Gonda János

VÉGES TESTEK

Budapest, 2011

Lektorálta Bui Minh Phong

Utolsó módosítás dátuma: 2018. április 5.

Előszó

Ez a jegyzet az ELTE-n tartott Véges testek illetve Véges testek alkalmazásokhoz című tárgy anyagát tartalmazza. A tárgy szerepel a mesterképzésben, valamint a doktori képzésben is. Mivel vannak hallgatók, akik mindkét képzés keretében hallgatják a tárgyat, és azonos tananyagot nem lehet kétszer „elszámolni", ezért a jegyzet két félév anyagát tartalmazza. A két félév anyaga nem különül el egymástól, így az oktató döntheti el, hogy mely részeket gondolja az alapképzésben elmondani, és melyeket hagy a doktori kurzus idejére. Azt azonban figyelembe kell venni, hogy a hallgatók túlnyomó többsége csupán a reguláris képzés keretében foglalkozik a témával, valamint azt is, hogy a tárgy elméleti alapot ad az Algebrai kódoláselmélet című tárgyhoz (elvileg a Rejtjelezéshez is, ám az kötelező tárgy, míg a Véges testek egy választható modul része).

Tekintettel arra, hogy a tárgy mind a reguláris, mind a doktori képzés keretében heti két (tan)órában, egy félév során kerül előadásra, az anyag ehhez a szűkre szabott időkerethez igazodik, így is az ennyi idő alatt elmondható ismeretek mennyiségének felső határát súrolva, esetleg ezt a korlátot kissé át is lépve. Éppen erre való tekintettel szükséges megjegyezni, hogy bizonyos részek a tényleges előadás és számonkérés során többé vagy kevésbé tömöríthetőek, belőlük egyes részek kihagyhatóak vagy csupán érintőlegesen kerülhetnek szóba. Ez függhet az előadó ízlésétől, a tárgyat hallgatók összetételétől és „előéletétől", a tárgyban tanultakra esetleg támaszkodó további tárgyaktól, az adott félév tényleges hosszától, és még más körülményektől is.

Miről szól a tárgy és ez a jegyzet? A címük szerint a véges testekről. A cím ilyen formán egy teljes, lezárt témát ígér a hallgatónak illetve olvasónak. A valóság ezzel szemben lényegesen szegényesebb. A már említett időkorlátot figyelembe véve nem vállalkozhattunk másra, és a valóság is az, hogy csupán az említett témakör egy kis, bár viszonylag jól körülhatárolható részével foglalkozzunk. Amiről szó lesz, az lényegében véve a véges testekkel kapcsolatos azon részeket tartalmazza, amelyek az Algebrai kódoláselmélet illetve Rejtjelezés című tárgyakhoz szükségesek. Az ezen túlmutató anyagrészeket elsősorban a doktori képzésben célszerű felhasználni.

Az anyag megértéséhez szükség van algebrai ismeretekre. Ez általános algebrai ismereteket (csoportokkal, gyűrűkkel, testekkel, polinomokkal kapcsolatos fogalmakat) jelent, jelenti azonban azt is, hogy támaszkodik az általában sokkal kisebb részben oktatott véges testek bizonyos fokú ismeretére. A biztonság kedvéért a szükséges testelméleti ismereteket röviden összefoglaljuk a jegyzet elején.

A téma iránt mélyebben érdeklődő olvasó az irodalomjegyzékben említett könyvekből szerezhet további ismereteket, éppen ezért nem csak olyan könyveket soroltunk ott fel, amelyek szorosan kapcsolódnak az általunk kifejtett részletekhez.

Végül néhány jelölésről szólunk. Ebben a jegyzetben $\mathbb{N}^+$ a pozitív egész számokat jelöli, és $\mathbb{N}$ jelöli a nemnegatív egész számokat. Egy polinomot például f-fel, és nem $f(x)$-szel jelölünk, megfelelően annak, hogy a polinom egy formális kifejezés, amelyet az együtthatói határoznak meg. Az f polinomhoz tartozó polinomfüggvény jele $\hat{f}$. A mátrixokat és vektorokat félkövér betű jelöli, a halmazokat dőlt nagybetű, és egy struktúrát a hozzá tartozó halmaztól a betű típusa különbözteti meg, például az A halmazra épített struktúra jele $\mathcal{A}$. A q-elemű test jele ebben a jegyzetben $\mathbb{F}_q$.

Tartalomjegyzék

1. Bevezetés

Ebben a fejezetben összefoglaljuk azokat az ismereteket, amelyek szükségesek a későbbiek megértéséhez. Mivel az itt elmondottakról feltételezzük, hogy nem új dolgok az olvasó számára, ezért bizonyítást csak olyan esetben adunk, amikor az vagy tanulságos a későbbi fejezetekre nézve, vagy kevésbé ismert állításról van szó.

1.1. Definíció

Legyen A egy halmaz és n egy nemnegatív egész szám. Ekkor $f: A^n \to A$ **n-változós művelet A-n**. A nullaváltozós műveletet **konstans művelet**nek is nevezzük. Egy $\mathcal{A} = (A, F_A)$ rendezett pár egy A **feletti algebrai struktúra**, ha F_A A feletti műveletek egy halmaza. A az előbbi algebrai struktúra **alaphalmaz**a.

Δ

Algebrai struktúra helyett röviden **algebrát** vagy **struktúrát**, alaphalmaz helyett **tartóhalmaz**t is mondunk.

A definícióból látszik, hogy minden művelet véges változós leképezés, ám a műveletek száma nem korlátozott, F_A bármilyen számosságú halmaz lehet.

Igen fontos fogalom a részstruktúra, a generátum valamint a homomorfizmus.

1.2. Definíció

Legyen $\mathcal{A} = (A, F_A)$, $\mathcal{B} = (B, F_B)$ és $\mathcal{C} = (C, F_C)$ algebrai struktúra, $D \subseteq A$ és $f \in F_A$ egy n-változós művelet. Ekkor

- D **zárt f-re nézve**, ha $f(\mathbf{a}) \in D$, valahányszor $\mathbf{a} \in D^n$;
- a D-n értelmezett n-változós g művelet az f **D-re való megszorítása**, ha minden $\mathbf{a} \in D^n$-re $g(\mathbf{a}) = f(\mathbf{a})$;
- $\mathcal{B}$ **az $\mathcal{A}$ részstruktúrája**, jelölésben $\mathcal{B} \leq \mathcal{A}$, ha $B \subseteq A$, és létezik F_A-nak F_B-re való olyan φ bijekciója, hogy minden $f \in F_A$-ra $\varphi(f)$ az f B-re való megszorítása;
- $\mathcal{B}$ **az $\mathcal{A}$ D által generált részstruktúrája**, vagy D **az $\mathcal{A}$ $\mathcal{B}$ részstruktúrájának generátorrendszere**, ha $\mathcal{B}$ az $\mathcal{A}$ legszűkebb olyan részstruktúrája, amely tartalmazza D-t;
- $\varphi: A \to C$ **A-nak $\mathcal{C}$-be való homomorfizmusa** vagy **művelettartó leképezése**, ha van olyan $\varphi_m: F_A \to F_C$ bijekció, hogy ha $f_A \in F_A$ n-változós művelet, akkor $\varphi_m(f_A) = f_C$ is n-változós, és bármely $\mathbf{a} \in A^n$-re $f_C\big(\varphi^n(\mathbf{a})\big) = \varphi\big(f_A(\mathbf{a})\big)$; ha φ szürjektív, akkor a homomorfizmus **epimorfizmus**, ha injektív, akkor **monomorfizmus**, és ha bijekció, akkor **izomorfizmus**, továbbá ha $\mathcal{A} = \mathcal{C}$, akkor a homomorfizmust **endomorfizmus**nak, az izomorfizmust **automorfizmus**nak mondjuk.

Δ

Nyilván tetszőleges struktúra önmagának részstruktúrája, ez **a struktúra** (egyetlen) **nem valódi részstruktúrája**, minden más részstruktúra **valódi részstruktúra**.

Nem nehéz ellenőrizni, hogy egy struktúra részstruktúráinak bármely metszete zárt a struktúra minden műveletére nézve, így a műveleteket megszorítva a metszetre, ismét részstruktúrát kapunk, a legbővebb olyan részstruktúrát, amely a metszet minden tagjának része.

Ha φ az $\mathcal{A}$-nak $\mathcal{C}$-be való homomorfizmusa, akkor A képe az F_C műveleteire nézve zárt, és $\mathrm{Im}(\varphi)$ a műveleteknek erre a képre való megszorításával részstruktúrája $\mathcal{C}$-nek. Amennyiben φ monomorfizmus, akkor minden képelemet azonosíthatunk a képével, vagyis $\mathcal{A}$-t **beágyazzuk** $\mathcal{C}$-be.

Tetszőleges $\varphi: A \to C$ leképezésnél $\mathrm{Ker}(\varphi) = \{(u, v) \in A^2 | \varphi(u) = \varphi(v)\}$, a **leképezés magja**, ekvivalencia-reláció A-n, és ha φ homomorfizmus és f_A az A n-változós művelete, akkor minden olyan esetben, amikor minden i-re $(a_i, b_i) \in \mathrm{Ker}(\varphi)$, egyben $\big(f_A(\mathbf{a}), f_A(\mathbf{b})\big)$ is eleme $\mathrm{Ker}(\varphi)$-nek, vagyis ha az argumentumokat velük ekvivalens elemekkel helyettesítjük, akkor a művelet eredménye is ekvivalens a korábbi eredménnyel. Általában az $\mathcal{A}$ struktúra alaphalmazán értelmezett ρ homogén binér **reláció kompatibilis az f_A művelette**l, ha $f_A(\mathbf{a})\rho f_A(\mathbf{b})$, valahányszor $\mathbf{a}\rho^n\mathbf{b}$, és ρ **kompatibilis $\mathcal{A}$-val**, ha $\mathcal{A}$ minden műveletével kompatibilis. Amennyiben az előbbi kompatibilis reláció ekvivalencia-reláció, akkor **kongruencia-reláció**, vagy egyszerűen **kongruencia**. Az ekvivalencia osztályainak halmaza az A ρ **szerinti faktorhalmaza**, amelyet A/ρ jelöl. Kongruencia esetén a faktorhalmazon az f_A-nak megfelelő műveletet definiál az $f_{A/\rho}(\bar{\mathbf{a}}) = \overline{f_A(\mathbf{a})}$ szabály, ahol $\bar{a}$ az a által reprezentált osztály. Az ezekkel a műveletekkel ellátott struktúra az $\mathcal{A}$ ρ **szerinti** $\mathcal{A}/\rho$ **faktorstruktúrája**.

1.3. Tétel

Legyen ρ kongruencia-reláció az $\mathcal{A} = (A, F_A)$ struktúrán. Ekkor az $a \mapsto \bar{a}$ **kanonikus szürjekció** az $\mathcal{A}$ $\mathcal{A}/\rho$-ra való epimorfizmusa. Amennyiben $\varphi: A \to C$ homomorfizmus, akkor $\mathrm{Ker}(\varphi)$ kongruencia-reláció $\mathcal{A}$-n és $\mathcal{A}/\mathrm{Ker}(\varphi) \cong \mathcal{I}m(\varphi)$, továbbá $\varphi = \kappa\psi$, ahol $\psi: a \mapsto \bar{a}$ a kanonikus szürjekció és $\kappa: \bar{a} \mapsto \varphi(a)$ monomorfizmus.

Δ

Az $\mathcal{A}$ **struktúra** $|A|$ **rendje** az A elemeinek száma, ha ez véges, különben a rend végtelen.

Most visszatérünk a műveletekhez.

Nullaváltozós művelet a halmaz egy elemének, egy **konstans**nak a kijelölése, és általában a műveletet és a művelet eredményét azonos jel jelöli. A konstans többnyire a struktúra egy speciális tulajdonságú eleme. Ilyen például a valós számok halmazában a 0 az összeadással vagy az 1 a szorzással.

Egyváltozós művelet a halmaz önmagába való leképezése. Egy ilyen f műveletet **involutórikus**nak vagy **involúció**nak mondunk, ha $f^2 = id_A$, ahol id_A az A halmaz önmagára való identikus leképezése, vagyis az a leképezés, amely minden elemnek önmagát felelteti meg. Egyváltozós műveletre példa a valós számok esetén az ellentett képzése, vagyis az a művelet, amely minden számhoz a -1-szeresét rendeli, vagy a komplex számok halmazán a konjugálás, vagy egy lineáris téren egy rögzített skalárral való szorzás. Az előbbi kettő involúció, az utóbbi csak akkor, ha a skalár az egységelem vagy annak az ellentettje. Az egyváltozós műveletet többféleképpen is jelöljük: szokásos a kitevős írásmód, például a^{-1} a pozitív valós számok szorzással vett halmazán, a prefix írásmód, amikor a művelet jele megelőzi az operandust, mint például az egész számok halmaza az összeadással $(-a)$ vagy rögzített skalárral való szorzás egy lineáris térben $(3\mathbf{a})$, vagy valamilyen kiegészítő jel az operandus fölött vagy mellett, amire jó példa a konjugálás a felülhúzással.

A leggyakoribb művelettípus a kétváltozós, vagy másként a **binér** művelet, amelyet általában infix írásmóddal adunk meg, vagyis úgy, hogy a műveleti jelet a két operandus közé írjuk (például $3 + 5$). A szokásos infix a $+$ jel, valamint a $\cdot$, és ez utóbbit sokszor nem is jelöljük. Az előbbi jelölés esetén a műveletet **összeadás**nak, a másik esetben **szorzás**nak, magát a struktúrát gyakran **additív** illetve **multiplikatív** struktúrának mondjuk az előbbi sorrendben. Multiplikáció esetén a műveletben résztvevő elemek a szorzás **tényező**i, és az eredmény a **szorzat**uk, míg az összeadásnak **tag**jai vannak, és az eredmény a tagok **összeg**e.

Kétváltozós műveletet természetesen csak két operandussal hajthatunk végre, ám maguk az operandusok is lehetnek ugyanezen kétváltozós művelet eredményei, vagyis a műveleteket tetszőleges, de véges mélységben egymásba ágyazhatjuk. Ekkor zárójelezéssel kell kijelölni, hogy a műveleteket milyen sorrendben kell végrehajtani. Legyen $\mathcal{A}$ egy multiplikatív struktúra. A művelet **asszociatív**, ha bármely a, b és c A-beli elem esetén $(ab)c = a(bc)$. Ekkor igaz az **általános asszociativitás törvénye**, amely szerint több elem szorzata nem függ a szorzások végrehajtásának sorrendjétől (nem az elemek,

hanem a szorzások sorrendjéről van szó!), így a zárójelezést el is hagyhatjuk. Ilyen értelemben beszélünk n-**tényezős szorzat**ról, és ennek speciális eseteként az **egytényezős szorzat**ról, amely valójában nem egy szorzat, csupán a struktúra egy eleme.

Ha két elem szorzata nem függ a két elem sorrendjétől, vagyis $ab = ba$, akkor a két elem **felcserélhető**, és ha bármely elempár felcserélhető, akkor a szorzás, illetve a struktúra **kommutatív**. *Amennyiben a szorzás asszociatív*, és egy többtényezős szorzatban bármely két tényező felcserélhető, akkor a szorzat nem függ a benne résztvevő tényezők sorrendjétől, vagyis egy egyszerre asszociatív és kommutatív struktúrában egy szorzat nem függ a benne megadott tényezők és a szorzások sorrendjétől. A szokások szerint csak akkor írunk egy műveletet additívként, ha a művelet asszociatív és kommutatív.

Az A valamely a eleme

- **balról reguláris**, ha bármely $b \in A$-hoz legfeljebb egy olyan $u \in A$ létezik, hogy $a \cdot u = b$ és **reguláris**, ha mindkét oldalról reguláris; maga a struktúra balról reguláris illetve reguláris, ha minden eleme balról reguláris illetve reguláris;
- **jobbról invertálható**, ha minden $b \in A$-hoz van olyan $u \in A$, hogy $a \cdot u = b$, és **invertálható**, ha mindkét oldalról invertálható; maga a struktúra jobbról invertálható illetve invertálható, ha minden eleme jobbról invertálható illetve invertálható;
- **bal oldali egységelem**, ha minden $b \in A$-ra $a \cdot b = b$, és **egységelem**, ha egyszerre bal és jobb oldali egységelem; a struktúra egységelemes, ha van egységeleme;
- **bal oldali zéruselem**, ha minden $b \in A$-ra $a \cdot b = a$, és **zéruselem**, ha egyszerre bal és jobb oldali zéruselem; a struktúra zéruselemes, ha van zéruseleme;
- **bal oldali inverze** $b \in A$-nak, ha a struktúra egységelemes az e egységelemmel, és $a \cdot b = e$, továbbá a inverze b-nek, ha egyidejűleg bal és jobb oldali inverze.

Természetesen a fentiekben értelemszerűen állhat bal oldali helyett jobb oldali is.

A definíció alapján, ha b az a bal oldali inverze, akkor a a b jobb oldali inverze és fordítva.

Additív struktúra esetén (bal oldali) egységelem helyett (**bal oldali**) **nullelem**et, (bal oldali) inverz helyett (**bal oldali**) **ellentett**et is szokás mondani. Gyakori, és elvileg jobb elnevezés, ha egységelem helyett **semleges elem**et vagy **neutrális elem**et mondunk, illetve adott esetben hasonló megnevezést használunk a bal oldali hasonló esetben. Felhívjuk a figyelmet a zéruselem és a nullelem közötti különbségre. Egy binér művelet esetén lehetséges, hogy nincs bal oldali egységelem, lehet, hogy pontosan egy ilyen elem van, lehetséges egynél több, de véges számú bal oldali egységelem, végtelen A esetén lehet végtelen sok bal oldali egységelem, végül mind véges, mind végtelen A esetén lehetséges, hogy A minden eleme bal oldali egységelem. Ám, ha létezik mind bal, mind jobb oldali egységelem, akkor ezek szükségszerűen azonosak, vagyis ekkor ez egységelem, és ekkor pontosan egy egységelem van, tehát, ha van egységelem, akkor egyetlen egységelem van és ekkor nincs más bal vagy jobb oldali egységelem. Az előbbiek értelemszerűen igazak a bal oldali zéruselemre és zéruselemre.

Az a elem inverzét – amennyiben létezik – általában a^{-1}, ellentettjét $-a$ jelöli. Megint az igaz, hogy egy elemnek lehet, hogy nincs bal oldali inverze, lehet, hogy egy, vagy egynél több, de véges sok, vagy végtelen sok bal oldali inverze van, és lehet, hogy a halmaz minden eleme bal oldali inverze. Az is lehetséges, hogy van bal oldali és jobb oldali inverze, amelyek nem egyenlőek, és az is lehetséges, hogy mindkét oldalról több különböző inverze van. *Ha* azonban *a szorzás asszociatív*, és van a-nak mind bal oldali, mind jobb oldali inverze, akkor ez a két elem azonos, tehát inverze a-nak, és ekkor a-nak ezen kívül nem lehet sem bal oldali, sem jobb oldali inverze, és így az inverz, ha létezik, egyértelmű.

Ha egy asszociatív szorzásnak van egységeleme, akkor értelmezzük a **nullatényezős szorzat**ot vagy **üres szorzat**ot is, amely definíciószerűen a struktúra egységelemével egyenlő, illetve additív művelet esetén az **üres összeg**et, amelyet a nullelemmel azonosítunk.

Asszociatív művelet esetén külön neve van az olyan műveletnek, amelyben az operandusok azonosak: az olyan n-tényezős szorzat, ahol n egy pozitív egész szám, és amelynek minden tényezője a, az a n-**edik hatványa**, és a jele a^n, ahol a a (**hatvány**) **alap**(**ja**), n a (**hatvány**) **kitevő**(**je**), és a^n a **hatvány**. Amennyiben a szorzás egységelemes, akkor a korábbiak szerint értelmezzük az üres szorzatot, amelynek 0 számú tényezője van, ennek megfelelően $a^0 = e$, ha e jelöli az egységelemet. Asszociatív szorzás esetén, ha két elemnek van inverze, akkor a szorzatuknak is van, és $(ab)^{-1} = b^{-1}a^{-1}$ (vagyis nem a

megszokott formában teljesül az egyenlőség, kivéve, ha a és b felcserélhető). Végül, ha a-nak van inverze (ekkor biztosan van egységelem), akkor definiáljuk a negatív egész kitevős hatványát is úgy, hogy ha $n < 0$, akkor $a^n = (a^{-n})^{-1}$ (ez az elem létezik, mert a zárójelben álló szorzat minden elemének létezik inverze, és a szorzat megegyező elemei felcserélhetőek). A hatványra teljesül a megszokott $a^{m+n} = a^m a^n$ és $(a^m)^n = a^{mn} = (a^n)^m$ egyenlőség, de $(ab)^n = a^n b^n$ általában nem (de nyilván teljesül, ha a és b felcserélhető). Az előbbiek értelemszerűen átírhatóak additív írásmód esetén, ekkor a^n helyett na-t írunk (ez általában nem egy szorzat, hanem egy olyan összeg, amelynek minden tagja a, és az összegnek n tagja van, illetve negatív n esetén egy $-n$-tagú összeg ellentettje!), és most n neve **együttható**.

Könnyű ellenőrizni, hogy

- a akkor és csak akkor balról reguláris, ha $ab = ac$-ből következik $b = c$, ekkor **a-val balról egyszerűsíthetünk** (illetve additív írásmód esetén **a-t balról törölhetjük**);
- bal oldali egységelem balról reguláris;
- bal oldali zéruselem csak akkor balról reguláris, ha A-nak csak egy eleme van;
- ha a művelet egységelemes, és a jobbról invertálható, akkor a-nak van jobb oldali inverze;
- bal oldali egységelem jobbról invertálható;
- bal oldali zéruselem csak akkor invertálható jobbról, ha A-nak csak egy eleme van;
- véges A esetén a pontosan akkor balról reguláris, ha jobbról invertálható;

A második és harmadik tulajdonság alapján, ha A-nak legalább két eleme van, akkor egy elem nem lehet egyszerre bal oldali zéruselem és bal oldali neutrális elem.

Ha a művelet asszociatív, akkor még

- a-val felcserélhető elemek szorzata is felcserélhető a-val;
- balról reguláris elemek szorzata is balról reguláris;
- ha a-nak van bal oldali inverze, akkor a balról reguláris;
- ha a balról reguláris, és létezik jobb oldali inverze, akkor ez is balról reguláris;
- jobbról invertálható elemek szorzata jobbról invertálható;
- ha a-nak van jobb oldali inverze, akkor jobbról invertálható;
- ha a jobbról invertálható, és van bal oldali inverze, akkor ez is jobbról invertálható.

Említünk még néhány további tulajdonságot, feltéve, hogy a művelet asszociatív:

- ha van balról reguláris elem, és valamelyikükhöz, mondjuk a-hoz olyan e, amellyel $a = ae$, akkor e bal oldali egységelem: tetszőleges u-val $au = (ae)u = a(eu)$, és innen $u = eu$;
- ha e bal oldali egységelem, és van jobbról reguláris elem, akkor e egységelem: bármely a elemmel $a = ea$, így, ha a jobbról reguláris, akkor az előző ponthoz hasonlóan e jobb oldali egységelem, tehát egységelem;
- ha a jobbról reguláris, és van bal oldali inverze, akkor van inverze, és ekkor a reguláris és invertálható: ha a bal oldali inverze a', akkor $ea = ae = a(a'a) = (aa')a$, tehát $aa' = e$, így a' jobb oldali inverz, és ekkor a jobbról invertálható, ha pedig van bal oldali inverz, akkor balról reguláris és invertálható a;
- ha $c = ab$ jobbról reguláris, akkor a jobbról reguláris: $ua = va$-ból $uc = u(ab) = (ua)b = (va)b = v(ab) = vc$, és így $u = v$;
- ha $c = ab$ balról invertálható, akkor b balról invertálható: ha $v = uc = u(ab) = (ua)b$, akkor ua megoldása a $v = xb$ egyenletnek.

Az n-változós f művelet esetén a **idempotens**, vagy f **megőrzi** a-**t**, ha $f(a, \dots, a) = a$, és a művelet idempotens, ha a halmaz minden eleme idempotens a műveletre. Egyszerűen látható, hogy egy

binér műveletre nézve bal oldali egységelem és bal oldali zéruselem mindig idempotens, és asszociatív művelet esetén egy balról reguláris elem csak akkor idempotens, ha bal oldali egységelem.

Igen fontosak az asszociatív binér műveletek.

1.4. Definíció

$\mathcal{A} = (A;\cdot)$ **grupoid**, ha A nem üres és · binér művelet. A grupoid **félcsoport**, ha · asszociatív, és a félcsoport **csoport**, ha egységelemes, és minden elemnek van inverze. Kommutatív csoport neve **Abel-csoport**.

Δ

Félcsoportot leggyakrabban $\mathcal{S}$-sel (semigroup), míg csoportot $\mathcal{G}$-vel (*g*roup), Abel-csoportot $\mathcal{A}$-val jelölünk, és ekkor a művelet általában az összeadás.

1.5. Tétel

Az alábbi állítások ekvivalensek:

- $\mathcal{G}$ félcsoport, amelyben van olyan e_b bal oldali egységelem és minden a-elemhez olyan a_b elem, amellyel $a_b a = e_b$;
- $\mathcal{G}$ csoport;
- $\mathcal{G}$ félcsoport, és G minden eleme reguláris és invertálható;
- $\mathcal{G}$ félcsoport, és G minden eleme invertálható.

Δ

A fenti, egymással ekvivalens állítások bármelyikét tekinthetjük a csoport definíciójának.

Az egyetlen elem által generált csoport a **ciklikus csoport**, ennek elemei a generátorelem hatványai. Ha egy ciklikus csoport rendje n, akkor a csoport elemei a generátorelem n-nél kisebb nemnegatív egész kitevős hatványai. Ekkor $a^n = e$, feltéve, hogy a generátorelem a, és n a legkisebb olyan k pozitív egész kitevő, amellyel $a^k = e$. Csoport esetén definiáljuk a g **elem** $|g|$ (vagy $o(g)$) **rendjét**, ami az elem által generált ciklikus részcsoport rendje. Ez lehet végtelen, ekkor a ciklikus csoport elemei a generátorelem egész kitevős hatványai, és két hatvány akkor és csak akkor egyenlő, ha a kitevők azonosak, és lehet véges. Ha a generált részcsoport véges, akkor a részcsoport rendje az előbbiek szerint egyben a legkisebb pozitív egész kitevő, amelyre emelve az elemet, az egységelemet kapjuk. Az elem rendjét ezzel a tulajdonsággal is definiálhatjuk, azzal a kiegészítéssel, hogy a rend végtelen, ha az elem egyetlen pozitív egész kitevős hatványa sem azonos a csoport egységelemével.

Könnyen be lehet látni, hogy ciklikus csoport minden részcsoportja ciklikus.

Csoport részstruktúrája a **részcsoport**. Maga $\mathcal{G}$, valamint a csak az egységelemből álló részhalmaz részcsoport, ezek **a csoport triviális részcsoportjai**, és (ha létezik,) a többi részcsoport **a csoport nem triviális részcsoportja.** Legyen $\mathcal{G}$ csoport, és legyen $\emptyset \neq H \subseteq G$. Ekkor $\mathcal{H} \leq \mathcal{G}$ pontosan akkor teljesül, ha $HH^{-1} \subseteq H$ (illetve additív művelet esetén ha $H - H \subseteq H$), ahol H^{-1} a H elemeinek inverzeiből álló halmaz. (Általában, ha A a $\mathcal{G}$ csoport tartóhalmazának nem üres részcsoportja, akkor A a $\mathcal{G}$ egy **komplexus**a, és az A és B komplexus ebben a sorrendben vett AB szorzata az A-beli a és B-beli b elemek szorzatának halmaza. Amennyiben A-nak egyetlen eleme van, akkor $\{a\}B$ helyett röviden aB-t írunk.) Ha $\mathcal{H} \leq \mathcal{G}$, akkor G bármely a és b eleme esetén egyértelmű, hogy $a^{-1}b$ eleme-e H-nak, vagyis ez egy binér reláció G-n. A reláció reflexív, szimmetrikus és tranzitív, így osztályoz. Az a-val reprezentált osztály aH, a $\mathcal{G}$ $\mathcal{H}$ **szerinti, a-val reprezentált bal oldali mellékosztálya**, és hasonlóan definiáljuk a jobb oldali mellékosztályokat is. aH számossága azonos H számosságával, és $aH \mapsto Ha^{-1}$ egy bijekció az ugyanazon részcsoport szerinti bal oldali és jobb oldali mellékosztályok halmaza között. Mindezek

alapján definiáljuk a $\mathcal{H}$ **részcsoport** ($\mathcal{G}$-beli) $|\mathcal{G}:\mathcal{H}|$ **indexét**, mint a $\mathcal{G}$ $\mathcal{H}$ szerinti bal oldali mellékosztályai halmazának számosságát. Véges csoportok egy fontos tulajdonságát mondja ki a **Lagrange-tétel**, amely szerint véges csoport részcsoportja rendjének és indexének szorzata a csoport rendje, vagyis $|\mathcal{G}| = |\mathcal{H}||\mathcal{G}:\mathcal{H}|$, és így a részcsoport rendje és indexe osztója a csoport rendjének. Fontos következmény, hogy véges csoportban minden elem rendje osztója a csoport rendjének (amiből például következik, hogy prímszámrendű csoport ciklikus, amelynek nincs nem triviális részcsoportja), és ha a csoport rendje n, akkor $g^n = e$ a csoport minden g elemére.

A $\mathcal{G}$ csoport egy $\mathcal{H}$ részcsoportja szerinti osztályozás akkor és csak akkor kompatibilis a csoport műveletével, ha a G minden a elemével $aH = Ha$. Ez a feltétel sok más alakban is megfogalmazható, az egyik ilyen ekvivalens feltétel, hogy minden G-beli a-val $aHa^{-1} \subseteq H$. Az ilyen tulajdonságú részcsoport egy **normális részcsoport**, **normálosztó**, **invariáns részcsoport** illetve **invariáns osztó.** Mivel normális részcsoport esetén a részcsoport szerinti osztályozás kompatibilis a csoport műveletével, ezért a normális részcsoport szerinti osztályok az osztályokon a reprezentánsok által meghatározott szorzással egy faktorstruktúrát, a **faktorcsoport**ot definiálják. Ennek rendje a részcsoport indexe.

Ha φ a $\mathcal{G}$ félcsoportnak a $\mathcal{T}$ grupoidba való műveletartó leképezése, és $H = \mathrm{Im}(\varphi)$, akkor H-ban a $\mathcal{T}$-beli művelet asszociatív, tehát H félcsoport ezzel a művelettel. Ha $\mathcal{G}$ csoport az e egységelemmel, akkor e képe a kép egységeleme, inverz képe a kép inverze, így csoport homomorf képe csoport. Ekkor a leképezés magjában az e-t tartalmazó osztály $\mathcal{G}$ egy $\mathcal{N}$ normális részcsoportja, és egy-egy osztály egy $\mathcal{N}$ szerinti mellékosztály, vagyis ekkor a leképezés magját egyértelműen meghatározza N. Csoportok esetén így definiáljuk a leképezés magját, és ekkor $\mathcal{G}/\mathcal{N} \cong \mathcal{H}$.

Fontos csoportot alkotnak a $\mathrm{modulo}\ m$ maradékosztályok az összeadással, illetve a redukált maradékosztályok a szorzással (az összes maradékosztály a szorzással félcsoportot alkot). A maradékosztályokon a műveleteket a reprezentánsokkal definiáljuk. Tekintettel arra, hogy az egész számok halmazán értelmezett $\mathrm{modulo}\ m$ kongruencia ekvivalencia-reláció $\mathbb{Z}$-n, és ez mind az összeadással, mind a szorzással kompatibilis, így a reprezentánsokkal való definíció valóban binér műveleteket eredményez. A létrejött két struktúra $(\mathbb{Z}_m; +)$ és $(\mathbb{Z}_m^*; \cdot)$. A definíció alapján bármely a és b egész szám esetén $a \equiv b\ (m)$ pontosan akkor igaz, ha $\bar{a} = \bar{b}$, $a + b \equiv c\ (m)$, ha $\bar{a} + \bar{b} = \bar{c}$, és $ab \equiv c\ (m)$, ha $\bar{a}\bar{b} = \bar{c}$ (ez utóbbi nem csak a redukált maradékosztályok esetén igaz). Ez azt jelenti, hogy a kongrueniáról mindig áttérhetünk a reprezentánsokkal megadott osztályok egyenlőségére és fordítva.

Ha $\mathcal{S}$ egységelemes félcsoport, akkor az invertálható elemei a félcsoport egy részcsoportját alkotják: a halmaz tartalmazza az egységelemet, tehát nem üres, és invertálható elemek szorzata, valamint invettálható elem inverze is invertálható. Az $\mathcal{S}$ egységelemes félcsoport ezen részcsoportja a félcsoport **egységcsoportja**, elemei a félcsoport **egység**ei. Csoportban nyilván minden elem egység.

1.6. Tétel

Legyen $(\mathcal{G};\cdot)$ csoport, g a csoport n-edrendű eleme, és e a csoport egységeleme. Ekkor

a) tetszőleges $u \in \mathbb{Z}$-re $g^u = e$ akkor és csak akkor, ha $n|u$;
b) bármely u és v egész számra $g^u = g^v$ akkor és csak akkor, ha $u \equiv v\ (n)$;
c) $n > k \in \mathbb{N}$-re a g^k elemek páronként különbözőek, és minden m egész számhoz van olyan egyértelműen meghatározott $n > j \in \mathbb{N}$, hogy $g^m = g^j$;
d) $|g^m| = \frac{n}{(m,n)}$;
e) $|g^m| = |g| \Leftrightarrow (m, n) = 1$, és ekkor tetszőleges k egész számra $\left|\left(g^k\right)^m\right| = \left|g^k\right|$;
f) ha $\mathcal{G}$ véges csoport, akkor $n\big||G|$;
g) tetszőleges u és v egész számra $|g^{uv}||(|g^u|, |g^v|)$.

Δ

Bizonyítás:

a) Ha $n|u$, akkor $u = rn$ egy r egész számmal, és ekkor $g^u = g^{rn} = (g^n)^r = e^r = e$. Fordítva, legyen $g^u = e$. Ha $u = rn + s$, ahol $n > s \in \mathbb{N}$, akkor $e = g^u = g^{rn+s} = (g^n)^r g^s = g^s$. Mivel n a legkisebb pozitív egész, amely kitevős hatványa g-nek az egységelem, ezért s nem lehet pozitív egész szám, így $s = 0$, de akkor $u = rn$, azaz $n|u$.

b) $g^u = g^v$-ből $g^{v-u} = g^0 = e$, és így a) alapján $n|v - u$, azaz $u \equiv v\ (n)$.

c) Ha i és j olyan egész számok, hogy $0 \leq i < j < n$, akkor $0 < j - i < n$, így, ha $n|j - i$, akkor $i = j$, amiből következik az állítás első fele. Az állítás második része egyszerű következménye annak, hogy bármely u egész számra $0 \leq u \bmod n \equiv u\ (n)$, és $u \bmod n$ egyértelműen meghatározott.

d) $e = (g^m)^l = g^{ml}$ akkor és csak akkor igaz az l egész számra, ha $n|ml$, ami viszont pontosan akkor teljesül, ha $\frac{n}{(m,n)} \Big| l$. A legkisebb ilyen pozitív egész $\frac{n}{(m,n)}$, tehát ez lesz g^m rendje.

e) Az előbbi pont alapján $|g^m| = \frac{n}{(m,n)}$, és ez pontosan akkor egyenlő n-nel, ha a nevező 1. Az állítás második fele pedig következik abból, hogy ha $(m, n) = 1$, akkor $(km, n) = (k, n)$.

f) Ez következik a Lagrange-tételből.

g) Legyen a g^u, g^v és g^{uv} elemek rendje az előbbi sorrendben r, s és t. Ekkor $(g^v)^s = e$, így $e = e^u = ((g^v)^s)^u = g^{suv} = (g^{uv})^s$, tehát $t|s$. Hasonlóan kapjuk a $t|r$ oszthatóságot, amiből következik, hogy t osztója r és s legnagyobb közös osztójának.

□

$\mathbb{Z}_m$ az összeadással csoport, a szorzással félcsoport, és a redukált maradékosztályok az utóbbi félcsoportban csoportot alkotnak, így a korábbiakkal összhangban van az alábbi definíció.

1.7. Definíció

$o_m^+(i) = \min\{k \in \mathbb{N}^+ | ki \equiv 0\ (m)\}$ az i **additív** és $o_m(i) = \min\{k \in \mathbb{N}^+ \big| i^k \equiv 1\ (m)\}$ – ha létezik – az i (**multiplikatív**) **rendje** modulo m, ahol $m \in \mathbb{N}^+$ és $i \in \mathbb{Z}$.

Δ

Az előbbi tételt alkalmazva kapjuk a következő eredményeket.

1.8. Tétel

Minden $m \in \mathbb{N}^+$ és $i \in \mathbb{Z}$ esetén létezik és egyértelmű $o_m^+(i)$, továbbá $o_m^+(i) = \frac{m}{(i,m)}$.

Δ

1.9. Következmény

Legyen m természetes szám, i, j és k egész számok. Ekkor

- $ji \equiv ki\ (m) \Leftrightarrow j \equiv k\ \left(o_m^+(i)\right)$;
- $ji \equiv 0\ (m) \Leftrightarrow o_m^+(i)|j$;
- $o_m^+(i)|m$, és $o_m^+(i) = m$ akkor és csak akkor, ha $(i, m) = 1$;
- $o_m^+(ki)\big|\left(o_m^+(k), o_m^+(i)\right)$;
- pontosan akkor lesz minden $u \in \mathbb{Z}$-vel $o_m^+(ku) = o_m^+(u)$, ha $(k, m) = 1$.

Δ

A multiplikatív tulajdonsággal kapcsolatban az alábbi megállapítás tehető.

1.10. Tétel

Akkor és csak akkor létezik n modulo m rendje, ha $(m,n)=1$. Ekkor a j és k nemnegatív egészre $n^j \equiv n^k\ (m)$ pontosan akkor igaz, ha $j \equiv k\ \left(o_m(n)\right)$ (speciálisan $n^i \equiv 1\ (m)$ pontosan akkor teljesül, ha $o_m(n)$ osztója i-nek), végül $o_m(n)|\varphi(m)$.

Δ

Az első állítás azért igaz, mert ha m és n nem relatív prímek, akkor n bármely pozitív egész kitevős hatványának van 1-nél nagyobb közös osztója m-mel, de akkor a hozzá relatív prím eggyel kisebb szám nem lehet osztható m-mel, így az n egyetlen pozitív egész kitevős hatványa sem lehet kongruens 1-gyel modulo m, míg ha n relatív prím m-hez, akkor az Euler-Fermat tétel szerint $n^{\varphi(m)} \equiv 1\ (m)$.

Számelméletből ismeretes az összegzési függvény és ennek megfordítása. Most ezt általánosítjuk. Emlékeztetőül, $n \in \mathbb{N}^+$-ra a Moebius-függvény értéke az n pontban 0, ha n-nek van prímnégyzet osztója, és az ellenkező esetben $(-1)^r$, ahol r az n prímtényezőinek száma.

1.11. Tétel

Legyen $\mathcal{S}$ a $\mathcal{G}=(G;+)$ kommutatív csoport részfélcsoportja. Ha f az $\mathbb{N}^+$-t S-be képezi, akkor $F(n)=\sum_{d|n} f(d)$ egy $F\colon \mathbb{N}^+ \to S$ függvény, és $\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$ a $\mathcal{G}$ műveleteivel. Fordítva, az $\mathbb{N}^+$-t S-be képező F függvényre $\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ egy $F\colon \mathbb{N}^+ \to G$ függvény, és $F(n)=\sum_{d|n} f(d)$ a $\mathcal{G}$-beli művelettel.

