy nilpotens minden $y \in A$-ra. Az erősen nilpotens elemek halmaza Rad(A) egy ideál A-ban, az A radikálja. Az A algebra féligegyszerű ha Rad(A)=(0). Könnyű látni, hogy A/Rad(A) féligegyszerű algebra. Féligegyszerű algebrákra egy igen erős struktúratétel érvényes.

Wedderburn – Artin struktúratétel Legyen A egy véges dimenziós féligegyszerű algebra az F test felett. Ekkor A előáll egyszerű algebrák direkt összegeként:

$$A=A_1+A_2+\ldots+A_k$$

ahol $A_1,\ldots,A_k$ az A algebra összes minimális ideáljai. Ezen felül A_i izomorf egy $M_{n_i}(F_i)$ alakú teljes mátrixalgebrával, ahol F_i egy az F-et a centrumában tartalmazó nem feltétlenül kommutativ test.

Legyen A egy asszociativ algebra, B egy egységelemes részalgebrája és legyen b a B egy eleme. Legyen továbbá L egy az F-et a centrumában tartalmazó részteste B-nek. A b elem B-beli L feletti minimálpolinomja $f_{b,B,L}$ az a legkisebb fokú normált L-beli együtthatós polinom, melynek b gyöke. A fenti polinom L-től való függése világos, de függ B-től is, hiszen különböző részalgebrák egységelemei lehetnek különbözők. Ha $f_{b,B,L}$ felbontható az L test felett nem állandó tényezők szorzatára, mondjuk $f_{b,B,L}=gh$ akkor világos, hogy g(b) és h(b) egy

nullosztópár. Ennél több is igaz, ha A kommutativ és g és h relativ primek. A következő állitás egyszerű számolással igazolható és a bizonyitást mellőzzük.

1.1. Lemma Legyen A egy az F test feletti egységelemes kommutativ algebra és legyen b az A algebrának egy olyan eleme, melyre $f_{b,A,F}=gh$ ahol $g,h\in F[x]$ és $gcd(g,h)=1$. Ekkor A felbontható az I:=g(b)A és J:=h(b)A ideálok direkt összegére. Az I és J ideálok szintén egységelemesek.

Legyen most A féligegyszerű kommutativ algebra az F test felett, ahol F vagy véges vagy algebrai számtest. Legyen az A algebra Wedderburn - Artin tétel szerinti direkt felbontása

$$A=A_1+\ldots+A_k.$$

Az A_i ideálok ekkor kommutativ testek. Tetszőleges A-beli b elem egyértelműen előáll

$$b=b_1+\ldots+b_k$$

alakban, ahol $b_i\in A_i$, $i=1,\ldots,k$. A következő lemma segitségével kapcsolat teremthető polinomok faktorizációja illetve algebrák Wedderburn - Artin felbontása között. Az állitások jól ismert tények, ezért a bizonyitást elhagyjuk.

1.2. Lemma Legyen $p\in F[x]$ és legyenek F, A, b, b_i a fentiek. Igazak az alábbiak:

1. $f_{b,A,F}=lcm(f_{b_1,A_1,F},\ldots,f_{b_k,A_k,F})$.
2. Az $f_{b,A,F}$ polinomnak nincs többszörös gyöke (semmilyen F-et tartalmazó testben).
3. A $p(b_i)$ elem akkor és csak akkor nem nulla, ha a p(b)A ideál tartalmazza az A_i ideált.

Szükségünk lesz néhány Lie algebrákkal kapcsolatos tényre is. A

felsorolt eredmények megtalálhatók Jacobson (JA) illetve Humphreys (HU) munkáiban.

A szorzás jelölésére * helyett a szokásosabb [ ] jelölést használjuk. Emlékeztetünk, hogy az F test feletti L algebra egy Lie algebra , ha a "szorzásra" teljesülnek a következők:

1. $[xx]=0$ az L minden x elemére.

2. $[[xy]z]+[[yz]x]+[[zx]y]=0$ minden $x, y, z \in L$ esetén.

Az L Lie algebra kommutátor sora a következő ideállánc:

$L^{(0)}:=L,\ldots,L^{(i+1)}:=[L^{(i)}L^{(i)}]$.

Az L Lie algebra feloldható, ha $L^{(n)}=(0)$, valamely n természetes számra. Ismert, hogy ha L egy véges dimenziós Lie algebra az F test felett, akkor L-ben egyetlen maximális feloldható ideál van. Ez az R(L) ideál az L algebra (feloldható) radikálja.

Hasonlóan, definiáljuk az L leszálló centrális láncát a következőképpen:

$L^{0}:=L,\ldots,L^{i+1}:=[LL^{i}]$.

Az L algebra nilpotens, ha $L^{n}=(0)$ valamely n természetes számra. Az L algebrában egyetlen maximális nilpotens ideál van. Ez az N(L) ideál az L nilradikálja.

Példa. Legyenek $A,B \in M_n(F)$ és legyen $[AB]:=AB-BA$ (vagyis az additiv kommutátor). Belátható, hogy erre az operációra teljesülnek az 1.-2. kikötések, tehát ha L az $M_n(F)$ egy tetszőleges olyan altere, mely zárt a [ ] operációra, akkor L egy Lie algebra. Az így adódó Lie algebrákat lineáris Lie algebráknak nevezzük.

A reguláris reprezentációhoz hasonlóan Lie algebrák esetén is van egy kényelmes és hasznos módszer, mellyel tetszőleges Lie algebra reprezentálható lineáris Lie algebraként (bár ez a reprezentáció általában nem hűséges). Tetszőleges $x \in L$ esetén legyen $ad(x):L\to L$ az a lineáris transzformáció, melyre

ad(x)y:=[xy] minden L-beli y elemre.

Az x→ad(x) megfeleltetés egy Lie algebra homomorfizmus. A képként adódó lineáris Lie algebra ad(L) az L adjungált reprezentációja. Megemlitjük itt, hogy Ado és Iwasawa egy mély eredménye szerint (Jacobson, loc. cit. Chapter 6) tetszőleges véges dimenziós Lie algebra izomorf egy lineáris Lie algebrával. Nekünk itt az adjungált reprezentáció is elegendő lesz.

1.2. Algoritmusok.

Ebben a részben a legfontosabb algoritmikus segédeszközöket tekintjük át. Először az inputtal foglalkozunk.

Racionális számokat, vektorokat, mátrixokat polinomokat illetve mod n maradékosztályokat, vektorokat, mátrixokat, polinomokat a szokásos bináris kódolásban tekintjük. Igy például az n egész szám hossza $1+\lceil \log_2(n+1) \rceil$, egy mod m maradékosztály hossza $\lceil \log_2(m+1) \rceil$. Ez a definició azután kiterjeszthető összetett objektumokra: összeadjuk a benne szereplő "részek" hosszát.

Ha F egy véges test, vagy algebrai számtest, akkor F megadható egy a P primtest feletti irreducibilis polinommal (egy olyan a elem P feletti f főpolinomjával, melyre F=P(a)). Ekkor az F elemei a testelméletből jól ismert módon reprezentálhatók mint mod f polinomok.

Egy az F test feletti (asszociativ vagy Lie) algebrát megadhatunk úgy, hogy megadjuk az F testet és az A algebra (valamely F feletti bázisra vonatkozó) struktúrakonstansait: ha $a_1,\ldots,a_n$ egy F feletti bázisa A-nak, akkor a disztributiv szabály szerint tetszőleges szorzatot megkaphatunk, ha ismerjük az a_i*a_j alakú szorzatokat. Fejezzük ki ezeket, mint az $a_1,\ldots,a_k$ elemek lineáris kombinációit.

$$a_i*a_j=c_{ij1}a_1+\ldots+c_{ijn}a_n \quad , \; i,j=1,\ldots,n$$

és $c_{ijk} \in F$. A c_{ijk} együtthatók a fenti bázisra vonatkozó struktúrakonstansok. Megjegyezzük még, hogy az F test főpolinommal való megadása lényegében tekinthető az F mint P-algebra struktúrakonstansokkal való megadásának.

Egy algoritmus bonyolultságán az elvégzéséhez szükséges bit műveletek számát értjük.

Algoritmusaink bonyolultságát illetően általában csak az érdekel bennünket, hogy polinomkorlátosak-e az input hosszában. Ezért nem foglalkozunk pontos korlátokkal a felhasznált módszerek esetében sem.

Polinom idejű algoritmusok ismeretesek (Knuth (K) újabb eredményekre nézve Lagarias (L)) az alapvető "szeminumerikus" feladatokra: primtestekbeli összeadásra , szorzásra, osztásra; primtestek feletti polinomok összeadására, szorzására. Ezek a módszerek különösebb nehézség nélkül általánosithatók primtestek véges bővitéseire, illetve ezek feletti véges dimenziós algebrákra (az osztás persze csak akkor ha értelmes).

Egész számok legnagyobb közös osztója hatékonyan meghatározható az euklideszi algoritmus különféle változataival (Knuth (K), Schönhage (SCHÖ)).

A dolgozatban igen fontos szerepet játszanak a szóbanforgó testek feletti polinomok faktorizálására szolgáló módszerek. Véges testek feletti polinomok faktorizálására Berlekamp ((B1), (LN), (K)) adott determinisztikus módszert. Ez sajnos nem polinom idejű módszer. Az eljárás futási ideje polinomiálisan függ ugyan a szóbanforgó $f \in F[x]$ polinom fokától és az F testnek a GF(p) primtest feletti fokától, de a primtest karakterisztikájától is (ezzel szemben az input hossza O(deg(f)log q), ahol q az F elemszáma). Berlekamp módszerét a 7. fejezetben vázolni fogjuk.

Még másodfokú polinomokra sem ismeretes determinisztikus polinom

Még másodfokú polinomokra sem ismeretes determinisztikus polinom idejű algoritmus. Itt azonban meg kell említeni egy izgalmas új eredményt. Schoof (SCH) talált egy polinom idejű algoritmust véges elliptikus csoportok rendjének meghatározására (kicsit pontosabban: egy F véges test feletti Weierstrass normálformában (Silverman (SI)) adott elliptikus görbe F felett racionális pontjainak a számát tudja kiszámitani). Ennek a módszernek a melléktermékeként az $x^2=a(\mathrm{mod}\ p)$ kongruenciát meg tudja oldani $O((|a|+\log p)^c)$ időben $-p<a<p$, ha létezik egész megoldás.

Ha véletlen lépéseket is megengedünk, akkor a véges testek feletti polinom faktorizáció problémája már kezelhető. Berlekamp (B2) talált polinom idejű Las Vegas módszert a problémára. Las Vegas algoritmuson olyan randomizációt is használó módszert értünk, amely tetszőleges inputra vagy helyes eredményt ad, vagy, kis valószinűséggel "bejelenti" hogy nem tudta megoldani a feladatot (tehát sohasem ad inkorrekt eredményt). A Las Vegas módszer fogalma Babai Lászlótól származik (BA).

További Las Vegas módszereket illetve ezekhez fűződő eredményeket találhat az olvasó a Ben-Or (BO), Camion (CA), Cantor - Zassenhaus (CZ) és Rabin (RA1) dolgozatokban.

A fenti Las Vegas módszerek igen hatékonyak, tehát a probléma gyakorlati szempontból megoldottnak tekinthető.

A racionális test feletti polinomok faktorizálásának problémája régóta foglalkoztatja a kutatókat. Az első módszerek Gauss, Abel és Kronecker nevéhez fűződnek (a probléma történetével kapcsolatos megjegyzések találhatók (K)-ban). Ezek a módszerek azonban exponenciális bonyolultságúak. Polinom idejű algoritmus létezése egészen 1982-ig nem volt ismert. A nagy áttörés A.K. Lenstra, H.W. Lenstra és Lovász László (LLL) nevéhez fűződik. Berlekamp determinisztikus módszerét és a Hensel lemmát használva visszavezették a problémát egy geometriai kérdésre: rövid vektor

keresésére egy rácsban. Utóbbi problémára és így a faktorizáció problémájára polinom idejű módszert adtak. Ezt a módszert azután többen egymástól függetlenül kiterjesztették algebrai számtestek feletti polinomok felbontására: Chistov - Grigoryev (CG) - ök valójában tetszőleges nulla karakterisztikájú globális testre megoldják a problémát, Landau (LA), Lenstra (LE).

Gyakran lesz szükségünk lineáris egyenletrendszerek megoldására is. Véges testek felett minden probléma nélkül alkalmazhatók a lineáris algebra elemeiből megismert módszerek. A végtelen esetben már gondosabban kell eljárni: ügyelni kell arra, hogy a számítások során adódó részeredmények hossza ne növekedjen túlságosan. A racionális test feletti lineáris egyenletrendszerek megoldására Frumkin (FRU), majd Kannan és Bachem (KB) adtak polinom idejű algoritmust; utóbbit Chou és Collins (CC) több részletet illetően megjavitották. A módszer könnyen kiterjeszthető tetszőleges algebrai számtestre.

Lineáris egyenletrendszerek megoldásával számos felmerülő részfeladat kezelhető. Ilyenek például: alterek metszetének meghatározása, minimálpolinomok ($f_{b,A,L}$ alakú polinomok) meghatározása, faktoralgebra, generált részalgebra (balideál, ideál) meghatározása, egységelem keresése algebrákban és polinomok legnagyobb közös osztójának a kiszámitása.

Megjegyezzük még, hogy az alábbi mátrixokkal kapcsolatos feladatok szintén kezelhetők polinom időben: mátrixok összeadása, szorzása, a rang a képtér és a mag meghatározása és a karakterisztikus polinom kiszámitása.

Végezetül megemlitjük, hogy tetszőleges A véges asszociativ algebra, $b \in A$ és n természetes szám esetén b^n kiszámitható polinom időben. A "gyors" modulo m hatványozás ötlete (lásd pl. Lagarias (L) Proposition 3.7) minden nehézség nélkül átvihető.

A számitáselmélet általunk használt alapfogalmait (pl. NP, co-NP,

Turing redukció, Karp redukció) illetően a Garey - Johnson (GJ), Hopcroft - Ullman (HUL) munkákra hivatkozunk.

Algoritmusaink leírásakor néhány esetben Dijkstra - Gries (D), (GR) stílusú annotációt használunk. Ezek olyan zárójelbe tett állítások, melyek az algoritmus "változói" közötti összefüggéseket mondanak ki. Ha a vezérlés egy ilyen állításhoz érkezik, akkor annak igaznak kell lennie. Bizonyos esetekben a módszer helyességének bizonyítása az annotáció helyességének bizonyításával egyenértékű.

2. A RADIKAL KISZAMITASA

Ebben a részben a Jacobson radikál meghatározásával foglalkozunk az (FR) dolgozat alapján. Ez, mint látni fogjuk, viszonylag egyszerű nulla karakterisztikájú test felett. Dickson egy tételét használva a probléma lényegében egy lineáris egyenletrendszer megoldására vezethető vissza. A véges eset nehezebb. A fejezet fő célja, hogy egy algoritmikusan kezelhető definiciót adjunk véges algebrák radikáljára.

A fejezet végén Lie algebrák feloldható radikáljának illetve nilradikáljának kiszámitásával foglalkozunk. Nulla karakterisztikájú test feletti Lie algebrák esetére Beck, Kolman és Stewart (BKS) találtak polinomiális bonyolultságú algoritmust. A véges esetben visszavezetjük a problémát asszociativ algebrák radikáljának megkeresésére, igy megmutatjuk , hogy ezek a problémák is polinomiális bonyolultságúak.

A probléma amit elöször vizsgálunk, a következő: Adott egy véges dimenziós asszociativ algebra A az F test felett, F véges algebrai bővitése a P primtestnek. Mind F a P felett, mind A az F felett egy-egy bázis és struktúra konstansok segitségével van megadva. Ez a probléma inputja. A feladat az, hogy találjunk Rad(A)-nak egy bázisát az F test felett.

A probléma könnyen visszavezethető arra az esetre, amikor F=P. Ha ugyanis d az F dimenziója P felett és n az A dimenziója F felett, akkor A felfogható egy nd dimenziós algebrának P felett. Másfelől, a radikál, mint az erősen nilpotens elemek halmaza, nem függ az alaptesttől. A következőkben tehát feltesszük hogy F=P.

További egyszerűsitést érhetünk el azzal, hogy mátrix algebrákra szoritkozunk. Ez, használva a reguláris reprezentációt, illetve azt, hogy egy ilyen reprezentációt hatékonyan kaphatunk a bázis és struktúrakonstansok segitségvel megadott inputból, nem jelenti az általánosság korlátozását.

2.1. A racionális eset.

Itt a problémát könnyen elintézhetjük Dicksonnak egy a mátrixalgebrák radikálját leiró tételével.

2.1. Tétel (Dickson (DI), 106-108.o.) Legyen A egy mátrixalgebra az F test felett és tegyük fel hogy charF=0. Ekkor

$$Rad(A)=\{\ x\in A\ ;\ Tr(xy)=0 \text{ minden A-beli y elemre }\}.$$

Mivel a nyom egy F-lineáris függvény, rögtön adódik a

2.2. Következmény. Legyen A egy mátrix algebra az F test felett és tegyük fel hogy charF=0. Legyen továbbá $a_1,\ldots,a_n$ egy bázisa A-nak az F test felett. Ekkor

$$Rad(A)=\{\ x\in A\ ;\ Tr(xa_i)=0\ \ i=1,\ldots,n\ \}.$$

A fenti következményből látszik, hogy Rad(A) leirható egy F feletti lineáris egyenletrendszer segitségével. Ehhez elegendő az x elemet felirni az $a_1,\ldots,a_n$ elemek határozatlan együtthatós lineáris kombinációjaként.

Megemlitjük, hogy Drazin (DR) a nyom és az algebrai tulajdonságok közötti további összefüggéseket tárgyal nulla karakterisztikájú testek feletti algebrák esetén.

2.2. A véges eset.

Legyen p egy primszám, F=GF(p) és tegyük fel, hogy A az $M_n(p):=M_n(F)$ egy részalgebrája melyre $\dim_F A=n$ vagy n-1 (a reguláris reprezentációval adódó részalgebrákra ez teljesül). Definiáljuk az l természetes számot a következő egyenlőtlenségekkel : $p^l \leq n < p^{l+1}$.

Jelölje B az $A \cup \{I\}$ <u>mátrixhalmazt</u>, ahol I az $M_n(p)$ egységelemét jelöli.

A célunk az hogy definiáljuk A ideáljainak egy $I_{-1}, I_0, \ldots, I_l$ valamint függvényeknek egy $g_i : I_{i-1} \to GF(p)$ sorozatát a következő tulajdonságokkal:

1. $I_{-1}=A$ és $I_l=\mathrm{Rad}(A)$.
2. g_i lineáris függvény az I_{i-1} ideálon, $i=0,\ldots,l$.
3. $I_i=\{ x \in I_{i-1} ; g_i(xy)=0$ minden $y \in B$-re $\}$.
4. $g_i(x)$ kiszámítható polinom időben tetszőleges A-beli x elemre (vagyis a bonyolultsága felülről becsülhető log (p) és n egy polinomjával).

A fentiekből rögtön adódik, hogy ha ismerjük I_{i-1} egy bázisát, akkor I_i egy bázisa megkapható egy GF(p) feletti lineáris egyenletrendszer megoldásával. Az egyenletrendszer együtthatói polinom időben meghatározhatók a g_i függvények tulajdonságai miatt. A szükséges iterácók száma l+1=O(log(n)), tehát a radikál megkapható $(n+\log(p))^c$ bit-művelet elvégzésével, ahol c egy alkalmas pozitiv állandó.

A következőkben definiáljuk a fenti ideálokat és lineáris függvényeket és bizonyitjuk az 1.-4. tulajdonságokat. Ehhez szükségünk lesz némi előkészületre.

Jelölje M_n az n-szer n-es mátrixok gyűrűjét Z felett és jelölje h az $M_n \to M_n(p)$ gyűrű homomorfizmust melyet a $Z \to GF(p)$ epimorfizmus indukál. Magyarul h az egész elemű mátrixok mod p redukálását jelenti.

Az egész elemű mátrixokat nagybetűvel (C,D,X,Y,Z_i), az $M_n(p)$ beli képeiket a megfelelő kisbetűvel jelöljük.

Szeretnénk c^{p^i} alakú elemek nyomát értelmezni $(\mathrm{mod}\ p^{i+1})$ ahol $c \in M_n(p)$ úgy, hogy veszünk egy egész elemű C mátrixot, melyre $h(C)=c$ és a $\mathrm{Tr}(C^{p^i})(\mathrm{mod}\ p^{i+1})$ elemet tekintjük. A következő lemmában megmutatjuk, hogy ez a definició értelmes.

2.3. Lemma Legyenek C,D egész elemű mátrixok és tegyük fel, hogy $h(C)=h(D)$. Ekkor tetszőleges i természetes számra

$$\mathrm{Tr}(C^{p^i}) \equiv \mathrm{Tr}(D^{p^i})(\mathrm{mod}\ p^{i+1}).$$

Bizonyitás. Legyen $P=D-C$. Világos, hogy a P mátrix minden eleme osztható p-vel. Megjegyezzük, hogy ha $B_1,\ldots,B_k$ egész elemű mátrixok és közülük m egyenlő P-vel, akkor a $B=B_1\ldots B_k$ mátrix minden eleme osztható p^m-mel, következésképpen $\mathrm{Tr}(B)$ osztható p^m-mel.