Δ

Bizonyítás:

$f(d)$ minden $d \in \mathbb{N}^+$-ra S-beli, és mivel $\mathcal{S}$ félcsoport az összeadással, ezért $F(n)$ is eleme S-nek. A kifejezés minden természetes számra értelmezett, továbbá az $\mathcal{S}$-beli művelet egyértelmű, így valóban függvényt definiál az összeg, egy olyan függvényt, amely $\mathbb{N}^+$-t képezi S-be.

Legyen $d|n \in \mathbb{N}^+$ és $\frac{n}{d}=m$. Ekkor $d=\frac{n}{m}$, és $\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$, hiszen különböző d-hez különböző m tartozik, továbbá

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \left(\mu\left(\frac{n}{d}\right) \sum_{d'|d} f(d') \right) = \sum_{d'|n} \left(f(d') \sum_{t\left|\frac{n}{d'}\right.} \mu(t) \right) = f(n),$$

ugyanis a Moebius-függvényt egy adott n pozitív egész szám osztóin kiszámítva és ezeket az értékeket összeadva, az összeg akkor és csak akkor különbözik 0-tól, ha $n=1$, és ekkor az összeg értéke 1, ez pedig esetünkben pontosan akkor teljesül, ha $d'=n$.

Az ellenkező irány esetén azt, hogy f a természetes számokat G-be képező függvény, hasonlóan láthatjuk be, mint az előbb F-ről, hogy $\mathbb{N}^+$-t képezi S-be, míg ha $f(n)=\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$, akkor

$$\sum_{d|n} f(d) = \sum_{d|n} \left(\sum_{d'|d} \mu\left(\frac{n}{d'}\right) F(d') \right) = \sum_{d'|n} \left(F(d') \sum_{d\left|\frac{n}{d'}\right.} \mu(d) \right) = F(n),$$

azaz F-ből indulva, f-en keresztül visszajutunk F-hez.

□

1.12. Kiegészítés

Legyen $\mathcal{S}$ a $\mathcal{G} = (G;\cdot)$ kommutatív csoport részfélcsoportja. Ha f az $\mathbb{N}^+$-t S-be képezi, akkor $F(n) = \prod_{d|n} f(d)$ egy $F\colon \mathbb{N}^+ \to S$ függvény, és $f(n) = \prod_{d|n}\big(F(d)\big)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n}\left(F\left(\frac{n}{d}\right)\right)^{\mu(d)}$ a $\mathcal{G}$-beli szorzással, míg $F\colon \mathbb{N}^+ \to S$ esetén $f(n) = \prod_{d|n}\left(F\left(\frac{n}{d}\right)\right)^{\mu(d)}$ $\left(= \prod_{d|n}\big(F(d)\big)^{\mu\left(\frac{n}{d}\right)}\right)$ egy $F\colon \mathbb{N}^+ \to G$ függvény, és $F(n) = \prod_{d|n} f(d)$ a $\mathcal{G}$ műveletével.

Δ

Ez az előző tételből kapható, összeadás helyett szorzást, együttható helyett kitevőt írva.

1.13. Megjegyzés

Az előző kiegészítés megfelelő része szerint az $u = \prod_{\substack{d|n \\ \mu(d)=1}} F\left(\frac{n}{d}\right)$ és $v = \prod_{\substack{d|n \\ \mu(d)=-1}} F\left(\frac{n}{d}\right)$ jelöléssel az S bármely ilyen u és v elemére a $vx = u$ egyenletnek van S-ben megoldása (és ekkor $\mathcal{S}$ regularitása miatt csupán egy megoldása), és ez éppen $f(n)$, és hasonló a helyzet az additív esetben is, ha a produktumjelet szummajelre cseréljük, és $vx = u$ helyett $v + x = u$-t írunk. Ha $\mathcal{R}$ gyűrű, akkor additív csoportjában az additív alak érvényes, és ha $\mathcal{R}$ kommutatív, és f a gyűrű reguláris elemeinek félcsoportjába képez, akkor a multiplikatív alak is alkalmazható, hiszen ekkor $\mathcal{R}$ beágyazható olyan gyűrűbe, amelyben a reguláris elemeknek van inverzük.

Δ

1.14. Definíció

1.11.-ben és 1.12.-ben F az f **összegzési** illetve **szorzatfüggvénye**, és f az F (**additív** illetve **multiplikatív**) **Moebius-transzformáltja**. Az $F \mapsto f$ hozzárendelés a **megfordítási képlet**.

Δ

A kétműveletes struktúrák közül különösen fontosak a **gyűrű**k, amelyeket leggyakrabban $\mathcal{R}$-rel jelölünk (*r*ing). A gyűrű „prototípusa" az egész számok halmaza az összeadással és a szorzással. A két műveletet összeköti a disztributivitás. Általában is igaz, hogy több művelet esetén csak akkor kapunk az egy-egy művelethez kapcsolódó tulajdonságokon túli új eredményeket, ha valami összekapcsolja az egyes műveleteket. Vagyis nincs értelme olyan struktúrákat vizsgálni, ahol a műveletek halmaza egynél több osztályra bontható úgy, hogy az egyes osztályok műveletei között semmi összefüggés sincs.

1.15. Definíció

$\mathcal{R} = (R; +,\cdot)$ gyűrű, ha $(R; +)$ Abel-csoport, $(R;\cdot)$ félcsoport, és a szorzás mindkét oldalról **disztributív** az összeadásra nézve, azaz $a(b + c) = ab + ac$ és $(b + c)a = ba + ca$ a gyűrű tetszőleges a, b és c elemeire.

Δ

A disztributivitás két feltétele kommutatív szorzás esetén nyilván egybeesik, ám ha a szorzás nem kommutatív, akkor az egyik teljesülhet anélkül, hogy a másik is igaz lenne a gyűrű bármely elemhármasára. Gyűrűben az összeadás semleges eleme, a **nulla**, amit általában 0 jelöl, egyben zéruseleme a szorzásnak, vagyis a gyűrű minden r elemével $0 \cdot r = 0 = r \cdot 0$ (amennyiben csak az egyik oldali disztributivitás teljesül, akkor az utóbbi egyenlőségek közül csak az egyik igaz, mégpedig bal oldali disztributivitás esetén 0 jobb oldali zéruselem, és fordítva!). A disztributivitás általában is igaz egy gyűrűben, azaz $\prod_{i=1}^{m}\sum_{j=1}^{n_i} a_j^{(i)} = \sum_{\mathbf{j}\in I}\prod_{i=1}^{m} a_{j_i}^{(i)}$, ahol $\mathbf{j} = (j_1, \dots, j_m)$, és minden i-re $n_i \geq j_i \in \mathbb{N}^+$. A disztributivitás alapján $(mr)s = m(rs) = r(ms)$ és $m(nr) = (mn)r = n(mr)$, ahol r és s a gyűrű elemei és m,

n egész számok, és ebből például $(mr)(ns) = (mn)(rs) = (nr)(ms)$, vagyis szorzatban az együtthatók kiemelhetőek és bevihetőek bármely tényező mellől illetve mellé.

A gyűrű mindkét műveletre zárt, nem üres részhalmaza a gyűrű **részgyűrű**je. A csoporthoz hasonlóan definiáljuk a **valódi** és **nem valódi**, a **triviális** és **nem triviális részgyűrű**ket.

Könnyen látható, hogy bármely additív Abel-csoportra építhető gyűrű úgy, hogy bármely két elem szorzatát az additív csoport neutrális elemével azonosítjuk. Ez a gyűrű a **zérógyűrű** (van olyan additív Abel-csoport, amelyre nem is lehet más gyűrűt építeni). Amennyiben a zérógyűrűnek egyetlen eleme van, akkor ez csak a nullelem lehet, és ekkor a gyűrűt **nullgyűrű**nek hívjuk.

A gyűrűben a nullával való szorzás eredménye a nulla, ám egy szorzat akkor is lehet nulla, ha egyik tényező sem nulla. Az ilyen elempárokat **nullosztópár**oknak hívjuk, és a bal oldali tényező **bal oldali nullosztó**, míg a másik egy **jobb oldali nullosztó**. Egy nem nulla elemmel akkor és csak akkor lehet balról egyszerűsíteni, ha nem bal oldali nullosztó, vagyis a balról reguláris elemek pontosan a nem nulla, balról nem nullosztó elemek. Balról reguláris elemek szorzata balról reguláris, és ha egy elemnek van jobb oldali inverze, akkor ez a jobb oldali inverz balról reguláris. Az is könnyen belátható, hogy ha egy elemnek van bal oldali inverze, akkor ez az elem balról reguláris.

Egy gyűrű **nullosztómentes**, ha nincs benne bal oldali nullosztó (és akkor jobb oldali sincs). Nullosztómentes gyűrű minden részgyűrűje is nullosztómentes a definíció alapján.

Amennyiben a gyűrűbeli szorzás kommutatív, akkor a gyűrű **kommutatív gyűrű,** ha van $\mathcal{R}$ multiplikatív félcsoportjában egységelem, akkor $\mathcal{R}$ **egységelemes gyűrű.** Kommutatív gyűrű minden részgyűrűje is kommutatív, ami azonnal következik a definícióból, ám egységelemesség szempontjából más a helyzet. Nem nehéz példát találni arra, hogy egy gyűrű és részgyűrűje egyszerre lehet egységelemes azonos vagy akár különböző egységelemmel, lehet, hogy kettőjük közül bármelyikben, de csak az egyikben van egységelem, végül az is lehetséges, hogy egyikben sincs egységelem.

Gyűrűkre igen fontos példák az egész számok, a racionális, a valós és a komplex számok halmaza a szokásos összeadással és szorzással, illetve tetszőleges, 1-nél nagyobb pozitív egész m-re a $\mathrm{modulo}\ m$ maradékosztályok halmaza az osztályokra a reprezentánsokkal definiált műveletekkel. Ezek mindegyike kommutatív és egységelemes, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ és $\mathbb{C}$ nullosztómentes, ám $\mathbb{Z}_{\boldsymbol{m}}$ akkor és csak akkor nullosztómentes, ha m felbonthatatlan, azaz ha prímszám.

1.16. Definíció

A legalább kételemű, kommutatív, nullosztómentes gyűrű **integritási tartomány**. Ha egy gyűrű nem nulla elemei a szorzással csoportot alkotnak, akkor **ferdetest**, és ez **test**, ha a szorzás kommutatív.

Δ

$\mathbb{Z}$ tehát integritási tartomány, $\mathbb{Q}$, $\mathbb{R}$ és $\mathbb{C}$ test, és $\mathbb{Z}_{\boldsymbol{m}}$ pontosan akkor test, amikor m prímszám. Ferdetestet alkotnak például a kvaterniók.

Nem mindig kötik ki, hogy integritási tartománynak legyen legalább két eleme. A testet általában $\mathcal{K}$-val, néha $\mathcal{F}$-fel jelöljük (*K*örper illetve *f*ield). A definíció alapján ferdetestnek, és így testnek is, legalább két eleme van, és nullosztómentes, így egy test mindig integritási tartomány (de fordítva nem igaz, amire példa az egyik legfontosabb integritási tartomány, az egész számok gyűrűje).

Nullosztómentes gyűrűkben a nem nulla elemek additív rendje, vagyis az additív csoportbeli rendje azonos, és ha ez a közös érték nem végtelen, akkor prímszám. Ez alkalmat ad az ilyen gyűrűkben egy új fogalom bevezetésére.

1.17. Definíció

Legyen $\mathcal{R}$ egy legalább kételemű, nullosztómentes gyűrű. Ha a gyűrű nem nulla elemeinek additív rendje a p prímszám, akkor **a gyűrű karakterisztikája** p, különben 0.

Δ

A definícióból következik, hogy nullosztómentes gyűrű legalább kételemű részgyűrűjének karakterisztikája azonos a teljes gyűrű karakterisztikájával.

Félcsoport, és így csoport és gyűrű esetén is fontosak a minden elemmel felcserélhető elemek.

1.18. Definíció

Az $\mathcal{S}$ **félcsoport centruma** $C = \{s \in \mathcal{S} | \forall (u \in S): su = us\}$. **Csoport centruma** a csoport mint félcsoport centruma, míg **gyűrű centruma** a gyűrű multiplikatív félcsoportjának centruma.

Δ

1.19. Tétel

Félcsoport centruma zárt a félcsoport műveletére. Egységelem és zéruselem – ha létezik – mindig eleme a centrumnak. Csoport centruma a félcsoport-művelet megszorításával normális részcsoport, míg gyűrű centruma a gyűrűműveletek megszorításával részgyűrű.

Δ

Bizonyítás:

a) Ha u és v eleme C-nek, akkor $(uv)s = u(vs) = u(sv) = (us)v = (su)v = s(uv)$ a félcsoport tetszőleges s elemével, ami mutatja C műveleti zártságát.

b) Ha e egységelem és z zéruselem a félcsoportban, akkor $es = s = se$ és $zs = z = sz$ a félcsoport bármely s elemével, vagyis e és z eleme a centrumnak.

c) b) szerint csoport illetve gyűrű centruma nem üres, így a) alapján a művelet (gyűrű esetén a szorzás) megszorításával C részfélcsoport. Ha $\mathcal{S}$ csoport, akkor u-nak van inverze, és $us = su$-ból $su^{-1} = u^{-1}s$, így $u^{-1} \in C$, C részcsoport. Ezen túl még $sus^{-1} = (su)s^{-1} = (us)s^{-1} = u(ss^{-1}) = ue = u$, tehát $sCs^{-1} = C$, C normális részcsoport $\mathcal{S}$-ben. Gyűrű esetén $(u - v)s = us - vs = su - sv = s(u - v)$ az S valamennyi s elemével, tehát $u - v$ is a centrumban van, így C mind a szorzásra, mind a kivonásra zárt, ennélfogva a műveletek C-re való megszorításával részgyűrű.

□

Ahogy egész számokból megkonstruálható a racionális számok teste, ugyanígy lehet egy integritási tartományt testbe ágyazni. Ennél általánosabb, ha az $\mathcal{R}$ gyűrűt olyan $\mathcal{S}$ gyűrűbe ágyazzuk be, ahol $\mathcal{R}$ minden reguláris centrumelemének van inverze. A legszűkebb ilyen gyűrűt a következőképpen kapjuk. Legyen M az $\mathcal{R}$ reguláris centrumelemeinek halmaza, és legyen $T = R \times M$. Tekintsük az $(r_1, m_1) \oplus (r_2, m_2) = (r_1 m_2 + r_2 m_1, m_1 m_2)$ és $(r_1, m_1) \otimes (r_2, m_2) = (r_1 r_2, m_1 m_2)$ szabályokat (könnyű észrevenni, hogy ezek éppen a racionális számok összeadásának és szorzásának szabályai). Ha ρ olyan, hogy $(r_1, m_1)\rho(r_2, m_2) \Leftrightarrow (r_1 m_2 = r_2 m_1)$, akkor ρ ekvivalencia-relációt definiál T-n, amelyben minden $m \in M$-re az (m, m) elemek egy osztályban vannak. Kevés számolással belátható, hogy ρ kompatibilis mindkét művelettel, így tekinthetjük a megfelelő faktorstruktúrát. Ez a struktúra gyűrű, amelyben $e = \overline{(m, m)}$ egységelem. $r \mapsto \overline{(rm, m)}$ monomorfizmus, így az $\overline{(rm, m)}$ elemek azonosíthatóak R elemeivel, $\mathcal{R}$ beágyazható a kapott gyűrűbe. A továbbiakban a gyűrű műveleteit a szokásos módon jelöljük, és $\overline{(rm, m)}$ helyett r-et írunk. Most $m \cdot \overline{(m', mm')} = \overline{(mm', m')} \cdot \overline{(m', mm')} = \overline{(mm'^2, mm'^2)} = \overline{(m, m)} = e$, vagyis az eredeti gyűrű minden reguláris centrumelemének van inverze a faktorgyűrűben. Ha az m ezen inverzét m^{-1}-gyel jelöljük (ez általában nem eleme az eredeti gyűrűnek!), akkor $\overline{(r, m)} = rm^{-1}$ alakban írható az új gyűrű bármely eleme. Azt is könnyű belátni, hogy m és m^{-1} az új gyűrű minden elemével felcserélhető, vagyis eleme a bővebb gyűrű centrumának. Belátható, hogy minden olyan gyűrű, amely tartalmaz az $\mathcal{R}$-rel izomorf részgyűrűt, és amelyben az $\mathcal{R}$ reguláris centrumelemeinek megfelelő elemeknek van inverze, szükség szerint tartalmaz az előbb megkonstruált gyűrűvel izomorf részgyűrűt is.

Amennyiben $\mathcal{R}$ integritási tartomány, akkor minden nem nulla eleme reguláris centrumelem, így az előbb konstruált gyűrűben az $\mathcal{R}$ valamennyi nem nulla elemének van inverze, és a szorzás kommutatív, tehát testet kapunk, vagyis integritási tartomány mindig beágyazható testbe.

Gyűrűben a normális részcsoportnak megfelelő részstruktúra az **ideál.** Az R egy nem üres I részhalmaza **bal oldali ideál** az $\mathcal{R}$ gyűrűben, ha $I - I \subseteq I$ és $RI \subseteq I$ (vagyis a bal oldali ideál egyben részgyűrű, de ez fordítva általában nem igaz). Hasonlóan definiáljuk a **jobb oldali ideál**t, és az egyszerre bal és jobb oldali ideál az ideál. A gyűrű egy részhalmaza által generált (bal oldali) ideál a gyűrű legszűkebb, a megadott halmazt tartalmazó (bal oldali) ideálja. Az egyetlen elem által generált (bal oldali) ideál (**bal oldali**) **főideál**. Egységelemes gyűrűben a bal oldali főideál a generáló elemnek a gyűrű összes elemével balról vett szorzata, és ha a gyűrű kommutatív, akkor ez az adott elem által generált főideál. Ideál mint a gyűrű additív csoportjának részcsoportja normális részcsoport, hiszen az additív csoport kommutatív, és így minden bal oldali mellékosztály egyben jobb oldali is ugyanazon reprezentánssal, így az ideál osztályoz. Ez az osztályozás kompatibilis a gyűrű mindkét műveletével. Az ideál szerinti mellékosztályokat szokás **maradékosztály**oknak nevezni, és az ideál szerinti faktorgyűrűt **maradékosztály-gyűrű**nek. Ha r a gyűrű egy eleme, akkor az r által reprezentált maradékosztály az $r + I$ halmaz. A csak a 0-t tartalmazó halmaz valamint a teljes gyűrű ideál, a gyűrű **triviális ideál**jai, a többi ideál a **nem triviális ideál**. A gyűrű **nem valódi ideál**, minden más ideál **valódi ideál**.

Egy ideál **maximális**, ha valódi ideál, és a gyűrű egyetlen valódi ideáljának sem valódi része.

1.20. Tétel

Egységelemes kommutatív gyűrű maximális ideálja szerinti maradékosztály-gyűrű test.

Δ

A gyűrű-homomorfizmusra hasonló tételek érvényesek, mint a csoportoknál. Most is igaz, hogy gyűrűt összeg- és szorzattartó módon leképezve olyan kétműveletes struktúrába, amely külön-külön mindkét műveletre nézve grupoid, akkor a képe gyűrű, azon elemek, amelyek képe a képhalmaz nulleleme, ideált alkotnak, ez a leképezés magja, és pontosan azon elemek képe lesz azonos, amelyek az ideál szerinti azonos maradékosztályban vannak. Minden elemet leképezve az őt tartalmazó osztályra, egy epimorfizmust kapunk, és minden osztálynak megfeleltetve az osztály egy reprezentánsának képét, egy monomorfizmust kapunk. Ennek a két leképezésnek a szorzata megegyezik az eredeti leképezéssel, továbbá a mag szerinti maradékosztály-gyűrű izomorf lesz a képstruktúrával.

Mint ahogyan az egész számok mint speciális gyűrű esetén, úgy általában is, gyűrűk vizsgálatánál az egyik legfontosabb terület az **oszthatóság** kérdése.

1.21. Definíció

Az $\mathcal{R}$ gyűrű u eleme $w \in R$ **bal** (**jobb**) **oldali osztója**, ha $w = uv$ ($w = vu$), ahol $v \in R$, és u **osztója** w-nek, ha egyszerre bal és jobb oldali osztója. Ha u bal oldali osztója w-nek, akkor w az u **jobb oldali többszöröse**. A **bal oldali többszörös** és a **többszörös** definíciója hasonló.

Δ

Az alábbi tulajdonságok elég természetesek:

- a 0-nak minden elem osztója, és a 0 csak önmagának bal oldali osztója;
- ha u minden $n > i \in \mathbb{N}$-re bal oldali osztója w_i-nek, akkor $\sum_{i=0}^{n-1}(w_i r_i + m_i w_i)$-nek is bal oldali osztója, ahol az r_i-k a gyűrű elemei, míg az m_i-k egész számok;
- bal oldali egységelem (ha létezik) minden elemnek bal oldali osztója.

A második tulajdonságból következik, hogy ha u bal oldali osztója v-nek, és v bal oldali osztója w-nek, akkor u bal oldali osztója w-nek (az oszthatóság tranzitív). Amennyiben a gyűrűben van jobb oldali egységelem, akkor a balról való oszthatóság reflexív. Most tegyük fel, hogy r balról osztója s-nek, míg ez utóbbi bal oldali osztója r-nek. Ekkor $s = ru$ és $r = sv$, és r **és** s job**bról asszociált**, amit

$r\sim_j s$ jelöl. Ha a két elem **balról** is **asszociált**, akkor **asszociált,** jelölésben $r\sim s$. Amennyiben a balról osztható b-vel, akkor a minden jobb oldali asszociáltja osztható b bármely jobb oldali asszociáltjával, hiszen ekkor $a = bt$, $a' = au$ és $b = b'v$, ahol a' az a és b' a b egy jobb oldali asszociáltja, és így $a' = au = (bt)u = b(tu) = (b'v)(tu) = b'(vtu) = b't'$. A definíció alapján a jobb oldali asszociáltság szimmetrikus, és könnyen igazolható, hogy tranzitív is. Ha még deklaráljuk, hogy minden elem önmaga jobb oldali asszociáltja, akkor a jobb oldali asszociáltság ekvivalencia-reláció a gyűrű alaphalmazán.

Ha egy gyűrűben van egy s balról reguláris elem, és egy jobbról reguláris r elemhez van olyan ε gyűrűelem, hogy $r = \varepsilon r$, akkor ε egységelem. Ekkor ugyanis bármely u-val $ur = u(\varepsilon r) = (u\varepsilon)r$-ből, mivel r jobbról reguláris, $ur = u\varepsilon$, vagyis ε jobb oldali egységelem, és ekkor minden u-val teljesül az $su = (s\varepsilon)u = s(\varepsilon u)$ egyenlőség, ahonnan $u = \varepsilon u$, hiszen s-sel balról lehet egyszerűsíteni. Ez azt jelenti, hogy ε jobb oldali egységelem is, és így egységelem. Speciális esetként kapjuk, hogy nullosztómentes gyűrűben már egyetlen $r = \varepsilon r$ (vagy $r = r\varepsilon$) egyenlőségből következik, hogy ε egységelem, ha $r \neq 0$.

1.22. Definíció

A gyűrű egy u eleme **bal oldali egység** a gyűrűben, ha a gyűrű minden r elemének bal oldali osztója, és **egység**, ha egyszerre bal és jobb oldali egység.

Δ

Ha az $\mathcal{R}$ nullosztómentes gyűrűben van bal oldali egység, akkor a definíció előtti bekezdés alapján a gyűrű egységelemes. Legyen az egységelem e. Most az u bal oldali egység balról osztja e-t, tehát alkalmas u'-vel $e = uu'$, így u-nak van jobb oldali inverze, u'. Ám u' bal oldali inverze is u-nak, ugyanis $eu' = u' = u'e = u'(uu') = (u'u)u'$, és $\mathcal{R}$ nullosztó-mentessége következtében $u'u = e$. Ekkor viszont tetszőleges r-rel $r = re = r(u'u) = (ru')u = su$, u jobb oldali egység is, vagyis $\mathcal{R}$-ben minden bal oldali egység egység, és ha van egység, akkor van egységelem, és minden egységnek van inverze. Ez fordítva, sőt, még általánosabban is igaz, ha ugyanis egységelemes gyűrűben egy u elemnek van jobb oldali inverze, akkor $r = er = (uu')r = u(u'r) = us$, u bal oldali egység. Ez azt jelenti, hogy $\mathcal{R}$-ben éppen az invertálható elemek az egységek. Az egységelem, ha van, mindig egység, és $\mathcal{R}$-ben az egységelem osztói egységek, hiszen ezeknek az elemeknek van inverzük, így igaz az alábbi tétel.

1.23. Tétel

Nullosztómentes gyűrűben akkor és csak akkor van bal oldali egység, ha van egységelem. Ekkor minden bal oldali egység egység, és az egységek pontosan az invertálható elemek, vagyis az egységelem osztói.

Δ

A tétel alapján ferdetest, és így test minden nem nulla eleme egység, és fordítva, ha egy gyűrű minden nem nulla eleme egység, akkor a gyűrű ferdetest.

Legyen egy nullosztómentes gyűrűben r és s jobbról asszociált. Ekkor $r = su$ és $s = rv$-ből $se = s = s(uv)$, vagyis u és v egymás inverze, és így egységek. Fordítva, legyen $r = su$, ahol u egység, és legyen v az inverze. Ekkor $s = rv$, vagyis r és s kölcsönösen egymás bal oldali osztói, tehát jobbról asszociáltak. Mindez azt jelenti, hogy nullosztómentes gyűrű két eleme pontosan akkor jobbról asszociált, ha egyenlő, vagy egyik a másiktól csak egy jobb oldali egységtényezőben különbözik.

Az oszthatóság további vizsgálata során feltesszük, hogy a gyűrű kommutatív.

1.24. Definíció

Az $\mathcal{R}$ gyűrű nem üres A részhalmazának a gyűrű valamely c eleme **közös osztója**, ha osztója A minden a elemének, és d az A **legnagyobb közös osztója**, ha d az A közös osztója, és A minden közös

osztójának többszöröse. h az A **közös többszöröse**, ha A minden elemének többszöröse, és t az A **legkisebb közös többszöröse**, ha közös többszöröse A-nak, és osztója A minden közös többszörösének.

Δ

Mivel u akkor és csak akkor osztója v-nek, ha bármely asszociáltja osztója v valamennyi asszociáltjának, ezért a legnagyobb közös osztó és a legkisebb közös többszörös legfeljebb csak asszociáltsággal tekintve egyértelmű, ám ilyen értelemben, ha létezik, valóban egyértelmű. Ha ugyanis d_1 és d_2 egyaránt legnagyobb közös osztója A-nak, akkor a definíció alapján egyrészt d_1 osztója d_2-nek, másrészt ez utóbbi osztója d_1-nek, tehát $d_1 \sim d_2$. Hasonló állítás igaz a legkisebb közös többszörösre is. Az is látható, hogy nullosztómentes gyűrűben legnagyobb közös osztó csak akkor létezhet, ha a gyűrű egységelemes, hiszen ha egy közös osztó minden közös osztónak osztója, akkor önmagának is osztója, és nullosztómentes gyűrűben ilyen feltétel mellett van egységelem.

Ha egy gyűrűben van egységelem, akkor az minden elemnek osztója, tehát a gyűrű bármely részhalmazának közös osztója. Fontos az az eset, amikor az egységelem egyben a legnagyobb közös osztója egy halmaznak.

1.25. Definíció

Az $\mathcal{R}$ gyűrű egy nem üres A **részhalmaz**ának **elemei relatív prímek**, ha legnagyobb közös osztójuk az egységelem. Ha A bármely kételemű részhalmazának elemei relatív prímek, akkor A **elemei páronként relatív prímek**.

Δ

Az egységek a gyűrű minden elemének osztói, és egységelemes gyűrűben minden elem osztója önmagának. Másik oldalról fontosak azok az elemek, amelyeknek a lehető legkevesebb osztói vannak. Az előbbiek szerint ezek az olyan elemek, amelyeknek csak az egységek, valamint a saját asszociáltjaik az osztói. Természetesen ilyen minden egység, ezért ezek most nem érdekesek.

1.26. Definíció

Az $\mathcal{R}$ gyűrű egy nem egység r eleme **felbonthatatlan $\mathcal{R}$-ben**, ha $\mathcal{R}$-beli bármely kéttényezős szorzat-felírásában az egyik tényező egység. Ellenkező esetben, ha $r \neq 0$, akkor **felbontható $\mathcal{R}$-ben**.

Δ

A gyűrű egy w elemének a gyűrű u eleme **valódi osztó**ja, ha osztója, és nem asszociáltja w-nek, ellenkező esetben u **nem valódi osztója** w-nek. Az u **triviális osztó**ja w-nek, ha vagy egység, vagy asszociáltja w-nek, egyébként u a w **nem triviális osztó**ja. Látható, hogy r pontosan akkor felbontható, ha felírható két valódi osztójának szorzataként. Mindezek alapján a gyűrű egy r eleme ebben a gyűrűben egymást páronként kizáró módon vagy a nullelem, vagy egység, vagy felbonthatatlan vagy felbontható. Felbonthatatlan helyett **irreducibilis**t, felbontható helyett **reducibilis**t is mondunk.

Oszthatóság szempontjából egy további központi fogalom a prímtulajdonság.

1.27. Definíció

Az $\mathcal{R}$ gyűrű p eleme **prímtulajdonság**ú, ha valahányszor osztója egy $\mathcal{R}$-beli szorzatnak, osztója legalább az egyik tényezőnek. A prímtulajdonságú p **prímelem**, vagy röviden **prím** $\mathcal{R}$-ben, ha nem nulla és nem egység.

Δ

A nullelem és az egységek prímtulajdonságúak. Nullosztómentes gyűrűben csak akkor van nullától különböző prímtulajdonságú elem, ha van egységelem, és ekkor igaz az alábbi tétel.

1.28. Tétel

Nullosztómentes gyűrűben minden prímelem felbonthatatlan.

Δ

A tételben megfogalmazott állítás visszafelé nem igaz, hiszen ha a gyűrűben nincs egységelem, akkor prímelem sem létezhet ebben a gyűrűben. Ha viszont a gyűrű nem nullosztómentes, akkor lehet benne olyan prímelem, amely felbontható.

Egy gyűrű vizsgálatát jelentősen egyszerűsíti, ha minden elem felírható véges sok felbonthatatlan elem szorzatára, és még kedvezőbb a helyzet, ha ez a felbontás lényegében véve egyértelmű. Ezen azt értjük, hogy ugyanazon elem két felbontása legfeljebb csak a tényezők sorrendjében és az összetartozó tényezőpárok asszociáltságában tér el egymástól.

1.29. Definíció

Az $\mathcal{R}$ integritási tartomány **Gauss-gyűrű**, vagy **egyértelműen faktorizálható gyűrű**, ha minden nem nulla és nem egység eleme lényegében véve egyértelműen bontható fel a gyűrűben felbonthatatlan elemek szorzatára.

Δ

Azt már mondtuk, hogy nullosztómentes gyűrűben egy prímelem felbonthatatlan. Gauss-gyűrűben ez visszafelé is igaz. Legyen ugyanis f felbonthatatlan az $\mathcal{R}$ Gauss-gyűrűben, és legyen osztója uv-nek, ahol u és v szintén R-beliek. Ekkor $uv = fw$, és ha mind u-t, mind v-t, mind w-t helyettesítjük a lényegében véve egyértelmű felbontásukkal, akkor a két oldalon lényegében véve ugyanazon felbonthatatlan elemek állnak, legfeljebb más sorrendben és asszociáltan. A jobb oldalon az egyik felbonthatatlan tényező f, így annak (pontosabban szólva valamely asszociáltjának) a bal oldalon is szerepelnie kell. De ott csak u és v felbonthatatlan tényezői találhatóak, így valamelyikük, mondjuk u felbontásában megtalálható f egy asszociáltja, ami azt jelenti, hogy u osztható f-fel.

Ha egy gyűrű Gauss-gyűrű, akkor azt is mondjuk, hogy **a gyűrűben érvényes a számelmélet alaptétele**, hiszen a nem nulla egész számok sorrendtől és előjeltől eltekintve egyértelműen bonthatóak fel felbonthatatlan egészek szorzatára (vagyis $\mathbb{Z}$ Gauss-gyűrű, hiszen integritási tartomány). Mivel a Gauss-gyűrűk vizsgálatához sokszor elegendő a felbonthatatlan elemek vizsgálata, ezért fontos lehet tudni gyűrűk egy osztályáról, hogy elemei Gauss-gyűrűk-e.

1.30. Definíció

Az $\mathcal{R}$ integritási tartomány **euklideszi gyűrű**, ha létezik olyan alulról korlátos $\varphi: R^* \to \mathbb{Z}$, hogy a gyűrű minden a eleme R-beli tetszőleges, nullától különböző b elemmel felírható $a = qb + r$ alakban, ahol q és r is R elemei, és vagy $r = 0$, vagy $r \neq 0$ és $\varphi(r) < \varphi(b)$.

Δ

Az euklideszi gyűrűben megadott φ függvény az **euklideszi norma**. Ez nem egyértelmű, például ha $g: \mathbb{Z} \to \mathbb{Z}$ szigorúan monoton növő függvény, akkor $g \circ \varphi: a \mapsto g\big(\varphi(a)\big)$ is euklideszi norma. Mivel tetszőleges k egész számra a $\mathbb{Z}$-t önmagába képező $g_k: u \mapsto u + k$ függvény szigorúan monoton növekvő, így bármely, a φ alsó korlátjánál nem kisebb r egésszel $g_r \circ \varphi$ az $\mathcal{R}$ gyűrű nem nulla elemét $\mathbb{N}$-be képezi, így eleve feltehetjük, hogy az euklideszi norma nemnegatív egész szám. Azt sem nagyon nehéz belátni, hogy euklideszi gyűrűhöz mindig lehet találni olyan euklideszi normát, amelyre még az is teljesül, hogy ha a és b a gyűrű nem nulla elemei, akkor $\varphi(a) \leq \varphi(ab)$ (ezt a legtöbb esetben eleve kikötik). Ha ugyanis φ tetszőleges euklideszi norma, akkor az R nullától különböző r elemein definiált $\varphi'(r) = \min\limits_{s \in R^*}\{\varphi(rs)\}$ függvény szintén euklideszi normája a gyűrűnek, amely még a mostani megkötéssel is rendelkezik.

1.31. Tétel

Euklideszi gyűrű Gauss-gyűrű.

Δ

Nem csak az euklideszi gyűrűk Gauss-gyűrűk. Egy ennél bővebb, az euklideszi gyűrűket valódi részként tartalmazó osztálya a Gauss-gyűrűknek a **főideálgyűrű**k osztálya. Egy egységelemes integritási tartomány főideálgyűrű, ha minden ideálja generálható egyetlen elemmel, vagyis valamennyi ideálja főideál. Ám még ez sem a legtágabb osztálya a Gauss-gyűrűknek, vannak ugyanis olyan Gauss-gyűrűk, amelyek nem főideálgyűrűk. Ilyenre példát majd a **polinom**ok körében találunk.

A későbbiekben előfordul, hogy bizonyos állítások egységelemes gyűrűre vonatkoznak. Gyakran ez nem jelenti az állítás lényeges megszorítását, mert az alábbi tétel szerint bármely gyűrű beágyazható egy egységelemes gyűrűbe.

1.32. Tétel

Legyen $\mathcal{R} = (R; +, \cdot)$ gyűrű és $S = R \times \mathbb{Z}$, továbbá az $(u, m) \in S$, $(v, n) \in S$ elemekkel legyen $(u, m) \oplus (v, n) = (u + v, m + n)$ és $(u, m) \otimes (v, n) = (uv + nu + mv, mn)$. Ekkor $\mathcal{S} = (S; \oplus, \otimes)$ egységelemes gyűrű, amely tartalmaz $\mathcal{R}$-rel izomorf részgyűrűt.

Δ

Bizonyítás:

Mivel $\oplus$ és $\otimes$ definíciójában az eredeti gyűrű műveletei szerepelnek, így a megadott szabályok az S bármely két, adott sorrendben vett eleméhez S egy egyértelműen meghatározott elemét rendeli, ezért mindkét szabály binér műveletet definiál az S halmazon. $\oplus$ kommutativitása és asszociativitása közvetlenül látszik, mint ahogyan az is, hogy a művelet semleges eleme a $(0,0)$ pár (ahol a pár első eleme $\mathcal{R}$ nulleleme, míg a második elem a 0 egész szám), és (u, m) ellentettje $(-u, -m)$, tehát $(S; \oplus)$ Abel-csoport.

$$\begin{aligned}\big((u,m)\otimes(v,n)\big)\otimes(w,q) &= (uv+nu+mv,mn)\otimes(w,q)\\ &= (uvw+nuw+mvw+quv+qnu+qmv+mnw,mnq)\end{aligned}$$

és

$$\begin{aligned}(u,m)\otimes\big((v,n)\otimes(w,q)\big) &= (u,m)\otimes(vw+qv+nw,nq)\\ &= (uvw+quv+nuw+nqu+mvw+mqv+mnw,mnq).\end{aligned}$$

Közvetlen összehasonlítás mutatja, hogy a tagok sorrendjétől és az együtthatókban a tényezők esetenkénti sorrendjétől eltekintve a két jobb oldali kifejezés azonos, így a $\otimes$ művelet is asszociatív, $(S; \otimes)$ félcsoport. Teljesül mindkét oldalról a disztributivitás is, ugyanis

$$\begin{aligned}\big((u,m)\oplus(v,n)\big)\otimes(w,q) &= (u+v,m+n)\otimes(w,q)\\ &= \big((u+v)w+q(u+v)+(m+n)w,(m+n)q\big)\\ &= \big((uw+qu+mw)+(vw+qv+nw),mq+nq\big)\\ &= (uw+qu+mw,mq)\oplus(vw+qv+nw,nq)\\ &= \big((u,m)\otimes(w,q)\big)\oplus\big((v,n)\otimes(w,q)\big)\end{aligned}$$

és

$$\begin{aligned}(w,q)\otimes\big((u,m)\oplus(v,n)\big) &= (w,q)\otimes(u+v,m+n)\\ &= \big(w(u+v)+(m+n)w+q(u+v),q(m+n)\big)\\ &= \big((wu+mw+qu)+(wv+nw+qv),qm+qn\big)\\ &= (wu+mw+qu,qm)\oplus(wv+nw+qv,qn)\\ &= \big((w,q)\otimes(u,m)\big)\oplus\big((w,q)\otimes(v,n)\big),\end{aligned}$$

így beláttuk, hogy $(S;\oplus,\otimes)$ *gyűrű*.

Legyen $\varepsilon=(0{,}1)$. Ekkor bármely (u,m) párral $\varepsilon\otimes(u,m)=(u,m)=(u,m)\otimes\varepsilon$, így ε semleges eleme a $\otimes$ műveletnek, a gyűrű egységelemes.

Végül legyen T az $(u,0)$ párok halmaza. A $\varphi\colon u\mapsto(u,0)$ megfeleltetés nyilvánvalóan bijekció R és T között. $\varphi(u+v)=(u+v,0)=(u,0)\oplus(v,0)=\varphi(u)\oplus\varphi(v)$, φ tehát összegtartó. Nézzük a szorzást. $\varphi(uv)=(uv,0)=(uv+0\cdot u+0\cdot v,0\cdot 0)=(u,0)\otimes(v,0)=\varphi(u)\otimes\varphi(v)$, így φ a szorzásra nézve is művelettartó, vagyis φ homomorf leképezés $\mathcal{R}$-ről T-re, azaz $\mathcal{S}$-be, tehát T az $\mathcal{S}$ műveleteinek T-re való megszorításával az $\mathcal{S}$ egy $\mathcal{R}$-rel izomorf részgyűrűje, így $\mathcal{S}$ egy, az $\mathcal{R}$-rel izomorf részgyűrűt tartalmazó egységelemes gyűrű.

□

2. Formális hatványsorok és polinomok

A Bevezetőben nem foglalkoztunk a modulussal, egy algebrai struktúrával, mert az nem mindig része az alapozó algebrai oktatásnak. Mivel a további tárgyalásaink ezzel a fogalommal egységesebb szerkezetűek, ezért ezt most megtesszük. Előtte felidézzük a lineáris tereket.