Fejtsük ki a bizonyitandó kongruencia jobboldalát. Ekkor

$$\mathrm{Tr}(D^{p^i})=\mathrm{Tr}((C+P)^{p^i})=\sum \mathrm{Tr}(Z_1Z_2\ldots Z_{p^i})$$

ahol $Z_i=C$ vagy $Z_i=P$ és az összegezés kiterjed minden ilyen szorzatra. Jelölje $G=\langle \pi \rangle$ a p^i elemű ciklikus csoportot. Definiáljuk G egy permutáció-reprezentációját a fenti szavakon mint jegyhalmazon a következő módon:

$$\pi(Z_1Z_2\ldots Z_{p^i})=Z_{p^i}Z_1\ldots Z_{p^i-1}\ ,$$

vagyis ciklikusan permutálja a tényezőket. Világos, hogy ha V és W két szó ugyanabból az orbitból, akkor $\mathrm{Tr}(V)=\mathrm{Tr}(W)$, mivel $\mathrm{Tr}(XY)=\mathrm{Tr}(YX)$ igaz minden $X,Y \in M_n$ esetén. Ha a V szó orbitja p^j elemet tartalmaz, akkor ennek az orbitnak az adaléka az összeghez $p^j\mathrm{Tr}(V)$. Másfelől ebben az esetben π^{p^j} fixálja V-t, vagyis V nem más mint a p^{i-j}-edik hatványa az első p^j tényezőnek.

Ha V (mint szó) nem C^{p^i}, akkor a Z_k mátrixok közül legalább p^{i-j} egyenlő P-vel. Használva, hogy p^{i-j} legalább i-j+1, kapjuk,hogy V nyoma osztható p^{i-j+1}-gyel és igy az orbit adaléka osztható p^{i+1}-

gyel. Észrevéve, hogy C^{p^i} fixeleme G-nek, a bizonyitás teljes.

A következő lemma indukciós bizonyitásoknál lesz hasznos.

2.4. Lemma Legyen H egy a szorzásra zárt részhalmaza M_n-nek. Legyen továbbá k egy pozitiv egész és tegyük fel, hogy $Tr(X^{p^i})$ osztható p^{i+1}-gyel minden $X \in H$ és $0 \leq i < k$ esetén. Ekkor tetszőleges $X, Y \in H$ esetén

$$Tr((X+Y)^{p^k}) \equiv Tr(X^{p^k}) + Tr(Y^{p^k}) \pmod{p^{k+1}}.$$

Bizonyitás. Fejtsük ki ezúttal az állitásban szereplő kongruencia baloldalát.

$$Tr((X+Y)^{p^k}) = \sum Tr(Z_1 Z_2 \ldots Z_{p^k})$$

ahol $Z_i = X$ vagy Y és az összegezés az összes ilyen szorzatra értendő. Az előző lemmához hasonlóan hassunk a ciklikus eltolás által generált G csoporttal a fenti szavakon és tekintsük az orbitokat. Ugyanúgy adódik, hogy ha V orbitja p^j elemet tartalmaz, akkor az orbit adaléka az összegben $p^j Tr(V)$ és hogy V előáll az első p^j tényező szorzatának p^{k-j}-edik hatványaként. Ha most j nem 0, akkor a feltételek szerint Tr(V) osztható p^{k-j+1}-gyel, vagyis az orbit összege osztható p^{k+1}-gyel. Az egyelemű orbitok összege pedig éppen a kongruencia jobboldala. A bizonyitást befejeztük.

Legyen F egy tetszőleges test és $f \in F[x]$ egy polinom, melynek főegyütthatója 1.

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

Legyenek $b_1, \ldots, b_n$ az f gyökei (F egy alkalmas bővitésében) és legyen

$$s_i = b_1^i + \ldots + b_n^i \qquad i = 1, 2, \ldots, n.$$

Az s_i elemek kifejezhetők f együtthatóival a jól ismert Newton azonosságok (Kuros (KU), 54. paragrafus) segitségével:

$$s_1+a_1=0$$

$$s_2+a_1s_1+2a_2=0$$

$$\vdots$$

$$s_n+a_1s_{n-1}+\ldots+a_{n-1}s_1+na_n=0.$$

A fenti azonosságok felhasználásával egy nilpotenciafeltételt bizonyitunk.

2.5. Lemma Legyen H egy szorzásra zárt részhalmaza M_n-nek és tegyük fel, hogy H minden X elemére $Tr(X^{p^l})$ osztható p^{l+1}-gyel, ahol l a $p^l \leq n < p^{l+1}$ egyenlőtlenségekkel meghatározott természetes szám. Ekkor h(X) nilpotens minden $X \in H$ esetén.

Bizonyitás. Elegendő látni, hogy $h(X)^{p^l} = h(X^{p^l})$ nilpotens. Legyen f az $Y=X^{p^l}$ normált karakterisztikus polinomja Q felett (az f főegyütthatója 1). Világos, hogy f együtthatói egészek, és h(Y) nilpotens pontosan akkor, ha minden a_i osztható p-vel. A Newton azonosságokat alkalmazzuk az f polinomra. Használva, hogy

$$s_i=Tr(Y^i)=Tr((X^i)^{p^l})$$

és $X^i \in H$, kapjuk, hogy s_i osztható p^{l+1}-gyel.

A Newton azonosságokból adódik, hogy $ia_i \equiv 0 \pmod{p^{l+1}}$ ha $i=1,\ldots,n$. Az l definiciójából következik, hogy i nem osztható p^{l+1}-gyel, tehát a_i osztható p-vel, amint azt bizonyitani akartuk.

A következő lemmában egy szükséges feltételt fogalmazunk meg a nilpotenciára.

2.6. Lemma Tegyük fel, hogy $X \in M_n$ és h(X) nilpotens. Ekkor minden i természetes számra

$$Tr(X^{p^i}) \equiv 0 \pmod{p^{i+1}}.$$

Bizonyitás. h(X) nilpotens, tehát (GF(p) felett) hasonló egy szigorúan felső triangularis mátrixhoz. Ezt a tényt megfogalmazva egész elemű mátrixok nyelvén, adódik, hogy vannak olyan C,D,P,R,U

elemei az M_n gyűrűnek, hogy

$$CXD=U+P \quad , \quad DC=I+R \quad , \; U^n=0 \text{ és } h(P)=h(R)=o$$

ahol I azegységmátrix, 0 és o pedig M_n illetve $M_n(p)$ zéruselemei.

A 2.3. Lemma szerint

$$0=Tr(U^{p^i})\equiv Tr((U+P)^{p^i})=Tr((CXD)^{p^i})$$

ahol a kongruencia modulo p^{i+1} értendő. Hasonlóan adódik

$$Tr((CXD)^{p^i})=Tr((DCX)^{p^i})=Tr((X+RX)^{p^i}).$$

Vegyük észre, hogy h(RX)=o, tehát a 2.3. Lemma szerint

$$Tr((X+RX)^{p^i})\equiv Tr(X^{p^i})(\text{mod } p^{i+1}).$$

Összehasonlítva a lánc két végét, látjuk, hogy

$$Tr(X^{p^i})\equiv 0(\text{mod } p^{i+i})$$

amint azt állitottuk.

Ezen előkészületek után visszatérünk az eredeti problémához. Legyen A az $M_n(p)$ egy részalgebrája. Definiáljuk az I_i ideálokat a következő módon. Legyen $I_{-1}=A$, továbbá i=0,1,...,l esetén legyen

$$I_i=(x \in A \; ; \; Tr((xy)^{p^j})=0(\text{mod } p^{j+1}) \text{ minden } y \in B \text{ és } 0\leq j\leq i \text{ esetén})$$

(B az A és (I) uniója.) Megjegyezzük még, hogy $u \in A$ esetén a $Tr(u^{p^j})(\text{mod } p^{j+1})$ maradékosztály nem más, mint $Tr(U^{p^j})(\text{mod } p^{j+1})$ ahol U egy tetszőleges olyan egész mátrix, melyre h(U)=u. Ez a definició a 2.3. Lemma szerint értelmes.

A definicióból nyilvánvaló, hogy az I_i halmazok az A részhalmazainak egy (nem feltétlenül szigorúan) csökkenő láncát alkotják. Most bebizonyitjuk, hogy ezek a részhalmazok ideáljai az A algebrának.

2.7. Tétel I_k ideálja A-nak k=-1,0,1,...,l estén. Ezen felül $I_l=Rad(A)$.

Bizonyitás. Az állitás nyilvánvaló k=-1 esetén. Feltehető tehát, hogy k nemnegatív. A definicióból azonnal látható, hogy ha $x \in I_k$

és $u \in A$, akkor $xu \in I_k$. Az, hogy $ux \in I_k$, rögtön következik az alábbi azonosságból

$$Tr(((UX)Y)^m)=Tr((X(YU))^m) \quad m \text{ pozitiv egész, } U,X,Y \in M_n.$$

Be kell látnunk még, hogy I_k additiv részcsoportja A-nak. Ez világos $k=0$ esetén, hiszen a nyom additiv függvény. Feltehető tehát, hogy $k>0$. Mivel I_k zárt a szorzásra, ugyanez elmondható az I_k h-ra vonatkozó teljes inverz képéről is. Legyen ez a halmaz J_k. A 2.4. Lemmát szeretnénk alkalmazni $H=J_k$ választással. Legyenek tehát $X,Y \in J_k$, és legyen $U \in M_n$ olyan, hogy $h(U) \in B$. Legyen $0 \leq j \leq k$ tetszőleges egész. Ekkor

$$Tr(((X+Y)U)^{p^j})=Tr(((XU+YU)^{p^j}) \equiv$$
$$\equiv Tr((XU)^{p^j})+Tr((YU)^{p^j}) \equiv 0 \pmod{p^{j+1}} ,$$

ahol az első kongruencia $j=0$ esetén a nyom additivitásából, pozitiv j-re a 2.4. Lemmából következik. A második kongruencia

$$Tr((XU)^{p^j}) \equiv 0 \pmod{p^{j+1}} \text{ és}$$
$$Tr((YU)^{p^j}) \equiv 0 \pmod{p^{j+1}}$$

miatt áll fenn. Ezzel beláttuk, hogy I_k ideál. Meg kell még mutatnunk, hogy $I_l=Rad(A)$. Valóban, ha x egy radikálelem, akkor xy nilpotens tetszőleges $y \in B$ esetén. Ha U egy tetszőleges egész mátrix, melyre $h(U)=xy$, akkor, mivel U nilpotens modulo p, a 2.6. Lemma szerint

$$Tr((xy)^{p^i}) \equiv Tr(U^{p^i}) \equiv 0 \pmod{p^{i+1}} ,$$

tetszőleges i természetes számra. Kaptuk, hogy $x \in I_l$. A forditott irányú tartalmazás azonnal adódik, ha a 2.5. Lemmát alkalmazzuk $H=J_l$ szereposztással. A bizonyitást befejeztük.

Most pedig hozzálátunk a g_i függvények megkonstruálásához. Tekintsük először az $f_i : M_n \to Q$ függvényeket $(i=0,\ldots,l)$, melyekre

$$f_i(X)=(1/p^i)Tr(X^{p^i}).$$

Emlékeztetünk, hogy J_i jelöli az I_i teljes inverz képét M_n-ben. Világos, hogy ha $X \in J_{i-1}$, akkor $f_i(X)$ egy egész szám, továbbá ha $X,Y \in J_{i-1}$, akkor

(2.1) $\quad f_i(X+Y) \equiv f_i(X)+f_i(Y) \pmod p$.

A (2.1) nyilvánvaló i=0 esetén, pozitiv i-re pedig következik a 2.4. Lemmából.

Definiáljuk ezután a $g_i : I_{i-1} \to GF(p)$ függvényeket (i=0,...,l) a következőképpen:

$$g_i(x)=f_i(X) \pmod p,$$

ahol X egy tetszőleges olyan egész mátrix, melyre h(X)=x. A definició helyességét igazolandó legyenek X,Y egész mátrixok, melyekre h(X)=h(Y)=x. Ekkor a 2.3. Lemma szerint

$$Tr(X^{p^i}) \equiv Tr(Y^{p^i}) \pmod{p^{i+i}}.$$

Másfelől ekkor $X,Y \in J_{i-1}$, tehát p^i osztja mindkét oldalt, amiből

$$f_i(X) \equiv f_i(Y) \pmod p$$

következik.

A g_i függvényekkel kapcsolatos tényeket foglalja össze az alábbi

2.8 Tétel Minden i=0,...,l esetén igazak a következők:

(i) A g_i függvények GF(p)-lineárisak.

(ii) $I_i = \{ x \in I_{i-1};\ g_i(xy)=0$ minden $y \in B$ esetén $\}$.

(iii) $g_i(x)$ kiszámitható $(\log(p)+n)^c$ időben ahol c egy alkalmas p-től és n-től független pozitiv konstans.

Bizonyitás. (i) nem más mint (2.1.) .

(ii) Ez az állitás az I_i definiciójának egyszerű átfogalmazása. Ugyanis $g_i(xy)=0$ pontosan akkor teljesül, ha $Tr((xy)^{p^i})$ osztható p^{i+1}-gyel.

(iii) A g_i függvények definiciója szerint elegendő egy egész elemű mátrix hatványának a nyomát kiszámitanunk modulo p^{n+1}. Figyelembe véve, hogy a kitevő legfeljebb n, továbbá hogy a

mátrix elemei választhatók a [0,p] intervallumból, az állitás világos.

A 2.7. és 2.8. Tételekkel maradéktalanul igazoltuk a fejezetrész eljén kimondott 1.-4. tulajdonságokat. Összefoglalásul kimondhatjuk a következőt:

2.9. Tétel Legyen A egy n dimenziós algebra GF(p) felett. Rad(A) egy bázisa kiszámitható polinom időben: módszerünk bonyolultsága polinomiális n-ben és log(p)-ben.

2.3. Lie algebrák radikálja

Először a nilradikállal foglalkozunk. Ezt a kérdést visszavezethetjük az asszociativ esetre, alkalmazva Jacobson egy tételét. Legyen L egy véges dimenziós Lie algebra az F test felett. Ekkor

2.10 Tétel (Jacobson (JA) 36.o.) Legyen L' az ad(L) által generált asszociativ (mátrix-) algebra. Ekkor az L algebra x elemére $x \in N(L)$ pontosan akkor teljesül, ha $ad(x) \in Rad(L')$.

Ez az eredmény a nilradikál kiszámitásának problémáját elintézi mind algebrai számtestek, mind pedig véges testek felett. Ki tudjuk ugyanis számitani az ad(L) és - a fejezet eddigi eredményei szerint - a Rad(L') altereket L'-ben. Ezután elegendő ezen két altér metszetét kiszámitani. Ez a feladat pedig egy lineáris egyenletrendszer megoldását jelenti. Kimondhatjuk tehát a következőt:

2.11. Következmény Legyen L véges dimenziós Lie algebra az F test felett (F algebrai számtest vagy véges test). Ekkor N(L)

kiszámítható polinomkorlátos algoritmussal.

Ezután nézzük a (feloldható) radikál R(L) meghatározásának problémáját. A nulla karakterisztikájú esetre Beck - Kolman - Stewart (BKS) adtak polinomiális algoritmust. Módszerük egy az R(L)-nek a Killing forma segítségével történő karakterizációján alapul, mely hasonlít Dickson általunk idézett tételéhez. Ez a jellemzés, csakúgy mint a 2.1. Tétel állítása, nem igaz pozitív karakterisztika mellett.
Ha F és L véges, akkor viszont R(L) kiszámítása hatékonyan visszavezethető (egészen pontosan: polinom időben Turing redukálható) N(L) kiszámolására. Valóban, tetszőleges L Lie algebrára $N(L) \leq R(L)$ és ha N(L)=(0), akkor R(L)=(0), hiszen az $L^{(i)}$ sorozat utolsó előtti eleme Abel féle, tehát nilpotens ideál.

Definiáljuk az L_i sorozatot a következőképpen: legyen $L_0=L$ és ha $N(L_i)$ nem (0), akkor legyen $L_{i+1}=L_i/N(L_i)$. Ha $N(L_i)=(0)$, akkor a következő elemet már nem definiáljuk. A sorozatnak legfeljebb $\dim_F L+1$ eleme van. A 2.11. Következmény szerint ha F véges, akkor a sorozat tagjai polinom időben kiszámíthatók, hiszen nem kell az együtthatók növekedésétől tartani. Ha minden lépésnél feljegyezzük $N(L_i)$ bázisának tetszőleges L-beli inverz képét, akkor végül - ezek uniójaként - R(L) egy bázisa adódik.

2.12 Következmény Legyen L véges dimenziós Lie algebra az F véges test felett. R(L) kiszámítható egy polinomkorlátos algoritmussal.

3. FÉLIGEGYSZERŰ ALGEBRÁK FELBONTÁSA

Ebben a fejezetben féligegyszerű asszociatív algebrák minimális ideáljainak, vagyis a Wedderburn - Artin tételben szereplő direkt összeg felbontásnak a kiszámitása a célunk. A probléma, mint azt korábban láttuk, általánositása a polinom faktorizáció problémájának a kérdéses test felett. Az itt bemutatásra kerülő eredmények szerint ez az általánosabb probléma lényegében ugyanolyan bonyolultságú, mint a polinomok faktorizációja.
Mind véges, mind algebrai számtest esetén lényegében ugyanaz a módszer használható. A végtelen esetben azonban az eredmények növekedésének problémáját is meg kell oldanunk.

3.1. Visszavezetés a kommutativ esetre

Legyen tehát A egy bázis és struktúrakonstansok segitségével megadott véges dimenziós féligegyszerű asszociativ algebra az F test felett, ahol F véges test vagy algebrai számtest. A Wedderburn - Artin struktúra tétel szerint A előáll mint az $A_1,\ldots,A_k$ minimális ideáljainak direkt összege. Célunk az, hogy A ismeretében meghatározzuk az A_i ideálokat, vagyis adjuk meg egy-egy bázisukat az F test felett. A probléma polinom időben visszavezethető arra az esetre, amikor A kommutativ. Legyen ugyanis B az A centruma. Világos, hogy B meghatározható egy F feletti lineáris egyenletrendszer megoldásával, hiszen x centrumelem A-ban pontosan akkor, ha $xa_i=a_ix$ teljesül $i=1,\ldots,n$, ahol $a_1,\ldots,a_n$ az A algebra egy bázisa F felett. Másfelől B egy

kommutativ féligegyszerű algebra, melynek minimális ideáljai $B_1,\ldots,B_k$ rendre az $A_1,\ldots,A_k$ ideálok centrumai. A B_i ideál ismeretében az A_i ideál könnyen megkapható, mivel fennáll az $A_i=B_iA$ összefüggés.

A komplexusszorzat pedig hatékonyan kiszámítható. Elegendő egy maximális lineárisan független elemrendszert kiválasztani a b_ja_r alakú szorzatok halmazából, ahol b_j és a_r függetlenül befutják B_i illetve A egy-egy bázisát.

További egyszerűsitést jelent ha feltételezzük, hogy F primtest. Ez megtehető, hiszen A nyilván véges dimenziós algebra az F test P primteste felett is, és a minimális ideálok (mint vektorterek P felett) mindkét esetben ugyanazok lesznek. Ha pedig az ideálokat mint F feletti altereket szeretnénk megkapni, akkor a P feletti bázisból kiválaszthatunk egy F feletti bázist.

A fejezet további részében tehát feltesszük, hogy A féligegyszerű kommutativ asszociativ algebra az F primtest felett.

3.2. Az általános módszer és a véges eset.

Ebben a részben bemutatjuk a módszer alapötletét, és elintézzük a véges esetet. Az itt leirt eredmények Friedl Katalintól származnak, ezért azokat csak olyan részletességgel tárgyaljuk, amennyire az a továbbiak szempontjából lényeges. Az olvasó részletes kifejtést találhat az (FR) dolgozatban.

A módszer gerincét egy iterációs eljárás képezi mely végigmegy A egy bázisán amig A-nak egy valódi direkt felbontását nem találja $A=I+J$ alakban, ahol I,J ideálok A-ban, vagy pedig bebizonyitja, hogy A test, vagyis direkt felbonthatatlan. Ezt a vágó eljárást azután használhatjuk az I és J ideálokra és igy tovább, amig A teljes felbontását meg nem kapjuk. Ez lehetséges, hiszen I és J ismét féligegyszerű kommutativ asszociativ algebrák F felett,

továbbá ideáljaik egyben A-nak is ideáljai. Itt már érzékelhető is egy különbség a véges és a végtelen eset között. A végtelen esetben fennáll annak a veszélye, hogy a vágó eljárás outputjaként keletkező ideálok mérete egyre növekszik. Ennek kezelésével a 3.3. részben foglalkozunk.

A vágó eljárás általános lépése a következőképpen működik: Kiindulunk az A algebra adott $a_1,\ldots,a_n$ bázisából. Az invariáns predikátum az, hogy F_i, az $a_1,\ldots,a_i$ elemek által generált részalgebra test (F_0:=F). Ha i=n akkor vége a munkának, hiszen ekkor A test. Különben tekintsük az a_{i+1} elem A-beli f minimálpolinomját az F_i test felett. Ha f irreducibilis F_i felett, akkor látjuk, hogy az első i+1 elem testet generál és a lépést befejeztük. Ha pedig f nem irreducibilis, akkor felirható f=gh alakban, ahol g és h nem állandó relativ prim polinomok. Utóbbi állitás azért igaz, mert A testek direkt összege. Ezek után az 1.1. Lemma szerint $I=Ag(a_{i+1})$ és $J=Ah(a_{i+1})$ választással A-nak egy valódi felbontása adódik.