Legyen $\mathcal{K} = (K; +, \cdot)$ ferdetest és $\mathcal{V} = (V; \oplus)$ Abel-csoport. $\mathcal{V}$ egy $\mathcal{K}$ **feletti vektortér** vagy $\mathcal{K}$ **feletti lineáris tér**, ha minden $a \in K$-hoz van V-n egy f_a egyváltozós művelet úgy, hogy ha e a ferdetest egységeleme, b is K eleme, és u valamint v V elemei, akkor

1. $f_{ab}(u) = f_a(f_b(u))$;
2. $f_{a+b}(u) = f_a(u) \oplus f_b(u)$;
3. $f_a(u \oplus v) = f_a(u) \oplus f_a(v)$;
4. $f_e(u) = u$.

$f_a(u)$ helyett általában egyszerűen au-t írunk, és a lineáris tér összeadására is a $+$ jelet használjuk. A ferdetest elemei a **skalár**ok, a V elemei a **vektor**ok, az $u \mapsto au$ hozzárendelés a **skalárral való szorzás**, pontosabban az u **vektornak** az a **skalárral való szorzása**, és au az u**-nak** az a **skalárral vett szorzata.** A vektorokat gyakran **u**-val vagy $\underline{u}$-val jelöljük.

Legyen $\mathcal{V}$ $\mathcal{K}$ feletti lineáris tér, és $u_1, \dots, u_n$ a V – nem feltétlenül különböző – elemei. Az előbbi elemek **lineárisan összefüggőek**, vagy másként, **lineárisan összefüggnek,** ha vannak olyan, nem csupa 0 K-beli $a_1, \dots, a_n$ elemek, hogy $\sum_{i=1}^{n} a_i u_i = 0 (\in V)$, ellenkező esetben az u_i-k **lineárisan függetlenek.** A V egy végtelen részrendszere lineárisan független, ha bármely véges részrendszere lineárisan független. A tér egy lineárisan független rendszere **maximális lineárisan független részrendszere** V**-nek**, ha lineárisan független, de bármely elemmel bővítve már lineárisan összefüggő rendszert kapunk. Nyilvánvaló, hogy az egyedül a nullvektort tartalmazó rendszer, valamint egy lineárisan összefüggő rendszert tartalmazó részrendszer lineárisan összefüggő, míg egy egyetlen, nem nulla vektorból álló rendszer lineárisan független. Megmutatható, hogy bármely lineáris térben van maximális lineárisan független rendszer.

Az $u = \sum_{i=1}^{n} a_i u_i$ vektor az u_i vektorok **lineáris kombináció**ja. A V egy A részrendszere **generátorrendszere** a $\mathcal{V}$ lineáris térnek, ha V bármely eleme előáll A-beli elemek lineáris kombinációjaként. A minimális generátorrendszer, ha generálja $\mathcal{V}$-t, de egyetlen valódi részrendszere sem állítja elő a tér valamennyi elemét.

Ha A a $\mathcal{K}$ feletti $\mathcal{V}$ lineáris tér egy részrendszere, akkor az alábbi tulajdonságok ekvivalensek:

1. A maximális lineárisan független rendszer;
2. A minimális generátorrendszer;
3. A lineárisan független és generálja $\mathcal{V}$-t;
4. V minden eleme pontosan egyféleképpen áll elő A-beli elemek lineáris kombinációjaként.

Az előbbi tulajdonságokból következik, hogy maximális lineárisan független rendszer generátorrendszer és minimális generátorrendszer lineárisan független rendszer. Az a nagyon fontos tulajdonság is következik a fentiekből, hogy egy lineáris térben vagy minden maximális lineárisan független rendszer végtelen számosságú, vagy mindegyik véges, és ugyanannyi elemet tartalmaz. Ez a közös érték a **tér dimenziója**, és bármely maximális lineárisan független rendszer a **tér bázisa.**

Most egy, a lineáris térhez hasonló, annál általánosabb, azt speciális esetként magában foglaló algebrai struktúrát definiálunk.

2.1. Definíció

Legyen $\mathcal{M} = (M; +)$ Abel-csoport és $\mathcal{R} = (R; +, \cdot)$ gyűrű. $\mathcal{M}$ egy $\mathcal{R}$ **fölötti bal oldali modulus**, vagy **bal oldali $\mathcal{R}$-modulus**, ha

1. minden $(\rho, a) \in R \times M$-hez van egy egyértelmű, $\rho \times a$ -val jelölt M-beli elem;
2. és ha σ az R-nek, b az M-nek további eleme, akkor teljesülnek az alábbi azonosságok:

a) $(\rho\sigma) \times a = \rho \times (\sigma \times a)$;
b) $(\rho + \sigma) \times a = (\rho \times a) + (\sigma \times a)$;
c) $\rho \times (a + b) = (\rho \times a) + (\rho \times b)$.

R elemei a **skalárok**, $\times$ a **skalárral való szorzás**, és $\rho \times a$ (**a** ρ) **skalárral való szorzat**.

Jobb oldali $\mathcal{R}$ -modulus definíciója hasonló az értelemszerű módosítással. Ha $\mathcal{S}$ is gyűrű, $\mathcal{M}$ egyszerre bal oldali $\mathcal{R}$ -modulus a $\times_b$ és jobb oldali $\mathcal{S}$-modulus a $\times_j$ művelettel, és minden R-beli ρ, $\mathcal{S}$ -beli σ és $\mathcal{M}$-beli a-val fennáll a $(\rho \times_b a) \times_j \sigma = \rho \times_b (a \times_j \sigma)$ egyenlőség, akkor $\mathcal{M}$ -et $\mathcal{R}$ - $\mathcal{S}$ **modulus**-nak, vagy röviden **kétoldali modulus**nak mondjuk. Az $\mathcal{M}$ $\mathcal{R}$ fölötti bal oldali, jobb oldali valamint az $\mathcal{R}$ és $\mathcal{S}$ fölötti kétoldali modulust ${}_R\mathcal{M}$-mel, $\mathcal{M}_S$ -sel és ${}_R\mathcal{M}_S$ -sel jelöljük.

Ha $\mathcal{R}$ egységelemes az ε_R és $\mathcal{S}$ az ε_S egységelemmel, és $\varepsilon_R \times_b a = a$ illetve $a \times_j \varepsilon_S = a$, akkor a bal oldali modulust **unitér bal oldali $\mathcal{R}$ -modulus**nak, a jobb oldali modulust **unitér jobb oldali $\mathcal{S}$ -modulus**nak, és a kétoldali modulust **unitér $\mathcal{R}$ - $\mathcal{S}$ modulus**nak mondjuk.

A $\mathcal{K}$ ferdetest feletti unitér bal oldali modulus $\mathcal{K}$ **feletti vektortér** vagy **lineáris tér**. Ha az $\mathcal{M}$ gyűrű additív csoportja $\mathcal{K}$ feletti vektortér, és teljesül a $\rho \times (a \cdot b) = (\rho \times a) \cdot b = a \cdot (\rho \times b)$ feltétel, ahol $\cdot$ a gyűrűbeli szorzás, akkor $\mathcal{M}$ egy $\mathcal{K}$ **feletti algebra**, és a vektortér dimenziója az algebra **rangja**.

$\mathcal{M}$ egy $\mathcal{N}$ részcsoportja illetve részgyűrűje (**unitér**) **részmodulus**, **altér** illetve **részalgebra**, ha $\mathcal{M}$ (unitér) modulus, vektortér vagy algebra, és minden N-beli a-val $\rho \times_b a \in N$ illetve $a \times_j \sigma \in N$.

Δ

Látható, hogy a modulus a lineáris tér fogalmának „gyengítése”, bár majdnem teljesen ugyanazok a definiáló tulajdonságok. Két fontos eltérés van. Az egyik, hogy láthatóan a „szimpla” modulus definíciójában nem szerepel az egységelemre vonatkozó megkötés. Ez nyilvánvaló, hiszen még azt sem kötöttük ki, hogy legyen a gyűrűben egységelem. A másik, esetleg aprónak tűnő, ám igen fontos következményekkel járó különbség, hogy a modulust tetszőleges gyűrű felett, míg a lineáris teret speciális gyűrűk, ferdetestek felett definiáltuk. Ennek az „apróság”-nak azonban igen komoly következményei vannak. Lineáris térben megszoktuk, hogy ha vektorok egy rendszere lineárisan összefüggő, akkor van a rendszerben lévő vektorok között legalább egy, amely a többinek lineáris kombinációja (és többek között ennek a tulajdonságnak egy következménye, hogy a lineárisan független maximális részrendszerek számossága azonos). Általános modulus esetén azonban ez általában nem igaz, hiszen abból, hogy $\sum_{i=0}^{n-1} c_i u_i = 0$ a gyűrűből vett c_i együtthatókkal és modulusbeli u_i elemekkel úgy, hogy valamely $n > k \in \mathbb{N}$-re $c_k u_k \neq 0$, csak annyi következik, hogy $c_k u_k = -\sum_{\substack{n>k\in\mathbb{N} \\ i\neq k}} c_i u_i$, de ha c_k-nak nincs bal oldali inverze, akkor ebből u_k-t nem tudjuk kifejezni.

Az $\mathcal{R}$ gyűrű bal oldali $\mathbb{Z}$-modulus, bármely bal oldali ideálja bal oldali $\mathcal{R}$ modulus, és ha $\mathcal{I}$ ideálja $\mathcal{R}$ -nek, akkor $\mathcal{I}$ egy $\mathcal{R}$ - $\mathcal{R}$ modulus. Algebrára példa a komplex számok teste a valós számok teste fölött (2-rangú algebra) vagy a kvaterniók ferdeteste a valós számok teste fölött (4-rangú algebra), illetve ismét a kvaterniók ferdeteste a komplex számok teste felett (2-rangú algebra), de algebra például egy test fölötti n-edrendű négyzetes mátrixok gyűrűje, amelynek rangja n^2.

A továbbiakban sokszor alkalmazzuk az alábbi tétel megállapításait.

2.2. Tétel

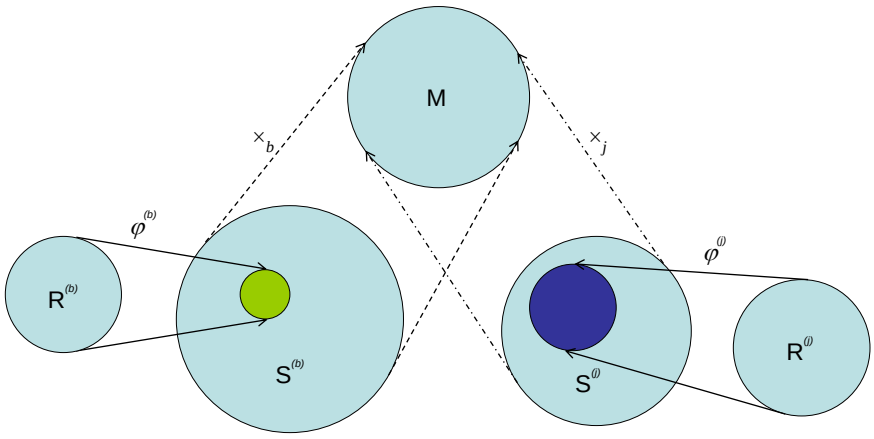
1. Ha $\mathcal{T} = (T; +, \cdot)$ gyűrű, és $\mathcal{S} \leq \mathcal{T}$, akkor $\mathcal{M} = (T; +)$ kétoldali $\mathcal{S}$-modulus a $\mathcal{T}$-beli műveletekkel, továbbá

   a) ha $\mathcal{T}$ egységelemes, és ez az egységelem eleme S-nek, akkor a modulus unitér;
   b) ha $\mathcal{S}$ ferdetest, és egységeleme egyben $\mathcal{T}$ -nek is egységeleme, akkor $\mathcal{M}$ $\mathcal{S}$ feletti lineáris tér, és ekkor $\mathcal{T}$ pontosan akkor algebra $\mathcal{S}$ felett, ha S része $\mathcal{T}$ centrumának;
   c) ha $\mathcal{T}$ test, és $\mathcal{S}$ a részteste, akkor az algebra rangja a bővítés foka;

2. ha $\mathcal{M}$ bal oldali $\mathcal{S}^{(b)}$-modulus a $\times_b$ skalárral való szorzással, $\mathcal{R}^{(b)}$ gyűrű, $\varphi^{(b)}: \mathcal{R}^{(b)} \to \mathcal{S}^{(b)}$ homomorfizmus, és az $R^{(b)}$-beli $r^{(b)}$-vel és M-beli u-val $r^{(b)} \times_b^{(R^{(b)})} u = \varphi^{(b)}\left(r^{(b)}\right) \times_b u$, akkor $\mathcal{M}$ bal oldali $\mathcal{R}^{(b)}$-modulus a $\times_b^{(R^{(b)})}$ skalárral való szorzással. A modulus unitér, ha $\mathcal{R}^{(b)}$ egységelemes és $\mathcal{M}$ unitér $\mathrm{Im}\left(\varphi^{(b)}\right)$ fölött. Hasonló igaz a jobb és a kétoldali modulusra is. Ha $\mathcal{R}^{(b)}$ ferdetest, és az $\mathcal{R}^{(b)}$ feletti modulus unitér, akkor $\mathcal{M}$ lineáris tér $\mathcal{R}^{(b)}$ felett, és ha még $\mathcal{M}$ egy $\mathcal{T}$ gyűrű additív csoportja, és $\mathcal{T}$ algebra $\times_b$-nek $\mathrm{Im}\left(\varphi^{(b)}\right)$-re való megszorításával, akkor $\mathcal{T}$ algebra $\mathcal{R}^{(b)}$ fölött.

Δ

A tételt az 1. ábra illusztrálja.



1. ábra

Bizonyítás:

1. Ha a skalárok S elemei, akkor egyben T-beliek is, és ekkor a modulus definíciójában szereplő minden művelet $\mathcal{T}$-beli művelet, márpedig ott minden megadott feltétel teljesül. Amennyiben egy gyűrű e egységeleme eleme a részgyűrűnek, akkor e a részgyűrűben is egységelem. Az algebránál tett, centrumra vonatkozó kikötés azért kell, hogy teljesüljön az $r(uv) = r \times (uv) = u(r \times \boldsymbol{v}) = u(rv)$ feltétel. Ami az algebra rangját illeti, ez a bővítés fokának definíciójából adódik (lásd a 3.16. Definíciót a 49. oldalon)
2. Az első állítás könnyen ellenőrizhető. Homomorfizmusnál a képhalmazban egységelem képe egységelem, inverz képe a kép inverze, így a többi állítást is könnyű belátni.

□

A tétel speciális eseteként $\mathcal{M}$ lehet egy $\mathcal{T}$ gyűrű additív csoportja, és $\mathcal{S}^{(b)} = \mathcal{T} = \mathcal{S}^{(j)}$, továbbá szintén speciális esetként kapjuk, hogy minden (egységelemes) gyűrű kétoldali (unitér) modulus önmaga fölött, és ha ez a gyűrű test, akkor 1-rangú algebra (ismét önmaga fölött).

A polinomok általában ismertek a Véges testek olvasói számára, ám ez kevésbé mondható el a formális hatványsorokról. Mint majd látjuk, a polinomok speciális formális hatványsorok, így a polinomokat ilyen felfogásban fogjuk bevezetni, és utána foglalkozunk a polinomok tulajdonságaival, az ismertnek vélt dolgokat nem részletezve. A polinomok általános jellemzőin túl a véges testek feletti polinomok további tulajdonságait egy külön fejezetben vizsgáljuk, és a formális hatványsorokkal kapcsolatos ismereteket elsősorban a rekurzív sorok elméletében fogjuk felhasználni.

2.3. Definíció

1. Ha $\mathcal{S}$ kommutatív, egységelemes, additív félcsoport a 0 egységelemmel, és Γ egy indexhalmaz, továbbá $\Lambda = \{\gamma \in \Gamma | s_\gamma \neq 0\}$ véges, akkor $\sum_{\gamma\in\Gamma} s_\gamma = \sum_{\gamma\in\Lambda} s_\gamma$;
2. ha $\cdot$ binér művelet az A halmazon, és Δ véges, rendezett halmaz, akkor $\prod_{\delta\in\Delta} a_\delta$, ahol minden $\delta \in \Delta$-ra $a_\delta \in A$, olyan szorzat, ahol a tényezők és a műveletek az indexek sorrendjében következnek.

Δ

2.4. Megjegyzés

Mivel a fenti definícióban a félcsoport egységelemes, ezért definiált $\sum_{\gamma\in\emptyset} s_\gamma$ is, és az értéke 0, így $\sum_{\gamma\in\Gamma} s_\gamma$ akkor is létezik, ha minden $\gamma \in \Gamma$-ra $s_\gamma = 0$, tudniillik ekkor $\sum_{\gamma\in\Gamma} s_\gamma = 0$.

Δ

2.5. Tétel

Legyen $\mathcal{S}$ egységelemes, kommutatív, additív félcsoport, Δ, valamint minden $\delta \in \Delta$-ra Γ_δ indexhalmaz, és a Γ_δ-k páronként idegenek. Legyen még $\Gamma = \bigcup_{\delta\in\Delta} \Gamma_\delta$. Ekkor, ha létezik $\sum_{\gamma\in\Gamma} s_\gamma$, akkor létezik $\sum_{\delta\in\Delta} \sum_{\gamma\in\Gamma_\delta} s_\gamma$ is, és $\sum_{\delta\in\Delta} \sum_{\gamma\in\Gamma_\delta} s_\gamma = \sum_{\gamma\in\Gamma} s_\gamma$.

Δ

Bizonyítás:

Ha létezik $\sum_{\gamma\in\Gamma} s_\gamma$, akkor véges azon γ indexek száma, amelyekre $s_\gamma \neq 0$. Ekkor csak véges sok olyan $\delta \in \Delta$ lehet, amelynél $\sum_{\gamma\in\Gamma_\delta} s_\gamma$ tagjai között van az egységelemtől különböző, és az ilyen összegekben is csak véges sok olyan tag van, amely nem az egységelem. Legyen Δ^* az előbbi véges sok δ halmaza, Γ_δ^* egy ilyen δ -hoz tartozó indexhalmaz azon elemeinek halmaza, amelyek által indexelt elemek nem a félcsoport egységelemével azonosak, és legyen $\Lambda = \bigcup_{\delta\in\Delta^*} \Gamma_\delta^*$. Ez utóbbi halmaz a Γ-nak pontosan azokat az elemeit tartalmazza, amelyek által indexelt elemek nem azonosak az egységelemmel. Ekkor $\sum_{\delta\in\Delta} \sum_{\gamma\in\Gamma_\delta} s_\gamma = \sum_{\delta\in\Delta^*} \sum_{\gamma\in\Gamma_\delta^*} s_\gamma = \sum_{\gamma\in\Lambda} s_\gamma = \sum_{\gamma\in\Gamma} s_\gamma$.

□

Megjegyezzük, hogy $\sum_{\delta\in\Delta} \sum_{\gamma\in\Gamma_\delta} s_\gamma$ akkor is létezhet, ha $\sum_{\gamma\in\Gamma} s_\gamma$ nem létezik, ugyanis az előbbi összeg végtelen sok tagja lehet úgy az egységelemmel azonos, hogy a részösszegekben nem minden elem az egységelem (például mindegyikben a félcsoport egy tetszőleges invertálható eleme és annak ellentettje található).

2.6. Tétel

Legyen $\mathcal{R}$ gyűrű, Δ véges halmaz és minden $\delta \in \Delta$-ra Γ_δ indexhalmaz, és ha $\mathcal{R}$ nem kommutatív, akkor legyen Δ rendezett. Ekkor $\prod_{\delta\in\Delta} \sum_{\gamma\in\Gamma_\delta} s_{\delta,\gamma}$ létezéséből következik $\sum_{\varphi\in\times_{\lambda\in\Delta}\Gamma_\lambda} \prod_{\delta\in\Delta} s_{\delta,\varphi(\delta)}$ létezése, és a két kifejezés értéke megegyezik.

Δ

Bizonyítás:

Mivel $\prod_{\delta\in\Delta}\sum_{\gamma\in\Gamma_\delta} s_{\delta,\gamma}$ véges tényezős kifejezés, így pontosan akkor definiált az értéke, ha minden tényezője, azaz mindegyik összeg létezik, ami akkor és csak akkor teljesül, ha minden összegben csak véges sok nem nulla tag van. Ekkor a teljes kifejezésben is csak véges sok olyan indexpár létezik, amely pár nem nulla elemet indexel, és így

$$\prod_{\delta\in\Delta}\sum_{\gamma\in\Gamma_\delta} s_{\delta,\gamma} = \prod_{\delta\in\Delta}\sum_{\gamma\in\Gamma_\delta^*} s_{\delta,\gamma} = \sum_{\varphi\in\times_{\lambda\in\Delta}\Gamma_\lambda^*}\prod_{\delta\in\Delta} s_{\delta,\varphi(\delta)} = \sum_{\varphi\in\times_{\lambda\in\Delta}\Gamma_\lambda}\prod_{\delta\in\Delta} s_{\delta,\varphi(\delta)},$$

ahol Γ_δ^* a Γ_δ azon γ elemeinek halmaza, amelyekre $s_{\delta,\gamma}\neq 0$, ugyanis $\prod_{\delta\in\Delta} s_{\delta,\varphi(\delta)}$ véges szorzat.

□

Visszafelé ismét nem feltétlenül igaz az állítás, ha ugyanis valamely végtelen tagú összeg minden tagja nullosztó (és ekkor minden tagja, tehát az összeg végtelen sok tagja különbözik nullától, ezért az összegük nem értelmezett), és a többi összegben a nem nulla elemek ezen nullosztók párjai, akkor valamennyi $\prod_{\delta\in\Delta} s_{\delta,\varphi(\delta)}$ nulla, és így $\sum_{\varphi\in\times_{\lambda\in\Delta}\Gamma_\lambda}\prod_{\delta\in\Delta} s_{\delta,\varphi(\delta)}$ létezik, míg a másik oldal nem, hiszen van a szorzatnak olyan tényezője, amely végtelen sok nem nulla elemből álló, tehát nem értelmezett összeg.

2.7. Definíció

Legyen S egy nem üres halmaz, és $f:\mathbb{N}\to S$. Ekkor $f(i)$-t f_i-vel jelölve $(f_i\in S|i\in\mathbb{N})$ egy S **fölötti** (**végtelen**) **sorozat**, amit röviden (f_i) vagy **f** jelöl. $f_i=(\mathbf{f})_i$ **a sorozat** i**-edik tagja**, és két sorozat akkor és csak akkor azonos, ha minden $i\in\mathbb{N}$-re a megfelelő tagjuk egyenlő.

Δ

A szokásoknak megfelelően az S fölötti sorozatok halmazát, tehát az $\mathbb{N}$-et S-be képező függvények halmazát $S^{\mathbb{N}}$-nel jelöljük.

2.8. Tétel

Legyen $\mathcal{R}=(R;+,\cdot)$ gyűrű, és az R fölötti $\mathbf{a}=(a_i)$ és $\mathbf{b}=(b_i)$ sorozatra $u_i=a_i+b_i$ valamint $v_i=\sum_{j=0}^{i} a_j b_{i-j}$. Ekkor az $(\mathbf{a}\oplus\mathbf{b})_i=(\mathbf{u})_i=u_i$ és $(\mathbf{a}\otimes\mathbf{b})_i=(\mathbf{v})_i=v_i$ szabállyal $\left(R^{\mathbb{N}};\oplus,\otimes\right)$ gyűrű. $P_R=\{\mathbf{u}\in R^{\mathbb{N}}\big|\exists(n_u\in\mathbb{N})\forall(n_u<i\in\mathbb{N}):u_i=0\}$ $R^{\mathbb{N}}$-nek a $\oplus$ és $\otimes$ műveletekre zárt részhalmaza, és ha $\oplus_P$ és $\otimes_P$ az előbbi műveletek P_R-re való megszorításai, akkor $\mathcal{P}_R=(P_R;\oplus_P,\otimes_P)$ tartalmaz $\mathcal{R}$-rel izomorf részgyűrűt.

Δ

$R^{\mathbb{N}}$ elemei az R **fölötti formális hatványsor**ok, és az $\left(R^{\mathbb{N}};\oplus,\otimes\right)$ gyűrűt egyelőre $\mathcal{PS}_R$-rel jelöljük (a *Power Series* – hatványsor – rövidítéseként), míg $R^{\mathbb{N}}$ helyett esetenként PS_R-et írunk. P_R azokat a sorozatokat tartalmazza, amelyeknek minden komponense egy adott (sorozatonként nem feltétlenül azonos, a sorozattól függő) indextől kezdve 0, vagyis azokat, amelyeknek csupán véges sok tagja különbözik az $\mathcal{R}$ gyűrű nullelemétől, 0-tól. Ha $\mathbf{f}\in P_R$, akkor **f** egy R **fölötti polinom.**

Bizonyítás:

a_i, b_i, a_j és b_{i-j} gyűrű elemei, és gyűrűben az összeg és szorzat egyértelmű és benne van a gyűrűben, ezért u_i és v_i minden $i\in\mathbb{N}$ -re az R egyértelműen meghatározott eleme. Ekkor maguk a sorozatok is $R^{\mathbb{N}}$ egyértelműen meghatározott elemei. A fenti operációkat bármely sorozatpár esetén elvégezhetjük, így a bevezetett $\oplus$ és $\otimes$ szabály egyaránt binér műveletet definiál $R^{\mathbb{N}}$-en.

Legyen $\mathbf{c}=(c_i)$ egy további sorozat. $(a_i+b_i)+c_i=a_i+(b_i+c_i)$ az $\mathcal{R}$ gyűrűben igaz, így $(\mathbf{a}\oplus\mathbf{b})\oplus\mathbf{c}=\mathbf{a}\oplus(\mathbf{b}\oplus\mathbf{c})$, az összeadás asszociatív. Ha $\mathbf{0}$ az a sorozat, amelyben minden $i\in\mathbb{N}$ -re az i-edik tag 0, és $\mathbf{a}'$ i-edik tagja $-a_i$, akkor $\mathbf{0}\oplus\mathbf{a}=\mathbf{a}$, $\mathbf{a}'\oplus\mathbf{a}=\mathbf{0}$, $\mathcal{PS}_R$- az összeadással csoport, és mivel $a_i+b_i=b_i+a_i$, ezért $\mathbf{a}\oplus\mathbf{b}=\mathbf{b}\oplus\mathbf{a}$, az összeadás kommutatív is. A szorzás is asszociatív:

$$\big((\mathbf{a}\otimes\mathbf{b})\otimes\mathbf{c}\big)_i = \sum_{j=0}^{i}(\mathbf{a}\otimes\mathbf{b})_j c_{i-j} = \sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right)c_{i-j} = \sum_{j=0}^{i}\sum_{k=0}^{j}\big(a_k b_{j-k}\big)\,c_{i-j}$$
$$= \sum_{j=0}^{i}\sum_{k=0}^{j} a_k\big(b_{j-k}c_{i-j}\big) = \sum_{k=0}^{i}\sum_{j=k}^{i} a_k\big(b_{j-k}c_{i-j}\big) = \sum_{k=0}^{i}\left(a_k\sum_{j=k}^{i}\big(b_{j-k}c_{i-j}\big)\right)$$
$$= \sum_{k=0}^{i}\left(a_k\sum_{j=0}^{i-k}\big(b_j c_{(i-k)-j}\big)\right) = \sum_{k=0}^{i} a_k(\mathbf{b}\otimes\mathbf{c})_{i-k} = \big(\mathbf{a}\otimes(\mathbf{b}\otimes\mathbf{c})\big)_i$$

minden értelmes i-re teljesül. Nézzük végül a disztributivitást.

$$\big((\mathbf{a}\oplus\mathbf{b})\otimes\mathbf{c}\big)_i = \sum_{j=0}^{i}(\mathbf{a}\oplus\mathbf{b})_j c_{i-j} = \sum_{j=0}^{i}\big(a_j+b_j\big)c_{i-j} = \sum_{j=0}^{i}\big(a_j c_{i-j}+b_j c_{i-j}\big)$$
$$= \sum_{j=0}^{i} a_j c_{i-j} + \sum_{j=0}^{i} b_j c_{i-j} = (\mathbf{a}\otimes\mathbf{c})_i + (\mathbf{b}\otimes\mathbf{c})_i = \big((\mathbf{a}\otimes\mathbf{c})\oplus(\mathbf{b}\otimes\mathbf{c})\big)_i$$

és a másik oldali disztributivitás hasonló módon igazolható, így valamennyi gyűrűaxióma teljesül.

P_R minden $\mathbf{u}$ eleméhez van olyan n_u index, hogy valamennyi ennél nagyobb indexre a sorozat megfelelő tagja nulla. Ha $\mathbf{b}$ additív inverzét $\mathbf{b}'$-vel jelöljük, akkor nyilván $n_b = n_{b'}$, hiszen $b_i = 0$ akkor és csak akkor, ha $b_i' = -b_i = 0$. Legyen $\max\{n_a, n_b\} \le n_{a+b} \in \mathbb{N}$ és $n_a + n_b \le n_{ab} \in \mathbb{N}$. Ekkor $n_{a+b} < i \in \mathbb{N}$-re $a_i = 0 = b_i'$, tehát $(\mathbf{a}\ominus\mathbf{b})_i = (\mathbf{a}\oplus\mathbf{b}')_i = a_i + b_i' = 0 + 0 = 0$, és ha $n_{ab} < i \in \mathbb{N}$, akkor

$$\sum_{j=0}^{i} a_j b_{i-j} = \sum_{j=0}^{n_a} a_j b_{i-j} + \sum_{j=n_a+1}^{i} a_j b_{i-j} = \sum_{j=i-n_a}^{i} a_{i-j} b_j + \sum_{j=n_a+1}^{i} a_j b_{i-j}$$
$$= \sum_{j=i-n_a}^{i}\big(a_{i-j}\cdot 0\big) + \sum_{j=n_a+1}^{i}\big(0\cdot b_{i-j}\big) = 0,$$

ugyanis ha $j \ge i - n_a$, akkor $j \ge i - n_a > n_{ab} - n_a \ge (n_a + n_b) - n_a = n_b$. Ez azt jelenti, hogy a különbség- és szorzatsorozatban is csupán véges sok nem nulla tag található, ami mutatja, hogy a P_R halmaz zárt a kivonásra és szorzásra. Ugyanakkor P_R nem üres, hiszen a csupa nullából álló sorozat biztosan benne van, ezért $\mathcal{P}_R \le \mathcal{PS}_R$.

Legyen $\bar{R}$ azon PS_R-beli sorozatok halmaza, amelyekben legfeljebb csak a 0-indexű tag nem nulla. Ez mindenesetre részhalmaza P_R-nek, és mivel az $\bar{R}$-beli $\mathbf{a}$ és $\mathbf{b}$ sorozatra $n_a < 1$ és $n_b < 1$, tehát $\max\{n_a, n_b\} < 1$ és $n_a + n_b < 1$, ezért a két sorozat különbsége és szorzata egyaránt benne van $\bar{R}$-ban, $\bar{\mathcal{R}} \le \mathcal{P}_R$, ahol $\bar{\mathcal{R}}$ az $\bar{R}$ elemeiből álló részgyűrű. Definiáljunk egy szabályt. Legyen az R tetszőleges r elemére $\bar{r} \in PS_R$ olyan, hogy $(\bar{r})_i = \delta_{i,0} r$, ahol $\delta_{i,j} = \begin{cases} 0, \text{ha } i \ne j \\ 1, \text{ha } i = j \end{cases}$ a Kronecker-szimbólum. R minden eleméhez tartozik egy és csak egy ilyen sorozat, különböző R-beli elem által meghatározott sorozat különböző, hiszen a nulla-indexű tagjaik különbözőek, és ezek a sorozatok valamennyien $\bar{R}$-hoz tartoznak, ezért a $\varphi(r) = \bar{r}$ szabály R-et $\bar{R}$-ba képezi, és ez a leképezés injektív. De φ szürjektív is, hiszen $\bar{R}$ bármely $\mathbf{u}$ eleme olyan, amelyben legfeljebb csak u_0 nem nulla, és ez az u_0 R-nek eleme, tehát $\mathbf{u} = \varphi(u_0)$, így φ bijekció a két halmaz között. Ha u és v az R két eleme, akkor a megfelelő két $\bar{R}$-beli sorozatban minden tag nulla a nullás indexűeket leszámítva, amelyek rendre u és v. Ekkor az összegsorozatban is csupán a 0-indexű tag lehet nullától különböző, és ez $u + v$, amiből következik, hogy $\varphi(u)\oplus_P\varphi(v) = \varphi(u+v)$. A szorzatban $u_j v_{i-j}$ csak akkor különbözhet nullától, ha mindkét index 0, vagyis ha $j = 0$ és $i = i - j = 0$, ezért a szorzatban sem lehet 0-nál nagyobb indexű tag nem nulla, ami azt jelenti, hogy a szorzatsorozat is benne van $\bar{R}$-ban. Ugyanakkor a 0-indexű tag uv, így

$\varphi(u)\otimes_P\varphi(v)=\varphi(uv)$, tehát ismét teljesül a művelettartás. Mivel φ bijektíven és művelettartó módon képezi le $\mathcal{R}$-et $\bar{\mathcal{R}}$-ra, ezért $\bar{\mathcal{R}}\cong\mathcal{R}$.

□

2.9. Definíció

$\mathcal{PS}_R$ a(z $\mathcal{R}$ **fölötti**) (**egyhatározatlanú**) **formális hatványsorok gyűrűje**, míg $\mathcal{P}_R$ a(z $\mathcal{R}$ **fölötti**) (**egyhatározatlanú**) **polinomok gyűrűje**.

Ha az **f** polinomban minden $n<i\in\mathbb{N}$ indexre, ahol n nemnegatív egész szám, $f_i=0$, akkor **f legfeljebb n-edfokú** (**polinom**). Ha még az is teljesül, hogy $f_n\neq 0$, akkor **f foka** n, és **f n-edfokú** (**polinom**). Az **f** polinom fokát (amennyiben létezik) $\deg(\mathbf{f})$ jelöli.

f_0 a formális hatványsor illetve polinom **konstans tag**ja. Legfeljebb 0-adfokú polinomot, azaz $\bar{R}$ elemeit, **konstans polinom**nak mondunk, és ha egy konstans polinom konstans tagja 0, akkor a polinom **nullpolinom**.

Δ

Mivel $\mathcal{R}\cong\bar{\mathcal{R}}\leq\mathcal{P}_R\leq\mathcal{PS}_R$, ezért $\mathcal{R}$ beágyazható $\mathcal{P}_R$-be, és ekkor egyúttal $\mathcal{PS}_R$-be is, így a továbbiakban úgy tekintjük, hogy $\mathcal{R}$ részgyűrűje a polinomok illetve a formális hatványsorok gyűrűjének, és a továbbiakban mindhárom struktúrában $+$ és $\cdot$ jelöli a műveleteket. A beágyazás után kapott gyűrűkben az R bármely r elemére $\bar{r}=r$.

2.10. Tétel:

Legyen $\mathcal{R}=(R;+,\cdot)$ gyűrű. Ekkor bármely R-beli r-rel és $\mathcal{PS}_R$-beli $\mathbf{a}$-val $(r\mathbf{a})_i=(\bar{r}\mathbf{a})_i=ra_i$ és $(\mathbf{a}r)_i=(\mathbf{a}\bar{r})_i=a_ir$ minden $i\in\mathbb{N}$-re.

Δ

Bizonyítás:

Az állítás a szorzás definíciójából közvetlenül adódik, hiszen az $\bar{r}$ sorozatnak csak a 0-indexű komponense különbözhet nullától, és ez a komponens éppen r.

□

2.11. Tétel

A nullpolinomnak nincs foka, míg a nullpolinom kivételével minden polinomnak van egyértelműen meghatározott foka, és ez nemnegatív egész. Az **f** polinom akkor és csak akkor legfeljebb n-edfokú, ha vagy a nullpolinom és $n\geq 0$, vagy $\deg(\mathbf{f})\leq n$.

Δ

Bizonyítás:

A fokszámot a sorozat egy indexével definiáltuk, és ez nemnegatív egész. Ismét a definíció szerint a nullpolinom az a polinom, amelyben valamennyi tag 0, így a nullpolinomban nincs olyan i index, amelyre teljesülne az $f_i\neq 0$ feltétel, ezért ennek a polinomnak nem lehet foka. Ha viszont **f** nem a nullpolinom, akkor van benne nullától különböző tag, és mivel polinom, ezért csak véges sok ilyen tag van benne, így az ilyen tagokhoz tartozó indexek halmaza a nemnegatív egészek halmazának nem üres véges részhalmaza. Egy ilyen halmaznak van legnagyobb eleme, és ha ez n, akkor n egyértelmű. Ha $i>n$, akkor $f_i=0$, tehát **f** legfeljebb n-edfokú, ugyanakkor $f_n\neq 0$, tehát $\deg(\mathbf{f})=n$.

$\mathbf{f}=\mathbf{0}$-ban minden $n\in\mathbb{N}$-re az n-nél nagyobb indexű tagok nullák, vagyis minden nemnegatív egész n-re a polinom legfeljebb n-edfokú. Ha **f** n-edfokú, akkor az előbbiek alapján minden $i>n$-re $f_i=0$, de ekkor $m\geq n$ esetén az is igaz, hogy valamennyi $i>m$ indexre $f_i=0$, tehát **f** legfeljebb m-edfokú. Amennyiben viszont $m<n$, akkor létezik m-nél nagyobb i index, nevezetesen n, amelyre nem igaz, hogy $f_i=0$, így az sem igaz, hogy **f** legfeljebb m-edfokú. Innen kapjuk az utolsó állítást.

□

Az előbbiek alapján tehát a nullpolinomnak és csak a nullpolinomnak nincs foka, ám ha azt mondjuk, hogy az $\mathbf{f}$ polinom foka legfeljebb n (ahol n egy nemnegatív egész), akkor ebbe beleértjük azt a lehetőséget is, hogy $\mathbf{f}$ esetleg a nullpolinom (hiszen ekkor is teljesül az a kritérium, hogy a polinom valamennyi tagja nulla, ha az indexük nagyobb n-nél). Bevezetünk egy célszerű jelölést.

2.12. Jelölés

Ha $\mathbf{0} \neq \mathbf{f} \in P_R$, akkor $\delta(\mathbf{f}) = \deg(\mathbf{f})$, míg $\delta(\mathbf{0}) = -\infty$. $n \in \mathbb{N}$-re $P_R^{(n)} = \{\mathbf{f} \in P_R | \delta(\mathbf{f}) \leq n\}$.

Δ

Nyilván igaz, hogy deg egy deg: $P_R \setminus \{\mathbf{0}\} \to \mathbb{N}$ függvény, míg δ egy $\delta: P_R \to \mathbb{N} \cup \{-\infty\}$ leképezés, továbbá minden nemnegatív egész i-re és k-ra $P_R^{(i)} \subseteq P_R^{(i+k)} \subseteq \bigcup_{n=0}^{\infty} P_R^{(n)} = P_R$. Azt is láthatjuk, hogy $P_R^{(0)} = \bar{R} = R$.

Ha egy gyűrűből egy új gyűrűt konstruálunk, akkor mindig érdemes megvizsgálni, hogy az eredeti gyűrű mely tulajdonságai öröklődnek az új gyűrűre. A legfontosabb ilyen tulajdonságok a kommutativitás, nullosztómentesség és a (bal oldali) egységelemesség.

2.13. Tétel

$\mathcal{R}$, $\mathcal{P}_R$ és $\mathcal{PS}_R$ egyszerre kommutatív, egyszerre (bal oldali) egységelemes, és egyszerre nullosztómentes. Ha $\mathcal{PS}_R$-ben van (bal oldali) egységelem, akkor van olyan is, amely benne van R-ben, és ha $\mathcal{R}$ nullosztómentes, akkor ez minden (bal oldali) egységelemre igaz.