Az eljárás során polinomokat kell faktorizálni az F test véges algebrai bővitései felett. A véges esetben erre a problémára nem ismeretes determinisztikus polinom idejű algoritmus. Berlekamp (B1) algoritmusának időigénye polinomiálisan függ ugyan a polinom fokától és az F test primtest feletti fokától, de F karakterisztikájától is. Másfelől a problémára létezik gyakorlatilag is jó polinom idejű Las Vegas módszer (Berlekamp (B2), Rabin (RA1)). Igaz tehát a

3.1. Tétel (Friedl, (FR)) A Wedderburn – Artin felbontás véges féligegyszerű algebrák esetén megtalálható egy polinom idejű Las Vegas algoritmussal. Ha az A algebra dimenziója az F=GF(q) test felett n, akkor az algoritmus várható futási ideje polinomiális n-ben és log(q)-ban.

Hasonlóan, a probléma megoldható determinisztikus algoritmussal is, melynek futási ideje polinomiális n-ben, m-ben és p-ben, ahol $q=p^m$.

3.3. A végtelen eset – előkészületek

Ebben a részben gyűjtöttük össze a méret probléma kezeléséhez használt algebrai jellegű állításokat. Alapvetően két célunk van. Először is a vágó algoritmusban fellépő közbülső testekben szeretnénk "kicsi" primitiv elemet találni. Ez azért fontos, mert a használt polinom faktorizáló módszerek (CG),(LA),(LE) a testet egy primitiv elemmel megadottnak tekintik, így annak mérete beleszámit az input méretébe. A másik problémáról már beszéltünk a 3.1. részben. Be fogjuk látni, hogy A minden ideáljának van "kicsi" bázisa. Ez lényegében azon fog múlni, hogy A idempotensei kicsik abban az értelemben, hogy polinomiális becslés adható az $a_1,\ldots,a_n$ bázisra vonatkozó koordinátáik méretére.
A következő lemma segitségével két test direkt összegében találhatunk kicsi nullosztókat.

3.2. Lemma Legyenek az F és L testek bővitései Q-nak. Tegyük fel, hogy az $a_1,\ldots,a_n$ illetve a $b_1,\ldots,b_n$ elemek lineárisan generálják F-et illetve L-et Q felett. Tegyük fel továbbá, hogy nincs olyan $h : F\to L$ test izomorfizmus, melyre $h(a_i)=b_i$ minden $i=1,\ldots,n$ esetén. Ekkor vannak olyan $c_1,\ldots,c_n$ egész számok melyekre $0\le c_i\le 2n$ és $\sum_{i=1}^{n} c_i a_i$ valamint $\sum_{i=1}^{n} c_i b_i$ Q feletti (F- illetve L-beli) minimálpolinomjai különbözőek.

Bizonyitás. Indirekt bizonyitunk. Ha az állitás nem igaz, akkor tetszőleges a fenti korlátoknak eleget tevő $c=(c_1,\ldots,c_n)$ vektor esetén van az F-nek olyan (a vektortól függő) h beágyazása L algebrai lezártjába, amelyik a $\sum_{i=1}^{n} c_i a_i$ elemet a $\sum_{i=1}^{n} c_i b_i$ elembe

viszi. Ebben az esetben azt mondjuk, hogy a $\underline{c}$ vektor a h beágyazáshoz tartozik. Válasszunk most egy olyan p primet, melyre $n<p\leq 2n$ teljesül és szoritkozzunk azokra a nemnegativ $\underline{c}$ vektorokra, melyeknek minden komponense kisebb mint p.

Ezen vektorok száma p^n. Mivel F foka Q felett legfeljebb n, ezért F-nek legfeljebb n beágyazása van L algebrai lezártjába. Másfelől minden vektor legalább egy beágyazáshoz tartozik, tehát van olyan h beágyazás amihez legalább $(1/n)p^n>(1/p)p^n=p^{n-1}$ vektor tartozik. Tekintsük most ezeket a vektorokat modulo p. Mivel a modulo p vett elem n-esek vektorterében egy valódi altér legfeljebb p^{n-1} elemet tartalmaz, ezek a vektorok nem lehetnek mind benne egy valódi altérben. Feltehető tehát hogy h a mod(p) független $\underline{c}^1,\ldots,\underline{c}^n$ vektorokhoz tartozik. Ezek a vektorok nyilván függetlenek Q felett is. A $\underline{c}^j:=(c_{j1},\ldots,c_{jn})$ jelöléssel élve kapjuk, hogy

$$h(\sum_{i=1}^{n} c_{ji}a_i)=\sum_{i=1}^{n} c_{ji}b_i \quad , \quad j=1,\ldots,n$$

amiből a $h(a_i)-b_i$ elemekre a következő lineáris egyenletrendszer adódik:

$$\sum_{i=1}^{n} c_{ji}(h(a_i)-b_i)=0 \quad , \quad j=1,\ldots,n.$$

Mivel ennek a rendszernek a mátrixa nem szinguláris, kapjuk, hogy $h(a_i)=b_i$ minden i=1,...,n esetén, ami ellentmondás. A bizonyitást befejeztük.

Legyen most A féligegyszerű kommutativ algebra Q felett, és jelölje K az A megadásának méretét (tehát a Q feletti struktúrakonstansok leirásának összhosszát). Mivel A az $A_1,\ldots,A_k$ (minimális) ideálok direkt összege, tetszőleges b elem az A-ból felirható egyértelműen

$$(3.1) \qquad b=b_1+\ldots+b_k \qquad b_i\in A_i$$

alakban. Igaz ez az a_i báziselemekre is:

$$a_i=a_{i1}+\ldots+a_{ik} \qquad a_{ij}\in A_j .$$

Világos, hogy rögzített j-re az a_{ij} elemek az A_j egy lineáris generátorrendszerét alkotják Q felett.

Legyenek $e_1,\ldots,e_k$ az A primitiv idempotensei (másképpen fogalmazva az $A_1,\ldots,A_k$ ideálok egységelemei). Fejezzük ki ezeket az elemeket az a_i elemek racionális lineáris kombinációjaként:

$$e_i=e_{i1}a_1+\ldots+e_{in}a_n$$

Ezekkel a jelölésekkel élve érvényes a következő

3.3. Lemma Az e_{ij} együtthatók mérete nem nagyobb mint $(nK)^c$ ahol c egy pozitív abszolút konstans.

Bizonyítás. Az általánosság korlátozása nélkül feltehető, hogy $i=1$. Először belátjuk, hogy tetszőleges r esetén ($r=2,\ldots,k$) van olyan r-től függő b eleme az A-nak, hogy b együtthatói az a_i bázisra nézve abszolút értékben kisebbek mint $2n+1$, és ha b-nek a (3.1) felírását nézzük, akkor b_1 A_1-beli és b_r A_r-beli Q feletti minimálpolinomjai különbözőek. Valóban, elegendő a 3.2. Lemmát használni az A_1 és A_r testekre és $a_{11},\ldots,a_{1n}$ valamint $a_{r1},\ldots,a_{rn}$ lineáris generátorrendszereikre. Mivel A_1 és A_r testek, b_1 és b_r minimálpolinomjai irreducibilisek Q felett. Mivel pedig ezek a polinomok különbözőek, adódik, hogy relatív primek is.

Ha most f jelöli b_r A_r-beli minimálpolinomját, akkor $f(b_1)$ nem nulla. Ebből az 1.2. Lemmát használva következik, hogy a $B_r=f(b)A$ ideál tartalmazza A_1-et, de nem tartalmazza A_r-et. Másfelől ismét az 1.2. Lemma szerint f osztója az $f_{b,A,Q}$ polinomnak (a b A-beli Q feletti minimálpolinomjának). Mivel b kicsi, $f_{b,A,Q}$ együtthatói polinomkorlátosak, amiből Mignotte (MIG) egy tétele szerint következik, hogy f együtthatóinak mérete is polinomkorlátos n-ben és K-ban. Ebből kifolyólag $f(b)$ együtthatóinak mérete is polinomkorlátos, tehát a B_r ideál is megadható kis koordinátájú

vektorokkal. Mivel A_1 nem más, mint a B_r ideálok metszete (és igy egy kezelhető méretű lineáris egyenletrendszerrel jellemezhető), kapjuk, hogy az A_1 ideálnak is létezik polinomiális méretű bázisa. Az e_1 az A_1 ideál egységeleme, ezért jellemezhető mint az $e_1c_i=c_i$ $i=1,\ldots,m$ lineáris egyenletrendszer egyetlen megoldása, ahol $c_1,\ldots,c_m$ az A_1 ideál egy kis méretű bázisa. Innen már következik a lemma állitása.

3.4. Következmény Az A algebra minden idempotensének a mérete polinomiális n-ben és K-ban.

Bizonyitás. Mivel minden idempotens előáll mint legfeljebb n primitiv idempotens összege, ez azonnal következik a 3.3. Lemmából.

Egy tetszőleges I ideál egy bázisát megkaphatjuk az I egységelemének e-nek az ismeretében úgy, hogy az ea_j $j=1,\ldots,n$ elemek közül kiválasztunk egy maximális lineárisan független rendszert. Egy ilyen bázist az I egy <u>standard bázisának</u> nevezünk.

3.5. Következmény Van olyan d pozitiv állandó, hogy A bármely ideáljának tetszőleges standard bázisa legfeljebb $(nK)^d$ méretű.

Bizonyitás. A 3.4. Következmény és a standard bázis definiciója alapján nyilvánvaló.

A következő állitás egy jól ismert testelméleti tény effektiv formája.

3.6. Lemma Legyen az F algebrai számtest, $\dim_{\mathbb{Q}}F=n$. Tegyük fel, hogy $b_1,\ldots,b_m$ egy (test-)generátorrendszere F-nek. Ekkor vannak olyan $c_1,\ldots,c_m$ egészek hogy $0\leq c_i\leq n^2$ és $F=\mathbb{Q}(\sum_{i=1}^{m} c_i b_i)$.

Bizonyitás. A primitiv elem létezését kimondó tétel szokásos bizonyitása (pl. Fuchs (FU)) szerint ha $\mathbb{Q}(a)$ és $\mathbb{Q}(b)$ k illetve k' fokú bővitései $\mathbb{Q}$-nak, akkor van olyan c egész, $0\leq c\leq kk'$, hogy $\mathbb{Q}(a,b)=\mathbb{Q}(a+cb)$.

Legyen $F_i=Q(b_1,\ldots,b_i)$. Használva, hogy F minden résztestének a foka legfeljebb n, az állitás F_i-re i szerinti teljes indukcióval bizonyitható.

3.4. A végtelen eset - algoritmusok

Először két segédeljárást irunk le. Az első ideálok egy standard bázisát számolja ki. A neve RED() és két input paramétere van. Az egyik egy algebra A, a másik egy A-beli ideál I, $c_1,\ldots,c_m$ bázisával megadva. Outputként I egy standard bázisát adja.

procedure RED(A,I)

begin

1. Számoljuk ki az I ideál e egységelemét az $ec_i=c_i$ $i=1,\ldots,m$ lineáris egyenletrendszer megoldásával.
2. Válasszunk ki egy maximális lineárisan független rendszert az ea_i elemek közül, legyenek ezek $d_1,\ldots,d_m$.
3. **return**$(d_1,\ldots,d_m)$.

end procedure

A RED() eljárásra igaz a következő

3.7. Lemma Tegyük fel hogy az I ideál megadásának mérete (a c_j elemek a_i bázisbeli felirásának összmérete) N. Ekkor van olyan egészegyütthatós p(x,y) polinom, hogy RED(I) futási ideje polinomiális az n, N és K paraméterekben, és az eredményként adódó bázis mérete legfeljebb p(n,K).

Bizonyitás. Az 1. lépéshez szükséges idő polinomiális az n, N és K paraméterekben. A 3.4. Következmény szerint az e idempotens mérete és igy a 2. lépés bonyolultsága polinomiális n-ben és K-ban. Utóbbi miatt a végeredmény mérete is polinomiális n-ben és K-ban. A bizonyitást befejeztük.

A következő eljárás PRIMELEM() az A algebra egy két elemmel generált résztestéből keres egy kis primitiv elemet. A bemenő paraméterei egy algebra A, továbbá annak két eleme a és b , melyekre Q(a,b) test. Outputként egy olyan a+cb alakú elemet ad, melyre Q(a,b)=Q(a+cb) és $0 \leq c \leq n^2$.

procedure PRIMELEM(A,a,b)

begin

Számitsuk ki minden $0 \leq c \leq n^2$ esetén az a+cb elem $f_{a+cb,A,Q}$ minimálpolinomját és legyen c_0 egy olyan érték melyre a minimálpolinom foka maximális. **return**($a+c_0 b$).

end procedure

Az, hogy az eljárás korrekt és tényleg kis primitiv elemet produkál, a 3.6. Lemma következménye.

Ezek után megszerkeszthetjük a vágó eljárást. A VAG() eljárás bemenő paraméterei az A algebra és annak egy I ideálja a $b_1,\ldots,b_m$ báziselemeivel megadva. Az eljárás vagy bebizonyitja hogy I test (találva egy olyan b elemet melyre I=Q(b) és b minimálpolinomja irreducibilis Q felett), vagy felbontja I-t két valódi ideáljának direkt összegére. A második esetben a kapott ideálokat egy-egy standard bázisukkal adja meg.

procedure VAG(A,I)

begin

primelem:=e. (Itt e az I ideál egységeleme.)

for i:=1 **to** m **do begin**

1. Számitsuk ki f-et a b_i minimálpolinomját a Q(primelem) test felett. (Itt I-beli minimálpolinomról van szó, vagyis az egységelem szerepét e játssza.)

2. Bontsuk f-et irreducibilis tényezőkre a Q(primelem) test felett.

3. **if** f=gh egy nemtriviális felbontás **then** **return**(RED(A,Ag(b_i)),RED(A,Ah(b_i))) **else**

primelem:=PRIMELEM(I,primelem,b_i).

end for

4. **return**("I egy test").

end procedure

3.8. Tétel A VAG() eljárás helyes. Továbbá ha I reprezentációjának a mérete N, akkor az eljárás futási ideje polinomiális az n, K és N paraméterekben.

Bizonyítás. Először megjegyezzük, hogy Q(primelem) mindig egy test, és I algebra ezen test felett. Ha tehát a 4. lépésnél állunk meg, akkor I test. Ha a 3. lépésnél állunk meg, akkor az 1.1. és 1.2. Lemmát alkalmazva az I algebrára adódik, hogy tényleg egy valódi felbontást kapunk.

Ami a bonyolultságot illeti, m legfeljebb n, tehát elég látni, hogy minden iterációs lépés bonyolultsága polinomiális, továbbá hogy primelem mérete polinomiális korlát alatt marad. Utóbbi állítás világos a 3.6. Lemma szerint, hiszen PRIMELEM() az ottani kikötésekenek eleget tevő $\sum c_j b_j$ alakú elemet produkál.

Az 1. lépés egy elem minimálpolinomjának a kiszámitása, tehát polinomiális bonyolultságú, a 3. lépés pedig a 3.7. Lemma szerint polinom időben elvégezhető. Végül a 2. lépés elintézhető azzal, hogy az (LLL), (CG), (LA), (LE) dolgozatokban megadott módszerek polinomiális bonyolultságúak. A bizonyitást befejeztük.

Ezek után a Wedderburn – Artin felbontás problémája Q feletti kommutativ féligegyszerű algebrákra könnyen megoldható. Kiindulunk az A algebrából és a VAG() eljárás ismételt

alkalmazásával addig bontjuk, amig a keletkező ideálok mindegyike test lesz. Igy megkapjuk az algebra összes minimális ideálját. Mivel a minimális ideálok száma legfeljebb n, és a VAG() eljárás minden egyes hivása vagy finomitja A megelőző direkt felbontását, vagy bebizonyitja hogy egy ideál minimális, a szükséges hivások száma legfeljebb 2n-1. A 3.5. Következmény szerint bármely híváshoz tartozó input mérete legfeljebb $(nK)^d$, ezért a 3.8. Tétel szerint a teljes felbontás megkapható polinom időben. A 3.1. részben leirt redukciót figyelembe véve a Wedderburn - Artin felbontás problémáját megoldottuk nem feltétlenül kommutativ algebrák esetére is:

3.9. Tétel Legyen A féligegyszerű algebra Q felett, $\dim_Q A=n$. Tegyük fel hogy A megadásának mérete K. Ekkor az A algebra minimális ideáljai megtalálhatók egy n-ben és K-ban polinomiális futási idejű algoritmussal.

4. NULLOSZTÓK VÉGES ALGEBRÁKBAN

A 3. fejezetben a Wedderburn - Artin felbontás megkeresésével foglalkoztunk. A VAG() eljárás tulajdonképpen kommutativ féligegyszerű algebrában keresett nullosztókat. Vagy talált egy nullosztópárt, vagy bebizonyította, hogy a kérdéses algebra test, tehát nullosztómentes. A következőkben szeretnénk ezt a problémát általánosabban vizsgálni. A szokásos módon adott egy A algebra az F test felett és szeretnénk egy nullosztópárt találni benne, ha A egyáltalán tartalmaz nullosztókat. Ezt a feladatot a továbbiakban nullosztó problémának fogjuk nevezni. A 2. fejezet eredményei szerint ez könnyű, ha Rad(A)>(0), hiszen bármely nem nulla radikálelem nullosztó. Ha A féligegyszerű, de nem egyszerű, akkor a 3.1. és 3.9 Tételek szerint a nullosztók keresésének a problémája legfeljebb olyan nehéz mint a polinomok faktorizációja a kérdéses test felett. Másfelől az $f(x) \in F[x]$ felbontása F felett lényegében ugyanaz mint nullosztót találni az F[x]/(f) algebrában. Ez mutatja, hogy a nullosztó probléma legalább olyan nehéz mint a polinomok faktorizációja a szóbanforgó test felett. Elmondhatjuk tehát, hogy a 2. és 3. fejezet eredményei kielégitő megoldást adnak a problémára, ha A nem egyszerű.

A fennmaradó esetben A egyszerű algebra, vagyis izomorf egy $M_k(L)$ alakú algebrával, ahol L egy az F-et a centrumában tartalmazó nem feltétlenül kommutativ test. Világos, hogy A pontosan akkor nullosztómentes, ha k=1.

Ebben a fejezetben feltesszük hogy F (és igy A is) véges. Ez

tovább egyszerűsiti a képet, hiszen Wedderburn tétele szerint L szükségképpen kommutativ. L könnyen meg is kapható, hiszen nem más, mint az A algebra centruma. Kiszámolva A-nak az L feletti dimenzióját, megkaphatjuk k értékét is. Feltesszük tehát, hogy A centruma F (F helyett L felett dolgozunk).

A 3.1. Tétel két különböző algoritmussal foglalkozik. Ezek azonban csak annyiban térnek el egymástól, hogy különböző eljárásokat alkalmaznak polinomok faktorizációjára. Hogy ezt a kettősséget kényelmesen kezelhessük, bevezetjük az f-algoritmus fogalmát. Olyan módszert nevezünk f-algoritmusnak, amely egy a véges testek feletti polinomok faktorizálására alkalmas orákulumot (eljárást) hivhat. Egy ilyen hivás költségén a hivás inputjának a hosszát (tehát a test és a felbontandó polinom leirásának összhosszát) értjük.

A fejezet fő eredménye egy polinom idejű f-algoritmus a nullosztó problémára véges egyszerű (és igy a 3.1. Tételt is figyelembe véve tetszőleges véges) algebrák esetén. A fejezetben közölt eredmények az (R) dolgozatból valók.

A módszer alapötlete Wedderburn egy tételének (miszerint minden véges nullosztómentes algebra kommutativ test) egy majdnem konstruktiv bizonyitásából (Herstein (H), 3.1.1 Tétel) ered. Ez a bizonyitás indirekt feltevéssel élve kiindul egy véges ferdetestből, amelyben végül kimutatja nullosztó létezését. A gondolatmenetet adaptáljuk teljes mátrixalgebrákra úgy, hogy a tisztán egzisztenciális lépéseket konstrukciókkal helyettesitjük.

A következő két fejezetben p egy primszám, $q=p^r$, $F=GF(q)$.

4.1. Nullosztók az $M_n(F)$ algebrában.

Ebben a részben a módszerünk algebrai alapját jelentő állitások

szerepelnek. Legyen a egy olyan eleme $M_n(F)$-nek, amely nincs benne F-ben és amelyre L=F(a) test. Legyen az L foka F felett l. Az utóbbi két kikötés azt jelenti, hogy az a elem F feletti $M_n(F)$-beli minimálpolinomja irreducibilis F felett és a foka l.

4.1. Lemma A fenti feltételek mellett van olyan $c \in M_n(F)$ hogy

(i) $c^{-1}ac=a^q$

(ii) Ha Alg(a,c) jelöli az a és a c által generált F-algebrát, akkor Alg(a,c) nem kommutatív.

(iii) $Alg(a,c)=L+cL+\ldots+c^{n_i}L+\ldots$, ahol + F-alterek nem feltétlenül direkt összegét jelöli.

Bizonyitás. Mivel L egyszerű részalgebra M_n-ben és L-nek az automorfizmusa mely a-t a^q-ba viszi elemenként fixen hagyja F-et, a Noether Skolem tétel (lásd pl. Herstein (H)) szerint ez az automorfizmus belső. Legyen c tetszőleges olyan elem, amely ezt az automorfizmust indukálja. Erre (i) definició szerint teljesül. Mivel a nincs benne az F testben , az a és a^q elemek különbözőek, tehát (i) alapján a és c nem felcserélhetők, ami bizonyitja az (ii) állitást. Az utolsó állitás azonnal következik az $ac=ca^q$ egyenlőségből.

A következő állitás a probléma jelentős egyszerűsitését teszi lehetővé. Legyen c tetszőleges, az előző lemma állitásainak eleget tevő elem.

4.2. Lemma Ha $Alg(a,c)=M_n(F)$ akkor l=n , $c^n \in F$ és

(4.1) $Alg(a,c)=L+cL+\ldots+c^{n-1}L.$

A fenti összeg direkt összeg, továbbá $\dim_F F(c)=n$.

Bizonyitás. Egyszerű számolással adódik, hogy tetszőleges nemnegativ egész i-re $c^{-i}ac^i=a^{q^i}$. Ebből következik, hogy $ac^l=c^la$, tehát ha $Alg(a,c)=M_n(F)$ akkor c^l benne van F-ben. A c elem tehát eleget tesz egy l-edfokú polinomnak F felett, ezért

érvényes az

$$Alg(a,c)=L+cL+\ldots+c^{l-1}L$$

összefüggés, az előző lemmát is figyelembe véve. Ebből a felirásból látható, hogy $\dim_F Alg(a,c)\leq l^2$ és egyenlőség pontosan akkor van, ha az összeg direkt összeg. Mivel l az a elem F feletti minimálpolinomjának a foka, $l\leq n$ is teljesül. Tudva másfelől, hogy Alg(a,c) dimenziója n^2, kapjuk, hogy n=l és az összeg direkt összeg. Ha c eleget tenne egy n-nél alacsonyabb fokú F feletti polinomnak, akkor Alg(a,c)-re egy a (4.1)-nél rövidebb előállitást kapnánk, ami a dimenziókat összeszámolva ellentmondást ad. A bizonyitást befejeztük.

Tovább foglalkozunk az $Alg(a,c)=M_n(F)$ esettel. Kiderült, hogy c eleget tesz ekkor egy x^n-e alakú polinomnak valamely F-beli e elemre. Azt is tudjuk, hogy a fenti polinom a c minimálpolinomja F felett.

Az L test egy d elemének a normáján a $norm(d):=dd^qd^{q^2}\ldots d^{q^{n-1}}$ elemet értjük (itt valójában az L/F relativ normáról van szó). A következő lemma igen fontos szerepet játszik a Wedderburn tétel idézett bizonyitásában.

4.3. Lemma Legyen d az L testnek egy olyan eleme, amelyre norm(d)=1/e teljesül. Ekkor 1-cd nullosztó az $Alg(a,c)=M_n(F)$ algebrában.

Bizonyitás. Definiáljuk az Alg(a,c) algebra z elemét a következőképpen

$$z:=1+cd+c^2dd^q+\ldots+c^{n-1}dd^q\ldots d^{q^{n-2}}.$$

Használva, hogy $dc=cd^q$, egyszerű számolással adódik, hogy

$$z(1-cd)=1-c^n norm(d)=0.$$

Mivel pedig (4.1) direkt felbontás, a fenti elemek egyike sem nulla, amivel az állitást igazoltuk.

A fenti norma egyenletet általában nem tudjuk hatékonyan megoldani a norma definíciójában szereplő polinom túl magas foka miatt. Ezért egy további kikötést teszünk c-re.

4.4. Lemma Tegyük fel, hogy $Alg(a,c)=M_n(F)$ mint előbb, és tegyük még fel, hogy c minimálpolinomja x^n-e irreducibilis F felett. Ekkor a $g(x)=x^n-(1/e)$ polinom szintén irreducibilis az F test felett. A g polinom lineáris tényezőkre bomlik az L testben és ha n páratlan, akkor tetszőlges olyan $d \in L$ esetén melyre $g(d)=0$, teljesül a $norm(d)=1/e$ összefüggés is.

Bizonyítás. Az x^n-e polinom irreducibilitása egyenértékű azzal, hogy F(c) test, mégpedig n-edfokú bővítése F-nek. Másfelől világos, hogy ekkor F(c)=F(1/c), tehát 1/c minimálpolinomja is n-edfokú irreducibilis. Mivel g olyan n-edfokú polinom, melynek 1/c gyöke, adódik, hogy g az 1/c elem minimálpolinomja, tehát irreducibilis az F test felett. A g polinom lineáris tényezőkre bomlik az F(c) testben. L és F(c) fokát összevetve kapjuk, hogy ez a két test izomorf, tehát g lineáris tényezőkre bomlik L-ben is. Ha most d tetszőleges gyöke g-nek L-ben és n páratlan, akkor g irreducibilitása miatt g konstans tagjára

$$-(1/e)=(-1)^n norm(d)=-norm(d)$$

adódik, bizonyítva utolsó állításunkat.

4.2. Norma egyenletek megoldása

Ebben a részben bizonyos, a 4.3. Lemma alkalmazásához szükséges norma egyenletek megoldásával foglalkozunk. Pontosabban, tegyük fel hogy n=2, vagy n páratlan, legyen az L test n dimenziós bővítése F-nek ($F=GF(q)$, $q=p^r$, p prím) és legyen továbbá $g(x)=x^n-b$ $b \in F$ az F test felett irreducibilis polinom. Egy olyan $d \in L$ elemet szeretnénk találni, melyre $norm(d)=b$.

A fenti problémára megadunk egy polinom idejű f-algoritmust. A 4.4. Lemmában alkalmazott gondolatmenet szerint ezt páratlan n esetére már elintéztük, hiszen elegendő g-nek egy gyökét találni L-ben, amit megtehetünk egy polinom idejű f-algoritmussal. Ezek után feltehetjük, hogy n=2. Két esetet különböztetünk meg.

1. eset. -b (kvadratikus) nemmaradék F-ben. Ha d egy gyöke az x^2+b polinomnak, akkor a másik gyök d^q, tehát az előbbi polinom konstans tagját kiszámolva $d^{q+1}=norm(d)=b$ adódik. Ismét elég egy kis fokú polinomot felbontani (mely tényleg felbomlik L-ben).

2. eset. -b kvadratikus maradék F-ben. Legyen u olyan eleme F-nek, melyre $u^2=-b$. Tegyük fel, hogy tudunk találni egy olyan v elemét az L testnek, melyre $norm(v)=v^{q+1}=-1$. Ekkor a d=uv elem jó lesz, hiszen $norm(d)=u^2v^{q+1}=b$. Elég tehát a norm(v)=-1 egyenlettel foglalkozni. Megjegyezzük, hogy esetünkben -1 nemmaradék F-ben, hiszen -b kvadratikus maradék és b pedig nemmaradék. Úgy is fogalmazhatunk, hogy -1 az egyetlen 2-hatvány rendű nemmaradék F-ben. Elég tehát olyan v elemet keresni, melynek rendje 2-hatvány, és amelyre norm(v) nemmaradék F-ben. Ebből a célból definiáljuk L elemeinek a következő sorozatát: Legyen $z_1=-1$. Ha z_i már definiált, akkor legyen z_{i+1} tetszőleges olyan eleme az L testnek, melyre $z_{i+1}^2=z_i$, feltéve hogy ilyen elem létezik. Legyen z_k a sorozat utolsó eleme. Világos, hogy z_k kvadratikus nemmaradék L-ben és hogy z_k egy 2^k rendű multiplikativ részcsoportot generál. Innen következik egyfelől, hogy k legfeljebb $2\log_2 q$, tehát egy ilyen sorozat legfeljebb $2\log_2 q$ másodfokú egyenlet megoldásával megtalálható. Másfelől $v=z_k$ jó választás, hiszen ha $norm(v)=z_k^{q+1}$ kvadratikus maradék volna F-ben, akkor $z_k^{(1/2)(q+1)(q-1)}=1$ teljesülne, ami lehetetlen, hiszen z_k nemmaradék L-ben.

Beláttuk a következőt:

4.5. Lemma A 4.2. rész elején megadott tipusú norma egyenletek megoldhatók egy f-algoritmussal, melynek futási ideje polinomiális az n, r és log(p) paraméterekben.

4.3. Algoritmusok

Először a CUT() segédeljárást ismertetjük. Ennek egyetlen bemenő paramétere A, egy véges egyszerű algebra a centruma, az F test felett. A tehát nem más, mint $M_n(F)$ alkalmas n-re. A CUT() eljárás vagy konstatálja, hogy A test, vagy talál egy nullosztópárt A-ban, vagy talál egy (két elemmel genrálható) valódi nem kommutativ részálgebrát A-ban. Az eljárás, mint f-algoritmus az n és log(q) paraméterekben (tehát az input hosszában) polinomiális időben terminál.

procedure CUT(A)

begin

1. Válasszunk egy tetszőleges $b \in A$ elemet, ami nincs F-ben. Számitsuk ki a b elem $f:=f_{b,A,F}$ minimálpolinomját. Ha f reducibilis F felett, akkor bontsuk fel nemtriviális módon f=gh alakban, **return**(g(b),h(b)).

2. (Ezen a ponton tudjuk hogy F(b) test.)
Keressünk egy olyan $a \in F(b)$ elemet, melyre L=F(a) foka F felett vagy 2 vagy páratlan szám. Ha F(b) foka páros, akkor az $u^{q^2}=u$ egyenlet bármely olyan F(b)-beli megoldása jó, mely nincs benne F-ben. A fenti egyenlet egy F feletti lineáris egyenletrendszerrel egyenértékű, melynek a megoldáshalmaza az F másodfokú bővitése. A megoldás bázisának valamelyik eleme biztosan jó az a elem szerepére.

3. Keressünk egy olyan nem nulla c elemet, melyre $ac=ca^q$ (ilyen a 4.1. Lemma szerint létezik és egy liniáris egyenletrendszer

megoldásával található). Számitsuk ki c minimálpolinomját az F test felett. Ha ez reducibilis, akkor az 1. lépéshez hasonlóan nullosztópárt találunk és befejezzük a munkát.

4. (A c elem invertálható eleme A-nak és $c^{-1}ac=a^q$.)

Számitsuk ki Alg(a,c), az a és c elemek által generált részalgebra egy bázisát. Ha Alg(a,c) valódi részalgebra, akkor **return**(Alg(a,c)).

5. (Itt Alg(a,c)=A=$M_n(F)$, n vagy 2 vagy páratlan, a c minimálpolinomja F felett x^n-e alakú az F felett irreducibilis polinom valamely e$\in$F-re.)

A 4.2. részben leirt módszerrel keressünk egy olyan d elemet L-ben, melyre norm(d)=1/e. Legyen ezután z az A algebra tetszőleges olyan nem nulla eleme melyre z(1-cd)=0. **return**(z,1-cd).

end procedure

4.6. Tétel A CUT() eljárás korrekt és a futási ideje, mint f-algoritmusé, polinomiális az n és log(q) paraméterekben.

Bizonyitás. Ha az 1. illetve a 3. lépésben végzünk, akkor világos hogy egy nullosztópárt kaptunk. Ha a 4. lépésben fejezzük be a munkát akkor, A-nak egy valódi nem kommutativ részalgebráját kapjuk a 4.1 Lemmát is figyelembe véve. Az 5. lépést megelőző zárójelbe tett állitások a 4.2. Lemma, az azt követő megjegyzés és c minimálpolinomjának irreducibilitása alapján valóban teljesülnek és igy a 4.3. Lemma alkalmazható. Az 1-cd elem valóban nullosztó, például a 4.3. Lemmában megadott z elem választható párjának.

Ami a módszer időigényét illeti, az állitás a 4.4. Lemmát figyelembe véve világos.

Ezután már könnyen megadhatunk egy olyan módszert mely tetszőleges véges algebrára megoldja a nullosztó problémát. A

NULLOSZTÓ() eljárásnak egyetlen paramétere van, ami egy véges asszociativ algebra. Az eljárás vagy megállapitja hogy A test, és ekkor nullosztómentes, vagy egy nullosztópárt talál.

procedure NULLOSZTÓ(A)

begin

1. Számoljuk ki a Rad(A) ideált a 2. fejezet módszerével. Ha Rad(A)>(0), akkor legyen x∈Rad(A) egy tetszőleges nem 0 elem, és legyen y az x-nek egy olyan nem 0 hatványa melyre xy=0. **return**(x,y).

2. (Itt A féligegyszerű.)

A 3. fejezet módszerével keressük meg az A Wedderburn - Artin felbontását. Ha A nem egyszerű, mondjuk A=I+J ahol I és J két valódi ideál, melyekre IJ=(0), akkor legyen x és y az I illetve J egy-egy nem nulla eleme, **return**(x,y).

3. (A egyszerű.)

Ha A kommutativ, akkor **return**("A egy test").

4. ($A=M_n(L)$, n>1, ahol L egy az A algebra F alaptestét tartalmazó véges test.)

Hivjuk a CUT() eljárást. A paraméter legyen A mint egy L-algebra. Ha a hivás egy x, y nullosztópárt adott, akkor **return**(x,y), különben egy Alg(a,c) alakú valódi részalgebrát kaptunk. Legyen A:=Alg(a,c) és menjünk vissza az 1. lépéshez.

end procedure

4.7. Tétel Legyen A m dimenziós algebra az F test felett. A fenti NULLOSZTÓ() eljárás talál egy A-beli nullosztópárt, ha A tartalmaz egyáltalán nullosztókat. A módszernek mint f-algoritmusnak a futási ideje polinomiális az m és log(q) paraméterekben.

Bizonyitás. Először megjegyezzük, hogy lényegében egy iterációról

van szó. A vizsgált algebra dimenziója csökken, tehát legfeljebb m az iterációs lépések száma. Ha CUT() egy kisebb algebrával tér vissza, akkor ez szükségképpen nem kommutativ, tehát Wedderburn tétele szerint tartalmaz nullosztókat és igy elég ezzel a részalgebrával foglalkozni. Az annotáció helyessége következik a Wedderburn – Artin struktúratételből, speciálisan CUT() hivása korrektül történik.

Az 1. és 2. lépések időigénye a 2.9. illetve a 3.1. Tételek szerint polinomiális az input méretében. A 3. lépés egy polinomiális méretü lineáris egyenletrendszer megoldását jelenti, mig a 4. lépésre a 4.6. Tétel ad polinomiális korlátot. A bizonyitást befejeztük.

Ha most a polinom faktorizáló fekete dobozunkat a determinisztikus, illetve a Las Vegas módszerrel helyettesitjük, akkor a 4.7. Tétel jelöléseivel élve kimondható a következő:

4.8. Következmény Véges algebrák esetén a nullosztó probléma megoldható determinisztikus algoritmussal, melynek futási ideje polinomiális az m, p és r paraméterekben.

Hasonlóan, a problémára létezik olyan Las Vegas módszer melynek várható futási ideje polinomiális az m és log(q) paraméterekben.

5. A NULLOSZTÓ ALGORITMUS ALKALMAZÁSAI

Ebben fejezetben továbbra is véges test feletti problémákkal foglalkozunk. Az előző fejezet jelöléseivel összhangban p egy prím, $q=p^r$ és $F=GF(q)$. A nullosztó kereső módszert fogjuk használni néhány algoritmikus probléma megoldására. Ezek a következők:

1. Mátrix algebrák explicit izomorfizmusa. A 3.1. Tétel szerint egy az F test feletti A algebráról polinom idejű f-algoritmussal el tudjuk dönteni, hogy izomorf-e egy teljes mátrixalgebrával. Igenlő válasz esetén, mondjuk ha A izomorf az $M_n(L)$ algebrával, akkor mind az n számot mind pedig az L testet meg tudjuk határozni. Célunk itt az, hogy explicite megadjunk egy ilyen izomorfizmust: konstruáljunk egy leképezését A-nak az L feletti n-szer n-es mátrixok algebrájára.
A problémára adott módszerünk segítségével egy igen fontos rokon problémát is kezelni tudunk. Tetszőleges A féligegyszerű F-algebrát fel tudunk hatékonyan bontani minimális balideálok direkt összegére.

2. Közös invariáns altér keresése. Adottak az $X_1,\ldots,X_k \in M_n(F)$ mátrixok, keressünk egy olyan U valódi alteret (az n hosszú F feletti oszlopvektorok vektorterében) melyre $X_jU\leq U$ teljesül minden $j=1,\ldots,k$ esetén. Erre a problémára is adunk egy polinom idejű f-algoritmust.

3. Minimális normálosztó keresése permutációcsoportok elemi Abel faktoraiban. Néhány a permutációcsoportokkal kapcsolatos

algoritmikus probléma visszavezethető invariáns altér keresésének problémájára kis véges testek felett. A következő probléma W.M. Kantortól (KN) származik. Legyen G egy n-edfokú permutációcsoport és K<H normálosztói G-nek úgy, hogy H/K egy elemi Abel p-csoport valamely p primre. A G, K, H permutációcsoportok egy-egy erős generátorrendszerrel (Luks (LU)) vannak megadva. Keressünk minimális a K<L≤H feltételnek elegettevő G-beli normálosztót. Erre a problémára n-ben polinomiális bonyolultságú algoritmust adunk.

5.1. Mátrix algebrák explicit izomorfizmusa

Tegyük fel, hogy adott az F test feletti A algebra mely izomorf az $M_n(F)$ algebrával. Szeretnénk egy explicit izomorfiát konstruálni a két algebra között.

Elegendő egy olyan V vektorteret találni, melyre $\dim_F V=n$ és A nemtriviálisan hat V-n, mint lineáris transzformációk egy algebrája. Valóban, ekkor a dimenziókat összehasonlítva adódik, hogy A képe ennél a reprezentációnál (ami izomorf A-val, hiszen A egyszerű) kiadja V összes lineáris transzformációját. Ezek után rögzítünk egy bázist V-ben és felírjuk A egy generátorrendszere elemeinek a mátrixát erre a bázisra vonatkozóan és készen vagyunk. A fentieknek eleget tevő V vektorteret kaphatunk, ha találunk egy e 1-rangú idempotens elemet A-ban (az 5.1. Lemma szerint ez rang független az aktuális $A\to M_n(F)$ izomorfizmustól). Valóban, ekkor $V:=M_n(F)e$ választással élhetünk. Jól ismert, hogy ekkor $\dim_F V=n$ és az $M_n(F)$ elemeivel balról szorzás egy nem triviális reprezentációt definiál.

Szükségünk lesz a következő egyszerű lemmára.

5.1. Lemma Ha e egy m rangú idempotens $M_n(F)$-ben akkor az $eM_n(F)e$ algebra izomorf az $M_m(F)$ algebrával.

A bizonyitás lineáris algebrai rutinmunka, ezért mellőzzük.

Az IDEMPOTENS() eljárás egyetlen bemenő paramétere egy az F test feletti egyszerű algebra A, melynek a centruma F (vagyis A centrális egyszerű algebra F felett). Az eljárás outputja egy 1 rangú idempotens A-ból.

procedure IDEMPOTENS(A)

begin

0. Legyen B:=A.

1. Hivjuk meg NULLOSZTÓ(B)-t. Ha B nem tartalmaz **nullosztót**, akkor **return**(1_B), ahol 1_B a B egységeleme.

2. (B tartalmaz nullosztókat.)

Legyen x egy az előző hivás által visszadott nullosztója B-nek. Határozzuk meg a Bx balideál e jobboldali egységelemét (a kézenfekvően adódó lineáris egyenletrendszer megoldásával).

3. (B=$M_m(F)$ valamilyen m>1 esetén és e egy szinguláris idempotens.)

Legyen B:=eBe és menjünk vissza az első lépéshez.

end procedure

Ha A izomorf $M_n(F)$-fel, akkor a 3. lépés utáni új algebra az 5.1. Lemma szerint izomorf $M_k(F)$-fel, és k<n. Ezt a gondolatmenetet ismételve adódik, hogy B aktuális értéke mindig egy F feletti teljes mátrixalgebrával izomorf. Az is látszik, hogy az iterációk száma legfeljebb n. Tegyük fel, hogy a 2. lépést összesen t-szer hajtjuk végre és legyen először t>0. A kapott idempotensek legyenek rendre $e_1,\ldots,e_t$. Használva hogy $e_j e_i = e_i e_j = e_j$ ha i<j, adódik, hogy B legutolsó értéke izomorf az $e_t A e_t$ algebrával. Mivel ez az algebra test, e_t szükségképpen 1 rangú idempotens az 5.1. Lemma szerint. Az e_t elem a B test

egységeleme, tehát az eljárás tényleg egy a kívánt tulajdonságú elemet produkál. Ha t=0, akkor nyilván n=1, tehát módszerünk ekkor is helyes eredményt ad.