Δ

Bizonyítás:

1. Kommutatív gyűrű bármely részgyűrűje kommutatív, így ha $\mathcal{PS}_R$ kommutatív, akkor hasonló tulajdonságú $\mathcal{P}_R$, míg $\mathcal{P}_R$ kommutativitása esetén kommutatív $\mathcal{R}$. Ha viszont $\mathcal{R}$ kommutatív, akkor $(\mathbf{ab})_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j=0}^{i} b_{i-j} a_j = \sum_{j=0}^{i} b_j a_{i-j} = (\mathbf{ba})_i$, tehát kommutatív a $\mathcal{PS}_R$ gyűrű.

2. Legyen e az $\mathcal{R}$ (bal oldali) egységeleme, és $\mathbf{a} \in \mathcal{PS}_R$. Ekkor $(e\mathbf{a})_i = e a_i = a_i$, tehát $e\mathbf{a} = \mathbf{a}$, e (bal oldali) egységelem a sorozatok gyűrűjében, és mivel $e \in R \subseteq \mathcal{P}_R \subseteq \mathcal{PS}_R$, így a polinomok gyűrűjében is (bal oldali) egységelem.

Most tegyük fel, hogy $\mathbf{e} = (e_i)$ (bal oldali) egységelem $\mathcal{PS}_R$-ben illetve $\mathcal{P}_R$-ben. Ekkor bármely $b \in R$-re $\mathbf{e}b = b$, vagyis $e_0 b = (\mathbf{e}b)_0 = (b)_0 = b$, és az $e = e_0$ jelöléssel $b = eb$, azaz e (bal oldali) egységelem $\mathcal{R}$ -ben. Ekkor viszont az eddigiek alapján a harmadik gyűrű is (bal oldali) egységelemes.

Ha most $\mathbf{e}'$ az a konstans sorozat, amelynek konstans tagja e, akkor $\mathbf{e}'$ (bal oldali) egységeleme $\mathcal{PS}_R$-nek, és benne van az eredeti gyűrűben. Megjegyezzük, hogy amennyiben $\mathbf{e}$ egységeleme $\mathcal{PS}_R$-nek, akkor egyértelmű, és így csak az előbbi konstans sorozat lehet.

Ha $\mathbf{e} = (e_i)$ bal oldali egységelem $\mathcal{PS}_R$-ben illetve $\mathcal{P}_R$-ben, akkor minden $i \in \mathbb{N}^+$ index esetén $0 = b_i = (\mathbf{e}b)_i = e_i b$, így pozitív i indexre e_i bal oldali annullátora az eredeti gyűrűnek, és nullosztómentes gyűrűben ez csak a 0 lehet, tehát ekkor $\mathbf{e}$ konstans sorozat, vagyis eleme R-nek.

3. Végül a nullosztómentesség. Nullosztómentes gyűrű részgyűrűje is nullosztómentes, tehát ha $\mathcal{PS}_R$ nullosztómentes, akkor nullosztómentes $\mathcal{P}_R$, míg $\mathcal{P}_R$ nullosztó-mentessége esetén nullosztómentes $\mathcal{R}$. Ha viszont $\mathcal{R}$ nullosztómentes, és sem $\mathbf{a}$, sem $\mathbf{b}$ nem $\mathbf{0}$, akkor van mindkettőben nem nulla tag. Legyen n_a és n_b a megfelelő sorozat legkisebb ilyen indexe. Ekkor

$$(\mathbf{ab})_{n_a+n_b} = \sum_{i=0}^{n_a+n_b} a_i b_{(n_a+n_b)-i} = \sum_{i=0}^{n_a-1} a_i b_{(n_a+n_b)-i} + a_{n_a} b_{n_b} + \sum_{i=n_a+1}^{n_a+n_b} a_i b_{(n_a+n_b)-i}$$
$$= \sum_{i=0}^{n_a-1} a_i b_{n_b+(n_a-i)} + a_{n_a} b_{n_b} + \sum_{i=0}^{n_b-1} a_{n_a+(n_b-i)} b_i,$$

és a jobb oldalon az első összegben valamennyi i-re a_i, az utolsóban pedig minden i-re b_i értéke 0, így az összeg a középső taggal egyenlő. De $\mathcal{R}$ nullosztó-mentessége alapján $a_{n_a} b_{n_b} \neq 0$, így viszont $\mathbf{ab}$ -ben van nullától különböző komponens, $\mathbf{ab}$ nem nulla, tehát $\mathcal{PS}_R$ nullosztómentes.

□

2.14. Tétel

Legyen $\mathbf{f}$ és $\mathbf{g}$ két $\mathcal{R}$ fölötti polinom. Ekkor

$\delta(\mathbf{f} \pm \mathbf{g}) \leq \max\{\delta(\mathbf{f}), \delta(\mathbf{g})\}$, és ha $\delta(\mathbf{f}) \neq \delta(\mathbf{g})$, akkor $\delta(\mathbf{f} \pm \mathbf{g}) = \max\{\delta(\mathbf{f}), \delta(\mathbf{g})\}$;
$\delta(\mathbf{fg}) \leq \delta(\mathbf{f}) + \delta(\mathbf{g})$, és $\delta(\mathbf{fg}) = \delta(\mathbf{f}) + \delta(\mathbf{g})$ akkor és csak akkor, ha $\mathbf{f}$ és $\mathbf{g}$ legalább egyike $\mathbf{0}$, vagy egyik sem $\mathbf{0}$, és $f_{\deg(\mathbf{f})} g_{\deg(\mathbf{g})} \neq 0$.

Δ

Bizonyítás:

0. Ha $\max\{\delta(\mathbf{f}), \delta(\mathbf{g})\} < i \in \mathbb{N}$, akkor $f_i = 0 = g_i$, tehát $(\mathbf{f} \pm \mathbf{g})_i = f_i \pm g_i = 0 + 0 = 0$, így $\delta(\mathbf{f} \pm \mathbf{g}) \leq \max\{\delta(\mathbf{f}), \delta(\mathbf{g})\}$. Ha $\delta(\mathbf{f}) \neq \delta(\mathbf{g})$, akkor mondjuk $\delta(\mathbf{f}) < \delta(\mathbf{g})$. Ekkor $\delta(\mathbf{g}) \neq -\infty$, ezért $\delta(\mathbf{g}) \in \mathbb{N}$. Most $f_{\delta(\mathbf{g})} = 0 \neq g_{\delta(\mathbf{g})}$, így $(\mathbf{f} \pm \mathbf{g})_{\delta(\mathbf{g})} = f_{\delta(\mathbf{g})} \pm g_{\delta(\mathbf{g})} = g_{\delta(\mathbf{g})} \neq 0$, és innen kapjuk, hogy $\delta(\mathbf{f} \pm \mathbf{g}) \geq \delta(\mathbf{g}) = \max\{\delta(\mathbf{f}), \delta(\mathbf{g})\}$. Ez az előbb belátott, fordított irányú egyenlőtlenséggel együtt azt jelenti, hogy $\delta(\mathbf{f} \pm \mathbf{g}) = \delta(\mathbf{g}) = \max\{\delta(\mathbf{f}), \delta(\mathbf{g})\}$.

0. Azt már korábban beláttuk, hogy a $\delta(\mathbf{f}) + \delta(\mathbf{g})$-nél nagyobb indexekre a szorzat minden tagja nulla, tehát $\delta(\mathbf{fg}) \leq \delta(\mathbf{f}) + \delta(\mathbf{g})$. Ha $\min\{\delta(\mathbf{f}), \delta(\mathbf{g})\} = -\infty$, akkor legalább az egyik polinom nullpolinom, de akkor a szorzatuk is az, márpedig $-\infty$-hez önmagát vagy egy véges számot adva ismét $-\infty$-t kapunk. Ha viszont egyik polinom sem a nullpolinom, azaz $\delta(\mathbf{f})$ és $\delta(\mathbf{g})$ egyaránt nemnegatív egész szám, akkor a már említett bizonyítás szerint a szorzatban a $\delta(\mathbf{f}) + \delta(\mathbf{g})$ indexhez tartozó tag éppen $f_{\deg(\mathbf{f})} g_{\deg(\mathbf{g})}$, ami most a feltétel szerint nem nulla, így a szorzatpolinom foka legalább $f_{\deg(\mathbf{f})} g_{\deg(\mathbf{g})} \neq 0$, de nagyobb nem lehet, amint azt már beláttuk.

□

A tételből következik, hogy nullosztómentes gyűrű feletti polinomgyűrűben bármely $\mathbf{f}$ és $\mathbf{g}$ polinom esetén $\delta(\mathbf{fg}) = \delta(\mathbf{f}) + \delta(\mathbf{g})$.

2.15. Definíció

Legyen $\mathcal{R}$ egységelemes gyűrű az e egységelemmel és i egy nemnegatív egész szám. Ekkor $\mathbf{x}_i$ azt az R fölötti sorozatot jelöli, amelyben minden nemnegatív j indexre $(\mathbf{x}_i)_j = \delta_{i,j} e$ ($\delta_{i,j}$ a Kronecker-szimbólum), és $\mathbf{x} = \mathbf{x}_1$.

Δ

2.16. Tétel

Egységelemes $\mathcal{R}$ gyűrűben $i \in \mathbb{N}$-re $\mathbf{x}_i = \mathbf{x}^i$. $\mathbf{x}^i$ az $\mathcal{R}$ gyűrű fölötti valamennyi $\mathbf{u}$ sorozattal felcserélhető.

Δ

Bizonyítás:

Legyen e a gyűrű egységeleme. Megmutatjuk, hogy $\mathbf{x}^u$-ban $(\mathbf{x}^u)_v = \delta_{u,v} e$. $\mathcal{R}$ egységelemes, így $\mathcal{PS}_R$ is egységelemes, és az egységelem az a sorozat, amelyben minden komponens 0, kivéve a 0. indexhez tartozót, amely az eredeti gyűrű egységeleme, vagyis a sorozatok gyűrűjének egységeleme éppen $\mathbf{x}_0$, és mivel egységelemes gyűrűben minden elem nulladik hatványa a gyűrű egységeleme, ezért $\mathbf{x}_0 = \mathbf{x}^0$. Most tegyük fel, hogy ha u egy nemnegatív egész, akkor minden, u-nál nem nagyobb nemnegatív

egész i-vel $\mathbf{x}_i = \mathbf{x}^i$. Ekkor $\mathbf{x}^{u+1} = \mathbf{x}^u\mathbf{x}$ alapján csak olyan j indexre kapunk $\mathbf{x}^{u+1}$-ben nullától különböző tagot, ahol az első tényező indexe $j = u$, a másodiké $i - j = 1$. Ennek egyetlen megoldása $i = u + 1$, ekkor mindkét tényező és a szorzatuk is az egységelem, így $\mathbf{x}^{u+1}$ valóban $\mathbf{x}_{u+1}$-gyel azonos.

Mivel $\mathbf{x}^i$-ben csak e és 0 áll, és ezek R minden elemével felcserélhetőek, így igaz a felcserélhetőségre vonatkozó állítás is.

□

2.17. Tétel

Legyen $\mathcal{R}$ egységelemes gyűrű, és $\mathbf{s}$ egy $\mathcal{R}$ feletti formális hatványsor, továbbá $k \in \mathbb{N}$. Ekkor $\left(\mathbf{x}^k\mathbf{s}\right)_i = 0$, ha $k > i \in \mathbb{N}$, és $\left(\mathbf{x}^k\mathbf{s}\right)_i = s_{i-k}$, amikor $k \leq i \in \mathbb{N}$.

Δ

Bizonyítás:

Ha $k = 0$, akkor $\mathbf{x}^k$ az egységelem, és igaz az állítás. Bármely nemnegatív egész i indexre $(\mathbf{x} \cdot \mathbf{s})_i = \sum_{j=0}^{i} x_j s_{i-j}$. Ha $i = 0$, akkor ez az összeg $x_0 s_0$, és $x_0 = 0$, tehát a szorzat is nulla, míg ha $i > 0$, akkor $j = 1$-re $x_j s_{i-j} = x_1 s_{i-1} = s_{i-1}$, és minden más j-re 0, így maga az összeg is s_{i-1}, ennélfogva $k = 1$-re is igaz a tétel állítása, innen pedig indukcióval kapjuk a bizonyítást tetszőleges pozitív egész k-ra.

□

A fejezet elején foglalkoztunk végtelen tagú összegekkel. Most ezt kiterjesztjük formális hatványsorokból álló végtelen összegekre is.

2.18. Definíció

Legyen $\mathcal{R}$ gyűrű, Γ indexhalmaz, és $\gamma \in \Gamma$-ra $\mathbf{s}^{(\gamma)} \in R^{\mathbb{N}}$. Ha minden $i \in \mathbb{N}$-re $\sum_{\gamma\in\Gamma} s_i^{(\gamma)}$ értelmezett, akkor $\sum_{\gamma\in\Gamma} \mathbf{s}^{(\gamma)}$ is értelmezett, eleme $R^{\mathbb{N}}$-nek, és $\left(\sum_{\gamma\in\Gamma} \mathbf{s}^{(\gamma)}\right)_i = \sum_{\gamma\in\Gamma} s_i^{(\gamma)}$.

Δ

Ez a szabály általánosabb a korábbinál, hiszen olyankor is értelmezzük az összeget, amikor esetleg az összeg végtelen sok tagja nem nulla, de minden indexhez csak véges sok nullától különböző tag tartozik, ugyanakkor elég kézenfekvő, természetes kiterjesztése az ott adott értelmezésnek. A korábban kapott eredményeink segítségével, az ott kapott eredmények felhasználásával könnyen meg lehet mutatni, hogy amennyiben $\prod_{\delta\in\Delta}\sum_{\gamma\in\Gamma_\delta} \mathbf{s}^{(\delta,\gamma)}$ létezik, akkor $\sum_{\varphi\in\times_{\lambda\in\Delta}\Gamma_\delta}\prod_{\delta\in\Delta} \mathbf{s}^{(\delta,\varphi(\delta))}$ is létezik (ahol nem kommutatív gyűrű esetén Δ rendezett), és ekkor a két kifejezés értéke megegyezik, vagyis az összegek szorzatánál elvégezhető a „beszorzás”.

2.19. Tétel

Egységelemes gyűrű fölötti $\mathbf{s}$ formális hatványsorra $\mathbf{s} = \sum_{i=0}^{\infty} s_i\mathbf{x}^i$, és ha $\mathbf{s}$ legfeljebb n-edfokú polinom, akkor $\mathbf{s} = \sum_{i=0}^{n} s_i\mathbf{x}^i$.

Δ

Bizonyítás:

$\left(\sum_{i=0}^{\infty} s_i\mathbf{x}^i\right)_j = \sum_{i=0}^{\infty} s_i\left(\mathbf{x}^i\right)_j = \sum_{i=0}^{\infty} s_i\delta_{i,j} = s_j$. Ha $\mathbf{s}$ legfeljebb n-edfokú polinom, akkor minden $n < j \in \mathbb{N}$ indexre $s_j = 0$, de akkor az ilyen indexekre $s_i\mathbf{x}^i = \mathbf{0}$, ezért $\sum_{i=0}^{\infty} s_i\mathbf{x}^i = \sum_{i=0}^{n} s_i\mathbf{x}^i$.

□

2.20. Tétel

Legyen $\mathcal{R} = (R; +, \cdot)$ gyűrű, és $\mathcal{P}_R$ és $\mathcal{PS}_R$ az $\mathcal{R}$ fölötti polinomok illetve sorozatok gyűrűje. Ekkor $\mathcal{PS}_R$ a $\mathcal{PS}_R$-beli műveletekkel $\mathcal{R}$ fölötti kétoldali modulus, amely akkor és csak akkor unitér, ha $\mathcal{R}$ egységelemes, akkor és csak akkor $\mathcal{R}$ feletti lineáris tér, ha $\mathcal{R}$ ferdetest, és pontosan akkor algebra, ha $\mathcal{R}$ test, és ez utóbbi esetben az algebra rangja végtelen. $\mathcal{P}_R$ az előbbi modulus, $\mathcal{PS}_R$ részmodulusa, amely akkor és csak akkor unitér, vagy lineáris tér, vagy algebra, ha $\mathcal{PS}_R$ rendelkezik a megfelelő tulajdonsággal, és az utolsó esetben ez a részmodulus is végtelen rangú. Az $\mathcal{R}$ fölötti legfeljebb $n-1$-edfokú polinomok halmaza részmodulus $\mathcal{P}_R$-ben, és ha $\mathcal{P}_R$ lineáris tér, akkor az n-nél alacsonyabb fokszámú polinomok összessége, kiegészítve a nullpolinommal, n-dimenziós altér a polinomok $\mathcal{R}$ fölötti lineáris terében.

Δ

Bizonyítás:

Bármely gyűrű kétoldali modulus tetszőleges részgyűrűje fölött, és mivel a modulusszorzást a sorozatok szorzásával definiáltuk, ezért a részgyűrűk egyben részmodulusok is. Mivel a három gyűrű egyszerre egységelemes, és a három gyűrű egységeleme azonos, ezért igaz az unitérségre és lineáris térre vonatkozó állítás is, és a modulus pontosan akkor lesz algebra, ha a modulus unitér, és a részgyűrű része a teljes gyűrű centrumának, vagyis ha $\mathcal{R}$ test.

Ha $\mathbf{a}$ és $\mathbf{b}$ legfeljebb $n-1$-edfokú polinom, akkor ez igaz $r\mathbf{a}$-ra és $\mathbf{a}-\mathbf{b}$-re is, ezért a legfeljebb $n-1$-edfokú polinomok (unitér) részmodulust illetve alteret alkotnak $\mathcal{P}_R$-ben.

Még a rangra illetve dimenzióra vonatkozó állításokat kell igazolni. Most $\mathcal{R}$ test, tehát egységelemes. Legyen n nemnegatív egész szám. $\mathbf{s} = \sum_{i=0}^{n-1} s_i \mathbf{x}^i = \mathbf{0}$ akkor és csak akkor teljesül, ha minden $n < j \in \mathbb{N}$-re $s_j = 0$, vagyis az előbbi j indexekkel az $\mathbf{x}^i$ sorozatok lineárisan függetlenek, és az is látszik, hogy generálják a legfeljebb $n-1$-edfokú polinomok halmazát. De ebből következik, hogy a legfeljebb $n-1$-edfokú polinomok halmaza az összeadásra és skalárral való szorzásra n-dimenziós lineáris tér.

Az előbbi eredmény azt is jelenti, hogy bármilyen nagy pozitív t-re van t lineárisan független vektor $\mathcal{P}_R$-ben, de akkor ez még inkább igaz a teljes $\mathcal{PS}_R$-re, ami mutatja, hogy a test fölötti polinomok és formális hatványsorok valóban végtelen rangú algebrát képeznek.

□

A fentebbi eredmények szerint egységelemes gyűrű feletti hatványsorok és polinomok felírhatóak végtelen illetve véges összeg alakjában. Mivel bármely gyűrű beágyazható egységelemes gyűrűbe, ezért ezt a felírást minden gyűrű esetén megtehetjük.

2.21. Definíció

Legyen x az $\mathcal{R}$ gyűrű felett transzcendens elem, az $\mathcal{R}$ feletti $\mathbf{s} = (s_i)$ sorozatra $\sum_{i=0}^{\infty} s_i x^i = \mathbf{s}$, ahol $s_0 x^0 = s_0$, valamint legyen minden nemnegatív egész i-re $0 \cdot x^i = 0$ és $sx^i = x^i s$. Ekkor x **határozatlan**, és az $\mathcal{R}$ feletti (egyhatározatlanú) formális hatványsorok és (egyhatározatlanú) polinomok halmazát rendre $R[\![x]\!]$ és $R[x]$, a megfelelő gyűrűket $\mathcal{R}[\![x]\!]$ illetve $\mathcal{R}[x]$ jelöli.

Ha $\mathbf{s} = \sum_{i=0}^{t} s_i x^i$ a nemnegatív egész t-vel, akkor t a polinom **formális foka**.

$s_i x^i$ a hatványsor illetve polinom i-**edfokú tag**ja, s_i az i-**edfokú tag együtthatója**. n-edfokú polinomban az n-edfokú tag együtthatója a polinom **főegyütthatój**a, és ha ez a gyűrű egységeleme, akkor a polinom **főpolinom**

Δ

2.22. Tétel

Ha $\mathcal{R}$ egységelemes gyűrű az e egységelemmel, akkor $e\mathbf{x} = \mathbf{x}$, ahol $\mathbf{x}$ az az $\mathcal{R}$ fölötti sorozat, amelyben csak az $i = 1$ indexű komponens nem nulla, és ez éppen e.

Δ

Bizonyítás:
ex a definíció alapján olyan sorozat, amelyben egyetlen, mégpedig az 1-indexhez tartozó komponens nem nulla, és ez a komponens e, tehát az ex formális hatványsor valóban **x**-szel azonos.

□

2.23. Megjegyzés

A fenti tétel szerint x pontosan akkor sorozat illetve polinom $\mathcal{R}$ fölött, ha a gyűrű egységelemes.

Δ

2.24. Tétel

Legyen **s** $\mathcal{R}$ feletti formális hatványsor. **s** akkor és csak akkor (bal oldali) egység $\mathcal{R}[\![x]\!]$-ben, ha s_0 (bal oldali) egység $\mathcal{R}$-ben. **s** felbonthatatlan $\mathcal{R}[\![x]\!]$-ben, ha s_0 felbonthatatlan $\mathcal{R}$-ben.

Δ

Bizonyítás:
Legyen s bal oldali egység $\mathcal{R}$-ben, és **s** olyan sorozat, amelyben $s_0 = s$. Ha **a** tetszőleges sorozat, akkor létezik R-ben olyan b_0, amellyel $sb_0 = a_0$. Tegyük fel, hogy $n > i \in \mathbb{N}$-re van olyan b_i, hogy $\sum_{j=0}^{i} s_j b_{i-j} = a_i$. Innen az $a_n = \sum_{j=0}^{n} s_j b_{n-j} = s_0 b_n + \sum_{j=1}^{n} s_j b_{n-j} = sb_n + t$ egyenlőségnek kell teljesülnie, ahol b_n ismeretlen, azaz olyan b_n-t keresünk, amellyel $sb_n = a_n - t = u$. De s bal oldali egység, ezért van ilyen elem R-ben, vagyis **b** olyan sorozat lesz, amellyel $\mathbf{s} \cdot \mathbf{b} = \mathbf{a}$, és így **s** bal oldali egység a formális hatványsorok gyűrűjében. Ugyanígy kapunk egy olyan **c** sorozatot, amellyel $\mathbf{c} \cdot \mathbf{s} = \mathbf{a}$, ha s egység, vagyis ekkor **s** is egység $\mathcal{R}[\![x]\!]$-ben. Fordítva, tegyük fel, hogy az **s** sorozat bal oldali egység az $\mathcal{R}$ fölötti formális hatványsorok gyűrűjében, és a az R tetszőleges eleme. Mivel **s** bal oldali egység, van olyan $\mathbf{b} \in \mathcal{R}[\![x]\!]$, hogy $\mathbf{s} \cdot \mathbf{b} = a$, ami csak úgy lehetséges, ha $(\mathbf{s} \cdot \mathbf{b})_0 = s_0 b_0 = a$, vagyis s_0 bal oldali egység $\mathcal{R}$-ben. Ha **s** egyben egység, akkor az előbbiekhez hasonlóan láthatjuk be, hogy s_0 egyben jobb oldali egység is az alapgyűrűben, vagyis egység $\mathcal{R}$-ben.

Amennyiben c az $\mathcal{R}$ felbonthatatlan eleme, és $\mathbf{c} = \mathbf{a} \cdot \mathbf{b}$, akkor $c_0 = a_0 b_0$-ban a_0 és b_0 egyike szükségszerűen a megfelelő oldalról egység $\mathcal{R}$-ben. Ekkor az adott sorozat is hasonló tulajdonságú a hatványsorok gyűrűjében, így **c** az $\mathcal{R}[\![x]\!]$ felbonthatatlan eleme.

□

Ferdetestben pontosan a nullától különböző elemek egységek, ezért igaz az alábbi eredmény.

2.25. Következmény

Ferdetest feletti formális hatványsor pontosan akkor egység, ha konstans tagja nem nulla.

Δ

2.26. Megjegyzés

Az előbbi tétel és az utána álló következménye $\mathcal{R}[x]$-re nem igaz: ha $\mathcal{R}$ a racionális számok teste, akkor $(1, -1)$ nem osztója $(1,1)$-nek mint polinomnak, tehát $(1, -1)$ nem egység, jóllehet 1 egység $\mathbb{Q}$-ban, ugyanakkor 5 felbonthatatlan $\mathbb{Z}$-ben, ám az $(5, -6,1)$ polinom előáll $(1, -1)(5, -1)$ alakban.

Δ

2.27. Tétel

Amennyiben $\mathcal{R}$ egységelemes gyűrű, akkor $\mathcal{R}[\![x]\!]$ minden **t** eleme $x^u \mathbf{s}$ alakú, ahol $u \in \mathbb{N}$, és $\mathbf{s} = \mathbf{0}$ vagy $s_0 \neq 0$, és az utóbbi esetben az ilyen felírás egyértelmű. Ha $\mathcal{R}$ ferdetest és $\mathbf{t} \neq \mathbf{0}$, akkor **s** egység $\mathcal{R}[\![x]\!]$-ben, és ha test, akkor $\mathcal{R}[\![x]\!]$ euklideszi gyűrű.

Δ

Bizonyítás:

$\mathcal{R}$ egységelemessége alapján x minden nemnegatív egész kitevős hatványa eleme $\mathcal{R}[\![x]\!]$-nek, és $x = \mathbf{x}$. $x^u\mathbf{s} = \mathbf{0}$ akkor és csak akkor, ha $\mathbf{s} = \mathbf{0}$, és ekkor minden $u \in \mathbb{N}$-nel $\mathbf{0} = x^u\mathbf{0} = x^u\mathbf{s} = \mathbf{t}$. Legyen $\mathbf{t} \neq \mathbf{0}$-ban az r-edik tag az első nullától különböző, és $\mathbf{s}$ az a sorozat, amelyben $s_i = t_{r+i}$. Korábban már beláttuk, hogy $(\mathbf{x}^r\mathbf{s})_i$ nulla, ha $r > i \in \mathbb{N}$, egyébként $s_{i-r} = t_{(r+i)-r} = t_i$ az értéke, így minden $i \in \mathbb{N}$-re $(\mathbf{x}^r\mathbf{s})_i = t_i$, tehát $\mathbf{x}^r\mathbf{s} = \mathbf{t}$. $s_0 \neq 0$, ezért ha $\mathcal{R}$ ferdetest, akkor egy korábbi tétel alapján $\mathbf{s}$ egység $\mathcal{R}[\![x]\!]$. Mivel nemnegatív egész számok nem üres halmazában a legkisebb elem egyértelmű, ezért az ilyen alakban való felírás egyértelmű.

A $\mathbf{0} \neq \mathbf{t} = \mathbf{x}^r\mathbf{s}$ alakú felírásban $\mathbf{s}$ konstans tagja nem nulla, ezért ha $\mathcal{R}$ test, akkor $\mathbf{s}$ egység az $\mathcal{R}[\![x]\!]$ gyűrűben. $\varphi(\mathbf{t}) = r$ az $\mathcal{R}$ feletti nem nulla formális hatványsorokat képezi le $\mathbb{N}$-be. Ha $\mathbf{a} = x^u\mathbf{a}_1$ és $\mathbf{b} = x^v\mathbf{b}_1$, ahol $\mathbf{a}_1$ és $\mathbf{b}_1$ egység, akkor $u \geq v$ esetén $\mathbf{a} = x^u\mathbf{a}_1 = (x^{u-v}\mathbf{q}_1)(x^v\mathbf{b}_1) = \mathbf{q} \cdot \mathbf{b}$, ahol $\mathbf{q}_1$ az $\mathbf{a}_1$ és $\mathbf{b}_1$ (asszociálttól eltekintve egyértelmű) hányadosa. Ez a hányados létezik, hiszen most $\mathbf{b}_1$ egység. Ha viszont $u < v$, akkor $\mathbf{a} = 0 \cdot \mathbf{b} + \mathbf{a}$, és $\varphi(\mathbf{a}) = u < v = \varphi(\mathbf{b})$.

□

2.28. Megjegyzés

Ha $\mathbf{a}$ és $\mathbf{b}$ polinomok, akkor $\mathbf{q}$ általában nem polinom, tehát *a fenti φ-vel* $\mathcal{R}[x]$ nem euklideszi gyűrű még akkor sem, ha $\mathcal{R}$ test (de test feletti polinomgyűrű euklideszi, csak nem ezzel a normával, hanem a fokszámmal mint normával).

Δ

2.29. Tétel

Ha $\mathcal{K}$ test, akkor létezik $\mathcal{K}[\![x]\!]$ hányadosteste, és ennek nem nulla elemei $\mathbf{x}^u\mathbf{s}$ alakúak, ahol $\mathbf{s}$ egy $\mathcal{K}[x]$-beli egység és $u \in \mathbb{Z}$.

Δ

Bizonyítás:

Test kommutatív és nullosztómentes, ezért $\mathcal{K}[\![x]\!]$ is kommutatív és nullosztómentes gyűrű, így létezik a hányadosteste. Test feletti hatványsor $\mathbf{x}^u\mathbf{a}$ alakban írható, ahol u nemnegatív egész szám, és vagy $\mathbf{a}$ konstans tagja nullától különböző, tehát egység $\mathcal{K}$-ban, és így $\mathbf{a}$ egység $\mathcal{K}[\![x]\!]$-ben, vagy $\mathbf{a} = \mathbf{0}$. A hányadostest elemei az olyan $(\mathbf{x}^u\mathbf{a}, \mathbf{x}^v\mathbf{b})$ alakú párok által reprezentált osztályok, amelyekben $\mathbf{b} \neq \mathbf{0}$, és ahol két ilyen pár, az előbbi mellett például az $(\mathbf{x}^w\mathbf{c}, \mathbf{x}^z\mathbf{d})$ pár akkor és csak akkor van egy osztályban, ha $\mathbf{x}^{u+z}\mathbf{ad} = x^{v+w}\mathbf{bc}$. A műveleteket a hányadostestekben megszokott módon definiáljuk, vagyis a fentebbi párokkal reprezentált osztályok összege az $(\mathbf{x}^{u+z}\mathbf{ad} + x^{v+w}\mathbf{bc}, \mathbf{x}^{v+z}\mathbf{bd})$ pár osztálya, míg a szorzata az $(\mathbf{x}^{u+w}\mathbf{ac}, \mathbf{x}^{v+z}\mathbf{bd})$ párt tartalmazó osztály. Legyen e a $\mathcal{K}$ test egységeleme, ekkor e $\mathcal{K}[\![x]\!]$-nek is az egységeleme. A hányadostestben az $(\mathbf{x}^u\mathbf{a}, e)$ alakú elemekkel reprezentált osztályok a $\mathcal{K}[\![x]\!]$-szel izomorf részgyűrűt alkotnak, ahol az izomorfizmus az előbbi $(\mathbf{x}^u\mathbf{a}, e)$ párhoz tartozó osztálynak a $\mathcal{K}[\![x]\!]$-beli $\mathbf{x}^u\mathbf{a}$ elemet felelteti meg. Az izomorfizmus alapján $\mathcal{K}[\![x]\!]$ beágyazható a hányadostestbe, így a testben az $(\mathbf{x}^u\mathbf{a}, e)$ párt tartalmazó osztályt és $\mathbf{x}^u\mathbf{a}$-t azonosnak tekinthetjük. A test egységeleme az azonos, nullától különböző elemekből álló párok osztálya. $\mathbf{b} \neq \mathbf{0}$ esetén az $(e, \mathbf{x}^v\mathbf{b})$ alakú elemmel reprezentált osztály láthatóan inverze az $(\mathbf{x}^v\mathbf{b}, e)$ párt tartalmazó osztálynak. Ezt az osztályt jelölhetjük $\mathbf{x}^{-u}\mathbf{b}^{-1}$-gyel ($\mathbf{b}^{-1}$ létezik, mivel $\mathbf{b}$ mint hatványsor egység). Ekkor $(\mathbf{x}^u\mathbf{a}, \mathbf{x}^v\mathbf{b}) = (\mathbf{x}^u\mathbf{a}, e)(e, \mathbf{x}^v\mathbf{b}) = \mathbf{x}^u\mathbf{a} \cdot \mathbf{x}^{-v}\mathbf{b}^{-1} = \mathbf{x}^w\mathbf{c}$, ahol $w = u - v \in \mathbb{Z}$, és vagy $\mathbf{c} = \mathbf{0}$ ($\mathbf{a} = \mathbf{0}$ esetén), vagy $\mathbf{c} = \mathbf{ab}^{-1}$ egység $\mathcal{K}[\![x]\!]$-ben.

□

2.30. Definíció

Ha $\mathcal{K}$ test, akkor $\mathcal{K}[\![x]\!]$hányadosteste a $\mathcal{K}$ **feletti Laurent-sorok teste**.

Δ

A Laurent-sorok testét $\mathcal{K}\langle x\rangle$ jelöli.

2.31. Tétel

Ha $\mathcal{R}$ egységelemes gyűrű az e egységelemmel, akkor $e - x$ inverze $\mathcal{R}[\![x]\!]$-ben $\sum_{i=0}^{\infty} x^i$.

Δ

Bizonyítás:

Legyen $\mathbf{s} = \sum_{i=0}^{\infty} x^i$, ekkor $(e-x)\sum_{i=0}^{\infty} x^i = (e-x)\mathbf{s} = \mathbf{s} - x\cdot\mathbf{s} = \mathbf{s} - \mathbf{t}$, ahol $\mathbf{t} = x\cdot\mathbf{s}$. $\mathbf{s}$ minden eleme e, míg $t_0 = 0$ és $i \in \mathbb{N}$-re $t_i = s_{i-1} = e = s_i$. Ebből $(\mathbf{s}-\mathbf{t})_0 = s_0 - t_0 = e$, és $i \neq 0$-ra $(\mathbf{s}-\mathbf{t})_i = s_i - t_i = 0$, azaz $(e-x)\mathbf{s} = e$. A másik oldali szorzás hasonló eredményt ad.

□

2.32. Következmény

Ha $p \in \mathbb{N}^+$ és $\mathbf{f} = \sum_{i=0}^{p-1} a_i x^i \in R[x]$ az $\mathcal{R}$ egységelemes gyűrűvel, akkor

1. $\mathbf{f}\cdot(e-x^p)^{-1} = \sum_{i=0}^{\infty} c_i x^i = (e-x^p)^{-1}\cdot\mathbf{f}$, ahol $c_i = a_{i \bmod p}$;
2. az előbbi c_l-lel minden nemnegatív egész i-re $c_i = c_{i+p}$, és ha j is nemnegatív egész szám, és $i \equiv j\ (p)$, akkor $c_i = c_j$;
3. $(e-x)^{-n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k$.

Δ

Bizonyítás

1. Az előző tétel alapján $(e-x^p)^{-1} = \sum_{i=0}^{\infty}(x^p)^i = \sum_{i=0}^{\infty} x^{pi} = \sum_{i=0}^{\infty} \delta_{i \bmod p,0} x^i$. Ekkor

$$(\mathbf{f}\cdot(e-x^p)^{-1})_i = \sum_{j=0}^{i} a_j \delta_{(i-j) \bmod p,0} = \sum_{j=0}^{p-1} a_j \delta_{(i-j) \bmod p,0} = \sum_{j=0}^{p-1} a_j \delta_{i \bmod p,j} = a_{i \bmod p},$$

mert ha $p \leq j \in \mathbb{N}$, akkor $a_j = 0$, míg $p > j > i \in \mathbb{N}$ esetén $-p < i - j < 0$, tehát $\delta_{(i-j) \bmod p,0} = 0$, és így $\mathbf{f}(e-x^p)^{-1} = \sum_{i=0}^{\infty} a_{i \bmod p} x^i$. $\mathbf{f}$-fel a másik oldalról szorozva ugyanezt az eredményt kapjuk.

2. $i \bmod p = (i+p) \bmod p$, és ha $i \equiv j\ (p)$, akkor $i \bmod p = j \bmod p$.

3. $(e-x)^{-n} = \left(\sum_{i=0}^{\infty} x^i\right)^n = \sum_{i_0=0}^{\infty} \cdots \sum_{i_{n-1}=0}^{\infty} x^{i_0+\cdots+i_{n-1}} = \sum_{i=0}^{\infty} t_i x^i$, ahol t_k az összes olyan $i_0 + \cdots + i_{n-1}$ összeg száma, amelynek az értéke k, és ahol minden tag nemnegatív. Ez éppen a $k+1$ elemből választott $n-1$-edrendű ismétléses kombináció. Egy ilyen kombináció ugyanis kölcsönösen egyértelmű módon megfeleltethető a $\{0,1,\ldots,k\}$ halmaz elemeiből álló $n-1$ hosszúságú monoton növekvő sorozatoknak. Nézzük az $s_j = i_0 + \cdots + i_{j-1}$ összegeket $j = 1,\ldots,n-1$-re. Mivel minden tag nemnegatív, ezért ez a sorozat monoton növekszik, a legkisebb érték $i_0 = 0$ esetén 0, a legnagyobbat pedig akkor kapjuk, ha $i_{n-1} = 0$, ekkor ugyanis s_{n-1} értéke k kell, hogy legyen. Az ilyen kombinációk számát viszont tudjuk: $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$.

□

Most a polinomok néhány tulajdonságát vizsgáljuk. Mivel a polinomok a korábbi tanulmányok során is előfordultak, ezért az ismertnek feltételezett ismeretek ismét bizonyítás nélkül szerepelnek.

Mivel az $\mathcal{R}$ gyűrű fölötti polinomok $R[x]$ halmaza a polinomokra megadott műveletekkel gyűrű, ezért mindazon fogalmak értelmezhetőek benne, amelyeket minden gyűrűre definiáltunk. Ennek megfelelően vizsgálhatjuk polinomgyűrűben az oszthatóságot. Indukcióval könnyen belátható, hogy ha az $R[x]$-beli g főegyüttható jobb oldali egység $\mathcal{R}$-ben, akkor az $R[x]$ bármely f polinomjához lehet találni $R[x]$-ben olyan q és r polinomot, amelyekkel $f = qg + r$, és ha r nem a nullpolinom, akkor a foka kisebb, mint g foka (vagyis elvégezhető a maradékos osztás). Még az is belátható, hogy q és r egyértelműen meghatározott. Mivel testben minden nem nulla elem egység, ezért test feletti polinomgyűrűben nem nulla polinommal a maradékos osztás mindig egyértelműen elvégezhető.

Legyen $\mathcal{S}$ gyűrű, A egy nem üres halmaz, és $F_{A,S}$ legyen az A-t S-be képező függvények halmaza. Ha f és g $F_{A,S}$ két eleme, akkor legyen $(f \oplus g)(a) = f(a) + g(a)$ és $(f \otimes g)(a) = f(a) \cdot g(a)$, ahol a az A eleme, és $+$ illetve $\cdot$ az $\mathcal{S}$ két művelete. Könnyű belátni, hogy a fenti két szabály egy-egy binér műveletet definiál $F_{A,S}$-en, és $F_{A,S}$ ezzel a két művelettel gyűrű. Az is könnyen ellenőrizhető, hogy ez a gyűrű pontosan akkor kommutatív, ha $\mathcal{S}$ kommutatív, akkor és csak akkor van benne bal oldali egységelem, ha $\mathcal{S}$-ben van bal oldali egységelem, és akkor és csak akkor nullosztómentes, ha $\mathcal{S}$ a nullgyűrű, vagy ha A-nak egy eleme van és $\mathcal{S}$ nullosztómentes. Most legyen R az $\mathcal{S}$ egy $\mathcal{R}$ részgyűrűjének alaphalmaza, és az R bármely r és az S tetszőleges s eleme esetén legyen definíció szerint $rs^0 = r$ (ami egységelemes gyűrű esetén eleve igaz). Ha $f = \sum_{i=0}^{n} f_i x^i \in R[x]$ egy $\mathcal{R}$ feletti polinom, akkor $\left\{\sum_{i=0}^{n} f_i s^i \,\middle|\, s \in S\right\}$ az S önmagába való leképezése, vagyis eleme $F_{S,S}$-nek. Ez az f polinomhoz tartozó **polinomfüggvény**, amelyet a továbbiakban $\hat{f}$ jelöl, és $\hat{f}(s)$ **az** f **(jobb oldali) helyettesítési értéke az** s **helyen.** Amennyiben f konstans polinom, és a konstans tagja f, akkor az S tetszőleges s elemével $\hat{f}(s) = \sum_{i=0}^{0} f_i s^i = f_0 = f$, vagyis konstans polinom helyettesítési értéke bármely helyen a polinom konstans tagjával, azaz magával a polinommal azonos.