Ami a futási időt illeti, a 4.7. Tétel szerint az 1. lépésbeli hívás költsége polinomiális az n és log(q) paraméterekben. A további lépésekben végzendő munka időigénye szintén polinomiális a fenti paraméterekben. A 2. illetve 3. lépésekben nincs is szükség polinom felbontásra. Kimondható tehát a következő

5.2. Tétel Legyen az F test feletti A algebra izomorf az $M_n(F)$ algebrával. Ekkor egy explicit izomorfizmus megadható a két algebra között egy f-algoritmussal, melynek futási ideje polinomiális az n és log(q) paraméterekben.

Bizonyítás. A fentiek alapján polinom időben találhatunk egy e 1 rangú idempotens elemet A-ban. Ezután az 5.1. rész elején vázolt módon (a faktorizáló orákulum hívása nélkül) kaphatunk egy izomorfizmust. Az utóbbi lépés szintén polinom időben elvégezhető (lineáris algebrai) teendőket jelent.

Egy explicit izomorfizmus azért hasznos, mert $M_n(F)$ szokásos megadása (mint n-szer n-es mátrixok algebrája) igen jól kezelhető. Például könnyen felbontható minimális balideálok direkt összegére. Jelölje ugyanis e_{ii} , i=1,...,n azt a mátrixot, melyben az i-edik diagonális elem 1, az összes többi 0. Az $M_n(F)$ algebra felbomlik minimális balideálok összegére az alábbi módon:

$$M_n(F)=M_n(F)e_{11}+\ldots+M_n(F)e_{nn}.$$

Ha most van egy explicit izomorfizmusunk az A algebra és $M_n(F)$ között, akkor az e_{ii} elemek képeivel A-nak egy felbontását kaphatjuk minimális balideálok direkt összegére.

A fenti módszer általánositható tetszőleges véges féligegyszerű A algebrára. A 3.1. Tétel szerinti módszerrel A felbontható

minimális ideálok direkt összegére. Az igy adódó A_i egyszerű algebrákat a fenti módszerrel tovább bonthatjuk, és végül A-nak egy felbontását nyerjük minimális balideálok direkt összegére.

5.3. Következmény. Legyen A féligegyszerű m dimenziós algebra az F test felett. A felbontható minimális balideálok direkt összegére egy f-algoritmussal, melynek futási ideje polinomiális m-ben és log(q)-ban.

5.2. Közös invariáns alterek.

Legyenek $X_1,\ldots,X_k \in M_n(F)$ és tekintsük a hatásukat az n hosszú F feletti oszlopvektorok V vektorterén. Szeretnénk eldönteni, hogy van-e olyan U nemtriviális (tehát V-től és (0)-től különböző) altere V-nek, melyre $X_i U \leq U$ minden i=1,...,k mellett. Abban az esetben, ha a válasz igenlő, egy ilyen U alteret is szeretnénk találni. Ezt a feladatot oldja meg az INVARIANS() eljárás, melynek egyetlen bemenő paramétere egy S - nem csupán a zérusmátrixból álló nem üres - mátrixhalmaz. Az outputja vagy egy nemtriviális invariáns altér, vagy egy üzenet miszerint nincs ilyen tulajdonságú altér.

procedure INVARIANS(S)

($S=\{X_1,\ldots,X_k\}$.)

begin

1. Számoljuk ki az S által generált A mátrixalgebrát, vagyis annak egy F feletti bázisát .

(Az S és az A mátrixhalmazoknak ugyanazok az invariáns alterei.)

2. Ha AV<V akkor **return**(AV).

3. Számoljuk ki Rad(A)-t. Ha Rad(A)>(0), akkor **return**(Rad(A)V).

4. (Itt A féligegyszerű és V unitér A modulus.)

Bontsuk fel A-t minimális balideálok direkt összegére:

$A=L_1+\ldots+L_m$.

Legyen v egy tetszőleges nem nulla vektor V-ből és tekintsük az $L_1v,\ldots,L_mv$ altereket. Legyen U ezek közül egy tetszőleges (0)-tól különböző. Ha U=V akkor **return**("nincs nemtriviális invariáns altér"), különben **return**(U).

end procedure

Vegyük először szemügyre az INVARIANS() eljárás helyességét. Nyilvánvaló, hogy S-nek és A-nak ugyanazok az invaráns alterei. Ha a 2. lépésnél végzünk, akkor egy nemtriviális invariáns alteret kaptunk, hiszen AV>(0). Ha a 3. lépésnél terminálunk, akkor egyfelől világos, hogy Rad(A)V egy A-invariáns altér. Másfelől ez (0)-tól különböző, hiszen $M_n(F)$ hűen hat V-n. Mivel Rad(A) nilpotens algebra, a Rad(A)V=V egyenlőség lehetetlen, tehát ekkor tényleg egy valódi invariáns altér adódik.

Ha a 4. lépésnél vagyunk, akkor A valóban féligegyszerű, tehát felbontható minimális balideálok direkt összegére. Mivel pedig az 1. lépés tesztjét túléltük, A hatása unitér, vagyis A egységeleme az egységmátrix. Ebből már következik, hogy az L_iv alakú alterek mindegyike nem lehet nulla. Jól ismert (például Herstein (H) 97-98 o.), hogy az L_iv altér vagy (0), vagy minimális A-invariáns altér (vagy modulus-elméleti terminológiával élve, egyszerű A modulus). Azt kapjuk tehát, hogy U minimális A-invariáns altér. Speciálisan, ha U=V, akkor nincs nemtriviális A-invariáns altér. A helyességet beláttuk.

Az első két lépés nyilvánvalóan befejezhető polinom időben. A 3. lépésre a 2.9. Tétel alkalmazásával adódik polinomiális korlát. Az 5.3. Következményt is figyelembe véve a 4. lépés megvalósitható egy polinom idejű f-algoritmussal. Érvényes a következő

5.4. Tétel Legyen $S=\langle X_1,\ldots,X_k\rangle \leq M_n(F)$. Az invariáns altér probléma megoldható egy f-algoritmussal, melynek futási ideje polinomiális az n, k és log(q) paraméterekben.

Ha az S generátumaként adódó A algebra féligegyszerű, akkor a hatása teljesen reducibilis, tehát V felbomlik egy T triviális és egy U unitér A modulus direkt összegére és az utóbbi összeadandó tovább bontható egyszerű modulusok direkt összegére. A triviális rész levágása könnyen elintézhető, hiszen T az $1_A v-v$ alakú, illetve U az $1_A v$ alakú vektorok halmaza, ahol v befutja V-t. U és T tehát hatékonyan meghatározható. Az INVARIANS() eljárás segitségével U felbontható egyszerű modulusok direkt összegére az alábbi recept szerint. Vegyük először észre hogy unitér modulus esetén az eljárás egyszerű részmodulust ad vissza. Ezután használható a bizonyitásokban szokásos módszer: tegyük fel hogy az U modulus W részmodulusát már előállitottuk mint egyszerűek direkt összegét. Ha W=U, akkor készen vagyunk. Különben hajtsuk végre az INVARIANS() eljárás 4. lépését egy olyan v vektorral, ami nincs W-ben. A szokásos érveléssel (Herstein loc. cit.) kapjuk, hogy a nem nulla $L_i v$ egyszerű modulusok közül legalább egy triviálisan metszi W-t, ami egy nagyobb direkt összeget eredményez.

5.5. Következmény Legyen A féligegyszerű F-algebra és V egy A-modulus. Legyenek $\dim_F A=n$ és $\dim_F V=m$. A V felbontható a T triviális és U unitér részének direkt összegére, továbbá U felbontható egyszerű A-modulusok direkt összegére egy f-algoritmussal, melynek futási ideje polinomiális az n, m, log(q) paraméterekben.

5.3. Minimális normálosztók permutációcsoportok elemi Abel faktoraiban

Legyen G egy n-edfokú permutációcsoport és legyenek K<H normálosztói G-nek. Tegyük fel hogy a fenti csoportok egy-egy erős generátorrendszerükkel adottak. (Itt az erős generátorrendszereknek csak arra a tulajdonságára van szükségünk, hogy $O(n^2)$ elemet tartalmaznak; pl. Luks (LU).) Tegyük fel továbbá, hogy H/K elemi Abel p-csoport valamilyen p primre. A feladat az, hogy találjunk minimális, a K<L≤H feltételnek eleget tevő normálosztóját G-nek. Erre a problémára akarunk $O(n^c)$ futási idejű algoritmust adni.

A feltételek szerint V:=H/K tekinthető vektortérnek GF(p) felett. A V vektortér dimenziója GF(p) felett O(nlog(n)) és polinom időben tudunk egy bázist találni benne. A G csoport hat V-n: a G elemeivel való konjugálások lineáris transzformációkat indukálnak V-n. Ebben a kontextusban problémánk ekvivalens egy minimális G-invariáns altér megkeresésével. Világos hogy elég egy a $g_1,\ldots,g_k$ elemek hatására invariáns alteret találni ahol $g_1,\ldots,g_k$ a G adott generátorrendszere. Irjuk fel ezen lineáris transzformációknak a V egy bázisára vonatkozó mátrixait. Ezután az INVARIANS() eljárás (esetleg többszöri) alkalmazásával találhatunk egy minimális invariáns alteret.

5.6. Következmény Legyenek $G<S_n$, K<H normálosztók G-ben erős genrátorrendszerekkel megadva. Tegyük fel, hogy H/K elemi Abel féle p-csoport valamilyen p primre. Ekkor egy a K<L≤H feltételeknek eleget tevő minimális G-beli normálosztót tudunk találni egy n-ben polinomiális idejű determinisztikus algoritmussal.

Bizonyitás. Elég észrevenni, hogy $k<n^2$ és hogy p nem nagyobb mint n, tehát Berlekamp determinisztikus "exponenciális" polinom faktorizáló módszere használható. Az állitás ezután az 5.4. Tételből következik.

6. NULLOSZTÓK KVATERNIÓALGEBRÁKBAN

A megelőző két fejezetben a nullosztó problémát vizsgáltuk véges test feletti algebrák esetében. A problémára sikerült elfogadható megoldást adni abban az értelemben, hogy polinomiális transzformáció erejéig ugyanolyan bonyolultságú algoritmusokat találtunk, mint amilyenek a fontos és sokat vizsgált speciális esetre a polinomok faktorizációjára ismeretesek.

A 4. fejezet bevezetőjében elmondottak szerint az F algebrai számtest feletti A algebrában hatékonyan tudunk nullosztót találni, ha A nem egyszerű. A problémát tehát ismét elég egyszerű algebrák esetén tekinteni. Ez az eset viszont sokkal nehezebbnek tűnik mint a véges testek feletti probléma. A célunk ebben a fejezetben az, hogy az (R1) dolgozat alapján a legkisebb nemtriviális esetet tisztázzuk, amikor $\dim_Q A=4$, A egyszerű nem kommutatív algebra. (Ha A egyszerű és $\dim_Q A<4$, akkor A szükségképpen test, tehát a probléma érdektelen.) Mivel az egyszerű algebrák centrum feletti dimenziója négyzetszám, a feltételeink szerint A centrális algebra Q felett, vagyis A centruma Q. Ugyanezen ok miatt látható, hogy A vagy egy ferdetest, vagy izomorf az $M_2(Q)$ algebrával. Hasznos lesz ezt a problémát megfogalmazni Garey - Johnson (GJ) stílusban:

6.1. Probléma

INPUT: Egy struktúrakonstansokkal adott centrális egyszerű A algebra Q felett, melyre $\dim_Q A=4$.

KÉRDÉS: Igaz-e hogy $A\cong M_2(Q)$? - vagy ami ezzel ekvivalens:

Van-e A-ban nullosztó?

Megmutatjuk, hogy a fenti problèma (a la Karp) ekvivalens a következő számelméleti kérdéssel:

6.2. Problèma

INPUT: a, b, c nem nulla egész számok.

KÉRDÉS: Léteznek-e olyan x, y, z egészek, $x^2+y^2+z^2>0$ hogy

$ax^2+by^2+cz^2=0$?

Megmutatjuk hogy a 6.1. és 6.2 Problémák között mindkét irányban létezik polinom idejű Karp redukció. Ezt az ekvivalenciát, valamint Legendre egy klasszikus tételét használva bizonyitjuk, hogy a 6.1. Probléma az NP∩co-NP bonyolultsági osztályba tartozik. Ezután, a probléma nehézségét illusztrálandó, "közismerten nehéz" számelméleti feladatokkal vetjük össze. Megmutatjuk, hogy feltéve az Általánositott Riemann Hipotézis egy változatát, létezik egy randomizált, polinom idejű redukció az ún. kvadratikus maradék problémáról a 6.1. Problémára (6.11. Tétel). Ennek következményeként az a (feltételes) eredmény is adódik, hogy a 6.1. Probléma - randomizációt is megengedve - legalább olyan nehéz, mint a primtényezős felbontás feladata négyzetmentes számokra.

A fejezet végén néhány kapcsolódó nyitott kérdést vetünk fel.

6.1. Kvaternióalgebrák

Ebben a részben definiáljuk a kvaternió algebrák fogalmát, majd ezek néhány tulajdonságát használva igazoljuk a 6.1. és 6.2. Problémák ekvivalenciáját.

Legyenek a, b nem nulla racionális számok. Definiáljuk a Q

feletti H(a,b) asszociativ algebrát "generátorokkal és relációkkal":

$$H(a,b):=\langle\ 1,\ u,\ v\ ;\ 1u=u1=u,\ 1v=v1=v,\ u^2=a,\ v^2=b,\ uv=-vu\ \rangle.$$

A relációkból következik, hogy 1 a H(a,b) algebra egységeleme. A H(a,b) algebrát egy kvaternió algebrának nevezzük. Nyilvánvaló, hogy H(-1,-1) a racionális Hamilton kvaterniók algebrája.

A következő állításban felsoroljuk a H(a,b) algebrák néhány fontos tulajdonságát. A (könnyű) bizonyitások megtalálhatók például O'Meara (O'M) könyvének 57. paragrafusában.

6.1. Állitás

(a) Az 1, u, v, uv elemek a H(a,b) algebra egy bázisát alkotják Q felett, tehát $\dim_Q H(a,b)=4$.

(b) H(a,b) centrális egyszerű algebra Q felett (tehát egyszerű és a centruma Q).

(c) $c1+du+ev+fuv$ (c, d, e, f racionális számok, nem mind nulla) pontosan akkor nullosztó a H(a,b) algebrában ha $c^2-d^2a-e^2b+f^2ab=0$.

(d) Ha H(a,b) tartalmaz nullosztókat, akkor az 1, u, v elemek által kifeszitett altér is tartalmaz nullosztókat.

Megjegyzés. Mint ahogy a Hamilton kvaterniók esetében, itt is definiálhatjuk az $x=c1+du+ev+fuv$ elem konjugáltját x'-t, mint $x':=c1-du-ev-fuv$ és az x elem normáját mint

$$N(x):=xx'=(c^2-d^2a-e^2b+f^2ab)1.$$

A (c) állitás azt mondja, hogy x nullosztó H(a,b)-ben pontosan akkor ha a normája nulla.

Példa. Könnyű látni, hogy H(1,-1) izomorf $M_2(Q)$-val. Legyen ugyanis e_{ij} az a kétszer kettes mátrix, melynek (i,j) poziciójában 1 van és máshol 0. Ezután legyen

$1:=e_{11}+e_{22}$, $u:=e_{21}+e_{12}$, $v:=e_{21}-e_{12}$.

A relációk könnyű számolással igazolhatók.

Most pedig igazoljuk a 6.1.(a) és (b) Állitások egyfajta algoritmikus megfordítását.

6.2. Tétel Legyen A négy dimenziós centrális egyszerű algebra Q felett. Ekkor A izomorf egy kvaternióalgebrával. Továbbá, ha A struktúra konstansokkal adott, akkor egy H(a,b) alakú reprezentáció (a, b nem nulla racionális egészek) található polinom időben.

Megjegyzés. A tétel egzisztenciális része jól ismert tény. A célunk itt egy hatékony algoritmus megadása.

Bizonyítás. Az A algebra vagy ferdetest, vagy izomorf $M_2(Q)$-val, tehát ha A tartalmaz nullosztót, akkor csak az utóbbi eset lehetséges. Ha pedig találunk egy x nullosztót, akkor az 5.1. részbeli eljáráshoz hasonlóan konstruálhatunk egy explicit izomorfizmust A és $M_2(Q)$ között. Ekkor ugyanis Ax egy kétdimenziós balideál és A hat Ax-en. Találtunk tehát A-nak egy nemtriviális, tehát hű kétdimenziós reprezentációját, amiből azonnal kaphatunk egy izomorfizmust. Ezután az e_{ij} elemeket használva az előző Példa szerint kapunk u, v elemeket, melyekre $u^2=1$, $v^2=-1$, $uv=-vu$ teljesül.

A módszer tehát a következő. Válasszunk egy tetszőleges nem Q-beli x elemet. Számoljuk ki az x elem $f_{x,A,Q}$ minimálpolinomját. Ha ez reducibilis, akkor találunk egy nullosztót és a bevezető észrevétel alapján A-nak egy kvaternió algebra reprezentációját. Feltehető tehát, hogy Q(x) test, mégpedig másodfokú bővitése Q-nak. Eszerint Q(x)=Q(u) alkalmas u elemmel, amelyre $u^2=a$ egy racionális egész. Ilyen u illetve a elemek hatékonyan találhatók x minimálpolinomjának ismeretében. A Q(u) testnek van olyan

automorfizmusa, mely az u elemet a -u elembe viszi. A Noether - Skolem tétel szerint (pl. Pierce (P), Section 12.6) ez egy belső automorfizmus, tehát van olyan invertálható v eleme A-nak, melyre $v^{-1}uv=-u$. Ilyen v elemet az uv=-vu lineáris egyenletrendszer (v az ismeretlen) megoldásával próbálunk találni. Válasszunk egy nem nulla v megoldást. Ha a kapott elem nullosztó, akkor készen vagyunk a korábbi recept szerint.

Feltehető ezért, hogy v nem nullosztó. Használva, hogy

$v^2u=-vuv=uv^2$,

továbbá hogy Q(u) maximális kommutativ részalgebrája A-nak, adódik, hogy $v^2=b$ egy nullától különböző racionális szám. A v elemet egy alkalmas egésszel megszorozva az is elérhető, hogy b egész szám.

Az $u^2=a$, $v^2=b$, uv=-vu összefüggések mutatják, hogy A izomorf a H(a,b) kvaternió algebrával.

Az eljárás konstans számú aritmetikai operációt jelent, továbbá a "tetszőlegesen" választandó elemek mindig választhatók kicsinek. Ha A struktúra konstansai legfeljebb n bit hosszúak, akkor a módszer O(nlog(n)loglog(n)) bitműveletet igényel. A bizonyitást befejeztük.

Ennek a résznek a fő eredménye a következő.

6.3 Tétel A 6.1. és 6.2. Problémák polinom idejű Karp redukciók erejéig ekvivalensek.

Bizonyitás. Legyenek a, b, c a 6.2. Probléma egy tetszőleges inputja, és legyen $f=ax^2+by^2+cz^2$ a megfelelő kvadratikus alak. Az f-et a-val elosztva feltehető, hogy a=1, b és c nem nulla racionális számok. Legyen a 6.1. Probléma megfelelő példánya az A:=H(-b,-c) kvaternió algebra. A 6.1. (a) és (b) Állitások szerint A centrális egyszerű Q felett és $\dim_Q A=4$. A 6.1. (c) és

(d) Állitások szerint az f=0 egyenletnek pontosan akkor van nemtriviális egész megoldása, ha A izomorf $M_2(Q)$-val.

A forditott irányú redukciót illetően legyen A centrális egyszerű algebra Q felett melyre $\dim_Q A=4$. A 6.2. Tétel szerinti algoritmussal keressünk olyan a, b egészeket melyekre A izomorf a H(-a,-b) algebrával. Legyen ezután a 6.2. Probléma megfelelő példánya az (1,a,b) hármas. A 6.1. (c) és (d) Állitások szerint H(-a,-b) pontosan akkor tartalmaz nullosztókat, ha az

$$x^2+ay^2+bz^2=0$$

egyenletnek van nemtriviális egész megoldása.

Megjegyzés. Az (1,a,b)→H(-a,-b) bijekció segitségével konstruáltunk polinom idejű transzformációkat mindkét irányban. Ezek a leképezések használható kapcsolatot létesitenek a megoldások között is. Pontosabban ha $x^2+ay^2+bz^2=0$, akkor rögtön adódik is egy nullosztó a H(-a,-b) algebrában, nevezetesen x1+yu+zv. Ezt az elemet használva a 6.2. Tételben leirt módon kaphatunk egy izomorfiát H(-a,-b) és $M_2(Q)$ között.

Forditva, ha van egy explicit izomorfiánk H(-a,-b) és $M_2(Q)$ között, akkor találhatunk egy nemtriviális yu+zv lineáris kombinációt (y,z racionális számok) melynek az (1,2) pozíciójában 0 van (itt u-t és v-t mint kétszer kettes mátrixokat nézzük). Alkalmas x racionális szám mellett az xI+yu+zv mátrix első sora a nullvektor lesz. Az igy nyert elem nyilván nullosztó H(-a,-b)-ben, tehát $x^2+ay^2+bz^2=0$. Az egyenlet egy racionális megoldásából pedig könnyen kaphatunk egy egész megoldást.