Legyen f egy legfeljebb n_f-fokú, g egy legfeljebb n_g-fokú $\mathcal{R}$ feletti polinom, és legyen $n \in \mathbb{N}$ olyan, hogy mindkét polinom legfeljebb n-edfokú. Most

$$\left(\hat{f} \oplus \hat{g}_{-}\right)(a) = \hat{f}(a) - \hat{g}(a) = \sum_{i=0}^{n} f_i a^i - \sum_{i=0}^{n} g_i a^i = \sum_{i=0}^{n} (f_i - g_i) a^i = \sum_{i=0}^{n} h_i a^i = \hat{h}(a),$$

ahol $h = f - g$, és ha R része $\mathcal{S}$ centrumának, akkor

$$\left(\hat{f} \otimes \hat{g}\right)(a) = \hat{f}(a) \cdot \hat{g}(a) = \left(\sum_{i=0}^{n_f} f_i a^i\right) \cdot \left(\sum_{i=0}^{n_g} g_i a^i\right) = \sum_{i=0}^{n_f+n_g} \left(\sum_{j=0}^{i} f_i g_i\right) a^i = \sum_{i=0}^{n_f+n_g} t_i a^i = \hat{t}(a)$$

a $t = fg$ jelöléssel, vagyis polinomfüggvények összege és szorzata a polinomok összegéhez illetve szorzatához tartozó polinomfüggvény (utóbbinál feltéve, hogy a polinomok együtthatói $\mathcal{S}$ centrumában vannak). Az $\mathcal{R}$ feletti polinomok halmaza nem üres, így az $\mathcal{R}$ feletti polinomfüggvények halmaza sem üres, tehát $\mathcal{F}_{S,S}$-nek egy $\mathcal{F}_S^{(R)}$ részgyűrűjét alkotják, ha R része $\mathcal{S}$ centrumának.

Ha $\mathcal{R} \leq \mathcal{S}$, akkor $\mathcal{R}[x] \leq \mathcal{S}[x]$. Legyen $\mathcal{S}$ egységelemes és u az S egy eleme. Ekkor $x - u$ $\mathcal{S}$ fölötti elsőfokú polinom, és ha f egy $\mathcal{R}$ fölötti tetszőleges polinom, akkor $\mathcal{S}$ fölötti alkalmas q és legfeljebb nulladfokú, azaz konstans r polinommal $f = q \cdot (x - u) + r$. Most az u-t f-be helyettesítve $\hat{f}(u) = \hat{q}(u) \cdot (u - u) + \hat{r}(u) = \hat{r}(u) = r$, vagyis $f = q \cdot (x - u) + \hat{f}(u)$.

2.33. Definíció

Legyen $\mathcal{S}$ gyűrű, $\mathcal{R}$ az $\mathcal{S}$ részgyűrűje, f egy $\mathcal{R}$ fölötti polinom, és s az S eleme. s **(jobb oldali) gyöke** f**-nek**, ha $\hat{f}(s) = 0$.

Δ

A fentebbi megfontolás alapján igaz az alábbi tétel.

2.34. Tétel

Ha $\mathcal{R}$ részgyűrűje az $\mathcal{S}$ egységelemes gyűrűnek, úgy az S-beli u pontosan akkor (jobb oldali) gyöke az $\mathcal{R}$ feletti f polinomnak, ha az $\mathcal{S}$ feletti $x - u$ polinom $\mathcal{S}[x]$-ben (jobb oldali) osztója f-nek.

Δ

Ha az $\mathcal{S}$ egységelemes gyűrű u eleme (jobb oldali) gyöke az $\mathcal{S}$ egy $\mathcal{R}$ részgyűrűje fölötti f polinomnak, akkor $x - u$ az f egy **(jobb oldali) gyöktényezője**. Ez tehát ekvivalens azzal, hogy $x - u$

(jobb oldali) osztója f-nek. Előfordulhat, hogy $x-u$-nak egy egynél nagyobb kitevős hatványa is osztója f-nek. Ha egy t pozitív egész kitevős hatványra ez igaz, akkor u az f **(legalább)** t**-szeres gyöke**, és **pontosan** t**-szeres gyöke**, ha t-szeres, de nem $t+1$-szeres gyöke. Ekkor t az u gyök **multiplicitása** (vagy **többszörössége**), és $f=g\cdot(x-u)^t$, de $\hat{g}(u)\neq 0$.

Gyökök többszörössége vizsgálható a polinom deriváltjának a segítségével. Az $f=\sum_{i=0}^{n} f_i x^i$ polinom deriváltja $f'=\sum_{i=0}^{n-1}(i+1)f_{i+1}x^i$. Ez a derivált formailag megegyezik egy polinom analízisbeli deriváltjával, és érvényes itt is az $(f+g)'=f'+g'$ és $(fg)'=f'g+fg'$ szabály, továbbá kommutatív gyűrű esetén $(f^n)'=nf^{n-1}f'$ pozitív egész n-nel.

A definíciót alkalmazva könnyű látni, hogy egy nullosztómentes gyűrű feletti polinomgyűrű karakterisztikája megegyezik az eredeti gyűrű karakterisztikájával.

2.35. Tétel

Legyen f az $\mathcal{R}$ integritási tartomány feletti polinom, és u az R eleme. Ha u az f m-szeres gyöke, ahol m pozitív egész szám, akkor f'-nek legalább $m-1$-szeres gyöke, és pontosan $m-1$-szeres gyöke, ha $f\neq 0$, f-nek pontosan m-szeres gyöke és m nem osztható a gyűrű karakterisztikájával.

Δ

A tételből látszik, hogy ha $\mathcal{R}$ 0-karakterisztikájú integritási tartomány, akkor egy többszörös gyök pontosan eggyel kisebb multiplicitású gyöke a polinom deriváltjának, mint magának a polinomnak. Ugyanakkor prímkarakterisztikájú integritási tartomány fölötti polinom többszörös gyöke a derivált polinomnak akármilyen nagy (a fokszám által korlátozott) multiplicitású gyöke is lehet.

Igen fontos az alábbi tétel.

2.36. Tétel

Az $\mathcal{R}$ integritási tartomány feletti n-edfokú f polinomnak multiplicitással együtt is legfeljebb n gyöke van R-ben. Ha $\mathcal{R}$ egységelemes, $u_0,\dots,u_{m-1}$ az f páronként különböző gyöke R-ben, és a gyökök multiplicitása rendre $t_0,\dots,t_{m-1}$, akkor $f=g\prod_{i=0}^{m-1}(x-u_i)^{t_i}$, és g-nek egyik u_i sem gyöke.

Δ

Igen lényeges, hogy ez a tétel csak integritási tartomány feletti polinomra igaz. Például a $\mathbb{Z}_6$ fölötti $x^2-\tilde{5}$ polinomnak gyöke a $\tilde{0}$, a $\tilde{2}$, a $\tilde{3}$ és az $\tilde{5}$, vagyis a másodfokú polinomnak négy különböző gyöke van, míg az x^2+1 polinomnak bármely olyan $a+bi+cj+dk$ kvaternió gyöke, amelyben $a=0$ és $b^2+c^2+d^2=1$, tehát most az ismét másodfokú polinomnak végtelen sok különböző gyöke van. Az első esetben a gyűrű nem nullosztómentes, míg a második esetben nem kommutatív, tehát egyik esetben sem integritási tartomány. Integritási tartomány testbe ágyazható, és test mindig bővíthető úgy, hogy a bővebb testben már a polinom lineáris tényezők és az eredeti gyűrű egy nem nulla elemének szorzatára bomlik, vagyis a bővebb testben a polinomnak multiplicitással számolva a fokszámával azonos számú gyöke van (ez akkor is igaz, ha a polinom foka 0, mert nullatényezős szorzat definíció szerint az egységelem). Egységelemes integritási tartomány fölött tehát egy nem nulla polinomnak pontosan akkor van többszörös gyöke, ha a polinomnak és deriváltjának a legnagyobb közös osztója legalább elsőfokú, és ekkor a többszörös gyökök ezen legnagyobb közös osztó gyökei.

$\mathbb{Z}[x]$ példa olyan Gauss-gyűrűre, amely nem főideálgyűrű, hiszen például az $\{1,x\}$ által generált ideál nem generálható egyetlen elemmel. Ugyanakkor igaz az alábbi tétel.

2.37. Tétel

Test fölötti egyhatározatlanú polinomgyűrű euklideszi gyűrű. Gauss-gyűrű fölötti polinomgyűrű Gauss-gyűrű.

Δ

A fenti tételből következik az az előbbi állításunk, hogy egész együtthatós polinomok gyűrűje Gauss-gyűrű, hiszen az egész számok gyűrűje ilyen. Indukcióval azt is kapjuk, hogy Gauss-gyűrű fölötti n-határozatlanú polinomgyűrű is Gauss-gyűrű, ahol n egy nemnegatív egész szám.

Most nézzük egy $\mathcal{R}$ egységelemes gyűrű fölött az $x^n - e$ alakú polinomokat.

Ha $\mathcal{R}$ egységelemes, akkor $\mathcal{R}[x]$ is egységelemes gyűrű, és ekkor x és tetszőleges nemnegatív egész n-re x^n is eleme a polinomgyűrűnek. Elsőként belátjuk, hogy ha m és n nemnegatív egész szám, úgy $x^m - e$ pontosan akkor osztója $x^n - e$-nek, ha $m|n$. Legyen először $m|n$, azaz $n = mt$ egy $\mathbb{N}$-beli t-vel. Ekkor $(x^m - e)\sum_{i=0}^{t-1}(x^m)^i = x^{tm} - e = \left(\sum_{i=0}^{t-1}(x^m)^i\right)(x^m - e)$, és $x^{tm} - e = x^n - e$, így teljesül az $x^m - e|x^n - e$ oszthatóság. Fordítva, tegyük fel, hogy $x^m - e|x^n - e$. Ha $m = 0$, akkor $x^m - e = 0$, és ekkor $x^n - e = 0$, hiszen a 0 csak önmagának osztója. De $x^n - e = 0$ csak úgy lehet, ha $n = 0$, és ekkor teljesül az $m|n$ reláció. Most nézzük az $m > 0$ esetet. Maradékosan osztva n-et m-mel, $n = tm + r$, ahol $t \in \mathbb{N}$ és $m > r \in \mathbb{N}$. Ekkor $x^n - e = x^r(x^{tm} - e) + (x^r - e)$. A feltevésünk szerint a bal oldal osztható $x^m - e$-vel, és az előbb igazoltuk, hogy ugyanez igaz $x^{tm} - e$-re, tehát $x^r(x^{tm} - e)$-re. Ekkor $x^m - e$ osztja $x^r - e$-t is, ami csak úgy lehet, ha $r = 0$, hiszen $0 \leq r < m$, és nem nulla polinom csak nála nem nagyobb fokszámú polinommal osztható (mert nem nulla polinomok szorzatának foka nem nagyobb a két polinom fokszámának összegénél). Ám ha $r = 0$, akkor $n = tm$, vagyis $m|n$.

Az $x^n - e = x^r(x^{tm} - e) + (x^r - e)$ felírás, ahol $m > r \in \mathbb{N}$, minden esetben igaz, ha $m > 0$, azaz ha $x^n - e \neq 0$, így azt is beláttuk, hogy a nemnegatív egész kitevős $x^u - e$ alakú polinomok körében a nullától különböző osztóval végzett maradékos osztás maradéka is ilyen alakú polinom.

Ha $x^m - e|x^n - e$, és $m \neq 0$, tehát $x^m - e \neq 0$, akkor van egy és csak egy olyan $g \in R[x]$ polinom, hogy $g \cdot (x^m - e) = x^n - e = (x^m - e) \cdot g$. Ezt a polinomot általában az $\frac{x^n - e}{x^m - e}$ alakban írjuk.

Nézzük most $x^m - e$ és $x^n - e$ legnagyobb közös osztóját, ahol m és n tetszőleges nemnegatív egész számok. Legyen a két kitevő legnagyobb közös osztója d, ekkor, az előbbiek szerint, $x^d - e$ közös osztója a két polinomnak. Megmutatjuk, hogy ez a polinom a legnagyobb közös osztó. Ha $d = m$, akkor az $x^m - e$ és $x^n - e$ bármely közös osztója osztója $x^m - e$-nek, tehát $x^d - e$-nek, így ez utóbbi polinom legnagyobb közös osztó, és nyilván ugyanezt az eredményt kapjuk akkor is, ha $d = n$. Ha $m \neq d \neq n$, akkor $m \neq 0 \neq n$, és ekkor $\min\{m, n\} > d \in \mathbb{N}^+$, és alkalmas u és v egész számokkal $d = um + vn$. Most sem u, sem v nem lehet 0, mert ha például $u = 0$, akkor $n|d$, ami lehetetlen, hiszen a 0-tól különböző d pozitív osztója nem lehet d-nél nagyobb. u és v egyike pozitív, a másik pedig negatív, mert m és n pozitív, és ha mind u, mind v pozitív, akkor $d = um + vn \geq m$, míg ha mindkettő negatív, akkor $d = um + vn < 0$. Nyilván akár u-ról, akár v-ről feltehetjük, hogy negatív, legyen például $u < 0$. Ekkor $x^{d+(-u)m} - e = x^{vn} - e$, ahol mindkét oldalon a kitevő pozitív egész szám. Ha $f \in R[x]$ közös osztója $x^m - e$-nek és $x^n - e$-nek, akkor $f|x^m - e|x^{(-u)m} - e$, valamint $f|x^n - e|x^{vn} - e = x^{d+(-u)m} - e = x^d\left(x^{(-u)m} - e\right) + \left(x^d - e\right)$, így f $x^d - e$-nek is osztója, amiből kapjuk, hogy most is $x^d - e$ az $x^m - e$ és $x^n - e$ polinomok legnagyobb közös osztója.

Ha $1 < q \in \mathbb{N}$, akkor x helyére q-t és e helyére 1-et írva igaz marad az oszthatóságra és legnagyobb közös osztóra vonatkozó állítás. Ehhez a fenti levezetésben csak annyit kell változtatni, hogy ha s az m-nél kisebb pozitív egész szám, akkor $1 < q$ következtében $0 < 1 \leq q^s - 1 < q^m - 1$, és így nem teljesülhet a $q^m - 1|q^s - 1$ oszthatóság.

A fejezet végén a polinomok kompozíciójával foglalkozunk.

2.38. Definíció

Legyen $f = \sum_{i=0}^{n_f} a_i x^i$ és $g = \sum_{i=0}^{n_g} b_i x^i$ az $\mathcal{R}$ gyűrű feletti polinom. Ekkor $f \circ g = \sum_{i=0}^{n_f} a_i g^i$ az f **és** g – ebben a sorendben vett – **kompozíciója**.

Δ

Egy polinomgyűrű akkor és csak akkor a nullgyűrű, ha maga az alapgyűrű is a nullgyűrű, és nullgyűrűben a kompozíció nem túl érdekes, hiszen ekkor a kompozíció eredménye is a gyűrű nulleleme, ezért az alábbiakban nem foglalkozunk a nullgyűrűvel.

2.39. Tétel

Legyen $\mathcal{R}$ legalább két elemet tartalmazó gyűrű. Az $\mathcal{R}[x]$-beli kompozíció binér művelet az $\mathcal{R}$ feletti polinomok halmazán, minden konstans polinom bal oldali zéruseleme a műveletnek, és $\circ$ jobbról disztributív a polinom-összeadásra nézve. $R[x]$-ben akkor és csak akkor van olyan $f \neq 0 \neq g$ polinom, amellyel $f \circ g = 0$, ha $\mathcal{R}$ nem nullosztómentes, és $(R[x];\circ)$ pontosan akkor (bal oldali) egységelemes, ha $\mathcal{R}$-ben létezik a megfelelő tulajdonságú elem. Ha $\mathcal{R}$ kommutatív, akkor $\circ$ jobbról disztributív az $\mathcal{R}[x]$-beli szorzásra nézve, és $(R[x];\circ)$ félcsoport.

Δ

Bizonyítás:

Legyen f, g és h $\mathcal{R}$ feletti polinom, $f = \sum_{i=0}^{n_f} a_i x^i$ és $g = \sum_{i=0}^{n_g} b_i x^i$. Ekkor $f \circ g = \sum_{i=0}^{n_f} a_i g^i$; $g \in R[x]$, így g^i és $a_i g^i$ is $\mathcal{R}$ feletti, egyértelműen meghatározott polinom, de akkor ezek összege is egyértelműen meghatározott eleme $R[x]$-nek, vagyis a polinomgyűrű zárt a kompozícióra. Ha f konstans polinom, azaz $f = c \in R$, akkor tetszőleges $g \in R[x]$ polinommal $f \circ g = c \circ g = c = f$, ami mutatja, hogy f bal oldali zéruseleme a kompozíciónak. Legyen $n \geq \max\{n_f, n_g\}$. Ezzel

$$\begin{aligned}(f+g)\circ h &= \left(\sum_{i=0}^{n}(a_i+b_i)x^i\right)\circ h = \sum_{i=0}^{n}(a_i+b_i)h^i \\ &= \sum_{i=0}^{n} a_i h^i + \sum_{i=0}^{n} b_i h^i = \sum_{i=0}^{n_f} a_i h^i + \sum_{i=0}^{n_g} b_i h^i \\ &= \left(\sum_{i=0}^{n_f} a_i x^i\right)\circ h + \left(\sum_{i=0}^{n_g} b_i x^i\right)\circ h = f\circ h + g\circ h,\end{aligned}$$

így a kompozíció jobbról disztributív a polinom-összeadásra nézve.

Legyen $a_{n_f} \neq 0 \neq b_{n_g}$, ekkor $f \circ g$-ben az $n_f n_g$-edfokú tag együtthatója $a_{n_f} b_{n_g}^{n_f}$. Ha $\mathcal{R}$ nullosztómentes, akkor az előbbi együttható nem nulla, így $f \circ g \neq 0$. Ellenkező esetben legyen az R u és v eleme – ebben a sorrendben vett – nullosztópár. Ekkor $(ux) \circ v = uv = 0$, jóllehet $ux \neq 0 \neq v$.

Ha $e_b \in \mathcal{R}$ bal oldali egységeleme $\mathcal{R}$-nek, akkor e_b bal oldali egységelem a polinomgyűrűben, így $(e_b x) \circ f = e_b f = f$. Hasonlóan, amennyiben e_j jobb oldali egységelem az $\mathcal{R}$ gyűrűben, akkor $f \circ (e_j x) = \sum_{i=0}^{n_f} a_i (e_j x)^i = \sum_{i=0}^{n_f} (a_i e_j^i) x^i = \sum_{i=0}^{n_f} a_i x^i = f$, végül ha e egységelem, akkor az előbbiek szerint $x = ex$ egyszerre bal és jobb oldali egységeleme, tehát egységeleme a kompozíciónak. Most tegyük fel, hogy a kompozíciónak van bal oldali egységeleme, és ez az $\varepsilon^{(b)}$ polinom. Konstans polinom bal oldali zéruseleme a kompozíciónak, és legalább két elemet tartalmazó grupoidban bal oldali zéruselem nem lehet bal oldali egységelem, ezért a polinom nem a nullpolinom, van foka, és a foka, n, legalább 1. Ekkor $ux = \varepsilon^{(b)} \circ (ux) = \sum_{i=0}^{n} \varepsilon_i^{(b)} (ux)^i = \varepsilon_0^{(b)} + \sum_{i=1}^{n} \left(\varepsilon_i^{(b)} u^i\right) x^i$, és ebből $\varepsilon_1^{(b)} u = u$ az R bármely u elemére, így $\varepsilon_1^{(b)}$ bal oldali egységelem az $\mathcal{R}$ gyűrűben. Most legyen $\varepsilon^{(j)}$ jobb oldali egységeleme a kompozíciónak. A gyűrű tetszőleges u elemével $ux = (ux) \circ \varepsilon^{(j)} = u\varepsilon^{(j)}$. Ha u nem a nullelem, akkor a bal oldalon álló polinom potosan elsőfokú, míg ha $\varepsilon^{(j)}$ konstans polinom, akkor $u\varepsilon^{(j)}$ is biztosan legfeljebb nulladfokú lehet, nem teljesülhet az egyenlőség, ezért most is igaz, hogy az $\varepsilon^{(j)}$ polinom legalább elsőfokú. Ezzel $ux = (ux) \circ \varepsilon^{(j)} = u\varepsilon^{(j)} = \sum_{i=0}^{n} \left(u\varepsilon_i^{(j)}\right) x^i$, ahol $n \in \mathbb{N}^+$, és az együtthatók összehasonlításával azt kapjuk, hogy $u\varepsilon_1^{(j)} = u$ ismét a gyűrű minden elemével, tehát $\varepsilon_1^{(j)}$ jobboldali egységelem $\mathcal{R}$-ben. Végül, ha a kompozíciónak egységeleme ε, akkor ε mind bal, mind jobb oldali egységeleme a kompozíciónak, és ekkor teljesülnie kell az előbbi mindkét feltételnek, vagyis $\varepsilon_1 u = u = u\varepsilon_1$, és ez éppen azt jelenti, hogy ε_1 egységelem $\mathcal{R}$-ben.

A továbbiakban legyen $\mathcal{R}$ kommutatív, és nézzük $(fg) \circ h$-t.

$$(fg)\circ h=\left(\sum_{i=0}^{n_f+n_g}\sum_{j=0}^{i}\left(a_jb_{i-j}\right)x^i\right)\circ h=\sum_{i=0}^{n_f+n_g}\sum_{j=0}^{i}\left(a_jb_{i-j}\right)h^i$$
$$=\left(\sum_{i=0}^{n_f}a_ih^i\right)\left(\sum_{i=0}^{n_g}b_ih^i\right)=(f\circ h)(g\circ h),$$

tehát teljesül a kompozíció jobb oldali disztributivitása a polinomok szorzása felett. Ezt alkalmazva megmutatjuk, hogy kommutatív gyűrű felett a kompozíció asszociatív. Legyen először $f=c\in R$. Ekkor tetszőleges g polinommal $f\circ g=c\circ g=c$, és ebből $(f\circ g)\circ h=c\circ h=c=c\circ(g\circ h)=f\circ(g\circ h)$. Most tegyük fel, hogy teljesül az asszociativitás, ha f legfeljebb n-edfokú, ahol n nemnegatív egész szám, és most legyen f $n+1$-edfokú, továbbá $\mathcal{R}$ egységelemes. Ekkor $f=f_1x+r$, ahol f_1 n-edfokú és r konstans. Ezzel a felírással

$$\begin{aligned}(f\circ g)\circ h&=\big((f_1x+r)\circ g\big)\circ h=\big((f_1\circ g)g+r\big)\circ h\\&=\big((f_1\circ g)\circ h\big)(g\circ h)+r=\big(f_1\circ(g\circ h)\big)(g\circ h)+r\\&=(f_1x)\circ(g\circ h)+r=(f_1x+r)\circ(g\circ h)=f\circ(g\circ h),\end{aligned}$$

vagyis $n+1$-edfokú f polinom esetén, tehát bármely f polinom esetén is asszociatív a kompozíció. Ha az $\mathcal{R}$ gyűrű nem egységelemes, akkor beágyazható egységelemes gyűrűbe (lásd az 1.32. Tételt a 20. oldalon), ott teljesül az asszociativitás, de akkor az eredeti gyűrű fölötti polinomok kompozíciója is asszociatív.

□

Egységelemes gyűrű esetén x eleme a polinomgyűrűnek, és x egységeleme a kompozíciónak. Mivel az egységelem, ha létezik, egyértelműen meghatározott, ezért ekkor x az egyetlen egységeleme ennek a műveletnek. Ebből az is következik, hogy ha a kompozíciónak van egységeleme, akkor ez sem lehet más, mint az x polinom, ugyanis a kompozíció egységelemességéből következik az $\mathcal{R}$ egységelemessége, ebből pedig az, hogy x egységeleme a $\circ$ műveletnek, de akkor az egyértelműség miatt más egységelem nincs, így a kiindulásul feltett egységelem is az x polinom.

Ha $\mathcal{R}$ nem a nullgyűrű, akkor van legalább két különböző eleme, mondjuk a és b. Legyen $f=a$ és $g=b$. Ekkor $f\circ g=a\circ b=a\neq b=b\circ a=g\circ f$, ami mutatja, hogy a kompozíció művelete általában még kommutatív gyűrű esetén sem kommutatív. A kompozíció balról általában nem disztributív az összeadásra nézve. Legyen például $f=a\neq 0$, g és h pedig $R[x]$ tetszőleges elemei. Ekkor

$$f\circ(g+h)=a\circ(g+h)=a\neq 2a=a+a=a\circ g+a\circ h=f\circ g+f\circ h,$$

vagyis az adott polinomokkal nem teljesül a bal oldali disztributivitás, de akkor a kompozíció balról nem disztributív általában az összeadásra nézve.

A fenti két eredmény azt jelenti, hogy ha $\mathcal{R}$ kommutatív gyűrű, akkor $(R[x];+,\circ)$ olyan struktúra, amelyben $(R[x];+)$ Abel-csoport, $(R[x];\circ)$ félcsoport, és $\circ$ jobbról disztributív az összeadásra nézve, de balról nem, vagyis $(R[x];\circ)$ csaknem gyűrű, de nem az. Ennek például egy egyszerű, de fontos következménye, hogy bár $\mathcal{R}$ nulleleme (vagyis $(R[x];+)$ semleges eleme) bal oldali zéruselem az $(R[x];\circ)$ félcsoportban, hiszen bármely f polinomra $0\circ f=0$, de nem jobb oldali zéruselem, mert ha f olyan polinom, amelynek konstans tagja $r\neq 0$, akkor $f\circ 0=r\neq 0$, vagyis nem teljesül, hogy 0-val szorozva, az eredmény is 0.

Közvetlenül látható, hogy ha f az $\mathcal{R}$ gyűrű feletti polinom, és $u\in R$, akkor $f\circ u=\hat{f}(u)$, ahol $f\circ u$-ban u konstans polinom, vagyis a polinomba való behelyettesítés speciális kompozíció..

3. Testek és véges testek

Ebben a részben elsősorban olyan kérdésekkel foglalkozunk, amelyek alapvetőek a véges testek elméletében, illetve amelyekre szükség van a véges testekkel kapcsolatban.

Az előző fejezetben már definiáltuk a testeket, illetve a valamivel általánosabb ferdetestet: az $\mathcal{R}$ gyűrű ferdetest, ha a nullától különböző elemek a szorzással csoportot alkotnak, és ha ez a szorzás még kommutatív is, akkor a ferdetest test. Van más szokás is: az általunk ferdetestnek definiált struktúrát nevezik testnek, és kommutatív szorzás esetén – ha ezt külön hangsúlyozni akarják – kommutatív testet mondanak. Mi a jogfolytonosság szem előtt tartásával az előbbi konvenciót alkalmazzuk, vagyis a ferdetest - test párosítást használjuk. Fontos kiemelni, hogy a definíció értelmében ferdetestnek legalább két eleme van, hiszen egy csoport soha nem üres. Ferdetest további lényeges tulajdonságai:

1. nullosztómentes;
2. az előbbi alapján ferdetest karakterisztikája 0 vagy prímszám. Nullosztómentes gyűrű (a ferdetest ilyen) karakterisztikája $n \in \mathbb{N}^+$, ha van a gyűrűnek olyan $u \neq 0$ eleme, amelyre $nu = 0$, de $n > k \in \mathbb{N}^+$-ra $ku \neq 0$, vagyis n a legkisebb ilyen tulajdonságú $\mathbb{N}^+$-beli elem, míg ha nincs ilyen u eleme a legalább kételemű gyűrűnek, akkor a karakterisztikája 0. Láttuk, hogy a karakterisztika egyértelmű, és ha nem 0 vagy 1, akkor prímszám (másként szólva legalább két elemet tartalmazó nullosztómentes gyűrű karakterisztikája a nullától különböző elemek azonos additív rendje). Az $\mathcal{R}$ gyűrű karakterisztikáját $\mathrm{char}(\mathcal{R})$ jelöli;
3. test feletti polinomgyűrű euklideszi $\varphi(f) = \deg(f)$-fel;
4. testre példa a racionális, valós és komplex számok teste, míg ferdetest a $\mathbb{C}$ fölötti $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$-alakú mátrixok halmaza a közönséges mátrixműveletekre. Vezessük be az

$$\mathbf{e} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

jelölést. Ha $a = a_1 + a_2\mathbf{i}$, $b = b_1 + b_2\mathbf{i}$, az előző mátrixban, akkor $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = a_1\mathbf{e} + a_2\mathbf{i} + b_1\mathbf{j} + b_2\mathbf{k}$ az új jelölésekkel. Ha **e**-t elhagyjuk, és **i**, **j**, **k** helyett egyszerűen azt írjuk, hogy i, j és k, akkor kapjuk a **kvaternió**kat, ezek az $a + bi + cj + dk$ formában megadott objektumok valós a, b, c és d számokkal. Hogy valóban ferdetestet kaptunk, továbbá hogy ez nem test, azt az eredeti mátrixalakkal igazolhatjuk legkönnyebben;
5. ha m egynél nagyobb pozitív egész, akkor $\mathbb{Z}_m$, azaz a $\mathrm{modulo}\ m$ maradékosztályok halmaza az osztályösszeadással és osztályszorzással kommutatív gyűrű, amely akkor és csak akkor test, ha m prímszám; az utóbbi esetben a test karakterisztikája m. Részletesebben: tetszőleges $1 < m \in \mathbb{N}$-re $\mathbb{Z}_m$-nek m eleme van, mégpedig egy elem azokat és csak azokat a racionális egész számokat tartalmazza, amelyek ugyanazt az m-nél kisebb nemnegatív maradékot adják m-mel való osztáskor. Egy ilyen elemet tetszőleges elemével, praktikusan a benne található legkisebb nemnegatív egésszel reprezentáljuk, tehát $k \in \mathbb{Z}$-re a k-val reprezentált maradékosztály $\bar{k}_m = \{n \in \mathbb{Z} | k \equiv n\ (m)\}$, és $\mathbb{Z}_m = \{\bar{k}_m | k \in \mathbb{Z}\}$. A definíció alapján $\bar{k}_m = \bar{j}_m \Leftrightarrow k \equiv j\ (m)$. Szintén a definícióból, ha $k_1 \equiv k_2\ (m)$ és $j_1 \equiv j_2\ (m)$, akkor $k_1 + j_1 \equiv k_2 + j_2\ (m)$ és $k_1 j_1 \equiv k_2 j_2\ (m)$, azaz $\overline{k_1 + j_1}_m = \overline{k_2 + j_2}_m$ és $\overline{k_1 j_1}_m = \overline{k_2 j_2}_m$. Ez azt jelenti, hogy a $\bar{k}_m + \bar{j}_m = \overline{k + j}_m$, $\bar{k}_m \bar{j}_m = \bar{k} \bar{j}_m$ definíció binér műveleteket határoz meg $\mathbb{Z}_m$-en, amelyekre teljesülnek a gyűrűaxiómák, sőt, a szorzás kommutatív és van egységelem, tehát $\mathbb{Z}_m$ a megadott úgynevezett osztályműveletekkel valóban egységelemes kommutatív gyűrű, ez a $\mathrm{modulo}\ m$ **maradékosztály-gyűrű**. $|\mathbb{Z}_m| = m$, elemei a **maradékosztály**ok, amelyek végtelen halmazok. Az osztályok neve melletti m index arra utal, hogy $\mathrm{modulo}\ m$ osztályokról van szó, amit általában nem teszünk ki, mivel a környezet alapján világos, hogy milyen modulusról van szó.

Testek speciális, és sok szempontból a többi testtől eltérő, fontos és a gyakorlat számára is érdekes tulajdonságot mutató esetei a véges testek.

3.1. Definíció

A véges sok elemet tartalmazó testet **véges test**nek mondjuk.

Δ

Lehetne definiálni a véges ferdetestet is, ám igaz az alábbi **Wedderburn-tétel** (amelyet majd a 6. fejezetben a 115. oldaltól kezdve bizonyítunk).

3.2. Tétel

Véges ferdetest kommutatív.

Δ

Ennél valamivel több is igaz, ugyanis belátjuk, hogy véges, reguláris félcsoport mindig csoport, így minden véges, nullosztómentes gyűrű test.

3.3. Tétel

Ha a $\mathcal{G}$ véges félcsoportban mindkét oldalról lehet egyszerűsíteni, akkor $\mathcal{G}$ csoport.

Δ

Bizonyítás:
G nem üres, mivel $\mathcal{G}$ félcsoport. Legyen $G = \{g_i | n > i \in \mathbb{N}\}$, $G_g = \{gg_i | n > i \in \mathbb{N}\}$, ahol g a G rögzített eleme. G_g minden eleme benne van G-ben, hiszen $\mathcal{G}$ félcsoport, ezért $G_g \subseteq G$. $gg_u = gg_v$ az egyszerűsíthetőség következtében pontosan akkor teljesül, ha $g_u = g_v$, azaz $u = v$, így a $g_i \mapsto gg_i$ leképezés G-nek önmagába való injektív leképezése. Viszont véges halmaz önmagába való injektív leképezése szürjektív is, ami azt jelenti, hogy tetszőleges $h \in G$-hez valamilyen w-re $gg_w = h$, vagyis g_w megoldása a $gx = h$ egyenletnek. Hasonló a helyzet az $yg = h$ egyenlettel, tehát ez is megoldható, $\mathcal{G}$ csoport.

□

3.4. Következmény

1. Csoport véges részfélcsoportja részcsoport;
2. legalább kételemű, véges, nullosztómentes gyűrű (véges) test.

Δ

Bizonyítás:
1. Csoportban a szorzás reguláris, de akkor a részfélcsoporban is lehet egyszerűsíteni.
2. Nullosztómentes gyűrűben minden nullától különböző elemmel lehet egyszerűsíteni, ezért, ha a gyűrű véges és van legalább két eleme, akkor nullától különböző elemei a szorzásra nézve csoportot alkotnak, így a gyűrű ferdetest, és a Wedderburn-tétel alapján egyben test is.

□

Tetszőleges p prímre $\mathbb{Z}_p$ test (mert ekkor az $ax \equiv 1\ (p)$ kongruenciának minden, a p-vel nem osztható a-ra van megoldása, vagyis $\mathbb{Z}_p$-ben minden nem nulla elemnek van ebben a gyűrűben inverze). Ebből következik az alábbi eredmény.

3.5. Tétel

Végtelen sok, páronként nem izomorf véges test létezik.

Δ

Bizonyítás:
A prímszámok száma végtelen, és a fentiek alapján minden prímhez tartozik legalább egy véges test. Ugyanakkor izomorf struktúrák között bijekció létesíthető, vagyis azonos az alaphalmazuk számossága, ezért különböző prímhez tartozó véges testek nem lehetnek izomorfak.

□

Kérdés, hogy van-e más véges test is. A továbbiakban belátjuk, hogy a válasz igenlő.

A testelmélet az algebrai egyenletek gyökeinek algebrai eszközökkel való megoldását célzó kutatások során alakult ki. Az már az eddigi algebrai ismeretek birtokában is látható, hogy ehhez a polinom együtthatóit általában egy test elemeinek célszerű tekinteni, és a gyökökhöz esetleg szükséges ezt a testet kiterjeszteni. Ha például tekintjük az $x^2 - 2$ polinomot, és az ezt kielégítő objektumokat keressük, akkor először is azt kell tisztázni, hogy mit takar a 2 jel, és mit kezdhetünk vele, vagyis milyen műveleteket hajthatunk rajta végre, továbbá, hogy mely elemek között keressük a megoldást. Tegyük fel, hogy 2 a modulo 7 maradékosztályoknak a 2 egésszel reprezentált osztálya, a megoldást is az ilyen maradékosztályok között keressük, és a műveletek az osztályműveletek. Ekkor x helyébe a 3-at tartalmazó osztályt helyettesítve a nullával reprezentált osztályt kapjuk, vagyis ekkor a polinomnak létezik gyöke az együtthatók által meghatározott testben. Más a helyzet, ha 2-t mint racionális számot tekintjük. Ismert, hogy nincs olyan racionális szám, amelyet x helyére írva és a racionális számokon ismert műveleteket elvégezve eredményül nullát kapnánk, vagyis az $x^2 - 2 \in \mathbb{Q}[x]$ polinomnak nincs gyöke a racionális számok körében. Ha viszont a valós számok körében keresünk megoldást, akkor már sikerrel járunk, hiszen $\sqrt{2}$ helyettesítésével a valós számokon értelmezett műveletekkel nullát kapunk. Vegyük most racionális a-val és b-vel az $a + b\sqrt{2}$ alakú valós számokat a közönséges összeadással és szorzással. Ekkor könnyű számolással kiadódik, hogy ez a $\mathbb{Q}(\sqrt{2})$ halmaz zárt a kivonásra és szorzásra, valamint a $0 + 0\sqrt{2} = 0$ kivételével valamennyi elem inverze maga is ehhez a halmazhoz tartozik, és így ez a halmaz a valós számok összeadásával és szorzásával testet alkot. Ez a test tartalmazza a racionális számokat, ezért az eredeti polinom egyben $\mathbb{Q}(\sqrt{2})$ fölötti polinom is, és ebben a testben már van gyöke, mivel $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ nyilván teljesül. Jóllehet $\mathbb{Q}$ részteste a most konstruált testnek, az előbb elmondottak alapján inkább a fordított irányt tekintik elsődlegesnek, így érthető a következő

3.6. Definíció

Legyen $\mathcal{L}$ test, és $\mathcal{K}$ az $\mathcal{L}$ részteste. Ekkor $\mathcal{L}$ a $\mathcal{K}$ **bővítése**, $\mathcal{L}$ **bővített test** vagy **relatív test** $\mathcal{K}$ **fölött**, míg $\mathcal{K}$ **alaptest**, jele: $\mathcal{L}|\mathcal{K}$. Ha $\mathcal{L}|\mathcal{K}$ és $\mathcal{M}|\mathcal{L}$ egyszerre teljesül, akkor ezt $\mathcal{M}|\mathcal{L}|\mathcal{K}$ jelöli, és $\mathcal{L}$ neve **közbülső test**.

$\mathcal{K}$ **az** $\mathcal{L}$ **valódi részteste**, ha $\mathcal{L} \neq \mathcal{K} \leq \mathcal{L}$, ekkor $\mathcal{L}$ **a** $\mathcal{K}$ **valódi bővítése**, **a bővítés valódi**; az ellenkező esetben $\mathcal{K}$ **az** $\mathcal{L}$ **nem valódi részteste**, illetve $\mathcal{L}$ **a** $\mathcal{K}$ **nem valódi bővítése**, **a bővítés nem valódi**.

Δ

A következő tétel szerint egy test résztestének részteste az első test részteste, így bővítés bővítése az eredeti test bővítése.

3.7. Tétel

Ha $\mathcal{K}$, $\mathcal{L}$ és $\mathcal{M}$ testek, és $\mathcal{M}|\mathcal{L}|\mathcal{K}$, akkor egyben $\mathcal{M}|\mathcal{K}$ is igaz. Véges test részteste is véges test.