6.2. Háromváltozós kvadratikus alakok a racionális test felett

Ebben a részben a 6.2. Problémát vesszük szemügyre. A fő eredmény az, hogy a probléma az NP∩co-NP osztályba tartozik. A 6.3.

Tételből ezután már következik, hogy ugyanezen állitás igaz a 6.1. Problémára is.

Megemlitjük itt, hogy Lagarias (L) dolgozata számos érdekes algoritmust tartalmaz kvadratikus alakok kezelésére.

6.4. Lemma A 6.2. Probléma az NP osztályba tartozik.

Bizonyitás. Elég belátni, hogy ha az

(6.1) $ax^2+by^2+cz^2=0$ a, b, c nem nulla egészek;

egyenletnek van nemtriviális egész megoldása, akkor van az a, b, c számok méretében polinomiális méretű ilyen megoldása is. Ez pedig ismert: ha (6.1) megoldható, akkor van olyan x_0, y_0, z_0 megoldás is amelyre

$$\max\{|x_0|, |y_0|, |z_0|\} < 3(|a|+|b|+|c|).$$

A fenti állitás bizonyitása megtalálható pl. Cassels (CAS) könyvében (mint Lemma 6.8.1).

A továbbiakban szükségünk lesz Legendre következő tételére.

Legendre tétele Tegyük fel hogy abc négyzetmentes. Ekkor a (6.1)-nek pontosan akkor van nemtriviális egész megoldása, ha az alak indefinit (vagyis az a, b, c számok nem azonos előjelűek) és vannak olyan e_1, e_2, e_3 egész számok, melyekre

$$ae_1^2+b=0(\mathrm{mod}\ c)$$
$$be_2^2+c=0(\mathrm{mod}\ a)$$
$$ce_3^2+a=0(\mathrm{mod}\ b).$$

Bizonyitások találhatók a (CAS) Chapter 6, és (NZ) Section 5.12 munkákban.

Az általános eset könnyen és hatékonyan visszavezethető arra az esetre amikor abc négyzetmentes, ha ismerjük abc primtényezőit. Először is elosztjuk az együtthatókat gcd(a,b,c)-vel, tehát feltehető, hogy gcd(a,b,c)=1. Ha d^2 osztja a (6.1) egyenlet egyik együtthatóját, mondjuk a-t, akkor $x_1=dx$ bevezetésével a

(6.2) $a'x_1^2+by^2+cz^2=0$

egyenlet adódik, ahol $a=a'd^2$. Világos hogy (6.1) akkor és csak akkor oldható meg, ha (6.2). Utóbbi egy megoldásából könnyen nyerhető (6.1)-nek egy megoldása.

Ha pedig az $e>1$ egész osztója két együtthatónak, mondjuk a-nak és b-nek, akkor $u=z/e$ választással e-vel való osztás után az ekvivalens

(6.3) $a'x^2+b'y^2+ceu^2=0$

egyenlet adódik, ahol $a'=a/e$ és $b'=b/e$.

Ha (6.1)-nek nincs nemtriviális megoldása, akkor ezt a következő rövid bizonyitvány mutatja: ha az alak (pozitiv vagy negativ) definit, akkor ez leolvasható az együtthatók előjeléről.

Ellenkező esetben vegyük abc primtényezős felbontását és annak bizonyitványát. Pratt (PR) tétele szerint a primtesztelés NP-ben van, tehát ez megtehető. A négyzetmentes esetre való visszavezetés abc felbontásának ismeretében polinom időben elvégezhető, tehát feltehető, hogy abc négyzetmentes. Most ha (6.1) nem megoldható, akkor a három kongruencia közül legalább egy (mondjuk az első) nem megoldható. Ez pedig egyenértékű azzal, hogy a c valamely p primosztójára -b/a kvadratikus nemmaradék modulo p, amit pedig a $(-b/a)^{(p-1)/2}\equiv -1 \pmod p$ kongruencia ellenőrzésével polinom időben igazolhatunk. Kimondható tehát a

6.5 Tétel A 6.2 és igy a 6.1 Probléma az NP∩co-NP bonyolultsági osztályba tartozik.

A következő eredmény azt jelzi, hogy (6.1) megoldása nem lényegesen nehezebb feladat, mint a primtényezős felbontás megkeresése.

6.6 Tétel Ha abc primtényezőit ismerjük, akkor (6.1) egy megoldása megtalálható egy polinom idejű Las Vegas algoritmussal (amennyiben létezik egyáltalán megoldása).

Bizonyítás. A Legendre tételére adott (CAS) Theorem 6.4.1 bizonyítás lényegében egy használható algoritmust is ad. A könnyen láthatóan polinomiális lépések mellett két problémát kell kezelni. Meg kell oldani prim modulusú kvadratikus kongruenciákat, illetve találni kell egy legrövidebb nem nulla vektort egy Q^3-beli rácsban. Az első feladatra Rabin (RA1) Las Vegas módszere, a másodikra Kannan (KA) determinisztikus algoritmusa használható.

6.3. Kapcsolat a kvadratikus maradék problémával.

Eddig két kvalitativ felső korlátot adtunk a 6.2. és így a 6.1. Probléma bonyolultságára. Megmutattuk hogy NP∩co-NP könnyű és azt is, hogy a Las Vegas algoritmusok körén belül nem nehezebb mint a primtényezős felbontás problémája. Ebben a részben egy ellenkező irányú eredményt szeretnénk igazolni azzal, hogy a 6.2. Problémára redukálunk egy nehéznek tekintett másik problémát. Ez a probléma a kvadratikus maradék (quadratic residuosity) probléma.

Kvadratikus maradék probléma. Adottak $0<m<n$ természetes számok, n négyzetmentes és páratlan és az (m/n) Jacobi jel értéke 1. Döntsük el, hogy m kvadratikus maradék-e modulo n, vagyis hogy az $x^2=m \pmod n$ kongruenciának létezik-e egész x megoldása.

A fenti problémának azt a speciális esetét, amikor n két prímszám szorzata, Goldwasser és Micali (GM) vizsgálták kriptográfiai kérdésekkel kapcsolatban. A fenti problémához szorosan kapcsolódó

feladat a következő:

Moduláris gyökvonás. Oldjuk meg az $x^2 = m \pmod n$ kongruenciát az egészek körében, ha létezik egész megoldás.

Ismeretes (Rabin (RA), Goldwasser - Micali (GM)), hogy a moduláris gyökvonás problémája legalább olyan nehéz mint a primtényezős felbontás megtalálása, abban az értelemben, hogy ha az első problémának van polinom idejű megoldása, akkor a másodikra létezik randomizált polinom idejű algoritmus.
A redukció, amit megadunk, egy feltételes eredmény lesz. Feltesszük, hogy a Riemann Hipotézis igaz az algebrai számtestek Dedekind féle dzetafüggvényeire (szokásos rövidítéssel GRH). A fenti feltétellel Lagarias és Odlyzko (LO) bizonyították a Csebotarjev Sűrűségi Tétel egy igen erős változatát. Ennek az eredménynek itt csak a racionális test mint alaptest feletti változatára lesz szükségünk. Az (LO) dolgozatot követve legyen az L test normális bővítése Q-nak, jelölje G a bővítés Galois csoportját és legyenek n illetve d a bővítés foka illetve diszkriminánsának abszolút értéke. Ha p egy az L-ben nemelágazó racionális prim, akkor az $\left[\frac{L}{p}\right]$ Artin jel a p-t osztó L-beli P primideálok Frobenius automorfizmusainak G csoportbeli konjugált elemosztályát jelenti. Egy tetszőleges G-beli C konjugált elemosztályra legyen

$$\pi_C(x,L) = \{\ p;\ p \text{ nemelágazó L-ben}, \left[\frac{L}{p}\right] = C,\ p \le x\ \}.$$

érvényes a következő ((LO) Theorem 1.1., racionális változat):

Lagarias - Odlyzko Tétel Tegyük fel hogy GRH igaz. Ekkor van olyan $c>0$ effektive meghatározható abszolút konstans, hogy tetszőleges $x>2$ esetén

$$\left| \pi_C(x,L) - \frac{|C|}{|G|} Li(x) \right| < c\left(\frac{|C|}{|G|} x^{1/2} \log(dx^n) + \log d\right).$$

A $\pi_C(x,L) \sim \frac{|C|}{|G|} Li(x)$ aszimptotikus egyenlőség a Csebotarjev Sűrűségi Tétel racionális változata. Látható, hogy a tétel speciális esetként tartalmazza a nagy primszámtételt. Ha L-et körosztási testnek választjuk, akkor Dirichletnek a számtani sorozatok primszámaira vonatkozó tétele adódik. A tétel legáltalánosabb formája, amikor az alaptest egy tetszőleges algebrai számtest, a primideáltételt is tartalmazza.

A fenti eredmény szerint viszonylag rövid intervallumban is sok olyan primet találhatunk, melyre az Artin jel értéke egy előre megadott konjugált elemosztály.

A következőkben egy algebrai számelméleti jellegű gondolatmenet következik. A használt fogalmak és tények megtalálhatók pl. Ireland – Rosen (IR) 12. fejezetében.

Legyenek $p_1,\ldots,p_k$ különböző páratlan racionális primek. Legyen $L=Q(i,sqrt(p_1),\ldots,sqrt(p_k))$, ahol $i=sqrt(-1)$. Ismeretes (Kaltofen – Musser – Saunders (KMS)), hogy a fenti test normális bővítése Q-nak és a foka Q felett 2^{k+1}. A bővítés G Galois csoportja könnyen leirható. Legyen s_0 a komplex konjugálás és $i=1,\ldots,k$ esetén legyen s_i az az automorfizmusa L-nek mely p_i-t $-p_i$-be viszi, az összes többi generátorelemet pedig fixen hagyja. Ekkor G az s_i elemek által generált elemi Abel 2-csoport. Legyen most r egy a p_i primektől különböző páratlan racionális prim és legyen R egy r-et tartalmazó L-beli primideál. Ha D jelöli az L egészeinek gyűrűjét, akkor ismert, hogy F=D/R egy véges test és hogy az F test Frobenius automorfizmusát G egy s eleme indukálja.

Mit mondhatunk a p_i és r viszonyáról, ha ismerjük ezt az s automorfizmust? Az s automorfizmus egyértelműen felirható mint különböző s_i elemek szorzata. Ha ebben a felirásban s_0 nem szerepel, akkor s F-beli fixteste (vagyis a Z/rZ primtest)

tartalmaz olyan x elemet, melyre $x^2=-1$. Eszerint $r=4l+1$ alkalmas l egészre. Legyen most $i>0$. Ha u jelöli $\mathrm{sqrt}(p_i)$ képét F-ben - az u és -u elemek különbözők. Valóban, ellenkező esetben fennállna F-ben a $0=u-u=2u$, amiből $0=4u^2=4p_i$ következne.Ez pedig ellentmondás, hiszen r nem egyenlő 2-vel és p_i-vel sem. Ha s_i szerepel s felírásában, akkor az $x^2=p_i$ egyenlet megoldásai, u és -u nincsenek a Z/rZ primtestben, tehát p_i kvadratikus nemmaradék modulo r.

Ha s_i nem szerepel s felírásában, akkor az i=0 esettel azonos érvelés szerint p_i kvadratikus maradék modulo r. Speciálisan, ha s a G egységeleme, akkor mindegyik primszámunk kvadratikus maradék lesz modulo r.

Azt is láttuk, hogy a T(R) inercia csoport triviális, tehát a feltételeinknek eleget tevő r primek nem ágaznak el L-ben. Összegezve, érvényes a következő:

6.7. Lemma Legyenek L, p_i, s_i, a fentiek és legyen r egy a p_i primektől különböző páratlan prim. Ekkor r nem ágazik el L-ben és ha az R ideálhoz tartozó Frobenius automorfizmust az $s=\prod_{j\in H} s_j$ automorfizmus indukálja, ahol H az (1,...,k) egy tetszőleges részhalmaza, akkor $r=4l+1$ alkalmas l egészre és p_j pontosan akkor kvadratikus maradék modulo r, ha j nem eleme H-nak.

Ezután a Lagarias - Odlyzko Tétel segitségével megmutatjuk, hogy tetszőleges H halmaz elég gyakran megkapható, ahogy r végigfut a $(0,n^3)$ intervallumon, ahol $n=p_1\ldots p_k$.

6.8. Lemma Legyenek $p_1,\ldots,p_k$ különböző páratlan primek úgy, hogy $n=p_1\ldots p_k$ elég nagy és legyen $0<c<2^{-k-1}$. Legyen H az (1,...,k) halmaz egy tetszőleges részhalmaza. Tegyük fel továbbá, hogy GRH igaz. Ekkor azon $0<r<n^3$ primek száma, melyekre $s=\prod_{j\in H} s_j$ teljesül,

legalább $cLi(n^3)$.

Bizonyitás. Alkalmazzuk a Lagarias - Odlyzko Tételt a fenti L testre, $x=n^3$, $C=(s)$ választással.

$$|\pi_C(n^3,L)-(1/2^{k+1})Li(n^3)| < c(2^{-k-1}n^{1,5}2^{k+1}\log(dn^3)+\log d).$$

Elég megmutatni, hogy a jobboldali kifejezés $o(Li(n^3))$ nagyságrendű. Ehhez a d diszkriminánsra kell korlátot adni. Vezessük be a $p_0:=-1$ jelölést . A $(0,1,...,k)$ halmaz tetszőleges S részhalmazára legyen $b_S:=\prod_{j\in S}\mathrm{sqrt}(p_j)$ (az üres szorzat értéke 1). Világos, hogy a b_S alakú elemek L-nek egy lineáris generátorrendszerét alkotják Q felett, ezért tekintettel L fokára, ezek elemek lineárisan függetlenek is. Másfelől nyilvánvaló, hogy a b_S alakú elemek egészek L-ben, tehát elegendő ennek a bázisnak a diszkriminánsát megbecsülni. A b_S elem konjugáltjai a b_S illetve $-b_S$ elemek közül kerülnek ki. Használva, hogy b_S abszolút értéke legfeljebb n, és hogy a determináns mérete $2^{k+1}\leq 2n$, a d-t triviálisan becsülve

$$d<((2n!)n^{2n})^2$$

adódik, amiből látható, hogy $\log d=o(n^{1,1})$. Ezt használva látjuk, hogy a jobboldal nagyságrendje $o(n^{2,7})$, amivel az állitást igazoltuk.

Az előző két állitás alapján igaz a következő.

6.9. Következmény Legyenek $p_1,...,p_k$ különböző páratlan primek, $n=p_1...p_k$ és legyen $0<c<2^{-k-1}$. Legyen H az $(1,...,k)$ halmaz egy tetszőleges részhalmaza. Legyen m_H azon 4l+1 alakú r primek, $0<r<n^3$ száma, melyekre p_i pontosan akkor kvadratikus maradék modulo r, ha i nem eleme H-nak $(i=1,...,k)$. Ha n elég nagy és GRH igaz, akkor m_H legalább $cn^3/(3\log n)$.

A GRH-t feltételezve adunk egy polinom idejű Las Vegas redukciót

a kvadratikus maradék problémáról a 6.2. Problémára. Ebből következni fog, hogy (Las Vegas módszereket is megengedve) a nullosztó probléma legalább olyan nehéz, mint a négyzetmentes számok felbontásának problémája.

Először nézzük a kvadratikus maradék problémát arra az esetre, amikor m prim.

6.10 Lemma Legyen r egy primszám, n egy pozitiv egész. Tegyük fel hogy rn négyzetmentes és hogy (n/r)=1. Ekkor r kvadratikus maradék modulo n pontosan akkor ha a

(6.4) $x^2-ry^2-nz^2=0$

egyenletnek van nemtriviális egész megoldása.

Bizonyitás. A fenti kvadratikus alak indefinit és rn négyzetmentes, tehát Legendre Tétele szerint (6.4) megoldható akkor és csak akkor ha az

$$e_1^2-r=0(\mathrm{mod}\ n)$$

$$-re_2^2-n=0(\mathrm{mod}\ 1)$$

$$-ne_3^2+1=0(\mathrm{mod}\ r)$$

kongruenciák mind megoldhatók az egész számok körében. A második kongruencia nyilvánvalóan megoldható. Mivel n kvadratikus maradék modulo r, ugyanez igaz az $n^{-1}(\mathrm{mod}\ r)$ elemre is, tehát a harmadik kongruencia is megoldható. Kapjuk tehát, hogy (6.4) pontosan akkor oldható meg, ha az első kongruencia megoldható, vagyis ha r kvadratikus maradék modulo n.

Megjegyezzük, hogy a (6.4) egy nemtriviális megoldásából azonnal adódik az $x^2=r(\mathrm{mod}\ n)$ kongruenciának egy megoldása.

Ezen előkészületek után már bizonyitani tudjuk ennek a résznek a fő eredményét.

6.11 Tétel Tegyük fel, hogy GRH igaz. Ekkor létezik egy polinom

idejű Las Vegas redukció a kvadratikus maradék problémáról a 6.1. Problémára.

Bizonyitás. A 6.3. Tétel alapján elég a kvadratikus maradék problémát a 6.2. Problémára redukálni.

Legyen tehát az m,n pár a kvadratikus maradék probléma egy példánya (n páratlan, négyzetmentes, $0<m<n$, $(m/n)=1$). Legyen n primtényezős felbontása $n=p_1 \ldots p_t$. Ha k egy egyenletes eloszlású véletlen elem, melyre $0<k<n^3$, $\gcd(k,n)=1$, akkor $r=mk^2 \pmod{n^3}$ egy egyenletes eloszlású véletlen eleme lesz az

$$S_m=\{\, r;\ 0<r<n^3,\ (r/p_i)=(m/p_i)\ \ i=1,\ldots,t \,\}$$

halmaznak. A kvadratikus reciprocitási tétel szerint egy 4l+1 alakú r prim ($0<r<n^3$) pontosan akkor tartozik az S_m halmazba, ha $(p_i/r)=(r/p_i)=(m/p_i)$ $i=1,\ldots,t$. Használva, hogy S_m elemszáma legfeljebb $n^3/2^t$, a 6.9. Következmény szerint annak az eseménynek a valószinüsége, hogy egy ilyen tulajdonságú primet kapunk, legalább $c'/(3\log n)$, ahol a c' konstans kicsit kisebb mint 1/2. Használva, hogy $(m/n)=1$ és innen $(r/p_i)=-1$ páros sok i esetén, látjuk, hogy $(n/r)=1$. Az is világos, hogy r kvadratikus maradék modulo n akkor és csak akkor, ha m kvadratikus maradék modulo n és hogy r egy négyzetgyökéből (k ismeretében) m egy négyzetgyöke megkapható.

Ezután a redukció már egyszerű. Válasszunk olyan független, egyenletes eloszlású k elemeket, melyekre $0<k<n^3$, $\gcd(k,n)=1$ teljesül. Ezután kiszámitjuk az $r=mk^2 \pmod{n^3}$ elemet. Ellenőrizzük, hogy r prim-e és hogy r-1 osztható-e néggyel. Ha bármelyik kérdésre nemleges a válasz, eldobjuk k-t és újat választunk. Ha r túléli mindkét tesztet, akkor tekinthetjük az $x^2-ry^2-nz^2=0$ egyenletet. A 6.10. Lemma szerint ennek pontosan akkor van nemtriviális egész megoldása, ha r és igy m kvadratikus maradék modulo n.

A próbálkozások (azaz a választandó k elemek) számának várható

értéke 3log(n)/c'. A bizonyitást befejeztük.

Megjegyzés. Mivel Las Vegas redukciót akarunk, olyan primtesztre van szükségünk, ami biztosan nem téved, ha azt állitja hogy a vizsgált szám prim és majdnem minden primet tényleg primnek talál. Ismeretesek olyan determinisztikus primtesztelő algoritmusok, melyek futási idejére polinomkorlát adható a Riemann hipotézis különféle általánositásait feltéve. Az első ilyen módszer Millertől (MI) származik. Bach (B) munkájában konkrét becsléseket is találhat az olvasó. Ezek az algoritmusok azon múlnak, hogy a felett hipotézis mellett létezik kicsi kvadratikus nemmaradék mod p (p páratlan prim). Ilyen állitás következik az általunk feltett GRH-ból is. Elég a Lagarias - Odlyzko Tételt az L=Q(i,sqrt(p)) testre alkalmazni.
Újabban Schoof (SCH) elliptikus csoportok rendjét kiszámitó brilliáns módszerét használva Goldwasser és Kilian (GK) adtak egy érdekes véletlen primtesztet. A módszer majdnem minden primre szolgáltat egy polinom időben ellenőrizhető bizonyitványt is. A fenti redukciónál ez a módszer is használható. A várható próbálkozások száma ekkor egy kicsit növekszik.

6.5. Problémák, megjegyzések.

Ebben a fejezetben a nullosztó problémát vizsgáltuk Q feletti 4 dimenziós algebrákra. A kvaternióalgebrák néhány tulajdonságát használva megmutattuk, hogy a probléma ekvivalens egy számelméleti kérdéssel, a háromváltozós kvadratikus alakok gyökeinek létezésével. Egy polinom idejű Las Vegas redukció segitségével kimutattuk, hogy ezen problémák szorosan kapcsolódnak néhány , a szakmai közvélemény által nehéznek tekintett algoritmikus problémához. Utóbbi bizonyitásához

feltettük az Általános Riemann Hipotézist algebrai számtestek Dedekind féle dzetafüggvényére.