Δ

Bizonyítás:
Test egyben kommutatív gyűrű, vagyis additív Abel-csoport és kommutatív multiplikatív félcsoport, ahol a két struktúrát mindkét oldalról összekapcsolja a disztributivitás. Mivel félcsoport részfélcsoportjának részfélcsoportja az eredeti félcsoportnak is részfélcsoportja, csoport részcsoportjának részcsoportja részcsoportja az eredeti csoportnak, és a disztributivitás is öröklődik, így test résztestének

részteste mindenesetre részgyűrűje az eredeti testnek. A kommutativitás és nullosztómentesség lefelé biztosan öröklődik, és ha egy egységelemes gyűrű egységeleme benne van a gyűrű egy részgyűrűjében, akkor az egyben a részgyűrűnek is egységeleme, így az előbbi részgyűrű biztosan egységelemes integritási tartomány. Az egyetlen probléma az, hogy a szorzás csoporttulajdonsága nem teljesül a teljes halmazon. A baj oka, hogy a multiplikatív invertálás csupán részleges művelet a testben, mivel a nullára nincs értelmezve. Résztesthez ezért úgy jutunk, hogy veszünk egy olyan részgyűrűt, amely a 0 elhagyása után részcsoport a szorzásra (elegendő, hogy zárt a szorzás inverzképzésére). Ebben az esetben külön megvizsgáljuk a részstruktúraság tranzitivitását. Az eddigiek alapján $\mathcal{K}$ az $\mathcal{M}$ részgyűrűje. Másrészt $\mathcal{K}$, $\mathcal{L}$ és $\mathcal{M}$ nulleleme azonos, ugyanis $\mathcal{M}$ additív csoportjának részcsoportja $\mathcal{L}$ additív csoportja, és ennek részcsoportja $\mathcal{K}$ additív csoportja, így $K^* \subseteq L^* \subseteq M^*$, tehát $\mathcal{K}^*$ részcsoportja $\mathcal{L}^*$-nak, ez pedig $\mathcal{M}^*$-nak. Részcsoport részcsoportja részcsoport, ezért $\mathcal{K}^*$ részcsoportja $\mathcal{M}^*$-nak, de akkor $\mathcal{K}$ valóban részteste $\mathcal{M}$-nek.

Ha a test véges, akkor véges a tartóhalmaza. Résztest tartóhalmaza az előbbi véges halmaz részhalmaza, és résztest maga is test, így a véges test definíciója alapján teljesül a tétel állítása.

□

Egyszerű kapcsolat van egy test és valamely bővítésének karakterisztikája között.

3.8. Tétel

Ha $\mathcal{R}$ az $\mathcal{S}$ nullosztómentes gyűrű legalább kételemű részgyűrűje, akkor $\mathrm{char}(\mathcal{R}) = \mathrm{char}(\mathcal{S})$.

Δ

Bizonyítás:

Ha a részgyűrűnek van legalább két eleme, akkor ez még inkább igaz az eredeti gyűrűre, továbbá nullosztómentes gyűrű minden részgyűrűje is nullosztómentes. Ám legalább két elemet tartalmazó nullosztómentes gyűrű karakterisztikája megegyezik bármely nullától különböző elemének additív rendjével, amely viszont nyilván azonos a két gyűrűben, hiszen tetszőleges pozitív egész n-nel az R minden u elemére nu mint R eleme azonos nu-val mint S-beli elemmel.

□

A tételből nyilvánvaló az alábbi.

3.9. Következmény

Ha $\mathcal{L}$ a $\mathcal{K}$ test bővítése, akkor a két test karakterisztikája azonos.

Δ

Bizonyítás:

Test legalább kételemű nullosztómentes gyűrű, így közvetlenül alkalmazható az előző tétel.

□

A következő tétel a véges testek karakterisztikájáról szól.

3.10. Tétel

Véges test karakterisztikája prímszám. p-elemű test karakterisztikája p, ahol p prímszám.

Δ

Bizonyítás:

Test legalább két elemet tartalmazó nullosztómentes gyűrű, így a karakterisztikája nulla vagy prímszám. Ám nulla-karakterisztikájú gyűrű elemeinek száma végtelen, hiszen pontosan akkor nulla a karakterisztika, ha legalább egy (de akkor valamennyi) nullától különböző elemnek az additív rendje

végtelen. A végtelen rend azt jelenti, hogy az elem különböző együtthatóval vett többszörösei páronként különbözőek, márpedig a lehetséges együtthatók az egész számok, és ezek száma végtelen.

p-elemű test additív csoportjának rendje a p prímszám, és prímszámrendű csoport ciklikus, így van benne p-edrendű elem, amiből következik, hogy a test karakterisztikája p.

□

Mivel $\mathbb{Z}_p$ karakterisztikája p, ahol p tetszőleges prímszám, ezért minden p prímszámhoz van p-karakterisztikájú véges test.

Most megvizsgáljuk egy test legszűkebb résztestét. Egyszerűen meg tudjuk adni a legkisebb elemszámú csoportot és gyűrűt: ezek egyetlen elemből állnak; gyűrűnél ezt nullgyűrűnek nevezzük. Hasonlóan triviális gyűrű a zérógyűrű, azaz olyan gyűrű, amelyben valamennyi szorzat értéke nulla. Ha ezektől a triviális esetektől eltekintünk, akkor nyilván az egyetlen (nem triviális) elemmel generált struktúrák a legegyszerűbbek: a ciklikus csoportok, ezek között is a prímszámrendűek, és például a modulo m maradékosztályok gyűrűje, kitüntetetten a prímmodulusúak (illetőleg az említett gyűrűkkel izomorf gyűrűk). A prímszámrendű csoport és a prímmodulusú maradékosztály-gyűrű egyszerűsége abban rejlik, hogy nincs nem triviális részstruktúrájuk. Ehhez hasonló az a kérdés, hogy milyen lehet egy csoport illetve gyűrű legszűkebb részcsoportja és részgyűrűje. Ismét az a helyzet, hogy csak az egységelemet és gyűrű esetén a csupán a nullelemet tartalmazó részhalmaz a keresett részstruktúra, míg ezektől a triviális esetektől eltekintve az egységelemtől különböző elem által generált ciklikus részcsoport, illetve egy nem nulla elemnek a gyűrű elemeivel felírt polinomja lesz ez a legkisebb részstruktúra. Testek esetében a helyzet bonyolultabb.

3.11. Tétel

Minden testnek van egyértelműen meghatározott legszűkebb részteste. Ez 0-karakterisztikájú test esetén $\mathbb{Q}$-val, míg p-karakterisztikájú test esetén, ahol p prímszám, $\mathbb{Z}_p$-vel izomorf.

Δ

A második állításból csak a prímkarakterisztikájú esetet vizsgáljuk.

Bizonyítás:

Ha e a $\mathcal{K}$ test egységeleme, akkor $\mathcal{K}$ bármely részteste tartalmazza e-t, így az e által generált résztestet is, ezért, ha ezt a testet $\mathcal{K}_P$ jelöli, akkor ez a $\mathcal{K}$ egyértelműen meghatározott legszűkebb részteste.

Legyen $T = \{ke | k \in \mathbb{Z}\}$, ekkor $T \subseteq K_P$, hiszen test zárt az összeadásra és ellentett-képzésre. Ha $\mathrm{char}(\mathcal{K}) = p$ prímszám, akkor $ue = ve$ valamely u és v egésszel pontosan akkor teljesül, amennyiben $u \equiv v\ (p)$, vagyis ha $\bar{u}_p = \bar{v}_p$, továbbá $ue + ve = (u + v)e$ és $(ue)(ve) = (uv)ee = (uv)e$, tehát a $\varphi: \bar{k} \mapsto ke$ szabály izomorfizmust létesít $\mathbb{Z}_p$ és T között. Ez viszont azt jelenti, hogy T már test, ennélfogva $K_P \subseteq T$, így $K_P = T$, és $\mathcal{K}_P \cong \mathbb{Z}_p$.

□

Az előbbi bizonyításból azt fontos többek között észrevenni, hogy prímkarakterisztikájú $\mathcal{K}$ testben K_P elemeinek, tehát az egységelem többszöröseinek hányadosai is – feltéve, hogy a nevező nem nulla – „egész” kifejezések, vagyis a tört az egységelem valamely többszörösével egyenlő. Később majd látjuk, hogy ez nem csupán a prímtest elemeire érvényes tulajdonság. A 0-karakterisztikájú eset éppen ebben különbözik a fentebb vizsgáltaktól.

A továbbiakban a $\mathcal{K}$ test legszűkebb résztestét, amint azt az előbbi bizonyításban is tettük, általában $\mathcal{K}_P$-vel jelöljük.

3.12. Definíció

Legyen $\mathcal{K}$ test. Ekkor

a) $\mathcal{K}$ legszűkebb részteste, $\mathcal{K}_P$, a $\mathcal{K}$ **prímteste**;
b) $\mathcal{K}$ **prímtest**, ha nincs valódi részteste.

Δ

Az alábbi tétel szerint a fenti definícióban szereplő két fogalom egybeesik, és ebből következően a nulla-karakterisztikájú prímtestek a racionális számok testével, míg a p-karakterisztikájú prímtestek $\mathbb{Z}_p$-vel izomorf testek.

3.13. Tétel

A tételben legyen p prímszám.

1. Test prímteste prímtest, és prímtest prímteste önmaga;
2. a p-karakterisztikájú $\mathcal{K}$ test akkor és csak akkor prímtest, ha $\mathcal{K} \cong \mathbb{Z}_p$;
3. minden p-elemű test $\mathbb{Z}_p$-vel izomorf;
4. ha $\mathcal{L}$ a $\mathcal{K}$ test bővítése, akkor a két test prímteste azonos.

Δ

Bizonyítás:

1. $\mathcal{K}_P$ a $\mathcal{K}$ legszűkebb részteste, így nem lehet valódi részteste. Ha viszont $\mathcal{K}$ prímtest, akkor nincs valódi részteste, tehát az egyértelműen meghatározott prímteste sem lehet más, mint maga a teljes test, $\mathcal{K}$.

2. Ha $\mathcal{K}$ p-karakterisztikájú prímtest, akkor a prímteste önmaga, vagyis $\mathcal{K} = \mathcal{K}_P \cong \mathbb{Z}_p$, míg ha $\mathcal{K} \cong \mathbb{Z}_p$, akkor K véges, továbbá $\mathbb{Z}_p \cong \mathcal{K}_P \leq \mathcal{K} \cong \mathbb{Z}_p$, így $\mathcal{K}$ izomorf egy résztestével, ami a végességgel csak úgy lehet, ha $\mathcal{K} = \mathcal{K}_P$.

3. Legyen a $\mathcal{K}$ test elemeinek száma a p prím, ekkor a karakterisztikája is p. A résztest egyben az eredeti test additív csoportjának is részcsoportja, és prímszámrendű csoportnak csak triviális részcsoportjai vannak, amelyek egyike egyelemű, így ez nem résztest, ezért $\mathcal{K}$ p-karakterisztikájú prímtest, azaz izomorf $\mathbb{Z}_p$-vel.

4. Ha $\mathcal{L}$ a $\mathcal{K}$ test bővítése, és $\mathcal{L}_P$, $\mathcal{K}_P$ a két prímtest, akkor $\mathcal{K}_P$ részteste $\mathcal{L}$-nek, és így $\mathcal{L}_P$, amely $\mathcal{L}$ minden résztestének részteste, részteste $\mathcal{K}_P$-nek. Innen viszont következik, hogy $\mathcal{L}_P \leq \mathcal{K}$, ahonnan pedig adódik, hogy $\mathcal{K}_P \leq \mathcal{L}_P$, vagyis a két prímtest megegyezik.

□

Tetszőleges test a prímtestének, tehát egy prímtestnek a bővítése. Az előbbi tételnek erre vonatkozóan egy fontos következménye az alábbi.

3.14. Következmény

Ha a $\mathcal{K}$ test karakterisztikája a p prímszám, akkor $\mathcal{K}$ lényegében véve (azaz izomorfizmustól eltekintve) $\mathbb{Z}_p$ bővítése.

Δ

Bizonyítás:

Mivel $\mathcal{K}$ tartalmaz $\mathbb{Z}_p$-vel izomorf résztestet, ezért $\mathbb{Z}_p$ beágyazható $\mathcal{K}$-ba, és az így nyert és $\mathcal{K}$-val izomorf test már $\mathbb{Z}_p$ bővítése.

□

Igen fontos segédeszközt ad az alábbi eredmény.

3.15. Tétel

Ha $\mathcal{L}|\mathcal{K}$, akkor $\mathcal{L}$ lineáris tér (vektortér) a $\mathcal{K}$ test fölött az $\mathcal{L}$-beli műveletekkel.

Δ

Bizonyítás:
Test additív Abel csoport a testbeli összeadással. Ha u, v az L és r, s a K eleme, akkor r és s L-nek is eleme, így $ru \in L$, $(rs)u = r(su)$, $r(u+v) = ru + rv$, $(r+s)u = ru + su$, hiszen testben a szorzás asszociatív és egyben disztributív az összeadásra vonatkozóan, végül, ha e a $\mathcal{K}$ (és akkor $\mathcal{L}$) egységeleme, úgy $eu = u$ is teljesül.

□

A lineáris terek fontos adata a dimenzió, és ennek lényeges szerepe van a testek esetében is.

3.16. Definíció

Ha $\mathcal{L}$ a $\mathcal{K}$ test bővítése, akkor $\mathcal{L}$-nek mint $\mathcal{K}$ feletti vektortérnek a dimenziója a **bővítés foka**, amit $[\mathcal{L}:\mathcal{K}]$ jelöl. Ha ez véges, akkor **a bővítés véges**, ellenkező esetben **végtelen.**

Δ

3.17. Tétel

Ha az $\mathcal{L}$ véges test a $\mathcal{K}$ test bővítése, akkor $[\mathcal{L}:\mathcal{K}] \in \mathbb{N}^+$.

Δ

Bizonyítás:
A bővítés foka egy vektortér dimenziója, ez pedig egy halmaz számossága, így véges esetben nemnegatív egész szám. Ám L-nek legalább két eleme van, van tehát nem nulla eleme, és egy nem nulla vektor önmagában lineárisan független, tehát a bővítés foka legalább 1, azaz véges esetben természetes szám. Ha viszont a bővítés foka végtelen, akkor már a bázis elemeinek száma is végtelen (mert a bázisvektorok páronként lineárisan függetlenek, de akkor különbözőek is), és a bázisvektorok maguk is elemei a vektortérnek, ezért ebben az esetben a bővített test is végtelen sok elemet tartalmaz, így véges test esetén a bővítés foka nem lehet végtelen, $[\mathcal{L}:\mathcal{K}]$ véges.

□

Az előbbiek alapján véges test elemszáma erősen korlátozott. Hogy mennyire, arról szól a következő tétel.

3.18. Tétel

Legyen az $\mathcal{L}$ véges test a q-elemű $\mathcal{K}$ test bővítése. Ekkor L elemeinek száma q^n egy alkalmas n pozitív egésszel.

Δ

Bizonyítás:
A feltételekből kapjuk, hogy $\mathcal{L}$ n-dimenziós vektortér a $\mathcal{K}$ test fölött, ahol $n \in \mathbb{N}^+$. De adott test feletti azonos dimenziójú vektorterek izomorfak, és a K elemeiből alkotott rendezett n-esek is egy ilyen vektorteret képeznek. Ezeknek a rendezett n-eseknek a száma viszont pontosan q^n, hiszen a sorozat minden egyes komponense egymástól függetlenül q különböző értéket vehet fel.

□

3.19. Következmény

p-karakterisztikájú véges test elemeinek száma p^n, ahol n egy pozitív egész szám.

Δ

Bizonyítás:
p-karakterisztikájú test a p-elemű prímtestének a bővítése, és ha véges, akkor a bővítés foka egy pozitív egész szám.

□

Azt már tudjuk, hogy véges test elemszáma nem lehet más, mint egy prímszám pozitív egész kitevős hatványa. A kérdés az, hogy van-e minden ilyen prímhatványhoz ennyi elemből álló véges test, illetve ha igen, akkor van-e egynél több lényegesen különböző. A kérdés megválaszolásához ad útmutatást a következő eredmény.

3.20. Tétel

Ha $\mathcal{L}$ a q-elemű $\mathcal{K}$ test n-edfokú bővítése, és $f = x^{q^n} - x \in L[x]$, akkor $f = \prod_{u \in L}(x - u)$. $u \in L$-re $u \in K$ ekvivalens az $u^q = u$ feltétellel.

Δ

Bizonyítás:
Legyen u az L tetszőleges eleme, és $t_u = \hat{f}(u) = u^{q^n} - u$. Ha $u = 0$, akkor t_u is nulla, tehát 0 gyöke f-nek. Ha viszont $u \neq 0$, akkor $u \in L^*$. L^* a szorzással csoport, és elemeinek száma $q^n - 1$, így ha e a test egységeleme, akkor $u^{q^n-1} = e$, ahonnan átrendezés és u-val való szorzás után ismét azt kapjuk, hogy $t_u = 0$, vagyis L minden eleme gyöke f-nek. Viszont L elemeinek száma q^n, f foka is q^n, és egy test fölötti polinomnak még multiplicitással együtt sem lehet a fokszámánál több gyöke, amiből kapjuk, hogy L elemei és csak ezek lesznek f gyökei, és minden ilyen gyök egyszeres; még azt kell figyelembe venni, hogy f főpolinom.
Ha $u \in K$, akkor az előbbi rész értelemszerű alkalmazásával $u^q = u$, és mivel így $x^q - x$-nek már van q gyöke, és több nem lehet, ezért L más elemeire nem teljesülhet az $u^q = u$ egyenlőség.

□

3.21. Kiegészítés

Legyen $\mathcal{L}$ a q-elemű $\mathcal{K}$ test n-edfokú bővítése. Ekkor $\mathcal{L}$ felett $f = x^{q^n-1} - e = \prod_{u \in L^*}(x - u)$, ahol e a test egységeleme.

Δ

Bizonyítás:
Ez egyszerűen az $u^{q^n-1} = e$ egyenlőség következménye.

□

Fontos észrevenni, hogy az $f = x^{q^n} - x$ polinom $K[x]$-nek is eleme, vagyis $\mathcal{L}$ a $\mathcal{K}$-nak olyan bővítése, amelyben a $\mathcal{K}$ feletti f-nek a fokszámával megegyező számú gyöke van (ha f-nek lenne többszörös gyöke, akkor ezt csak a multiplicitás figyelembevételével várhatnánk el). A következő részben megmutatjuk, hogy ilyen bővítés tetszőleges test feletti bármely nem nulla polinom esetén létezik.

Egy korábbi példában adott volt a valós számok teste, amelynek részteste a racionális számok teste, és ez utóbbiból $\mathbb{R}$-nek egy olyan új résztestét konstruáltuk, amely a $\mathbb{Q}$ bővítése, és amely tartalmazza $\sqrt{2}$-t. Ezt általánosítjuk az alábbi definícióban.

3.22. Definíció

Ha $\mathcal{M}$ a $\mathcal{K}$ test bővítése, $A \subseteq M$, és $\mathcal{L}$ az $\mathcal{M}$ legszűkebb olyan részteste, amelynek része K és A, akkor $\mathcal{L} = \mathcal{K}(A)$ **a $\mathcal{K}$ A-val való bővítése.** Ha A véges, és $A = \{u_0, \dots, u_{n-1}\}$, akkor $K(\{u_0, \dots, u_{n-1}\})$ helyett egyszerűen $K\{u_0, \dots, u_{n-1}\}$ írható. Amennyiben A egyelemű, akkor a bővítés **egyszerű.**

Δ

3.23. Tétel

Legyen $A \subseteq M$ és $\mathcal{M}|\mathcal{K}$. $\mathcal{K}(A)$ létezik és egyértelmű, $\mathcal{M}|\mathcal{K}(A)|\mathcal{K}$ és $K \cup A \subseteq K(A)$, és van M-nek olyan B részhalmaza, hogy $\mathcal{M} = \mathcal{K}(B)$.

Δ

Bizonyítás:

Legyen $\mathcal{L}$ az $\mathcal{M}$ összes olyan résztestének metszete, amelyek résztestként tartalmazzák $\mathcal{K}$-t és részhalmazként A-t. Ilyen résztest létezik, például maga $\mathcal{M}$. Résztestek metszete is résztest: az additív csoportok metszete additív csoport, a nulla azonos a résztestekben, és a nulla elhagyása utáni csoportok valamennyien az $\mathcal{M}^*$ részcsoportjai, így ezek metszete is részcsoport. A disztributivitás a teljes test bármely elemhármasára teljesül, így érvényes lesz a metszet három elemére is, tehát a metszet valóban résztest. Legyen ez a résztest $\mathcal{L}$, akkor $\mathcal{L}$-nek részteste $\mathcal{K}$ és részhalmaza A. Ugyanakkor minden ilyen tulajdonságú $\mathcal{L}'$ bővítése $\mathcal{L}$-nek, mert az $\mathcal{L}'$ tagja a metszetnek, és a metszet a metszetképzésben szereplő valamennyi tag részhalmaza. Ez azt jelenti, hogy $\mathcal{L}$ az $\mathcal{M}$ egyetlen olyan részteste, amely bővítése $\mathcal{K}$-nak és tartalmazza A-t, valamint amelynek nincs mindezen tulajdonsággal rendelkező valódi részteste, tehát a definíció alapján $\mathcal{L} = \mathcal{K}(A)$.

$\mathcal{M}|\mathcal{K}(A)|\mathcal{K}$ és $K \cup A \subseteq K(A)$ a definíció alapján igaz. Végül $\mathcal{K}(M)$ létezik, és ez nem lehet más, mint $\mathcal{M}$, hiszen $M \subseteq K \cup M \subseteq K(M) \subseteq M$.

□

3.24. Következmény

Ha $\mathcal{K}_1$ és $\mathcal{K}_2$ az $\mathcal{L}$ test résztestei, A_1 és A_2 pedig részhalmazai L-nek, és $K_1 \cup A_1 \subseteq K_2 \cup A_2$, akkor $\mathcal{K}_2(A_2)|\mathcal{K}_1(A_1)$.

Δ

Bizonyítás:

$K_1 \subseteq K_1 \cup A_1 \subseteq K_2 \cup A_2 \subseteq K_2(A_2)$ és $\mathcal{K}_1$ test, így $\mathcal{K}_1 \leq K_2(A_2)$. Hasonlóan, a részhalmaz-lánc elején K helyére A_1-et írva kapjuk, hogy $A_1 \subseteq K_2(A_2)$, és a definíció alapján a kettő együtt kiadja a $\mathcal{K}_2(A_2)|\mathcal{K}_1(A_1)$ relációt.

□

Vezessük be a következő jelöléseket: ha $\mathcal{K}$ egy $\mathcal{L}$ test részteste, amelynek A_1 és A_2 részhalmazai, akkor $\mathcal{K}(A_1)(A_2)$ jelentse azt a testet, amelyet úgy kapunk, hogy $\mathcal{K}$-t először A_1-gyel, majd az így létrejött testet A_2-vel bővítjük, míg $\mathcal{K}(A_1, A_2) = \mathcal{K}(A_1 \cup A_2)$. Mivel $\mathcal{K}(A_1)$ is az $\mathcal{L}$ részteste, és $A_1 \cup A_2$ az L részhalmaza, ezért mind $\mathcal{K}(A_1)(A_2)$, mind $\mathcal{K}(A_1 \cup A_2)$ létezik, és részteste $\mathcal{L}$-nek.

3.25. Tétel

Legyen $\mathcal{L}|\mathcal{K}$ és A_1, A_2 az L részhalmazai. Ekkor $\mathcal{K}(A_1)(A_2) = \mathcal{K}(A_1, A_2) = \mathcal{K}(A_2)(A_1)$.

Δ

Bizonyítás:

$K \cup A_1 \subseteq (K \cup A_1) \cup A_2 = K \cup (A_1 \cup A_2)$ így $\mathcal{K}(A_1, A_2)|\mathcal{K}(A_1)$ és $\mathcal{K}(A_1)(A_2) \subseteq \mathcal{K}(A_1, A_2)$, mert $A_2 \subseteq K \cup (A_1 \cup A_2) \subseteq K(A_1, A_2)$. Az ellenkező irányú tartalmazás is igaz: $\mathcal{K}(A_1)(A_2)$ bővítése

$\mathcal{K}(A_1)$-nek, ez pedig $\mathcal{K}$-nak, így a bővítés tranzitivitása következtében $\mathcal{K}(A_1)(A_2)|\mathcal{K}$, továbbá teljesül, hogy $A_1 \cup A_2 \subseteq K \cup (A_1 \cup A_2) = (K \cup A_1) \cup A_2 \subseteq K(A_1) \cup A_2 \subseteq K(A_1)(A_2)$, így valóban igaz, hogy $K(A_1, A_2) \subseteq K(A_1)(A_2)$. A másik egyenlőséget az A_1 és A_2 felcserélésével kapjuk.

□

3.26. Következmény

Ha $\mathcal{L}$ és $\mathcal{K}$ test, $\mathcal{L}|\mathcal{K}$, $n \in \mathbb{N}$, $A = \{a_0, \dots, a_{n-1}\}$ az L részhalmaza, és π a $\{0, \dots, n-1\}$ halmaz permutációja, akkor $\mathcal{K}(A) = \mathcal{K}\left(a_{\pi(0)}\right) \dots \left(a_{\pi(n-1)}\right)$.

Δ

Bizonyítás:
Ez az állítás $n = 0$ és $n = 1$ esetén semmitmondó, $n = 2$-re az előbbi tétel speciális esete, míg ha $n > 2$, akkor indukcióval kapjuk a bizonyítást.

□

A bővítésnek a bővítő elem alaptesthez való viszonya alapján két lényegesen eltérő típusa van.

3.27. Definíció

Legyen $\mathcal{L}$ a $\mathcal{K}$ test bővítése, és $u \in L$. u **algebrai** (**elem**) $\mathcal{K}$ **fölött**, ha létezik olyan nem nulla $K[x]$-beli polinom, amelynek u a gyöke, ellenkező esetben u **transzcendens** (**elem**) $\mathcal{K}$ **fölött.** (**Az**) $\mathcal{L}$ (**test**) **a** $\mathcal{K}$ (**test**) **algebrai bővítése**, ha $\mathcal{L}$ valamennyi eleme algebrai $\mathcal{K}$ fölött, egyébként a bővítés **transzcendens**.

Δ

Legyen $\mathcal{K}$ test, és $\mathcal{K}(x)$ a $\mathcal{K}$ feletti racionális függvények teste. Ha K elemeit és a konstans polinomokat azonosnak tekintjük, akkor $\mathcal{K}(x)$ a $\mathcal{K}$ bővítése, és $x \in K(x)$. x transzcendens $\mathcal{K}$ fölött, hiszen $\hat{f}(x) = f$, és így x csak a nullpolinomnak gyöke, ezért $\mathcal{K}(x)$ a $\mathcal{K}$ transzcendens bővítése.

A továbbiakban csak algebrai bővítésekkel foglalkozunk.

3.28. Tétel

Legyen $\mathcal{K}$, $\mathcal{L}$ és $\mathcal{M}$ három test, $\mathcal{M}|\mathcal{L}|\mathcal{K}$, és $u \in M$. u algebrai $\mathcal{M}$ fölött, és ha algebrai $\mathcal{K}$ fölött, akkor algebrai $\mathcal{L}$ fölött is.

Δ

Bizonyítás:
$x - u$ minden együtthatója M-beli, így $x - u \in M[x]$, továbbá ez a polinom nem a nullpolinom, és u gyöke, tehát u algebrai $\mathcal{M}$ fölött.
Amennyiben u algebrai $\mathcal{K}$ fölött, akkor van olyan $K[x]$-beli nem nulla f polinom, amelynek u gyöke. De f egyben $L[x]$-nek is eleme, így a definíció szerint u algebrai $\mathcal{L}$ fölött.

□

Egy elem algebrai vagy transzcendens volta függ attól, hogy mely testre vonatkoztatjuk: ha $\mathcal{L}$ a $\mathcal{K}$ test transzcendens bővítése, akkor a definíció szerint van legalább egy olyan u eleme $\mathcal{L}$-nek, amely transzcendens $\mathcal{K}$ fölött, viszont ez az u gyöke az $\mathcal{L}$ fölötti $x - u$ polinomnak, tehát $\mathcal{L}$-re vonatkoztatva már algebrai. Az viszont igaz, hogy léteznek „abszolút algebrai" elemek: egy test prímtestének v eleme a prímtestre vonatkoztatva algebrai, és az eredeti test bármely részteste a prímtest bővítése. Ekkor viszont az előbbi tétel szerint v algebrai a bővebb résztest fölött is.

Algebrai elemhez kapcsolódó fontos fogalom a minimálpolinom.

3.29. Definíció

Legyen $\mathcal{L}$ a $\mathcal{K}$ test bővítése, és u az $\mathcal{L}$-nek $\mathcal{K}$ felett algebrai eleme. Az $m_u^{(K)} \in K[x]$ főpolinom az u $\mathcal{K}$ **feletti minimál-polinom**ja, ha

1. u gyöke $m_u^{(K)}$-nak, és
2. ha u gyöke a $0 \neq g \in K[x]$ polinomnak, akkor $\deg\left(m_u^{(K)}\right) \leq \deg(g)$.

Δ

Ezúttal is felhívjuk arra a figyelmet, hogy a minimálpolinom adott testre vonatkozik: $\sqrt{2}$-nek mint valós számnak a minimál-polinomja a racionális számok teste felett $x^2 - 2$, hiszen elsőfokú racionális együtthatós polinomnak nem gyöke, viszont $\mathbb{R}$ feletti minimál-polinomja $x - \sqrt{2}$.

3.30. Tétel

Legyen $\mathcal{L}$ a $\mathcal{K}$ test bővítése, és u az $\mathcal{L}$-nek $\mathcal{K}$ felett algebrai eleme. u $\mathcal{K}$ feletti minimál-polinomja létezik és egyértelmű, a minimálpolinom felbonthatatlan $\mathcal{K}$ fölött, és ha ez $m_u^{(K)}$, továbbá f tetszőleges $\mathcal{K}$ feletti polinom, úgy $\hat{f}(u) = 0$ akkor és csak akkor, ha f osztható $m_u^{(K)}$-val.

Δ

Bizonyítás:

u a feltétel szerint algebrai $\mathcal{K}$ felett, így van olyan $K[x]$-beli nem nulla polinom, amelynek u a gyöke, tehát $\{\deg(f) | 0 \neq f \in K[x] \wedge \hat{f}(u) = 0\}$ $\mathbb{N}$ nem üres részhalmaza. Ilyen halmazban van legkisebb elem, és egy halmaz legkisebb eleme – ha létezik – egyértelmű, továbbá ha ez a legkisebb elem n, akkor van olyan f polinom $K[x]$-ben, amelynek a foka éppen ez a minimális n, és amelynek gyöke u. Legyen c ennek az f-nek a főegyütthatója, akkor $c \in K^*$, és $m = c^{-1}f$ nyilván olyan $K[x]$-beli főpolinom, amelynek a foka szintén n, és amelynek u gyöke. Eddig azt láttuk be, hogy u-hoz létezik a definíció feltételeit kielégítő polinom, vagyis u-nak létezik $\mathcal{K}$ fölötti minimál-polinomja.

Legyen $f \in K[x]$. Ha $m|f$, akkor $f = gm$ egy $K[x]$-beli g polinommal, és behelyettesítve u-t, $\hat{f}(u) = \hat{g}(u)\hat{m}(u) = 0$. Most legyen $\hat{f}(u) = 0$. Test fölötti polinomok gyűrűje euklideszi, így alkalmas h és r $\mathcal{K}$ feletti polinomokkal $f = hm + r$, ahol ha r nem nulla, akkor $\deg(r) < \deg(m)$. Ismét helyettesítve u-t $0 = \hat{f}(u) = \hat{h}(u)\hat{m}(u) + \hat{r}(u) = \hat{r}(u)$, ami csak úgy lehet, ha r a nullpolinom, hiszen ellenkező esetben u gyöke lenne egy m fokánál alacsonyabb fokú $K[x]$-beli polinomnak, ami az m választása folytán lehetetlen. Ez viszont azt jelenti, hogy m osztója az f polinomnak.

Az előbbi oszthatóság alapján belátjuk az egyértelműséget. Ha m' is $\mathcal{K}$ feletti minimál-polinomja u-nak, akkor mind m m'-nek, mind fordítva, m' m-nek osztója, vagyis m és m' asszociáltak, ami csak úgy lehet, ha megegyeznek, hiszen mindkettő főpolinom.

Végül szintén az oszthatóságból következik a minimálpolinom felbonthatatlansága. A definíció alapján ugyanis $m_u^{(K)}$ főpolinom, tehát nem a nullpolinom, és van gyöke, így nem lehet nem nulla konstans polinom, vagyis nem lehet egység. Ha viszont $m_u^{(K)} = gh$, akkor $0 = \hat{g}(u)\hat{h}(u)$, ami csak úgy lehet, ha u gyöke a g és h polinomok közül legalább az egyiknek, mondjuk g-nek. Ekkor $m_u^{(K)}$ osztója g-nek, és hasonlóan, g osztója $m_u^{(K)}$-nak, vagyis g és $m_u^{(K)}$ asszociáltak, tehát azonos a fokszámuk, amiből következik, hogy h nem nulla konstans polinom, vagyis egység $K[x]$-ben, tehát a minimálpolinom irreducibilis $\mathcal{K}$ fölött.

□

3.31. Kiegészítés

Legyen $\mathcal{L}$ a $\mathcal{K}$ test bővítése, és u az $\mathcal{L}$-nek $\mathcal{K}$ felett algebrai eleme, továbbá $m_u^{(K)}$ az u $\mathcal{K}$ feletti minimál-polinomja. Ekkor

1. $\deg\left(m_u^{(K)}\right) \geq 1$, és egyenlőség akkor és csak akkor áll, ha $u \in K$;
2. ha $f \in K[x]$ $\mathcal{K}$ felett irreducibilis, és $\hat{f}(u) = 0$, akkor $f \sim m_u^{(K)}$, ahol $\sim$ az asszociáltság jele.

Δ

Bizonyítás:

1. Minimálpolinom felbonthatatlan, így legalább elsőfokú. Másrészt u pontosan akkor gyöke a $\mathcal{K}$ feletti $x - v$ polinomnak, ha $v = u$, vagyis ha u eleme K-nak.

2. A tétel alapján $m_u^{(K)}$ osztója f-nek. De a feltétel szerint f felbonthatatlan, így nincs más osztója, mint az egységek, valamint az asszociáltjai. 1. alapján viszont $m_u^{(K)}$ legalább elsőfokú, így nem egység.

□

3.32. Definíció

A $\mathcal{K}$ test felett algebrai u elem $m_u^{(K)}$ minimál-polinomjának foka, n, az u $\mathcal{K}$ **feletti foka**, és u n-**edfokú algebrai elem** $\mathcal{K}$ **fölött**; jele $\deg_K(u)$.

Δ

A definíció azt a tényt fejezi ki, hogy algebrai elem minimál-polinomjának foka bizonyos értelemben azt méri, milyen messze van u a viszonyításra kiszemelt $\mathcal{K}$ testtől.

3.33. Tétel

Véges bővítés algebrai, és a bővítés foka legalább 1.

Δ

Bizonyítás:

Azt, hogy a bővítés foka legalább 1, már korábban bebizonyítottuk, ezért csak a másik állítást kell igazolni. Legyen $\mathcal{L}$ a $\mathcal{K}$ test bővítése, és legyen a bővítés foka n. Ha u az L tetszőleges eleme, akkor $u^0, \ldots, u^n$ az L $n+1$ darab (nem feltétlenül különböző) vektora, és így lineárisan összefüggő vektorrendszer $\mathcal{K}$ fölött, azaz $c_0u^0 + \cdots + c_{n-1}u^n = 0$ K-beli nem csupa 0 $c_0, \ldots, c_{n-1}$ elemmel. Ekkor u gyöke a $K[x]$-beli nem nulla $f = c_0x^0 + \cdots + c_{n-1}x^n$ polinomnak, tehát u algebrai $\mathcal{K}$ fölött. Mivel u az L bármely eleme lehet, ezért L minden eleme algebrai $\mathcal{K}$ felett, vagyis $\mathcal{L}$ a $\mathcal{K}$ algebrai bővítése.

□

Az eddigiek során adott volt egy test, annak egy részteste, és ezt a résztestet bővítettük a teljes test valamely elemével. Ha a bővítés algebrai, akkor ez az elem gyöke a szűkebb test felett irreducibilis valamely polinomnak. A kérdés az, hogy mi a helyzet, ha csupán egy test és egy irreducibilis polinom ismert, és olyan testet keresünk, amelyben már van gyöke ennek a polinomnak. Előtte belátunk három gyűrűelméleti tételt.

3.34. Tétel

Kommutatív egységelemes gyűrű maximális ideálja szerinti maradékosztály-gyűrű test.

Δ

Bizonyítás:

Ha van maximális ideál, akkor a gyűrűben van legalább két ideál, vagyis van valódi ideál, és valódi ideál szerinti maradékosztály-gyűrűnek van legalább két eleme. Legyen $\mathcal{M}$ az $\mathcal{R}$ gyűrű maximális ideálja. Ekkor M az R valódi részhalmaza, de $\mathcal{M}$-et bármely rajta kívül lévő gyűrűelemmel a legszűkebb ideállá bővítve a teljes gyűrűt kapjuk. A maradékosztály-gyűrű nulleleme az ideál, és az egységeleme

az $\mathcal{R}$ egységelemét tartalmazó osztály. Legyen u a gyűrű egy M-en kívüli eleme. Ekkor a maradékosztály-gyűrűben az u-val reprezentált osztály nem a nullelem. A legszűkebb ideál, amely tartalmazza mind u-t, mind M-et, a teljes gyűrű, ezért a gyűrű egységeleme, e is benne van ebben a bővítésben. A bővítés elemei $ru + m$ alakúak, ahol r az R és m az M tetszőleges eleme, így $e = vu + m$ a gyűrű egy alkalmas v elemével. Ekkor $\bar{e} = \overline{vu + m} = \overline{vu} = \bar{v}\bar{u}$, ugyanis az m által reprezentált maradékosztály a maradékosztály-gyűrű nulleleme, és ez éppen azt jelenti, hogy $\bar{v}$ az $\bar{u}$ inverze a maradékosztály-gyűrűben. Mivel így a maradékosztály-gyűrűben minden nem nulla elemnek van inverze, és kommutatív gyűrű maradékosztály-gyűrűje kommutatív, ezért a maradékosztály-gyűrű test.

□

3.35. Tétel

Euklideszi gyűrű főideálgyűrű.

Δ

Bizonyítás:

Legyen $\mathcal{R}$ euklideszi gyűrű, és $\mathcal{J}$ az $\mathcal{R}$ legalább két elemet tartalmazó ideálja (a csak a nullelemet tartalmazó ideál nyilván főideál). Mivel az ideál tartalmaz nem nulla elemet, az ideálbeli elemek euklideszi normáinak halmaza a nemnegatív egész számok halmazának nem üres részhalmaza, így van benne egyértelműen meghatározott legkisebb elem, mondjuk s, és az ideálnak van s-normájú eleme, például u. Ha most v az ideál egy tetszőleges eleme, akkor v-t maradékosan osztva u-val, $v = qu + r$, ahol vagy r a gyűrű nulleleme, vagy r normája kisebb, mint u normája. De ez utóbbi nem lehetséges, ugyanis u és v eleme az ideálnak, ekkor qu és $r = v - qu$ is benne van az ideálban, és $\mathcal{J}$-ben minden nem nulla elem normája legalább akkora, mint u normája, hiszen u egy minimális normájú eleme az ideálnak. Ebből következik, hogy $r = 0$, tehát $v = qu$, vagyis az ideál minden eleme az u többszöröse, és kommutatív egységelemes gyűrűben – márpedig euklideszi gyűrű ilyen – egy elem többszörösei főideált alkotnak.

□

3.36. Tétel

Főideálgyűrű nem triviális ideálja pontosan akkor maximális, ha generáló eleme irreducibilis.