6.1. Nyitott kérdés. Bizonyitsuk be a 6.10 Tételt GRH nélkül.

Itt szükségesnek tartjuk megjegyezni, hogy valójában eléggé speciális számtestekkel foglalkoztunk (pl. a Galois csoportjuk elemi Abel 2-csoport). Másfelől a becslést illetően sincs szükség a Lagarias - Odlyzko Tétel teljes erejére. A maradéktagban $x^{1/2}$ helyén tetszőleges x^c, $c<1$ jó lenne.

A fő nyitott kérdés ezen a területen a nullosztó probléma.

6.2. Nyitott kérdés. Mi mondható a Q feletti nullosztó probléma bonyolultságáról?

A 6.2. Tételben olyan F maximális résztestet találtunk A-ban, mely a Q-nak ciklikus bővitése. Albert - Brauer - Hasse - Noether egy igen mély eredménye (Pierce (P)) szerint ilyen résztest létezik tetszőleges L algebrai számtest feletti A centrális egyszerű algebrában. Pontosabban van olyan maximális K részteste A-nak, hogy K/L Galois bővités és Gal(K/L) egy ciklikus csoport.

6.3. Nyitott kérdés. Ha adott A és L, tudunk-e a fenti tulajdonsággal rendelkező K testet találni polinom időben?

7. POLINOMOK VÉGES TESTEK FELETT

Az általunk vizsgált problémakör egyik kulcsfontosságú feladata a polinomok faktorizációja a kérdéses test felett. Algebrai számtestek felett ez a feladat megoldható polinom idejű algoritmussal. A véges testek feletti problémára azonban determinisztikus polinomidejű módszer nem ismeretes. Berlekamp (B1) módszerét még eddig nem sikerült lényegesen megjavitani.

Ennek a módszernek a vázlata a következő. Legyen $f \in K[x]$, $\deg(f)=n$, $K=GF(p^m)$. Feltehető, hogy nincs f-nek többszörös gyöke, ugyanis ezektől könnyű megszabadulni (lásd pl. Lidl - Niederreiter (LN) 4. fejezet). Feltehető, hogy $f=f_1 \ldots f_k$ ahol az f_i tényezők páronként relativ prim a K felett irreducibilis polinomok. A Bevezetésben láttuk, hogy f felbontása egyenértékű az $A=K[x]/(f)$ algebra minimális ideáljainak megtalálásával. Azt is tudjuk, hogy a fenti algebra k darab a K-t tartalmazó véges test direkt összege, tehát tartalmazza az GF(p) primtest k példányának a direkt összegét. Legyen ez a GF(p) feletti részalgebra B. Világos, hogy ha B-t sikerül felbontani, akkor A-t is, hiszen a két algebra idempotensei ugyanazok. Másfelől B polinom időben megkapható A-ból, egy lineáris egyenletrendszer megoldásával, hiszen B nem más, mint a Frobenius automorfizmus, tehát egy GF(p)-lineáris leképezés fixponthalmaza.

Világos, hogy B felbontásához elegendő B egy bázisában szereplő elemek GF(p) feletti B-beli minimálpolinomjait felbontani.

A B részalgebra elemeinek minimálpolinomjai lineáris tényezőkre

bomlanak GF(p)-ben, tehát B és így f felbontásának a problémáját visszavezettük primtest feletti polinomok primtestbeli gyökeinek a megkeresésére. Az eddig körvonalazott lépések mind polinomiális bonyolultságúak voltak, így a faktorizáció problémáját polinom időben Turing értelemben redukáltuk a primtestbeli gyökkeresés problémájára.

A gyökkeresés feladatára viszont eddig nem ismeretes lényegesen jobb módszer, mint hogy sorra vesszük a primtest elemeit és behelyettesitjük a felbontandó polinomba amig minden gyökőt meg nem kapunk. A módszer futási ideje polinomiális az n, m és p paraméterekben (az input hossza pedig n>0 esetén O(mnlog(p)).

Ha nem ragaszkodunk a determinisztikus módszerekhez, akkor sokkal jobb a helyzet. A problémára gyakorlatilag is igen hatékony polinom idejű Las Vegas módszerek vannak: Berlekamp (B2), Rabin (RA1), Cantor - Zassenhaus (CZ), Ben-Or (BO).

Az utóbbi időben számos, a probléma determinisztikus bonyolultságával kapcsolatos eredmény született, mely használja a Riemann hipotézis különféle általánositásait. A következő feladatok az előző fejezetben használt GRH teljesülése esetén polinom időben megoldhatók:

- kvadratikus polinomok felbontása (Adleman - Manders - Miller (AMM)).
- az x^n-a alakú binomok felbontása ((AMM), Huang (H1), (H2)).
- az olyan egészegyütthatós f polinomok felbontása melyeknek Q feletti Galois csoportja Abel féle (H1), (H2).
- a $GF(p^n)$ test konstrukciója (Adleman - Lenstra (AL)).
- tetszőleges polinom felbontása, ha p-1 primosztói kicsik (von zur Gathen (GA)): a módszer futási ideje $(ntlog\ p)^c$, ahol n a felbontandó poliom foka, és t a p-1 legnagyobb primosztója.

A későbbiekhez hasznos lesz egy további ilyen eredmény. Mielőtt ezt megfogalmazzuk, bevezetünk néhány jelölést.

A fejezet további részében p és r különböző primek, GF(p) jelöli a p elemű testet. Legyen F az "r-edik körosztási test" GF(p) felett, vagyis F az x^r-1 polinom GF(p) feletti felbontási teste. Jelölje F' az F nullától különböző elemeinek halmazát. Tegyük fel, hogy F elemszáma q és a k illetve r' egészeket definiáljuk a

$q-1=r^k r'$, $\gcd(r,r')=1$

összefüggésekkel. Legyen c egy tetszőleges primitiv r-edik egységgyök F-ből. Érvényes a következő

Huang Tétele Tegyük fel, hogy GRH igaz. Ekkor F megkonstruálható, valamint egy F-beli r-edik nemmaradék található egy determinisztikus algoritmussal, melynek futási ideje polinomiális az r és log(p) paraméterekben.

A fenti eredmény bizonyitása megtalálható (H2)-ben, mint a 4. fejezetbeli diszkusszió része. Külön állitásként nincs megfogalmazva.

A fejezet fő eredménye (R2) a következő:

7.1 Tétel Legyen $f\in GF(p)[x]$ egy polinom, melynek gyökei a GF(p) testben vannak. Legyen r az $n=\deg(f)>1$ egy primosztója és tegyük fel hogy az F test valamint egy F-beli r-edik nemmaradék adottak. Ekkor f felbontható <u>két</u> nem állandó polinom szorzatára egy determinisztikus algoritmussal, melynek időigénye polinomiális log p-ben és n^r-ben.

Huang Tételét használva azonnal kapjuk az alábbi következményt.

7.2 Következmény. Legyen $f\in GF(p)[x]$ és tegyük fel hogy f gyökei a GF(p) testben vannak. Legyen r az $n=\deg(f)>1$ egy primosztója. Ha GRH igaz, akkor f felbontható $f=f_1f_2$ alakban, ahol a tényezők egyike sem állandó. Az algoritmus futási ideje polinomiális a

log p és n^r paraméterekben.

Alkalmazzuk az előző eredményt korlátos sok irreducibilis tényezőre bomló polinomokra.

7.3. Következmény Ha GRH igaz, akkor a korlátos sok irreducibilis tényezőre bomló polinomok felbontása polinom időben megtalálható.

Bizonyitás. Berlekamp módszerének ismertetésénél láttuk, hogy ha a felbontandó polinomnak m irreducibilis tényezője van, akkor a probléma polinom időben Turing redukálható legfeljebb m-1 primtest feletti legfeljebb m-edfokú polinom primtestbeli gyökeinek a megtalálására. Erre a helyzetre pedig alkalmazható az előző következmény.

Megjegyzés. Ha a szóbanforgó f polinomot a $GF(p^s)$ test felett tekintjük és az f irreducibilis tényezőinek száma m, akkor a módszer bonyolultságára $O((m^m+\deg(f)+s\log p)^c)$ adódik egy alkalmas pozitiv c konstanssal.

Jól ismert, hogy némi "prekondicionálás" után a binom egyenletek modulo p polinom időben megoldhatók(Tonelli (T), Shanks (S), (AMM), (H2)). Pontosabban, ha rendelkezünk egy GF(p)-beli m-edik nemmaradékkal, akkor polinom időben meg tudunk oldani tetszőleges GF(p) feletti $x^m-a=0$ alakú egyenletet. Egy hasonló állitás kimondható a korlátos sok irreducibilis tényezőre bomló polinomokról is.

7.4. Következmény. Legyen d egy rögzitett pozitiv egész. Tegyük fel, hogy rendelkezünk polinomok egy $f_r, g_r \in GF(p)[x]$ listájával, $r \leq d$, r prim úgy, hogy f_r az GF(p) feletti r-edik körosztási polinom egy irreducibilis faktora, $\deg(g_r)<\deg(f_r)$ és $g_r \pmod{f_r}$

egy r-edik nemmaradék az $GF(p)[x]/(f_r)$ testben. Ekkor polinom időben fel tudunk bontani tetszőleges olyan p karakterisztikájú véges test feletti polinomot, melynek a kérdéses test felett legfeljebb d irreducibilis faktora van.

Megemlitjük még, hogy a binom egyenletek esetéhez hasonlóan a fentieknek eleget tevő polinomok találhatók egy polinom idejű Las Vegas algoritmussal.

Az algoritmus vázlata

Ismertetni szeretnénk a 7.1. Tétel algoritmusának alapgondolatát. Az f polinom egy "jó mátrixreprezentációját" fogjuk megadni. Pontosabban konstruálni fogunk egy olyan D mátrixot F felett, melynek a sajátértékei mind gyökei az f-nek és D mérete nem osztható az f fokával. Ha ez sikerült, akkor már könnyű f-et két tényezőre bontani.

Ami ezt a D mátrixot illeti, kiindulunk az f polinom A kisérő (companion) mátrixából és tekintjük az A által generált **A** mátrixalgebrát az F test felett. Ezután vesszük az **A** algebra r-edik tenzorhatványát az F test felett $\mathbf{B}:=\mathbf{A}\otimes\mathbf{A}\otimes\ldots\otimes\mathbf{A}$. A **B** algebra elemeit tekinthetjük n^r-szer n^r-es mátrixoknak F felett. Ezután konstruálunk egy a **B** elemeinek hatására invariáns **U** alteret, melyre $\dim_F \mathbf{U}=(1/r)n(n-1)\ldots(n-r+1)$. Ez a szám nem osztható n-nel.

A D mátrix ezután legyen $D:=A\otimes I\otimes\ldots\otimes I$, megszoritva az **U** altérre.

A konstrukció során fel kell bontanunk néhány speciális alakú polinomot. Az erre szolgáló módszereket irjuk le a 7.1. részben. A 7.2. részben definiáljuk a fontosabb altereket és lineáris transzformációkat, végül a 7.3. rész tartalmazza az algoritmus leirását és a 7.1. Tétel bizonyitását.

7.1. Speciális polinomok.

Legyen $S=(a_1,\ldots,a_n)$ az F elemeinek egy sorozata. S^k jelölje az $(a_1^k,\ldots,a_n^k)$ sorozatot. A fenti S esetén f_S jelölje az alábbi polinomot:

$$f_S(x)=(x-a_1)\ldots(x-a_n).$$

Világos, hogy ha $f \in F[x]$, f főegyütthatója 1, és f minden gyöke F-ben van, akkor $f=f_S$ alkalmas S sorozatra.

Megjegyezzük, hogy f_S ismeretében, és anélkül hogy az S halmazt explicite ismernénk, az f_S^k polinom hatékonyan megkapható. Valóban, ha A az f_S polinom kisérő mátrixa, akkor elegendő az A^k mátrix karakterisztikus polinomját kiszámitani. (Karakterisztikus polinomon mindig normált, tehát 1 főegyütthatós polinomot értünk.)

Az f_S polinomot <u>r-polinomnak</u> nevezzük, ha $S^{r^m}=(1,\ldots,1)$ teljesül valamely pozitiv egész m esetén.

Nyilvánvaló, hogy f egy r-polinom akkor és csak akkor, ha f főegyütthatója 1, f minden u gyöke F-ben van továbbá érvényes az $u^{r^k}=1$ összefüggés, ahol k a $q-1=r^k r'$, $\gcd(r,r')=1$ relációkkal meghatározott szám. Speciálisan az u multiplikativ rendje egy r-hatvány.

Ha $f=f_S$ egy r-polinom, akkor $f_S i$ szintén egy r-polinom, tetszőleges i természetes számra.

Ismert (például Huang (H2) Section 2) hogy ha rendelkezünk egy F testbeli r-edik nemmaradékkal, akkor tetszőleges F feletti x^r-u alakú polinom F-beli gyökeit meg tudjuk találni polinom időben. Ezt az algoritmust használva bizonyitható a következő

7.5. Lemma Tegyük fel, hogy adott egy b elem, ami r-edik nemmaradék az F testben. Ekkor tetszőleges r-polinomot lineáris tényezőkre tudunk bontani egy algoritmussal, melynek a futási ideje polinomja az r, deg(f), és log p paramétereknek.

Bizonyitás. Elég látni, hogy f hatékonyan felbontható két tényező szorzatára, mivel az r-polinomok osztói szintén r-polinomok. Nyilván feltehetjük, hogy f-nek nincsenek többszörös gyökei.

Legyen most A az f kisérő mátrixa. Számitsuk ki rendre az

(7.1) $A, A^r, A^{r^2}, \ldots, A^{r^i}$

mátrixokat, amig egy C=diag(l,l,...,l) skalár mátrixot nem kapunk. Ha B jelöli a sorozat utolsó előtti elemét, akkor B nem egy skalár mátrix és B eleget tesz az $x^r-l=0$ egyenletnek.

A következő lépésben megkeressük az $x^r-l=0$ egyenlet gyökeit. Világos, hogy ezek mind F-ben vannak, és a b elem segitségével polinom időben megkaphatók. Ezután felbonthatjuk a B mátrix g karakterisztikus polinomját $g=g_1g_2$ alakban, ahol a g_i tényezők relativ prim nem állandó polinomok. Világos, hogy $\mathrm{Ker}(g_1(B))$ egy nemtriviális invariáns altere A-nak, amiből azonnal adódik f-nek egy nemtriviális faktora.

Nézzük meg a fenti munka időigényét. n-szer n-es mátrixokkal dolgozunk, ahol n=deg(f). A (7.1) sorozat hossza legfeljebb $\log_2 q$, ezért B megkapható $(\log_2 q+n)^c$ lépésben. Az x^r-l polinom felbontására Huang (H2) alapján következik hasonló korlát. A fennmaradó lépések "szokásos" polinom aritmetikai és lineáris algebrai számitások, és igy ezek is polinom időben elvégezhetők. Végül, mivel $\log_2 q=r(\log_2 p)$, az állitást bebizonyitottuk.

Azt mondjuk, hogy az $f\in F[x]$ polinom <u>r-jó</u> ha f gyökei az F' halmazban vannak és $f(x)=g(x^r)$ teljesül alkalmas $g\in F[x]$ mellett. Ezek a polinomok jól jellemezhetők gyökeik segitségével.

7.6. Lemma Az f polinomra ekvivalensek a következők:

(a) f egy r-jó polinom.

(b) Az f gyökei F'-ben vannak és ha u egy i multiplicitású gyöke f-nek, akkor cu is egy i multiplicitású gyöke f-nek (c egy

primitiv r-edik egységgyök F-ben)

Bizonyitás. A következő azonosság használható mindkét irányban:

(7.2) $x^r-d^r=(x-d)(x-cd)\ldots(x-c^{r-1}d)$

Figyelembe véve még, hogy az r-jó polinomok zártak a szorzásra, az állitás világos. A részleteket az olvasóra hagyjuk.

Megjegyezzük, hogy a fentiek szerint ha $f=f_S$ egy r-jó polinom, akkor f_Si szintén egy r-jó polinom, feltéve, hogy gcd(i,r)=1. Speciális esetként f_Sr' egy r-jó r-polinom.

Alkalmazzuk a 7.5. Lemmát ezekre a polinomokra.

7.7. Lemma Tegyük fel, hogy adott egy F-beli r-edik nemmaradék b és legyen f egy r-jó r-polinom. Az f felbontható $f=f_1\ldots f_r$ alakban, ahol az f_i polinomok megegyező fokúak és páronként relativ primek, egy olyan algoritmussal, melynek futási ideje polinomiális a log p és deg(f) paraméterekben.

Bizonyitás. Feltehetjük, hogy f nem állandó. Tudjuk, hogy $f(x)=g(x^r)$ alkalmas és könnyen megtalálható $g\in F[x]$ mellett. Mivel g egy r-polinom, a 7.5 Lemma szerint, felbontható a deg(f) és log p paraméterekben polinom időben

(7.3) $g(y)=\prod_j (y-d_j)^{n_j}$

alakban, mivel $r\leq deg(f)$ és $deg(g)<deg(f)$.

Ezután keresünk olyan a_j elemeket, melyekre $a_j^r=d_j$. Ez elvégezhető a deg(g), r és log p paraméterekben polinomiális módszerrel, Huang ((H2) Section 2) módszerét alkalmazva a binom egyenletek megoldására.

Legyenek az f_i , i=1,2,...,r polinomok az alábbiak

(7.4) $f_i(x)=\prod_j (x-a_jc^i)^{n_j}$.

Ezek a polinomok hatékonyan megkaphatók. Világos, hogy $f=f_1f_2\ldots f_r$ és hogy mindegyik f_i foka deg(g). Használva, hogy a d_j elemek egymástól és nullától is különbözők, azonnal kapjuk, hogy az f_i polinomok páronként relativ primek. A bizonyitást

befejeztük.

7.2. Tenzor hatványok.

Tegyük fel, hogy $f \in GF(p)[x]$, f főegyütthatója 1, $\deg(f)=n>1$, melynek az $a_1,a_2,\ldots,a_n$ gyökei a GF(p) primtest különböző elemei. Tegyük fel továbbá, hogy r az n egy primosztója és $n^r<p$ (utóbbi feltevést csak a 7.11. Lemmában fogjuk használni, a többi állításhoz az a tény is elegendő, hogy r és p különbözők). Jelölje A az f kisérő mátrixát. A egy n-szer n-es mátrix GF(p) felett, melynek karakterisztikus polinomja f. Jelölje V_n az F feletti n hosszú oszlopvektorok vektorterét. Léteznek olyan az F felett lineárisan független $e_1,e_2,\ldots,e_n$ elemei a V_n vektortérnek, hogy $Ae_i=a_ie_i$ teljesül i=1,...,n esetén, ahol az a_i elemek az f gyökei. Ha **A** jelöli az A által generált F test feletti mátrixalgebrát, akkor az e_i vektorok sajátvektorai minden $B \in \mathbf{A}$ mátrixnak, vagyis léteznek olyan $u_{B,i} \in F$ elemek, hogy $Be_i=u_{B,i}e_i$ teljesül i=1,...,n esetén.

Legyen $\mathbf{B}:=\mathbf{A}\otimes\mathbf{A}\otimes\ldots\otimes\mathbf{A}$ az **A** algebra r-edik tenzor hatványa (Kronecker hatványa) az F test felett. A **B** algebra elemei n^r-szer n^r-es mátrixoknak tekinthetők F felett. (A tenzorszorzatokkal kapcsolatos alapvető tények megtalálhatók Greub (G) munkájában.) A **B** elemei hatnak a $\mathbf{V_n}:=V_n\otimes\ldots\otimes V_n$ (r-szer) tenzor hatványon az alábbi definició, illetve annak lineáris kiterjesztése szerint:

(7.5) $\quad (A_1\otimes\ldots\otimes A_r)(x_1\otimes\ldots\otimes x_r)=Ax_1\otimes\ldots\otimes Ax_r$.

Definiáljuk a $\mathbf{V_n}$ vektortér **V** alterét, mint

(7.6) $\quad \mathbf{V}=\mathrm{lin}(\, e_{i_1}\otimes\ldots\otimes e_{i_r}$; ha $i_j=i_l$, akkor $j=l$).

Szavakkal kifejezve, **V** a különböző e_i elemek szorzatai által generált F feletti altér. Mivel az e_i elemek lineárisan függetlenek F felett, $\dim_F\mathbf{V}=n(n-1)\ldots(n-r+1)$. Módszerünk egyik

legfontosabb lépése a **V** altér kiszámitása lesz.

A $\mathbf{V}_n$ vektortér egy **U** altere <u>felbontható</u>, ha generálható $e_{i_1} \otimes \ldots \otimes e_{i_r}$ alakú tenzorok egy (esetleg üres) részhalmazával. A fenti alakú tenzorokat <u>alaptenzoroknak</u> nevezzük.

Nyilvánvaló, hogy $\mathbf{V}_n$, **V** és (0) felbontható alterek. A (7.5) összefüggés szerint tetszőleges felbontható altér invariáns altere **B**-nek.