Δ

Bizonyítás:

Legyen $\mathcal{J}_1 = (u_1)$ és $\mathcal{J}_2 = (u_2)$ az $\mathcal{R}$ főideálgyűrű két ideálja. Ekkor $I_1 \subseteq I_2$ akkor és csak akkor, ha u_2 osztója u_1-nek, $I_2 = R$ akkor és csak akkor, ha $u_2 = e$ (pontosabban szólva, ha u_2 egység), és $\mathcal{J}_1$ pontosan akkor maximális, ha $I_1 \neq R$, de minden olyan $\mathcal{J} \neq \mathcal{R}$ ideálra, amellyel $I_1 \subseteq I$, $I = I_1$. Most legyen I_1 legalább kételemű, ekkor $u_1 \neq 0$. Az előbbiek szerint I_1 akkor és csak akkor maximális, ha nincs más osztója, mint az egységek valamint a saját asszociáltjai, vagyis akkor és csak akkor, ha u_1 irreducibilis.

□

Az előbbi három tételből következik, hogy euklideszi gyűrű egy ideálja szerinti maradékosztály-gyűrű akkor és csak akkor test, ha az ideál egy irreducibilis elem többszöröseinek halmaza. Ezt majd felhasználjuk a következő tétel bizonyításában.

3.37. Tétel

Legyen $\mathcal{K}$ test, és m a $\mathcal{K}$ felett felbonthatatlan polinom. Ekkor létezik $\mathcal{K}$-nak olyan bővítése, amelyben m-nek van gyöke.

Δ

Bizonyítás:

a) Legyen $(m) = \{gm | g \in K[x]\}$, ekkor (m) maximális ideál $\mathcal{K}[x]$-ben és $\mathcal{T} = \mathcal{K}[x]/(m)$ test, hiszen test feletti egyhatározatlanú polinomgyűrű, tehát $\mathcal{K}[x]$ is, euklideszi gyűrű.

b) $\mathcal{K}[x]$-ben a konstans polinomok halmaza $\mathcal{K}$-val izomorf résztestet alkot, ezért $\mathcal{K}$ beágyazható $\mathcal{K}[x]$-be, így eleve azt tételezzük fel, hogy $\mathcal{K}[x]$-ben a konstans polinomok maguk a megfelelő $\mathcal{K}$-beli elemek, vagyis hogy $K \subseteq K[x]$. Ekkor az a $\varphi: K[x] \to T$ leképezés, amelynél f képe az f által reprezentált $\bar{f}$ maradékosztály, a K-t is leképezi T egy részhalmazába, $\overline{K}$-ba. Legyen $U = \{\bar{f} | f \in K\}$ (vagyis a konstans polinomokkal reprezentált maradékosztályok halmaza). Konstans polinom képe konstans polinom által reprezentált maradékosztály, így $\overline{K} \subseteq U$, másrészről U minden eleme egy K-beli elem képe, vagyis $\overline{K} = U$. Mivel m legalább elsőfokú, és két konstans polinom különbsége is konstans polinom, így ez a különbség csak akkor lehet osztható m-mel, ha 0-val egyenlő (mármint a különbség), tehát különböző K-beli elem képe különböző eleme $\overline{K}$-nak, φ bijektíven képezi le K-t $\overline{K}$-ra. φ egyben művelettartó is, és konstans polinomok összege valamint szorzata is konstans polinom, így φ izomorfizmust létesít $\mathcal{K}$ és $\overline{\mathcal{K}}$ között, azaz $\mathcal{K}$ beágyazható $\mathcal{T}$-be: a konstans polinomok által reprezentált maradékosztályokat és csak azokat azonosíthatjuk a megfelelő K-beli elemmel. Jelöljük a létrejött testet $\mathcal{L}$-lel. Innen látható, hogy $\mathcal{L}$ a $\mathcal{K}$ egy bővítése.

c) $m \in K[x]$, és $\mathcal{L}$ a $\mathcal{K}$ bővítése, ezért $m \in L[x]$. Ha $m = \sum_{i=0}^{n} a_i x^i$, és figyelembe vesszük, hogy K elemeit, tehát a polinom együtthatóit valamint a 0-t azonosítottuk az általuk mint konstans polinomok által reprezentált maradékosztályokkal, akkor

$$\hat{m}(\bar{x}) = \sum_{i=0}^{n} a_i \bar{x}^i = \overline{\sum_{\iota=0}^{n} a_\iota x^\iota} = \bar{m} = 0,$$

és ez azt jelenti, hogy m-nek van L-ben gyöke, nevezetesen $\bar{x}$.

□

3.38. Kiegészítés

Ha m a $\mathcal{K}$ test fölött irreducibilis n-edfokú polinom, és $\mathcal{L}$ a $\mathcal{K}[x]/(m)$-ből $\mathcal{K}$ beágyazásával kapott test, akkor $\mathcal{L} = \mathcal{K}(\bar{x})$, az $\mathcal{L}|\mathcal{K}$ bővítés foka n, és $\mathcal{L}$ egy $\mathcal{K}$ fölötti bázisa $\{\bar{x}^k | n > k \in \mathbb{N}\}$.

Δ

Bizonyítás:

A feltétel szerint $\mathcal{L}|\mathcal{K}$, másrészt $\bar{x} \in L$, így mindenesetre $K(\bar{x}) \subseteq L$. Legyen most f tetszőleges polinom $\mathcal{K}$ fölött. $\mathcal{K}$ test, ezért f egyértelműen írható $f = um + r$ alakban, ahol $\delta(r) < n$. Innen az osztályműveletek tulajdonságaival $\bar{f} = \overline{um + r} = \bar{u}\bar{m} + \bar{r} = \bar{r} = \sum_{i=0}^{n-1} c_i \bar{x}^i$, hiszen $\mathcal{L}$-ben $\bar{m} = 0$, $r = \sum_{i=0}^{n-1} c_i x^i$. $c_i \in K \subseteq K(\bar{x})$, $\bar{x} \in K(\bar{x})$, így $\bar{f} \in K(\bar{x})$, amiből következik az $L \subseteq K(\bar{x})$ tartalmazás, tehát $L = K(\bar{x})$.

Már láttuk, hogy L bármely eleme felírható az $\bar{x}$ legfeljebb $n-1$-edfokú hatványainak $\mathcal{K}$ feletti lineáris kombinációjaként, így ezek a hatványok generálják $\mathcal{L}$-et mint $\mathcal{K}$ feletti vektorteret. Ez az n hatvány lineárisan független is $\mathcal{K}$ fölött: $\sum_{i=0}^{n-1} b_i x^i = 0 = \bar{m}$ esetén m osztja a $g = \sum_{i=0}^{n-1} b_i x^i$ polinomot, ami m irreducibilitása és a fokszámok figyelembevételével csak úgy lehetséges, ha $g = 0$, vagyis ha g minden b_i együtthatója 0. Ebből azt is megkaptuk, hogy a bővítés foka n.

□

Tekintsük a valós együtthatós $x^2 + 1$ polinomot. Ez felbonthatatlan a valós számok teste fölött, hiszen másodfokú és nincs valós gyöke. Ha a valós számok testét az előbbiekben leírtak szerint bővítjük, akkor egy olyan legszűkebb testet kapunk, amelyben már van gyöke a polinomnak. De ugyanilyen tulajdonságú test a komplex számok teste, amelyet a valós számok testéből az i-vel való bővítéssel kapunk. Van-e valamilyen kapcsolat, és ha igen, akkor milyen a két test között? És mi a helyzet azzal a testtel, amely azokat és csak azokat a másodrendű valós mátrixokat tartalmazza, amelyek $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$-alakúak?

Vagy például mi a kapcsolat azon testek között, amelyeket egy test fölött irreducibilis polinom különböző gyökeivel való bővítéssel kapunk (például az x^3-2 polinomnak van valós és van komplex gyöke)? Érezzük, de azért pontosan megmutatjuk, hogy algebrai szempontból a megfelelő testek lényegében véve azonosak, vagyis izomorfak. Ehhez egyéb tulajdonságokat látunk be.

3.39. Tétel

Legyen $\mathcal{R}_1$ és $\mathcal{R}_2$ egységelemes kommutatív gyűrű, φ az $\mathcal{R}_1$-nek $\mathcal{R}_2$-be való homomorfizmusa, $f=\sum_{i=0}^{n} a_i x^i \in R_1[x]$, és u az R_2 tetszőleges eleme. Ekkor a $\psi\colon \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i)u^i$ szabály $\mathcal{R}_1[x]$-nek $\mathcal{R}_2$-be való műveletartó leképezése.

Δ

Bizonyítás:

Az azonnal látszik, hogy ψ az $R_1[x]$ minden eleméhez az R_2 egy és csak egy elemét rendeli, hiszen φ az R_1 bármely elemét az R_2 egy és csak egy elemére képezi le, és $\mathcal{R}_2$ mint gyűrű zárt a szorzásra és összeadásra. Belátjuk a műveletartást.

Legyen $f^{(1)}$ és $f^{(2)}$ két polinom az $\mathcal{R}_1$ gyűrű felett, és $f^{(j)}=\sum_{i=0}^{n_j} a_i^{(j)} x^i$, ahol $j\in\{1,2\}$, továbbá legyen $n\geq \max\{n_1,n_2\}$. $f^{(j)}$ felírható $\sum_{i=0}^{n} a_i^{(j)} x^i$ alakban is az $n_j<i\leq n\colon a_i^{(j)}=0$ definícióval. Ekkor

$$\begin{aligned}
\psi\left(f^{(1)}+f^{(2)}\right) &= \psi\left(\sum_{i=0}^{n_1} a_i^{(1)}x^i+\sum_{i=0}^{n_2} a_i^{(2)}x^i\right)=\psi\left(\sum_{i=0}^{n} a_i^{(1)}x^i+\sum_{i=0}^{n} a_i^{(2)}x^i\right)\\
&=\psi\left(\sum_{i=0}^{n}\left(a_i^{(1)}+a_i^{(2)}\right)x^i\right)=\sum_{i=0}^{n}\varphi\left(a_i^{(1)}+a_i^{(2)}\right)u^i\\
&=\sum_{i=0}^{n}\left(\varphi\left(a_i^{(1)}\right)+\varphi\left(a_i^{(1)}\right)\right)u^i=\sum_{i=0}^{n}\varphi\left(a_i^{(1)}\right)u^i+\sum_{i=0}^{n}\varphi\left(a_i^{(2)}\right)u^i\\
&=\sum_{i=0}^{n_1}\varphi\left(a_i^{(1)}\right)u^i+\sum_{i=0}^{n_2}\varphi\left(a_i^{(2)}\right)u^i=\psi\left(\sum_{i=0}^{n_1}a_i^{(1)}x^i\right)+\psi\left(\sum_{i=0}^{n_2}a_i^{(2)}x^i\right)\\
&=\psi\left(f^{(1)}\right)+\psi\left(f^{(2)}\right),
\end{aligned}$$

tehát ψ összeget összegbe képez, ψ összegtartó leképezés. A szorzatra vonatkozó állítást hasonlóan egyszerűen igazolhatjuk:

$$\begin{aligned}
\psi\left(f^{(1)}f^{(2)}\right) &= \psi\left(\left(\sum_{i=0}^{n_1}a_i^{(1)}x^i\right)\left(\sum_{i=0}^{n_2}a_i^{(2)}x^i\right)\right)=\psi\left(\sum_{i=0}^{n_1+n_2}\left(\sum_{j=0}^{i}a_j^{(1)}a_{i-j}^{(2)}\right)x^i\right)\\
&=\sum_{i=0}^{n_1+n_2}\varphi\left(\sum_{j=0}^{i}a_j^{(1)}a_{i-j}^{(2)}\right)u^i=\sum_{i=0}^{n_1+n_2}\left(\sum_{j=0}^{i}\varphi\left(a_j^{(1)}\right)\varphi\left(a_{i-j}^{(2)}\right)\right)u^i\\
&=\left(\sum_{i=0}^{n_1}\varphi\left(a_i^{(1)}\right)u^i\right)\left(\sum_{i=0}^{n_2}\varphi\left(a_i^{(2)}\right)u^i\right)=\psi\left(\sum_{i=0}^{n_1}a_i^{(1)}x^i\right)\psi\left(\sum_{i=0}^{n_2}a_i^{(2)}x^i\right)\\
&=\psi\left(f^{(1)}\right)\psi\left(f^{(2)}\right).
\end{aligned}$$

□

3.40. Következmény

Ha az $\mathcal{R}_1$ és $\mathcal{R}_2$ egységelemes kommutatív gyűrűk izomorfak, akkor a két gyűrű fölötti polinomgyűrű is izomorf, az izomorfizmusnál egymásnak megfeleltetett polinomok egyszerre nullák illetve nem nullák, és az utóbbi esetben a fokszámuk azonos, így az egyik polinom pontosan akkor egység, felbonthatatlan vagy felbontható a megfelelő gyűrű fölött, amikor a másik hasonló tulajdonságú.

Δ

Bizonyítás:

Legyen a két polinomgyűrű $\mathcal{R}_1[x_1]$ és $\mathcal{R}_2[x_2]$, és φ a két eredeti gyűrű közötti izomorfizmus. Az előző tétel értelemszerű alkalmazásával a $\psi^{(1)}: \sum_{i=0}^{n} a_i^{(1)} x_1^i \mapsto \sum_{i=0}^{n} \varphi\left(a_i^{(1)}\right) x_2^i$ szabály homomorfizmus az 1-indexű polinomgyűrűről a másikba, és mivel φ izomorfizmus, tehát az inverze létezik és szintén izomorfizmus, ezért az ellenkező irányú $\psi^{(2)}: \sum_{i=0}^{n} a_i^{(2)} x_1^i \mapsto \sum_{i=0}^{n} \varphi^{-1}\left(a_i^{(2)}\right) x_1^i$ leképezés hasonlóképpen homomorfizmus. Ha $f^{(1)}$ az $R_1[x_1]$-beli, előbb már látott $\sum_{i=0}^{n} a_i^{(1)} x_1^i$ polinom, és ugyanilyen módon megadva $f^{(2)} = \sum_{i=0}^{n} a_i^{(2)} x_2^i \in R_2[x_2]$, akkor

$$\begin{aligned}\left(\psi^{(2)}\psi^{(1)}\right)\left(f^{(1)}\right) &= \psi^{(2)}\left(\psi^{(1)}\left(f^{(1)}\right)\right) = \psi^{(2)}\left(\psi^{(1)}\left(\sum_{i=0}^{n} a_i^{(1)} x_1^i\right)\right) \\ &= \psi^{(2)}\left(\sum_{i=0}^{n} \varphi\left(a_i^{(1)}\right) x_2^i\right) = \sum_{i=0}^{n} \varphi^{-1}\left(\varphi\left(a_i^{(1)}\right)\right) x_1^i \\ &= \sum_{i=0}^{n} \left(\varphi^{-1}\varphi\right)\left(a_i^{(1)}\right) x_1^i = \sum_{i=0}^{n} a_i^{(1)} x_1^i = f^{(1)},\end{aligned}$$

és teljesen hasonlóan kapjuk, hogy $\left(\psi^{(1)}\psi^{(2)}\right)\left(f^{(2)}\right) = f^{(2)}$, amiből következik, hogy $\psi^{(1)}$-nek (és $\psi^{(2)}$-nek) van inverze, tehát bijektív, ami a művelettartással együtt azt jelenti, hogy izomorfizmus.

Mivel izomorfizmusnál a nullának és csak a nullának a képe a kép nulleleme, ezért a nullpolinomok egymásnak felelnek meg, és nem nulla polinom sem képe, sem őse nem lehet a nullpolinomnak. Maga φ is izomorfizmus, így rá is vonatkozik, hogy pontosan a nullelemet képezi le a nullába, amiből következik, hogy egy nem nulla polinom főegyütthatójának képe nem nulla, az ennél magasabb fokú tagok együtthatója viszont a képpolinomban is nulla, azaz a két polinom fokszáma megegyezik. Innen az is következik, hogy egységnek és csak egységnek a képe egység, és a szorzattartással együtt még azt is megkapjuk, hogy egy polinom akkor és csak akkor felbonthatatlan az egyik polinomgyűrűben, amikor a neki megfelelő polinom irreducibilis a másik polinomgyűrűben. Ekkor viszont már csak az a lehetőség marad, hogy a felbontható polinomok is egymás megfelelői.

□

Az előző eredmények birtokában már könnyen adódik a következő eredmény.

3.41. Tétel

Legyen φ a $\mathcal{K}$ testnek $\mathcal{K}'$ testre való izomorfizmusa, $\mathcal{L}|\mathcal{K}'$, $u \in L$ algebrai $\mathcal{K}'$ fölött az m' minimál-polinommal, és m az m'-nek a φ izomorfizmus $\mathcal{K}[x]$-re történő homomorf kiterjesztésénél $\mathcal{K}[x]$-ben megfelelő polinom. Ekkor $\mathcal{K}[x]/(m)$ izomorf $\mathcal{K}'(u)$-val.

Δ

Bizonyítás:

Legyen ψ a φ azon homomorf kiterjesztése $\mathcal{K}[x]$-re, amelynél x képe u. Határozzuk meg a leképezés magját. $f \in \mathrm{Ker}(\psi)$ akkor és csak akkor, ha $\sum_{i=0}^{n_f} \varphi(a_i) u^i = 0'$, vagyis ha u gyöke a $\mathcal{K}'$ fölötti

$\sum_{i=0}^{n_f} \varphi(a_i)x^i$ polinomnak, tehát ha ez a polinom osztható m'-vel. De $\mathcal{K}$ és $\mathcal{K}'$ izomorfizmusából következik a megfelelő polinomgyűrűk izomorfizmusa is, és ekkor az előbbi oszthatóság pontosan akkor teljesül, ha m osztója f-nek, vagyis $\mathrm{Ker}(\psi) = (m)$. Ebből adódik, hogy $\mathcal{I}m(\psi) \cong \mathcal{K}[x]/(m)$, ezért már csak azt kell belátni, hogy $\mathrm{Im}(\psi) = K'(u)$. Az rögtön látszik, hogy $\mathrm{Im}(\psi)$ része $K'(u)$-nak: a konstans polinomok képe éppen K', x képe u, és $\mathcal{K}'(u)$ test, tehát zárt a szorzásra (és így a hatványozásra is), valamint az összeadásra. Viszont $\mathcal{K}[x]$ euklideszi gyűrű, m felbonthatatlan, ennélfogva $\mathcal{K}[x]/(m)$ test, ekkor a vele izomorf $\mathcal{I}m(\psi)$ egy olyan részteste $\mathcal{L}$-nek, amely tartalmazza mind K'-t, mind u-t, és mivel az ilyen tulajdonságú testek között $\mathcal{K}'(u)$ a legszűkebb, ezért $K'(u) \subseteq \mathrm{Im}(\psi)$ is teljesül.

□

3.42. Következmény

Ha u a $\mathcal{K}$ test egy bővítésének $\mathcal{K}$ felett n-edfokú algebrai eleme, akkor a $\mathcal{K}(u)|\mathcal{K}$ bővítés foka n, a bővített testnek az eredeti test fölötti egyik bázisa az u n-nél kisebb nemnegatív egész kitevőkkel vett hatványainak halmaza, és ha K q-elemű, akkor $K(u)$ elemeinek száma q^n.

Δ

A fenti állítás szerint, ha egy olyan algebrai elemmel bővítünk egy testet, amelynek a minimál-polinomja n-edfokú, akkor a bővített test elemei az u legfeljebb $n-1$-edfokú polinomjai. Két ilyen elem összegét az együtthatók összegzésével kapjuk, míg a szorzat a két polinom szorzatának a bővítő elem minimál-polinomjával való osztási maradéka. Azt is érdemes észrevenni, hogy egy ilyen testben nincsenek törtek, az osztás mindig elvégezhető úgy, hogy a hányados is a bővítő elem valamely polinomjával egyenlő.

Bizonyítás:
Láttuk, hogy ha m a $\mathcal{K}$ felett irreducibilis n-edfokú polinom, és $\mathcal{L}$ a $\mathcal{K}[x]/(m)$-ből a $\mathcal{K}$ beágyazásával kapott test, akkor $\mathcal{L}$ a $\mathcal{K}$ n-edfokú bővítése. Amennyiben u $\mathcal{K}$ feletti minimál-polinomja m, akkor $\mathcal{L} = \mathcal{K}[x]/(m) \cong \mathcal{K}(u)$, amiből az is következik, hogy $\mathcal{L}$ és $\mathcal{K}(u)$ mint $\mathcal{K}$ feletti vektorterek is izomorfak, és az izomorfizmusnál $\bar{x}$ képe u, amiből kapjuk a bázisra és a bővítés fokára vonatkozó állítást. A véges testre vonatkozó kijelentés viszont az előbbiek közvetlen következménye, hiszen q-elemű test n-edfokú bővítésében éppen q^n elem van.

□

Az eddigiekből következik, hogy tetszőleges test feletti bármely nem nulla polinomhoz lehet találni olyan testet, amely már az adott polinom valamennyi gyökét tartalmazza.

3.43. Tétel

Ha $\mathcal{K}$ tetszőleges test, és $f \in K[x]$ n-edfokú, akkor van $\mathcal{K}$-nak olyan $\mathcal{M}$ bővítése, hogy $\mathcal{M}$ fölött $f = c\prod_{i=0}^{n-1}(x-u_i)$ alakú, ahol $c \in K^*$, és $n > i \in \mathbb{N}$-re $u_i \in M$.

Δ

A tétel más fogalmazásban azt állítja, hogy adott test fölötti bármely nem nulla polinomhoz meg lehet adni a testnek olyan bővítését, amelyben a polinomnak a fokszámával azonos számú gyöke van, persze az esetleges többszörösség figyelembevételével.

Bizonyítás:
f-nek van foka, tehát nem nulla. Ha $n = 0$, akkor f nemnulla konstans polinom, vagyis $f = c$ a K valamely c elemével. Ez azonban felírható $f = c\prod_{i=0}^{0-1}(x-u_i)$ alakban, hiszen egy olyan szorzat értéke, amelyben az index felső határa eggyel kisebb, mint az alsó, a szokásos konvenció értelmében az egységelemmel, e-vel egyenlő.

Tegyük fel, hogy a tétel állítását már beláttuk minden olyan esetre, amikor a polinom foka kisebb, mint egy pozitív egész n, és most adott az n-edfokú f polinom. f felbontható $\mathcal{K}$ felett irreducibilis polinomok szorzatára, így felírható $f = f^{(1)}g^{(1)}$ alakban, ahol $f^{(1)}$ felbonthatatlan $\mathcal{K}$ felett. $\mathcal{K}$-nak van olyan $\mathcal{L}$ bővítése, amelyben van $f^{(1)}$-nek u gyöke. $f \in K[x]$-ből és $\mathcal{L}|\mathcal{K}$, tehát $K \subseteq L$-ből következik, hogy $f \in L[x]$, és $\mathcal{L}$ felett $f = (x-u)g^{(2)}$ egy $L[x]$-beli $g^{(2)}$ polinommal. De $g^{(2)}$ foka $n-1$, így az indukciós feltevés értelmében van $\mathcal{L}$-nek olyan $\mathcal{M}$ bővítése, amely fölött L^*-beli c-vel és M-beli $u_1, \dots, u_{n-1}$-gyel $g^{(2)} = c\prod_{i=1}^{n-1}(x-u_i)$. A bővítés tranzitív, tehát $\mathcal{M}$ egyben $\mathcal{K}$-nak is bővítése, továbbá az L-beli u egyben M-nek is eleme, így az $u_0 = u$ jelöléssel $x - u_0 \in M[x]$, amiből kapjuk, hogy f mint $\mathcal{M}$ feletti polinom $c\prod_{i=0}^{n-1}(x-u_i)$-vel egyenlő. Ez mutatja azt is, hogy f-nek M-ben n gyöke van. Végül még azt kell belátni, hogy c a K nemnulla eleme. Az, hogy nem nulla, igaz, hiszen $c \in L^*$. De a szorzások elvégzése után látjuk, hogy c az f főegyütthatója, és f $K[x]$-beli, vagyis minden együtthatója, de akkor a főegyütthatója is K eleme.

□

3.44. Definíció

A $\mathcal{K}$ test feletti n-edfokú f polinom $\mathcal{K}$ **feletti felbontási teste** a $\mathcal{K}$ legszűkebb olyan bővítése, amelyben f-nek – multiplicitással számolva – n gyöke van.

Δ

A definíció szerint f-nek van foka, tehát nem a nullpolinom.

3.45. Tétel

Tetszőleges $\mathcal{K}$ test feletti bármely nemnulla f polinomnak létezik felbontási teste. Ha f n-edfokú, $\mathcal{M}$ a $\mathcal{K}$ olyan bővítése, amelyben f-nek n gyöke van, és a polinom páronként különböző gyökei $u_0, \dots, u_{m-1}$ akkor f $\mathcal{K}$ feletti – egyik – felbontási teste $\mathcal{K}(u_0, \dots, u_{m-1})$.

Δ

Bizonyítás:

Olyan $\mathcal{M}$ test van, amelyben f-nek n gyöke van (multiplicitással). Ha ezek a gyökök ismétlés nélkül $u_0, \dots, u_{m-1}$, akkor $\mathcal{K}(u_0, \dots, u_{m-1})$ mint $\mathcal{M}$ részteste tartalmazza f valamennyi gyökét. Ha viszont $\mathcal{T}$ a $\mathcal{K}(u_0, \dots, u_{m-1})$ valódi részteste, amely $\mathcal{K}$ bővítése, akkor T az $u_0, \dots, u_{m-1}$ elemek legalább egyikét nem tartalmazza. Ha T-ben is lenne f-nek – multiplicitással számolva – n gyöke, akkor lenne közöttük legalább egy, amely különbözik valamennyi korábbi gyöktől. Amennyiben ez a gyök v, akkor f-nek $\mathcal{L}$-ben gyöke $u_0, \dots, u_{m-1}$ és v, és multiplicitásokkal együtt az u-val jelölt gyökök száma n, vagyis v-vel együtt f-nek n-nél több gyöke lenne, ami lehetetlen. Így $\mathcal{K}(u_0, \dots, u_{m-1})$ az $\mathcal{M}$ legszűkebb olyan részteste, amely tartalmazza f minden gyökét, vagyis $\mathcal{K}(u_0, \dots, u_{m-1})$ az f $\mathcal{K}$ feletti felbontási teste.

□

Most hasonló kérdéseket lehet feltenni, mint amilyenek az irreducibilis polinom gyökével való bővítéssel kapcsolatban felmerültek, és a válaszok is hasonlóak.

3.46. Tétel

Ha $\mathcal{K}_1$ és $\mathcal{K}_2$ izomorf testek a φ izomorfizmussal, $0 \neq f^{(1)} \in K_1[x]$, $f^{(2)}$ a φ-nek a polinomgyűrűre való kiterjesztésénél $f^{(1)}$-nek megfelelő polinom, és $i \in \{1,2\}$-re $\mathcal{L}_i$ az $f^{(i)}$ $\mathcal{K}_i$ feletti felbontási teste, akkor $\mathcal{L}_1 \cong \mathcal{L}_2$.

Δ

Bizonyítás:

Ha $f^{(1)}$ konstans, akkor $f^{(2)}$ is az, a felbontási test maga az eredeti test, és ezek a feltétel szerint izomorfak. Tegyük fel, hogy ha $f^{(1)}$ legfeljebb n-edfokú, akkor igaz az állítás, és $f^{(1)}$ $n+1$-edfokú

polinom. Legyenek $f^{(1)}$ gyökei a felbontási testben $u_0, u_1, \dots, u_{n-1}$, továbbá $g^{(1)}$ az $f^{(1)}$ olyan, $\mathcal{K}_1$ felett felbonthatatlan tényezője, amelynek gyöke u_0, és $g^{(2)}$ a $g^{(1)}$-nek $\mathcal{K}_2[x]$-ben megfelelő polinom. Ekkor $g^{(2)}$ is irreducibilis $\mathcal{K}_2$ fölött, és ha $f^{(2)}$ $\mathcal{L}_2$-beli gyökei $v_0, v_1, \dots, v_{n-1}$, akkor van ezek között olyan, amely $g^{(2)}$-nek a gyöke; nyilván eleve indexelhetünk úgy, hogy ez a gyök v_0 legyen. Az előző tétel szerint $\mathcal{K}_1(u_0) \cong \mathcal{K}_2(v_0)$, és $\mathcal{L}_i = \mathcal{K}_i(u_0, u_1, \dots, u_{n-1}) = \mathcal{K}_i(u_0)(u_1, \dots, u_{n-1})$ a 3.25. Tétel szerint, és ugyanez igaz a 2-indexű testekre a v gyökökkel. Innen viszont az indukciós feltevés alapján valóban teljesül a felbontási testek izomorfizmusa.

□

A 3.20. Tétel szerint (lásd a 50. oldalon) ha a q-elemű $\mathcal{K}$ testnek van n-edfokú bővítése, $\mathcal{L}$, akkor ez nem lehet más, mint a $\mathcal{K}$ feletti $x^{q^n} - x$ polinom $\mathcal{K}$ feletti felbontási teste, ugyanakkor az előbbiek alapján $x^{q^n} - x$-nek tetszőleges test felett létezik a felbontási teste. A tételt úgy interpretálhatjuk, hogy amennyiben van q^n-elemű test, akkor egy ilyen test valamennyi eleme gyöke kell, hogy legyen az $x^{q^n} - x$ polinomnak. Másrészt, ha $a^q = a$ nem is teljesül az L valamennyi elemére, amennyiben $n > 1$, és így az $a \mapsto a^q$ szabály csupán L egy részén, nevezetesen a K elemein az identikus leképezés, azért ennek a leképezésnek igen fontos tulajdonságai, és ezért jelentős szerepe van a véges testek esetén.

3.47. Tétel

Ha az $\mathcal{R}$ kommutatív gyűrűhöz van olyan p prímszám, hogy R minden r elemére $pr = 0$, akkor a $\varphi_n: a \mapsto a^{p^n}$ szabály tetszőleges nemnegatív egész n-nel $\mathcal{R}$-nek endomorfizmusa, azaz önmagába való homomorfizmusa. Amennyiben $\mathcal{R}$ nullosztómentes, akkor a leképezés injektív; ha ezen kívül még

- $\mathcal{R}$ test, akkor φ_n testhomomorfizmus,
- illetve ha R véges, akkor φ_n automorfizmus (azaz önmagára való izomorfizmus).

Δ

Legalább két elemből álló nullosztómentes gyűrűre a tétel elején álló kikötés egyszerűen azt jelenti, hogy a gyűrű karakterisztikája p.

Bizonyítás:

$\varphi_0(r) = r^{p^0} = r$, így ha $n = 0$, akkor φ_n az R önmagára való identikus leképezése, és nyilván igaz valamennyi állítás.

Most legyen $n = 1$, ekkor $\varphi_1(r) = r^{p^1} = r^p$. A megadott szabály a gyűrű minden eleméhez hozzárendel egy és csak egy R-beli elemet, így φ_1 egy $R \to R$ leképezés. Mivel a gyűrű kommutatív, ezért tetszőleges r és s gyűrűelemekre $\varphi_1(rs) = (rs)^p = r^p s^p = \varphi_1(r)\varphi_1(s)$, tehát φ_1 szorzattartó. Az összegtartás bizonyításához felhasználjuk a kommutatív gyűrűben érvényes Newton-féle binomiális tételt:

$$(r+s)^p = \sum_{k=0}^{p} \binom{p}{k} r^{p-k} s^k = r^p + s^p + \sum_{k=1}^{p-1} \binom{p}{k} r^{p-k} s^k.$$

Mivel $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ egész szám, ezért $k!\,(p-k)!$ osztja $p! = p(p-1)!$-t. $1 \le k \le p-1$-ből $k!$ valamennyi j tényezőjére is igaz, hogy $1 \le k \le p-1$, így p nem osztója $k!$ egyetlen tényezőjének sem. p prímszám, így relatív prím minden tényezőhöz, és akkor a szorzatukhoz, $k!$-hoz is. $1 \le k \le p-1$-ből $1 \le p-k \le p-1$, ezért az előbbihez hasonlóan p relatív prím $(p-k)!$-hoz is. Ekkor $k!\,(p-k)!$ relatív prím p-hez, viszont osztója $p(p-1)!$-nak, amiből következik, hogy osztója $(p-1)!$-nak, és így, ha $1 \le k \le p-1$, akkor $\binom{p}{k} = pu_k$ egy u_k egész számmal. Ekkor

$$\sum_{k=1}^{p-1}\binom{p}{k}r^{p-k}s^k=\sum_{k=1}^{p-1}(pu_k)r^{p-k}s^k=\sum_{k=1}^{p-1}p\left(u_kr^{p-k}s^k\right)=p\sum_{k=1}^{p-1}u_kr^{p-k}s^k=0,$$

hiszen $u_kr^{p-k}s^k$ a gyűrű eleme, tehát

$$\varphi_1(r+s)=(r+s)^p=r^p+s^p=\varphi_1(r)+\varphi_1(s),$$

vagyis a φ_1 leképezés összegtartó. Gyűrű az összeadásra csoport, így φ_1 többek között az $\mathcal{R}$ additív csoportjának $\mathcal{R}$-be való félcsoport-homomorfizmusa. A csoportok homomorfizmusánál azonban kiderült, hogy ekkor a képhalmaz csoport, és a szorzattartó leképezés egységelemet egységelembe, elem inverzét a kép inverzébe visz, tehát φ_1 egyben csoport-homomorfizmus is, ezért a szorzattartással együtt kapjuk, hogy φ_1 az $\mathcal{R}$-nek önmagába való gyűrű-homomorfizmusa.

$r^p=s^p$ csak akkor teljesülhet, ha $0=r^p-s^p=(r-s)^p$. Ha $\mathcal{R}$ nullosztómentes, akkor ez csak $r-s=0$, azaz $r=s$ esetén lehetséges, ami azt jelenti, hogy ebben az esetben φ_1 injektív.

Ha $\mathcal{R}$ test, akkor egyben nullosztómentes is, és ekkor $0=\varphi_1(r)=r^p$ akkor és csak akkor lehet, ha $r=0$. Ennek alapján φ_1 a szorzásra nézve egyben $(R^*;\cdot)$-nak is homomorf leképezése $(R^*;\cdot)$-ba, ezért $\mathrm{Im}(\varphi_1)\setminus\{0\}$ csoport a szorzással, $\mathcal{Im}(\varphi_1)$ test, és φ_1 az $\mathcal{R}$-nek $\mathcal{R}$-be való test-homomorfizmusa.

A véges esetre vonatkozó állítás annak egyszerű következménye, hogy véges halmaz önmagába való injektív leképezése szürjektív.

Most tegyük fel, hogy $n\in\mathbb{N}$ esetén teljesülnek a tételbeli állítások, és nézzük a $\varphi_{n+1}\colon r\mapsto r^{p^{n+1}}$ leképezést. Minden R-beli r-re

$$\varphi_{n+1}(r)=r^{p^{n+1}}=r^{p^np}=\left(r^{p^n}\right)^p=\varphi_1\left(\varphi_n(r)\right)=(\varphi_1\varphi_n)(r).$$

φ_1 és φ_n egyaránt R-et R-be képezi és művelettartó. Ekkor a szorzatuk is hasonló tulajdonságú, és ugyanez igaz az injektivitásra is, így φ_{n+1}-re is teljesülnek a tételben megfogalmazott állítások.

□

Fontos megjegyezni, hogy a tételben megadott homomorfizmus csak egyetlen prímmel, nullosztómentes gyűrű, és így test esetén csupán a test karakterisztikájával teljesül, vagyis csak ezzel a prímmel igaz, hogy a p^n-kitevős hatványozás összegtartó.

3.48. Kiegészítés

Ha $\mathcal{L}$ a q-elemű $\mathcal{K}$ test tetszőleges bővítése, akkor az $u\mapsto u^{q^n}$ szabály, ahol n nemnegatív egész, $\mathcal{L}$ automorfizmusa.

Δ

Bizonyítás:

Ha a $\mathcal{K}$, tehát egyben az $\mathcal{L}$ test karakterisztikája p, akkor $q=p^m$ és $q^n=(p^m)^n=p^{mn}=p^s$, ahol mind m, mind s nemnegatív egész.

□

Most már rendelkezésünkre állnak azok az eszközök, amelyekkel igazolhatjuk minden p prímszámra és $n\in\mathbb{N}$-re p^n-elemű test létezését.

3.49. Tétel

Legyen n pozitív egész szám. Ha van q-elemű test, akkor van q^n-elemű test is.

Δ

Bizonyítás:

Legyen $\mathcal{K}$ egy q-elemű test és $f = x^{q^n} - x \in K[x]$. Tudjuk, hogy van $\mathcal{K}$-nak olyan $\mathcal{M}$ bővítése, amely fölött f elsőfokú polinomok szorzata, vagyis $\mathcal{M}$ fölött $f = x^{q^n} - x = \prod_{i=0}^{q^n-1}(x - \alpha_i)$ M-beli α_i elemekkel. f deriváltja $q^n x^{q^n-1} - e = -e$ (mert a polinomgyűrű karakterisztikája azonos a test karakterisztikájával, és q a test karakterisztikájának pozitív egész kitevős hatványa, tehát osztható a karakterisztikával), és ennek a polinomnak nincs gyöke, így f valamennyi gyöke egyszeres. Jelöljük a gyökök halmazát L-lel, akkor tehát L elemeinek száma pontosan q^n, és $L \subseteq M$.

Megmutatjuk, hogy L már testet alkot az $\mathcal{M}$-beli műveletekkel. $q^n \geq q \geq 2$, ezért L-nek legalább két eleme van. q a $\mathcal{K}$ test elemszáma, ezért q a p prím egy hatványa, ahol p a $\mathcal{K}$ és ezzel együtt az $\mathcal{M}$ test karakterisztikája, és így ugyanezen p hatványa lesz q^n is, ebből következően $r \mapsto r^{q^n}$ automorfizmus $\mathcal{M}$-en. Ha u és v eleme L-nek, akkor gyöke f-nek, tehát $u^{q^n} - u = 0$, vagyis $u^{q^n} = u$, és hasonlóan, $v^{q^n} = v$. Ezt alkalmazva kapjuk, hogy $(u - v)^{q^n} = u^{q^n} - v^{q^n} = u - v$ és $v \neq 0$ esetén $(uv^{-1})^{q^n} = u^{q^n}\left(v^{q^n}\right)^{-1} = uv^{-1}$, azaz mind $u - v$, mind uv^{-1} eleme L-nek, $\mathcal{L}$ zárt a kivonásra és a nem nulla elemmel való osztásra, és így test.

□

A fenti eredmény alapján már meg tudjuk válaszolni a korábban feltett kérdést.

3.50. Tétel

Minden p prímszámhoz és n pozitív egészhez létezik p^n-elemű véges test, ez a test izomorfizmustól eltekintve egyértelműen meghatározott, és nincs más véges test.

Δ

Bizonyítás:

1. Azt már a 3.19. Következményben beláttuk, hogy egy véges test elemszáma csak prímhatvány lehet.
2. Az előző tételben bebizonyítottuk, hogy ha van q-elemű véges test, akkor bármely $n \in \mathbb{N}^+$-ra van q^n-elemű test. De minden p prímszámra $\mathbb{Z}_p$ test, tehát tetszőleges p prímszám esetén van p-elemű test, és akkor az előbbiek szerint minden p prímszámhoz és n természetes számhoz van p^n-elemű test.
3. Legyen $\mathcal{L}_1$ és $\mathcal{L}_2$ azonos elemszámú véges test. A közös elemszám egy prím pozitív egész kitevős hatványa, mondjuk p^n. Ekkor mindkét test prímteste $\mathbb{Z}_p$-vel izomorf, tehát ha a két prímtest $\mathcal{K}_1$ és $\mathcal{K}_2$, akkor $\mathcal{K}_1 \cong \mathcal{K}_2$. De $\mathcal{L}_1$ a $\mathcal{K}_1$ feletti $f_1 = e_1 x^{p^n} - e_1 x$, $\mathcal{L}_2$ a $\mathcal{K}_2$ feletti $f_2 = e_2 x^{p^n} - e_2 x$ polinom felbontási teste, ahol e_1 és e_2 az azonos indexű test egységeleme, és a két prímtest közötti izomorfizmusnak a polinomgyűrűre való kiterjesztésénél f_1 és f_2 egymásnak megfeleltetett polinomok, hiszen nullelem képe nullelem és egységelem képe egységelem a művelettartó leképezésnél, így a 3.46. Tétel szerint $\mathcal{L}_1$ és $\mathcal{L}_2$ izomorf.