$0<i<j<r+1$ esetén legyen a $B_{ij} \in \mathbf{B}$ a következő lineáris transzformáció:

$$(7.7) \qquad B_{ij}=(I\otimes\ldots\otimes\underset{i}{I}\otimes A\otimes I\otimes\ldots\otimes I)-(I\otimes\ldots\otimes\underset{j}{I}\otimes A\otimes I\otimes\ldots\otimes I)\ .$$

7.8. Lemma Legyen **U** egy felbontható altér. Ekkor **U** egy invariáns altere a B_{ij} lineáris transzformációnak és ha **U** generálható alaptenzorok egy H halmazával, akkor $B_{ij}(\mathbf{U})$ generálható H azon elemeivel, melyeknek i-edik és j-edik komponense különböző.

Bizonyitás. Nézzük meg B_{ij} hatását az alaptenzorokon

$$(7.8) \qquad B_{ij}(e_{o_1}\otimes\ldots\otimes e_{o_r})=(a_{o_i}-a_{o_j})(e_{o_1}\otimes\ldots\otimes e_{o_r}).$$

A fenti összefüggés szerint B_{ij} az alaptenzorokat F egy elemével szorozza, tehát $B_{ij}(\mathbf{U})$ generálható H egy részhalmazával. Másfelől $a_{o_i}-a_{o_j}=0$ akkor és csak akkor, ha $o_i=o_j$, vagyis ha az i-edik és a j-edik komponensek megegyeznek. A lemmát beláttuk.

Tetszőleges **A**-beli B elemre legyen

$$(7.9) \qquad H(B):=\sum_{i=1}^{r} c^{i}(I\otimes\ldots\otimes\underset{i}{I}\otimes B\otimes I\otimes\ldots\otimes I)$$

és tekintsük H(B) hatását a **V** altéren. Mivel $H(B)\in\mathbf{B}$ és **V** egy felbontható altér, a **V** egy invariáns altere H(B)-nek. Beszélhetünk a tehát H(B)-nek mint **V** lineáris transzformációjának a g karakterisztikus polinomjáról.

7.9. Lemma Ha H(B) reguláris a **V** vektortéren, akkor g egy r-jó polinom.

Bizonyitás. Legyen $v=v_1\otimes\ldots\otimes v_r$ egy alaptenzor **V**-ből, ahol $v_j=e_{i_j}$ és legyen $l_j=u_{B,i_j}$. Legyen továbbá $w=v_2\otimes\ldots\otimes v_r\otimes v_1$, a v-ből a tényezők ciklikus permutációjával kapott tenzor. Egyszerű számolással adódik, hogy

$$H(B)v=(\sum_{i=1}^{r}c^{i}l_i)v$$

és

$$H(B)w=(\sum_{i=1}^{r}c^{i-1}l_i)w.$$

A fenti egyenletek szerint a v vektorhoz tartozó sajátérték c-szerese a w vektorhoz tartozónak. A H(B) lineáris transzformáció reguláris **V**-n, tehát ezek a sajátértékek nullától különbözők. Mivel a ciklikus permutáció a **V** alaptenzorainak egy permutációját indukálja, a 7.6. Lemma szerint készen vagyunk.

Legyen $B\in\mathbf{A}$ olyan, hogy H(B) reguláris **V**-n és legyen

(7.10) $\quad C:=H(B)^{r'}$.

Jelölje h(x) a C-nek, mint **V** lineáris transzformációjának a karakterisztikus polinomját. A 7.9. Lemmát használva érvényes a

7.10 Következmény. h(x) egy r-jó r-polinom.

A megelőző állitások olyan B-vel foglalkoztak melyre H(B) reguláris a **V** vektortéren. Ilyen B létezéséről és megtalálásáról szól a

7.11. Lemma Van olyan B eleme **A**-nak, melyre H(B) reguláris. Egy ilyen B található egy n^r-ben és log p-ben polinomiális idejű algoritmussal.

Bizonyitás. Először megjegyezzük, hogy a $B\to H(B)$ megfeleltetés egy F-lineáris leképezés. Másodszor, ha **W** egy tetszőleges nem nulla felbontható altere **V**-nek, akkor van olyan B, hogy $H(B)\mathbf{W}>(0)$ és egy ilyen B-t a **W** ismeretében hatékonyan találni is tudunk. Az egzisztenciához elég észrevenni, hogy tetszőleges i-re van olyan C eleme **A**-nak, melyre $Ce_i=e_i$ és bármely az i-től különböző j-re

$Ce_j=0$. Ezután alkalmas B található úgy, hogy a H(C) alakú lineáris transzformációk vektorterének egy bázisát végignézzük. Valamelyik báziselem biztosan jó lesz.

Ezek után elég belátni a következőt: tetszőleges **A**-beli B és D esetén van olyan i egész $0\leq i<n^r$, hogy

(*) Im H(B+iD)=Im H(B)+Im H(D) .

Ekkor ugyanis a kézenfekvő iterációval kaphatunk egy a kívánt tulajdonságú B mátrixot.

A (*) összefüggés igazolásához elég megmutatni, hogy alkalmas i-re H(B+iD)v nem nulla egyetlen a jobboldali összegbe tartozó v alaptenzorra sem. Ha v eleme Im H(B)-nek és Ker H(D)-nek, akkor ez teljesül minden i-re. Ha a v alaptenzor eleme Im H(D)-nek, akkor F-nek pontosan egy olyan d eleme van, melyre H(B+dD)v=0 teljesül. Használva hogy a szóbanforgó alaptenzorok száma kisebb mint n^r, és hogy a $0\leq i<n^r$ feltételnek eleget tevő i egész számok $n^r<p$ miatt inkongruensek modulo p, van olyan i a fenti intervallumból, mely eleget tesz a feltételünknek. A lemmát igazoltuk.

7.3. A faktorizáló módszer.

Minden együtt van az algoritmus leírásához. A felbontandó f polinomról nyilván feltehető, hogy a főegyütthatója 1 és hogy nincsenek többszörös gyökei. Ha utóbbi nem teljesül, akkor Berlekamp módszerével poli(n,log p) időben kaphatunk egy valódi tényezőt.

INPUT: Egy $f\in GF(p)[x]$ polinom, melynek gyökei egyszeresek és a primtestben vannak, az n=deg(f)>1 egy r prímosztója, valamint az F test egy reprezentációja (vagyis az r-edik körosztási polinom egy GF(p) feletti irreducibilis faktora) és egy F-beli b r-edik nemmaradék.

OUTPUT: Nem állandó f_1, $f_2 \in GF(p)[x]$ polinomok, melyekre $f=f_1 f_2$.

A módszer fő lépései a következők:

1. Ha $n^r \geq p$, akkor f_1, f_2 található GF(p) végignézésével.

2. (Innentől feltehető, hogy $n^r < p$.) Számitsuk ki az f polinom A kisérő mátrixát, majd az n^r-szer n^r-es B_{ij} mátrixokat (7.7) definició alapján minden $0<i<j\leq r$-re.

3. $W:=V_n$.

for $0<i<j<r+1$ **do** $W:=B_{ij}(W)$ **od**

(Altereket bázissal adunk meg, tehát $B_{ij}(W)$ kiszámitása egy bázis megadását jelenti. Az iteráció befejezésekor $W=V$ ahol V a (7.6) beli altér.)

4. Keressünk a 7.11. Lemma módszerével egy olyan B mátrixot, melyre a (7.9) összefüggéssel definiált H(B) reguláris W-n és erre a B-re számitsuk ki (7.10) összefüggéssel definiált C-nek, mint W lineáris transzformációjának a h(x) karakterisztikus polinomját.

(h egy r-jó r-polinom és $\deg(h)=n(n-1)\ldots(n-r+1)$.)

5. Bontsuk fel a h polinomot $h=h_1 \ldots h_r$ tényezőkre úgy, hogy a h_i polinomok páronként relativ primek és fokuk $(1/r)\deg(h)$, a 2.7. Lemma szerinti módszerrel.

6. Legyen $h'=h_2 h_3 \ldots h_r$ és számitsuk ki a W vektortér $U=\mathrm{Ker}\, h'(C)$ alterét. (U egy felbontható altér és $\dim_F U=(1/r)\deg(h)$.)

7. Legyen D az $A \otimes I \otimes \ldots \otimes I \in B$ tenzor által indukált lineáris transzformációja U-nak. Számitsuk ki D egy mátrixát, majd a mátrix g karakterisztikus polinomját. Irjuk fel a g polinomot $g=f^j g_1$ alakban úgy, hogy g_1 nem osztható f-fel és legyenek $f_1:=\gcd(f,g_1)$ és $f_2=f/f_1$. **return**(f_1,f_2).

(Igaz, hogy $f=f_1 f_2$, f_i nem állandó.)

A helyesség bizonyitása.

Igazolni fogjuk a 3.-7. lépések annotációját. A 3. lépés utáni

$W=V$ egyenlőség következik a 7.8. Lemma ismételt alkalmazásával. A 4. lépést követő állitás a 7.10. Következmény. Az 5. lépésbeli felbontás a 7.7 Lemma szerint lehetséges.

Ami a 6. lépést illeti, $\gcd(h,h')=1$ és

$\deg(h_1)=(1/r)n(n-1)\ldots(n-r+1)$ miatt $\dim_F U=(1/r)n(n-1)\ldots(n-r+1)$.

U egy felbontható altér, mivel $h'(C)\notin B$.

A 7.lépést illetően először megjegyezzük, hogy $A\otimes I\otimes\ldots\otimes I$ sajátértékei egyben az f polinomnak is gyökei, tehát g gyökei az f gyökei is. Innen már adódik, hogy $\deg(f_1)>0$, feltéve, hogy g_1 nem állandó. De g_1 nem lehet állandó, mert akkor fennállna a

$jn=\deg(g)=\dim_F U=(1/r)n(n-1)\ldots(n-r+1)$

egyenlőség. Ez pedig lehetetlen, hiszen az első szám osztható n-nel, az utolsó pedig nem.

A $\deg(f_1)<n$ egyenlőtlenség azért igaz, mert g_1 nem osztható az f polinommal.

A módszer időigénye.

Ha $p\leq n^r$, akkor $n^{r.c}$ időben végzünk az 1. lépésnél. Ellenkező esetben a 2.-3. és 6.-7. lépésekben lineáris algebrai műveleteket végzünk n^r-szer n^r-es mátrixokon illetve legfeljebb n^r fokú polinomokon. Az összes ilyen operáció száma n^d, alkalmas pozitiv d konstanssal, tehát a szükséges idő polinomiális n^r-ben és log p-ben. A 4. lépés időigénye a 7.11. Lemmát figyelembe véve szintén polinomiális ezekben a paraméterekben. Az 5. lépés időigénye a 7.7. Lemma szerint polinomiális log p-ben és n^r-ben. Ezzel a 7.1. Tétel bizonyitását befejeztük.

IRODALOM

(AL) L. M. Adleman, H. W. Lenstra Jr., Finding irreducible polynomials over finite fields; Proc. 18th ACM STOC, Berkeley, California, 1986, 350-355.

(AMM) L. M. Adleman, K. Manders, G. Miller, On taking roots in finite fields; Proc. 18th IEEE FOCS, 1977, 175-178.

(AR) V. A. Andrunakievics, Ju. M. Rjabuhin, Radikalû algebr i sztrukturnaja tyeorija; Nauka, Moszkva, 1979.

(B) E. Bach, Fast algorithms under the extended Riemann Hypothesis: a concrete estimate; Proc 14th ACM STOC, San Francisco, California, 1982, 290-295.

(B1) E. R. Berlekamp, Algebraic coding theory; McGraw-Hill, 1968.

(B2) E. R. Berlekamp, Factoring polynomials over large finite fields; Math. Computation 24, 1970, 713-715.

(BA) L. Babai, Monte Carlo algorithms in graph isomorphism testing; Techn. Rep. 79-10, Dep. Math. Stat., Universite de Montreal, 1979.

(BKS) R. E. Beck, B. Kolman, I. N. Stewart, Computing the structure of a Lie algebra; Computers in nonassociative rings and algebras, Academic Press, 1977, 167-188.

(BO) M. Ben-Or, Probabilistic algorithms over finite fields; Proc. 22th IEEE FOCS, 1981, 394-398.

(CA) P. Camion, A deterministic algorithm for factorizing polynomials of $F_q[x]$; Ann. Discr. Math. 17, 1983, 149-157.

(CAS) J. W. S. Cassels, Rational quadratic forms; Academic Press, 1978.

(CC) T. J. Chou, G. E. Collins, Algorithms for the solution of systems of linear diophantine equations; SIAM J. on Computing, No. 4, 1982, 687-708.

(CG) A. L. Chistov, D. Yu. Grigoryev, Polynomial-time factoring of the multivariable polynomials over a global field; LOMI preprint, Leningrád 1982.

(CZ) D. G. Cantor, H. Zassenhaus, A new algorithm for factoring polynomials over finite fields; Math. Comp. 36, 1981, 587-592.

(D) E. W. Dijkstra, A discipline of programming; Prentice Hall, 1976.

(DI) L. E. Dickson, Algebras and their arithmetics; University of Chicago 1923.

(DK) Ju. D. Drozd, V. V. Kirivenko, Konyecsnomernûe algebrû; Kijev, 1980.

(DR) M. P. Drazin, Srtucture matrices of algebras; Journal of Algebra, 87, 1984, 247-260.

(FR) K. Friedl, L. Rónyai, Polynomial time solutions of some problems in computational algebra; Proc. 17th ACM STOC, Providence, Rhode Island, 1985, 153-162.

(FRU) M. A. Frumkin, Polynomial time algorithms in the theory of linear diophantine equations; FCT'76 (szerk. Marek Karpinski), Lecture Notes in Computer Science, Springer, 1976, 386-392.

(FU) Fuchs L., Algebra; Egyetemi jegyzet, 1963.

(G) W. Greub, Multilinear algebra (2nd ed.); Springer, 1978.

(GA) J. von zur Gathen, Factoring polynomials and primitive elements for special primes; megjelenés alatt: Theoretical Computer Science, 1986.

(GJ) M. R. Garey, D. S. Johnson, Computers and intractability: a guide to the theory of NP-completeness; H. Freeman, San Francisco, 1978.

(GK) S. Goldwasser, J. Kilian, Almost all primes can be quickly certified; Proc. 18th ACM STOC, Berkeley, California 1986, 316-329.

(GM) S. Goldwasser, S. Micali, Probabilistic encryption and how to play mental poker keeping secret all partial information; Proc. 14th ACM STOC, San Francisco, California, 1982, 365-378.

(GR) D. Gries, The science of programming; Springer, 1981.

(H) I. N. Herstein, Noncommutative rings; Math. Association of America, 1968.

(H1) M.A. Huang, Factorization of polynomials over finite fields and factorization of primes in algebraic number fields; Proc. 16th ACM Symp. on Theory of Comuting, 1984, 175-182.

(H2) M. A. Huang, Riemann Hypothesis and finding roots over finite fields; Proc. 17th ACM Symp. on Theory of Comuting, 1985, 121-130.

(HU) J. E. Humphreys, Introduction to Lie algebra and representation theory; GTM 9, Springer 1980.

(HUL) J. E. Hopcroft, J. D. Ullman, Introduction to automata theory, languages and computation; Addison-Wesley, 1979.

(IR) K. Ireland, M. Rosen, A classical introduction to modern number theory; Springer-Verlag, 1982.

(JA) N. Jacobson, Lie algebras; John Wiley, 1962.

(JAC) N. Jacobson, Structure of rings, Amer. Math. Soc., 1956.

(K) D. E. Knuth, The art of computer programming, Vol. 2, Seminumerical algorithms; Addison-Wesley, 1981.

(KA) R. Kannan, Improved algorithms for integer programming and related lattice problems; Proc 15th ACM STOC, Boston, Massachusetts, 1983, 193-206.

(KB) R. Kannan, A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix; SIAM J. on Computing, No. 4, 1979, 499-507.

(KMS) E. Kaltofen, D. R. Musser, D. Saunders, A generalized class of polynomials that are hard to factor; SIAM Journal on Computing; vol. 12, no. 3, 1983, 473-483.

(KN) W. M. Kantor, szóbeli közlés, 1984.

(KU) A. G. Kuros, Felsőbb algebra; Tankönyvkiadó, 1967.

(L) J. C. Lagarias, Worst-case complexity bounds for algorithms in the theory of integral quadratic forms; Journal of Algorithms, vol. 1, 1980, 142-186.

(LA) S. Landau, Factoring polynomials over algebraic number fields in polynomial time; SIAM J. Comput. 1985.

(LE) A. K. Lenstra, Factoring polynomials over algebraic number fields; Proc. Eurocal'83, Springer 1983, 245-254.

(LLL) A. K. Lenstra, H. W. Lenstra, L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. 261, 1982, 515-534.

(LN) R. Lidl, H. Niederreiter, Finite fields; Addison-Wesley 1983.

(LO) J. C. Lagarias, A. M. Odlyzko, Effective versions of the Chebotarev density theorem; Algebraic number fields (L-functions and Galois theory) A. Frölich, ed., Academic Press 1977, 409-464.

(LU) E. M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time; J. Comput. Syst. Sci. 25, 1982, 42-65.

(MI) G. Miller, Riemann's hypothesis and tests for primality; J. Comput. System Sci. 13, 1976, 300-317.

(MIG) M. Mignotte, An inequality about factors of polynomials; Math. Computation,28, 1974, 1153-1157.

(NZ) I. Niven, H. S. Zuckerman, An introduction to the theory of Numbers; (third ed.) John Wiley and Sons 1971.

(O'M) O. T. O'Meara, Introduction to quadratic forms; Springer-Verlag 1963.

(P) R. S. Pierce, Associative algebras; Springer-Verlag 1982.

(PR) V. R. Pratt, Every prime has a succint certificate; SIAM J. on Computing, vol.4, 3, 1975, 214-220.

(R) L. Rónyai, Zero divisors and invariant subspaces; University of Oregon Technical Report CIS-TR 85-11, 1985.

(R1) L. Rónyai, Zero divisors in quaternion algebras; megjelenés alatt, Journal of Algorithms.

(R2) L. Rónyai, Factoring polynomials over finite fields; megjelenés alatt, Journal of Algorithms.

(RA) M. O. Rabin, Digitalized signatures and public-key functions as intractable as factorization; MIT/LCS/TR-212, Technical Memo MIT, 1979.

(RA1) M. O. Rabin, Probabilistic algorithms in finite fields; SIAM Journal on Computing, Vol. 9, No. 2, 1980, 273-280.

(S) D. Shanks, Five number-theoretic algorithms; in: Proc. 1972 Number Theory Conference, University of Colorado, Boulder 1972, 217-224.

(SCH) R. Schoof, Elliptic curves over finite fields and the computation square roots mod p; Math. Computation, Vol. 44. April 1985, 483-494.

(SCHÖ) A. Schönhage, Schnelle berechnung von Kettenbruchentwicklungen; Acta Informatica, 1, 1971, 139-144.

(SI) J. H. Silverman, The arithmetic of elliptic curves; GTM 106, Springer, 1986.

(T) A. Tonelli, Göttingen Nachrichten (1891); 344-346. Lásd még: L. E. Dickson, History of the theory of numbers; Chelsea, Vol. I., 215.

(WE) J. M. Wedderburn, On hypercomplex numbers; Proc. London Math. Soc., 6, 1908, 77-118.

1986-BAN MEGJELENTEK:

179/1986 Terlaky Tamás: Egy véges criss-cross módszer és alkalmazásai

180/1986 K.N. Čimev: Separable sets of arguments of functions

181/1986 Renner Gábor: Kör approximációja a számitógépes geometriai tervezésben

182/1986 Proceedings of the Joint Bulgarian-Hungarian Workshop on "Mathematical Cybernetics and Data Processing" Scientific Station of Sofia University, Giulecica /Bulgaria/, May 6-10, 1985 /Editors: J. Denev, B. Uhrin/ Vol I

183/1986 Proceedings of the Joint Bulgarian-Hungarian Workshop on "Mathematical Cybernetics and Data Processing" Scientific Station of Sofia University, Giulečica /Bulgaria/, May 6-10, 1985 /Editors: J. Denev, B. Uhrin/ Vol II

184/1986 HO THUAN: Contribution to the theory of relational databases

185/1986 Proceedings of the 4th International Meeting of Young Computer Scientists IMICS'86 /Smolenice, 1986/ /Editors: J. Demetrovics, J. Kelemen/

186/1986 PUBLIKÁCIÓK - PUBLICATIONS 1985 Szerkesztette: Petróczy Judit

187/1986 Proceedings of the Winter School on Conceptual modelling /Visegrád, 27-30 January, 1986/ /Editors: E. Knuth, A. Márkus/

188/1986 Lengyel Tamás: A Cluster analizis néhány kombinatorikai és valószinüségszámitási problémája

189/1986 Bernus Péter: Gyártórendszerek funkcionális analizise és szintézise

190/1986 Hernádi Ágnes: A tipus fogalma, és szerepe a modellezésben

191/1986 VU DUC THI: Funkcionális függőséggel kapcsolatos néhány kombinatorikai jellegü vizsgálat a relációs adatmodellben

192/1986 Márkusz Zsuzsanna: P a p e r s on Many-stored logic as a tool for modelling

193/1986 KNVVT Conference on Automation of Information Processing on Personal Computers
Budapest, May 5-9, 1986 Vol I.
Szerkesztette: Ratkó István

194/1986 KNVVT Conference on Automation of Information Processing on Personal Computers
Budapest, May 5-9, 1986 Vol II.
Szerkesztette: Ratkó István