□

3.51. Jelölés

Az izomorfizmustól eltekintve egyértelmű q-elemű test jele $\mathbb{F}_q$.

Δ

q-elemű test másik szokásos jelölése $GF(q)$. GF a **G**alois **F**ield, azaz **Galois-test** rövidítése a francia matematikus *Evariste Galois* (kiejtésben Évariszt Gáloá) tiszteletére. Mi a továbbiakban a rövidebb $\mathbb{F}_q$ jelölést alkalmazzuk.

Véges testeknél nem csupán az elemek száma erősen korlátozott, de a multiplikatív csoport szerkezete is a lehető legegyszerűbb. Ennél többet bizonyítunk, aminek egyrészt később hasznát látjuk, másrészt az általánosabb megfogalmazás ellenére a bizonyítás azonos. A kérdésre részletesebben egy későbbi fejezetben ismét visszatérünk.

3.52. Tétel

Legyen $\mathcal{K}$ test, n a $\mathcal{K}$ karakterisztikájával nem osztható pozitív egész és $\mathcal{L}$ a $\mathcal{K}$ feletti $x^n - e$ polinom felbontási teste. Ekkor a polinom gyökeinek halmaza $(L^*;\cdot)$ n-edrendű ciklikus részcsoportja.

Δ

Bizonyítás:

a) Legyen a gyökök halmaza T, és $u \in T$, $v \in T$, vagyis $u^n = e$ és $v^n = e$. Ekkor $v \neq 0$, v-nek van inverze, és $(uv^{-1})^n = u^n(v^n)^{-1} = ee^{-1} = e$, így $uv^{-1} \in T$, és mivel $e^n = e$, vagyis $e \in T$, tehát T nem üres, T a szorzással csoport. Ha $n = 1$, akkor egyetlen gyök van; legyen most $n > 1$. $x^n - e$ deriváltja nx^{n-1}, és mivel n nem osztható a karakterisztikával, ezért a derivált egyetlen gyöke 0, ami viszont nem gyöke az eredeti polinomnak, így minden gyök egyszeres, ennek alapján a gyökök, vagyis T elemeinek száma pontosan n, $\mathcal{T} = (T;\cdot)$ n-edrendű csoport. Véges csoportban minden elem rendje osztója a csoport rendjének, tehát valamennyi T-beli elem rendje osztója n-nek, ami azt is jelenti, hogy egyetlen elem rendje sem haladhatja meg a pozitív n-et . A ciklikussághoz azt kell belátni, hogy van T-ben olyan elem, amelynek a rendje n.

b) Elsőként bebizonyítjuk, hogy ha egy $\mathcal{G}$ kommutatív csoport g és h elemének rendje, m és n, véges és relatív prím, akkor gh rendje mn.

$(gh)^{mn} = (g^m)^n(h^n)^m = ee = e$, tehát gh rendje véges, és osztója mn-nek. Legyen t ez a rend. Ekkor $(gh)^t = e$, és minden olyan s egész, amellyel $(gh)^s = e$, osztható t-vel. Most írhatjuk, hogy $e = e^m = (gh)^{mt} = (g^m)^t h^{mt} = h^{mt}$. Ez csak úgy lehetséges, ha $n|mt$, ami viszont pontosan akkor teljesül, ha $n|t$, mert m és n relatív prím. Hasonlóan kapjuk, hogy $m|t$, így t osztható m és n legkisebb közös többszörösével, ami ismét $(m,n) = 1$ következtében mn, vagyis $mn|t$. Ugyanakkor láttuk, hogy $t|mn$, és mivel t és mn egyaránt pozitív egész szám, ezért a kölcsönös oszthatóság egyenlőséget jelent, $t = mn$.

c) Másodikként igazoljuk, hogy ha a $\mathcal{G}$ kommutatív csoportban az elemek rendjének halmaza felülről korlátos, akkor valamennyi rend osztója a rendek maximumának. Először is a korlátosság következtében minden rend véges, ekkor a rendek halmaza a természetes számok halmazának nem üres véges részhalmaza, így van benne legnagyobb elem, amely egyértelmű, és van G-ben olyan elem, amelynek a rendje éppen ez a maximum. Legyen m a legnagyobb rend, és g egy G-beli m-edrendű elem. Tegyük fel, hogy nem igaz az állítás. Ekkor van olyan n-edrendű h elem G-ben, hogy n nem osztója m-nek. Ez csak úgy lehet, ha van n-nek olyan p prímosztója, amely magasabb hatványon szerepel n felírásában, mint az m felbontásában (esetleg m nem is osztható ezzel a p-vel, ekkor p a 0 kitevővel szerepel m-ben). Ha p^t a p maximális hatványa, amellyel m osztható, akkor $\frac{m}{p^t}$ már nem osztható p-vel, és a feltevésünk szerint p^{t+1} osztója n-nek. Nézzük a szintén G-beli $g_1 = g^{p^t}$ valamint $h_1 = h^{\frac{n}{p^{t+1}}}$ elemeket. Könnyen látható, hogy az előbbi rendje $\frac{m}{p^t}$, az utóbbié pedig p^{t+1}. Ez a két rend relatív prím, ezért g_1h_1 rendje $\frac{m}{p^t}p^{t+1} = pm$. De p prímszám, így nagyobb, mint 1, tehát $pm > m$, és g_1h_1 is G eleme, ami lehetetlen, hiszen G-ben az elemek rendjeinek maximuma m. Az előbbi ellentmondás igazolja az állítást, tehát n osztója m-nek.

d) Most már könnyű az állítást bizonyítani. Ha $\mathcal{T}$-ben a maximális rend m, akkor valamennyi T-beli u-ra $u^m = e$, azaz minden elem gyöke a $\mathcal{K}$ feletti $x^m - e$ polinomnak, ezért a gyökök száma legalább n. De test feletti polinom gyökeinek száma nem haladja meg a polinom fokát, ahonnan $n \leq m$. Ugyanakkor korábban láttuk, hogy bármely elem rendje legfeljebb n, vagyis $m \leq n$, és a rendezés antiszimmetriája következtében $m = n$.

□

3.53. Következmény

Véges test multiplikatív csoportja ciklikus.

Δ

Bizonyítás:
Ha $|K| = q$, akkor q a test p karakterisztikájának pozitív egész kitevős hatványa, így $p|q$, de ekkor p nem osztója $q-1$-nek, tehát relatív prím hozzá, hiszen a karakterisztika prímszám, másrészt K^* elemei a $\mathcal{K}$ feletti $x^{q-1} - e$ polinom gyökei, mert K^* a szorzással egy $q-1$-elemű csoport.

□

3.54. Definíció

Az $x^n - e \in K[x]$ polinom gyöke ($\mathcal{K}$ **feletti**) n**-edik egységgyök**, és ha a gyök n-edrendű, akkor a neve ($\mathcal{K}$ **feletti**) **primitív** n**-edik egységgyök**. Ha $\mathcal{K}$ véges test, akkor $\mathcal{K}^* = (K^*;\cdot)$ (mint a szorzásra nézve ciklikus csoport) bármely generátoreleme **primitív elem** $\mathcal{K}$**-ban**.

Δ

Mivel véges test multiplikatív csoportja ciklikus, ezért, ha rögzítjük a csoport generátorelemét, akkor a csoport minden eleme egyértelműen megadható a generátorelem megfelelő kitevőjével.

3.55. Definíció

Legyen g a q-elemű $\mathcal{K}$ test primitív eleme, és a K^* u elemére $u = g^i$, ahol $q-1 > i \in \mathbb{N}$. Ekkor i **az** u (g**-re vonatkozó** vagy g**-alapú**) **indexe** vagy **diszkrét logaritmusa**, amit $\mathrm{ind}_g u$ jelöl.

Δ

3.56. Tétel

Ha g az $\mathbb{F}_q$ primitív eleme, akkor $\mathrm{ind}_g(uv) = \left(\mathrm{ind}_g u + \mathrm{ind}_g v\right) \bmod (q-1)$ az $\mathbb{F}_q^*$ minden u és v elemére.

Δ

Bizonyítás:
Legyen $u = g^i$, $v = g^j$, ahol $q-1 > i \in \mathbb{N}$ és $q-1 > j \in \mathbb{N}$. u és v, de akkor uv is $\mathbb{F}_q^*$ eleme, tehát $uv = g^k$ egy $q-1 > k \in \mathbb{N}$ kitevővel. Ekkor $g^k = g^i g^j = g^{i+j}$, és így $k \equiv i + j\ (q-1)$. De a jobb oldalon u és v indexének összege, a bal oldalon pedig uv indexe áll, így igaz az állítás.

□

3.57. Következmény

Legyen g az $\mathbb{F}_q$ primitív eleme, e az egységelem, $u \in \mathbb{F}_q^*$. Ekkor

a) $\mathrm{ind}_g u = 0 \Leftrightarrow u = e$;
b) $u \neq e$ esetén $\mathrm{ind}_g u^{-1} = (q-1) - \mathrm{ind}_g u$;
c) bármely $n \in \mathbb{N}$-re $\mathrm{ind}_g u^n = \left(n \cdot \mathrm{ind}_g u\right) \bmod (q-1)$.

Δ

Bizonyítás:
a) Ha $\mathrm{ind}_g u = 0$, akkor $u = g^0 = e$. Fordítva, ha $u = e(\neq 0)$, akkor $g^k = u = e = g^0$, azaz $k \equiv 0\ (q-1)$. De $q-1 > k \in \mathbb{N}$, így a kongruencia csak $k = 0$ esetén teljesülhet, tehát $\mathrm{ind}_g u = 0$.
b) A szorzat logaritmusával $q-1 \equiv 0 = \mathrm{ind}_g e = \mathrm{ind}_g(uu^{-1}) \equiv \left(\mathrm{ind}_g u + \mathrm{ind}_g u^{-1}\right)(q-1)$, és ezzel $\mathrm{ind}_g u^{-1} \equiv \left((q-1) - \mathrm{ind}_g u\right)(q-1)$. $u \neq e$ következtében $q-1 > \mathrm{ind}_g u \in \mathbb{N}^+$, és ezzel $q-1 > (q-1) - \mathrm{ind}_g u \in \mathbb{N}^+$, továbbá $q-1 > \mathrm{ind}_g u^{-1} \in \mathbb{N}$ az index definíciója alapján teljesül, így az előbbi kongruencia ekvivalens az $\mathrm{ind}_g u^{-1} = (q-1) - \mathrm{ind}_g u$ egyenlőséggel.

c) Ez $n = 0$-ra igaz, és ha $n \in \mathbb{N}$-re teljesül a kongruencia, akkor

$$\begin{aligned}\operatorname{ind}_g u^{n+1} &= \operatorname{ind}_g(u^n u) \equiv \operatorname{ind}_g u^n + \operatorname{ind}_g u \\ &\equiv n \cdot \operatorname{ind}_g u + \operatorname{ind}_g u = (n+1) \cdot \operatorname{ind}_g u \ (q-1),\end{aligned}$$

és $q - 1 > \operatorname{ind}_g u^{n+1} \in \mathbb{N}$, így $\operatorname{ind}_g u^{n+1} = (n+1) \cdot \operatorname{ind}_g u \ (q-1)$.

□

A diszkrét logaritmus elnevezést az indokolja, hogy a diszkrét logaritmus csak véges sok különböző értéket vehet fel, másrészt a fentiek szerint hasonló tulajdonságú a szokásos logaritmushoz.

A diszkrét logaritmus nagyban egyszerűsíti a szorzást egy véges testben. Véges testbeli műveleteket elvégezhetjük úgy, hogy egyszer és mindenkorra meghatározzuk az **összeadó-** és a **szorzó táblát**, ám ehhez q^2-elemű táblázatokat kell tárolnunk, ha a test elemeinek száma q. A diszkrét logaritmus alkalmazásával azonban a szorzó tábla helyett elegendő az egyes elemek logaritmusát tárolni, hiszen a szorzat logaritmusa – ha egyik tényező sem nulla – a logaritmusok modulo q összege. Ha a logaritmustáblát magukkal az elemekkel indexeljük, akkor ez csupán egy $q-1$-méretű táblát jelent. A gyors eredmény elérése érdekében célszerű lehet a **log-tábla** mellett az úgynevezett **antilog-tábla** tárolása is, ami nem más, mint az inverz log-tábla, vagyis ahol a logaritmushoz adjuk meg a megfelelő elemet (a kitevőhöz a hatványt). Most egy ügyes fogással az összeadó táblát is helyettesíthetjük egy $q-1$-méretű táblával. Legyen a és b a q-elemű test két eleme, és legyen z a test egy primitív eleme. Ha $a = 0$, akkor $a + b = b$, különben $a + b = a(e + a^{-1}b) = ac$, ahol $c = e + a^{-1}b$. Amennyiben $c \neq 0$, vagyis ha $b \neq -a$, akkor létezik mind a-nak, mind c-nek a z-alapú diszkrét logaritmusa, és ekkor $a + b$ logaritmusa az a és a c logaritmusának összege, figyelembe véve a maradékképzést, vagyis ekkor az összeadást visszavezettük a szorzásra. Legyen tehát $r \neq -e$-re $Z(r) = \log_z(e + r)$. Ezzel

$$\begin{aligned}\log_z(a+b) &= \log_z\big(a(e+a^{-1}b)\big) = (\log_z(a) + \log_z(e+a^{-1}b)) \bmod (q-1) \\ &= \big(\log_z(a) + Z(a^{-1}b)\big) \bmod (q-1),\end{aligned}$$

és Z egy $q-1$ elemből álló táblázat. $Z(c)$ a c **Zech-logaritmus**a vagy **Jacobi-logaritmus**a. $b = 0$ esetén $a + b = a$, nincs mit számolnunk. Ha viszont $b \neq 0$, akkor $a^{-1}b$ sem nulla, létezik a diszkrét logaritmusa, és $\log_z(a^{-1}b) = (\log_z(b) - \log_z(a)) \bmod (q-1)$ meghatározható a log-táblával. Mivel $a + b$ meghatározásához szükségünk van $a^{-1}b$ ismeretére, ezt viszont a log-táblával számítjuk, ezért célszerű, ha nem az egyes elemekhez tartozó Zech-logaritmust, hanem a logaritmusukhoz tartozó értéket adjuk meg. Legyen tehát $0 \neq c \neq -e$-re $Z'(\log_z(c)) = Z(c)$. Ezzel a táblázattal

$$\begin{aligned}\log_z(a+b) &= \log_z\big(a(e+a^{-1}b)\big) = (\log_z(a) + \log_z(e+a^{-1}b)) \bmod (q-1) \\ &= \big(\log_z(a) + Z(a^{-1}b)\big) \bmod (q-1) \\ &= \Big(\log_z(a) + Z'\big((\log_z(b) - \log_z(a)) \bmod (q-1)\big)\Big) \bmod (q-1),\end{aligned}$$

vagyis a log-táblával, az antilog-táblával és a Z' táblázatával, három $q-1$-méretű táblával a q-elemű testben bármely műveletet gyorsan el tudunk végezni (figyelembe véve a 0 és összeadásnál – e speciális helyzetét). Nagyméretű test, azaz nagy q esetén ez jelentős mértékű tárigény-csökkenést jelent.

Korábban láttuk, hogy ha egy q-elemű $\mathcal{K}$ test fölött van n-edfokú irreducibilis polinom, akkor $\mathcal{K}$-nak egy n-edfokú bővítése $\mathcal{K}(u)$, ahol u a polinom gyöke. Ez fordítva is igaz abban az értelemben, hogy a $\mathcal{K}$ minden olyan bővítése, ahol a bővített test is véges, $\mathcal{K}(u)$-alakú egy alkalmas u elemmel.

3.58. Tétel

Véges test bármely résztestének egyszerű algebrai bővítése.

Δ

Bizonyítás:

Legyen az $\mathcal{L}$ véges test a $\mathcal{K}$ test bővítése. Azt már tudjuk, hogy véges test a résztestének véges bővítése, és véges bővítés algebrai (lásd a 3.17. és 3.33. Tételeket), így csak azt kell belátni, hogy a bővítés egyszerű, vagyis van L-nek olyan u eleme, hogy $\mathcal{L} = \mathcal{K}(u)$.

Legyen u az $\mathcal{L}$ egyik primitív eleme. Az eleve teljesül, hogy $K(u) \subseteq L$. Ugyanakkor $K(u)$ tartalmazza a $\mathcal{K}$ nullelemét, ami viszont egybeesik az $\mathcal{L}$-beli zérussal, továbbá tartalmazza u-val együtt u valamennyi nemnegatív egész kitevős hatványát, de akkor L^* és a nullával együtt L valamennyi elemét, következésképpen $L \subseteq K(u)$. A kétirányú tartalmazás alapján viszont $\mathcal{L} = \mathcal{K}(u)$.

□

3.59. Következmény

Bármely véges $\mathcal{K}$ test felett tetszőleges $n \in \mathbb{N}^+$-ra létezik n-edfokú, a $\mathcal{K}$ fölött irreducibilis polinom, ezért minden véges test megkapható valamely p-elemű test egyszerű algebrai bővítéseként.

Δ

Bizonyítás:

Legyen $\mathcal{L}$ a $\mathcal{K}$ véges test n-edfokú bővítése és $\mathcal{L} = \mathcal{K}(u)$. k-adfokú irreducibilis polinom gyökével bővítve a bővítés foka k, ezért az a $\mathcal{K}$ felett felbonthatatlan g polinom, amelynek u a gyöke, pontosan n-edfokú. Bármely véges testnek minden n természetes számra van n-edfokú bővítése, ezért igaz az első megállapítás; a második viszont azért, mert minden véges test egy p-elemű test bővítése.

□

3.60. Megjegyzés

1. Azt láttuk, hogy ha $\mathcal{L}$ a q-elemű $\mathcal{K}$ test n-edfokú bővítése, akkor bármely primitív eleme egy $\mathcal{K}$ fölötti n-edfokú irreducibilis polinom gyöke, és ezzel bővítve $\mathcal{K}$-t egy q^n-elemű testet kapunk. Az viszont egyáltalán nem igaz, hogy bármely $\mathcal{K}$ felett n-edfokú irreducibilis polinom valamely gyökével bővítve $\mathcal{K}$-t, a kapott q^n-elemű testben ez a gyök primitív elem lesz. Például $m = x^2 + \overline{1} \in \mathbb{Z}_3[x]$ irreducibilis $\mathbb{Z}_3$ fölött, hiszen mint másodfokú polinom, ha felbontható, akkor a tényezők elsőfokúak lennének, azaz m-nek lenne gyöke $\mathbb{Z}_3$-ban, ugyanakkor m-be $\mathbb{Z}_3$ elemeit, $\overline{0}$-t, $\overline{1}$-et és $\overline{2}$-t helyettesítve rendre $\overline{1}$-et, $\overline{2}$-t és ismét $\overline{2}$-t kapunk. Ha ennek a polinomnak u a gyöke a bővített testben, akkor $\mathbb{Z}_3(u)$ a $\mathbb{Z}_3$ másodfokú bővítése, vagyis egy 9-elemű test, amelynek multiplikatív csoportjában bármely primitív elem rendje nyolc. De $u^2 + \overline{1} = \overline{0}$, innen $u^2 = -\overline{1} = \overline{2}$, így $u^4 = \overline{2}^2 = \overline{1}$, u negyedrendű a mondott multiplikatív csoportban, tehát u nem primitív elem.

2. A $\mathcal{K}$ test **algebrailag zárt**, ha a $\mathcal{K}$ feletti bármely, legalább elsőfokú polinomnak van K-ban gyöke. Ekkor a $K[x]$ tetszőleges, nem nulla elemének minden gyöke benne van ebben a testben, így az ilyen test minden eleme algebrai ezen testre vonatkozóan, a test minden valódi bővítése transzcendens. A fenti tétel szerint tehát véges test nem lehet algebrailag zárt.

Δ

Az előbbi tételnek egy fontos következménye, hogy bármely p^n-elemű testet megkapunk, ha a modulo p maradékosztályok gyűrűjét a $\mathbb{Z}_p$ feletti legalább egy n-edfokú felbonthatatlan polinom bármelyikének tetszőleges gyökével bővítjük.

Végezetül egy, a továbbiakban többször használt fogalmat definiálunk.

3.61. Definíció

Ha $\mathcal{L}$ a $\mathcal{K}$ test bővítése, akkor az $\mathcal{L}$ egy $\mathcal{K}$ **feletti relatív automorfizmus**a az $\mathcal{L}$-nek önmagára való olyan izomorfizmusa, amely K elemeit helyben hagyja.

Δ

Az identikus leképezés automorfizmus, és a struktúra bármely részstruktúráján is az identikus leképezés, így ez mindig relatív automorfizmus. Könnyű ellenőrizni, hogy egy test valamely résztestére vonatkozó relatív automorfizmusainak szorzata is ilyen tulajdonságú, az identikus leképezés neutrális eleme ennek a szorzásnak, és relatív automorfizmus inverze is olyan automorfizmusa a testnek, amely a résztest elemeit helyben hagyja, amiből következik, hogy az $\mathcal{L}$ testnek a $\mathcal{K}$ résztestére vonatkozóan relatív automorfizmusai csoportot képeznek.

4. Véges test feletti polinomok

Azok az összefüggések, amelyek általában egy test feletti polinomra vonatkoznak, természetesen most is érvényben vannak, így ebben a fejezetben főleg olyan tulajdonságokat vizsgálunk, amelyek specifikusak a véges test feletti polinomokra.

4.1. Tétel

Ha $\mathcal{K}$ egy q-elemű véges test, akkor tetszőleges $\varphi: K \to K$ leképezéshez van olyan egyértelműen meghatározott, azonosan nulla vagy legfeljebb $q-1$-edfokú $\mathcal{K}$ feletti f polinom, hogy a K minden u elemére $\varphi(u) = \hat{f}(u)$. Ez az f polinom megadható az $f = \sum_{u \in K}\left(\varphi(u)(e-(x-u)^{q-1})\right)$ alakban, továbbá ha $g \in K[x]$-re is igaz, hogy $\hat{g} = \varphi$, akkor $g = f + t \cdot (x^q - x)$ valamilyen $t \in K[x]$ polinommal.

Δ

Bizonyítás:

Nézzük a felírt polinomot. Az összeg minden tagja – egymástól függetlenül – nulla vagy pontosan $q-1$-edfokú, így az összegük vagy a nullpolinom, vagy legfeljebb $q-1$-edfokú. Legyen b a K tetszőleges eleme. x helyére b-t írva, $u \neq b$ esetén $(b-u)^{q-1} = e$, és minden ilyen tag nulla lesz az összegben. Ha viszont $u = b$, akkor a megfelelő tag $\varphi(b)$, tehát $\hat{f}(b) = \varphi(b)$ a test minden elemére.

Ha h egy másik olyan $\mathcal{K}$ feletti polinom, amely vagy 0, vagy a foka legfeljebb $q-1$, és K minden u elemére $\hat{h}(u) = \varphi(u)$, akkor a $t = f - h$ polinomhoz tartozó $\hat{t}$ leképezés K valamennyi elemét a 0-ba viszi, vagyis a különbség-polinomnak K minden eleme gyöke, ami azt jelenti, hogy van q különböző gyök. Viszont polinomok különbsége vagy a nullpolinom, vagy a fokszám nem nagyobb a fokszámmal rendelkező tagok fokainak maximumánál, így t is vagy a nullpolinom, vagy a foka kisebb, mint q. De test feletti nem nulla polinomnak még multiplicitással számolva sem lehet több gyöke, mint amekkora a fokszáma, így $f - h = 0$, $f = h$, ami azt jelenti, hogy f egyértelmű.

Most legyen g $\mathcal{K}$ feletti olyan polinom, hogy minden K-beli u-ra $\hat{g}(u) = \varphi(u)$. Mivel g egyértelműen írható $g = t \cdot (x^q - x) + r$ alakban, ahol $r = 0$, vagy r foka kisebb, mint q, ezért áttérve a megfelelő leképezésre, $\varphi(u) = \hat{g}(u) = \hat{t}(u) \cdot (u^q - u) + \hat{r}(u) = \hat{r}(u)$ (mert q-elemű test minden u elemére érvényes az $u^q = u$ egyenlőség), és ilyen r pontosan egy van, nevezetesen f, tehát $r = f$.

□

A 4.1. Tételben megadott kifejezés tulajdonképpen a polinom **Lagrange-interpolációj**a. Ismeretes, hogy tetszőleges $\mathcal{K}$ testben adott $n \in \mathbb{N}^+$-hoz az $n > i \in \mathbb{N}$ indexekre megadva az $u_i \in K$ és $v_i \in K$ elemeket úgy, hogy az u_i-k páronként különbözőek, van egy és csak egy olyan, legfeljebb $n-1$-edfokú, $\mathcal{K}$ feletti f polinom, hogy minden $n > i \in \mathbb{N}$-re $\hat{f}(u_i) = v_i$. Ezt a polinomot különböző módon meg lehet határozni, közülük az egyik a **Lagrange-féle alappolinom**okkal oldja meg a feladatot. Ha ugyanis

$$L^{(k)}_{(u_0,\dots,u_{n-1})} = \frac{\prod_{\substack{n>i\in\mathbb{N} \\ i\neq k}}(x-u_i)}{\prod_{\substack{n>i\in\mathbb{N} \\ i\neq k}}(u_k-u_i)},$$

akkor látható, hogy $\hat{L}^{(k)}_{(u_0,\dots,u_{n-1})}(u_i) = \delta_{i,k}e$, és így $f = \sum_{k=0}^{n-1} v_i L^{(k)}_{(u_0,\dots,u_{n-1})}$. Most legyen $\mathcal{K} = \mathbb{F}_q$ és $n = q$. Ekkor, figyelembe véve, hogy az u_i-ként megadott elemek páronként különbözőek és számuk azonos a test rendjével,

$$(x-u_k)\prod_{n>i\in\mathbb{N}\setminus\{k\}}(x-u_i)=\prod_{u\in\mathbb{F}_q}(x-u)=\prod_{u\in\mathbb{F}_q}\big(x-(u+u_k)\big)$$
$$=\prod_{u\in\mathbb{F}_q}\big((x-u_k)-u\big)=\left(\prod_{u\in\mathbb{F}_q}(x-u)\right)\circ(x-u_k)$$
$$=(x^q-x)\circ(x-u_k)=(x-u_k)^q-(x-u_k)$$

és

$$\prod_{n>i\in\mathbb{N}\setminus\{k\}}(u_k-u_i)=\prod_{u\in\mathbb{F}_q^*}u=\prod_{i=0}^{q-2}t^i=t^{\sum_{i=0}^{q-2}i}=t^{\frac{(q-1)(q-2)}{2}}=-e,$$

ahol t a test egy primitív eleme (mert ha q páratlan, akkor $q-1$ páros, $t^{q-1}=e$-ből $t^{\frac{q-1}{2}}$ az e valamelyik négyzetgyöke, vagyis e vagy $-e$, de az előbbi nem lehet, mivel t primitív elem, és $t^{\frac{(q-1)(q-2)}{2}}$ a $-e$ $q-2$-dik, tehát páratlan kitevős hatványa, míg páros q esetén $t^{\frac{(q-1)(q-2)}{2}}=(t^{q-1})^{\frac{q-2}{2}}=e=-e$, mivel most a test karakterisztikája 2). Ezt alkalmazva

$$f=\sum_{k=0}^{n-1}v_iL^{(k)}_{(u_0,\dots,u_{n-1})}=\sum_{k=0}^{n-1}\hat{f}(u_i)\left(-\frac{(x-u_k)^q-(x-u_k)}{x-u_k}\right)$$
$$=\sum_{k=0}^{n-1}\hat{f}(u_i)(e-(x-u_k)^{q-1}),$$

és ez valóban azonos a tételben megadott kifejezéssel.

4.2. Kiegészítés

Legyen $\varphi\colon\mathbb{F}_q^n\to\mathbb{F}_q$, ahol $n\in\mathbb{N}^+$. Ekkor $f=\sum_{\mathbf{u}\in\mathbb{F}_q^n}\big(\varphi(\mathbf{u})\prod_{i=0}^{n-1}(e-(x_i-u_i)^{q-1})\big)$ egy minden határozatlanban legfeljebb $q-1$-edfokú, n-határozatlanú polinom, amelyhez tartozó $\hat{f}$ polinomfüggvény megegyezik φ-vel, és nincs más ilyen polinom.

Δ

Bizonyítás:

f-ről az előbbiek alapján könnyű belátni, hogy minden határozatlanban legfeljebb $q-1$-edfokú, és a polinom bármely $\mathbf{a}\in\mathbb{F}_q^n$ helyen vett helyettesítési értéke $\varphi(\mathbf{a})$.

Az egyértelműséget kissé általánosabb formában bizonyítjuk. Legyen $\mathbb{N}_r=\{k\in\mathbb{N}|r>k\}$ és $\mathbb{N}_{\mathbf{r}}=\times_{i=0}^{s-1}\mathbb{N}_{r_i}$, ahol $r\in\mathbb{N}^+$, $s\in\mathbb{N}^+$, $\mathbf{r}\in\mathbb{N}^{+s}$, és legyen $f^{(1)}$, $f^{(2)}$ m-határozatlanú polinom az $\mathcal{R}$ integritási tartomány felett. Ha $m>i\in\mathbb{N}$-re $n_i^{(j)}$ az $f^{(j)}$ fokszáma x_i-ben, $\max\left\{n_i^{(1)},n_i^{(2)}\right\}<n_i\in\mathbb{N}^+$, és $T^{(m)}=\left\{\left(u_{k_0}^{(0)},\dots,u_{k_{m-1}}^{(m-1)}\right)\in R^m\middle|(k_0,\dots,k_{m-1})\in\mathbb{N}_{\mathbf{r}}\right\}$ $n_0\cdots n_{m-1}$-számú, páronként különböző olyan pont, amelyben a két függvény értéke azonos, akkor a két polinom is azonos. Ez ekvivalens azzal, hogy amennyiben az $\mathcal{R}$ fölötti m-határozatlanú polinom az i-edik határozatlanban legfeljebb n_i-1-edfokú, és az előbb megadott pontok mindegyike gyöke a polinomnak, akkor f a nullpolinom. A határozatlanok száma szerinti indukcióval végezzük a bizonyítást. $m=1$-re igaz az állítás. Tegyük fel, hogy egy $m\in\mathbb{N}^+$-ra is teljesül az állítás, és legyen $f=\sum_{(\mathbf{i},i_m)\in\mathbb{N}_{\mathbf{n},n_m}}c_{\mathbf{i},i_m}\prod_{j=0}^{m}x_j^{i_j}$, továbbá legyen $T^{(m+1)}=T^{(m)}\times T^{(1)}=\left\{\left(u_{k_0}^{(0)},\dots,u_{k_{m-1}}^{(m-1)},u_{k_m}^{(m)}\right)\in R^{m+1}\middle|(k_0,\dots,k_{m-1},k_m)\in\mathbb{N}_{(\mathbf{r},n_m)}\right\}$ a polinom $n_0\cdots n_{m-1}n_m$ különböző gyökének halmaza. f minden $m\geq i\in\mathbb{N}$ indexre legfeljebb n_i-1-edfokú

x_i-ben, és $f = \sum_{i=0}^{n_m-1} f_i x_m^i$, ahol $f_i = \sum_{\mathbf{i}\in\mathbb{N}_\mathbf{n}} c_\mathbf{i} \prod_{j=0}^{m-1} x_j^{i_j}$. Bármely $\left(u_{k_0}^{(0)}, \dots, u_{k_{m-1}}^{(m-1)}\right) \in T^{(m)}$ pontban $f\left(u_{k_0}^{(0)},\dots,u_{k_{m-1}}^{(m-1)}\right) = \sum_{i=0}^{n_m-1} \hat{f}_i\left(u_{k_0}^{(0)}, \dots, u_{k_{m-1}}^{(m-1)}\right) x_m^i$ egyhatározatlanú polinom, amelynek $T^{(1)}$ valamennyi eleme gyöke. Ez a polinom pontosan akkor lesz valamennyi megadott $u_i^{(m)} \in T^{(1)}$ helyen 0, ha minden együtthatója 0, azaz, ha minden $i \in \mathbb{N}_m$-re $\hat{f}_i\left(u_{k_0}^{(0)}, \dots, u_{k_{m-1}}^{(m-1)}\right) = 0$. Ez azt jelenti, hogy minden rögzített i-re az f_i polinom a $T^{(m)}$ minden pontjában, vagyis $n_0 \cdots n_{m-1}$ pontban 0. Ez viszont az indukciós feltevés alapján pontosan akkor igaz, ha f_i a nullpolinom, tehát valamennyi együtthatója, így minden $c_{\mathbf{i},i_m}$ értéke 0, és ezt akartuk bizonyítani.

Az egyértelműségre adunk egy másik, kombinatorikus bizonyítást is. A q-elemű testet önmagába képező m-változós függvények száma q^{q^m}, és ugyanennyi a q-elemű test fölötti, minden határozatlanjában legfeljebb $q-1$-edfokú, m-határozatlanú polinomok száma. Egy ilyen polinomhoz pontosan egy előbb említett leképezés tartozik, és minden ilyen leképezéshez találtunk olyan, minden határozatlanjában legfeljebb $q-1$-edfokú, m-határozatlanú polinomot, amelyhez tartozó polinomfüggvény megegyezik az adott leképezéssel, vagyis az a megfeleltetés, amely a polinomhoz hozzárendeli a leképezést, szürjektív a leképezések halmazára. Mivel a leképezések halmazában és a q-elemű test fölötti, minden határozatlanjában legfeljebb $q-1$-edfokú m-határozatlanú polinomok halmazában ugyanannyi elem van, ezért a szürjektivitásból következik az injektivitás, tehát az egyértelműség is.

□

4.3. Megjegyzés

A tétel szerint véges testet önmagába képező függvény lényegében véve polinomfüggvény.

Ha $\mathcal{R}$ gyűrű, és φ illetve ψ egyaránt R-et R-be képező függvény, vagyis R transzformációja, akkor az $u \mapsto \varphi(u) + \psi(u)$ és $u \mapsto \varphi(u)\psi(u)$ szabály, ahol $u \in R$, szintén R feletti transzformáció, amelyeket $\varphi + \psi$ és $\varphi\psi$ jelöl, továbbá könnyen lehet ellenőrizni, hogy ezzel gyűrűt kapunk, ahol a nullelem az a transzformáció, amely minden elemhez a 0-t rendeli, a φ ellentettje pedig az, amely u-t $-\varphi(u)$-ra képezi. Jelöljük ezt a gyűrűt $\mathcal{T}_R$-rel. Ennek P_R részhalmazát képezik az $u \mapsto \sum_{i=0}^{n} a_i u^i$ alakú leképezések, ahol $n \in \mathbb{N}$, és valamennyi i-re a_i az $\mathcal{R}$ gyűrű eleme, vagyis a polinomfüggvények. Az nyilvánvaló, hogy minden polinomhoz tartozik egy és csak egy polinomfüggvény, és minden ilyen függvény képe egy polinomnak, vagyis $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} a_i u^i$ szürjekció $R[x]$-ről P_R-re. Ez a leképezés összegtartó, továbbá, ha $\mathcal{R}$ kommutatív, akkor teljesül a szorzattartás is, így kommutatív gyűrűben az előbbi megfeleltetés egyben homomorfizmus is (amiből a szürjektivitással együtt az is következik, hogy a polinomfüggvények P_R halmaza részgyűrűt alkot $\mathcal{T}_R$-ben). Mármost az előbbi tétel azt jelenti, hogy véges test esetén $\mathcal{T}_R$ azonos $\mathcal{P}_R$-rel, így az előbbi szabály $\mathcal{R}[x]$ szürjektív homomorfizmusa $\mathcal{T}_R$-re. Ez a mefeleltetés viszont biztosan nem injektív, ugyanis q-elemű test esetén a test bármely u elemére $u^q - u = 0$, ezért tetszőleges $f \in R[x]$, $g \in R[x]$ esetén f és $f + g \cdot (x^q - x)$ képe azonos polinomfüggvény. Ugyanakkor végtelen elemű R esetén a szürjektivitás biztosan nem igaz. Ezt két módon is bizonyítjuk.

Tekintsük azt a $\sigma: R \to R$ leképezést, amely a 0 kivételével R minden eleméhez a 0-t, míg a 0-hoz az R egy nem nulla u elemét rendeli. Ha lenne egy $\mathcal{R}$ feletti f polinom, amelyre $\hat{f} = \sigma$, akkor ennek a polinomnak a 0 kivételével valamennyi R-beli elem gyöke lenne, vagyis f-nek végtelen sok gyöke lenne. Ilyen polinom csak egy van, a nullpolinom. Ám a nullpolinomhoz tartozó polinomfüggvény értéke mindenütt 0, tehát a 0-ban is. Ugyanakkor $\sigma(0) = u \neq 0$, a nullpolinomhoz tartozó polinomfüggvény sem lehet σ-val egyenlő, így nincs olyan polinom, amelyhez tartozó polinomfüggvény megegyezik σ-val, ami azt jelenti, hogy az $f \mapsto \hat{f}$ leképezés végtelen gyűrű esetén nem szürjektív.

Az előzőekben csak annyit mutattunk meg, hogy az a $\varphi: R[x] \to T_R$ leképezés, ahol f képe $\hat{f}$, nem szürjektív. Ez még nem zárná ki, hogy valamilyen más hozzárendeléssel szürjektíven képezzük le a polinomgyűrűt a gyűrűt önmagába képező leképezések halmazába. A következőkben kimutatjuk, hogy T_R számossága nagyobb, mint a polinomgyűrű számossága, ami kizárja, hogy létezzen a polinomgyűrűnek T_R-re való bármilyen szürjektív leképezése.

Az $\mathcal{R}$ feletti polinomok lényegében véve R feletti véges hosszúságú sorozatok. Egy halmaz fölötti n hosszúságú sorozatok halmaza R^n, ahol a szorzás a Descartes-szorzat, és ha R végtelen, akkor $|R^n| =$

$|R|$. A polinomgyűrű az összes véges sorozat halmaza, vagyis ekvivalens az $\bigcup_{n=1}^{\infty} R^n$ halmazzal. Megszámlálható sok azonos számosságú végtelen halmaz uniójának számossága megegyezik az unióban szereplő tagok számosságával, így $|R[x]| = |\bigcup_{n=1}^{\infty} R^n| = |R|$. Ezzel szemben legalább kételemű halmaz esetén $|T_R| = |R^R| > |R|$, és ezt egybevetve az előzőekkel kapjuk, hogy $|R[x]| < |T_R|$.

Végtelen gyűrű esetén tehát az $f \mapsto \hat{f}$ leképzés nem szürjekció $R[x]$-ről T_R-re. Ha viszont $\mathcal{R}$ végtelen elemszámú integritási tartomány, akkor az előbbi megfeleltetés injektív homomorfizmus. Egyrészt a kommutativitás következtében a leképezés művelettartó. Másrészt integritási tartomány feletti nem nulla polinom gyökeinek száma nem haladhatja meg a polinom fokát, ezért két polinomfüggvény csak úgy lehet egyenlő, ha maga a két polinom is azonos (polinomok egyenlősége ekvivalens azzal, hogy minden együtthatójuk azonos, míg két polinomfüggvény, mint tetszőleges két leképezés is, pontosan akkor egyenlő, ha az értelmezési tartomány minden eleméhez azonos elemet rendel).

Δ

A fentebb megadott $f = \sum_{\mathbf{u}\in\mathbb{F}_q^n}\left(\varphi(\mathbf{u})\prod_{i=0}^{n-1}(e-(x_i-u_i)^{q-1})\right)$ polinom az $\mathbb{F}_q$ fölötti n-határozatlanú polinomgyűrű, azaz $\mathbb{F}_q[x_{n-1},\dots,x_0]$ egy eleme, így $f = \sum_{(k_0,\dots k_{n-1})\in\mathbb{N}_q^n} a_{k_0,\dots k_{n-1}} \prod_{i=0}^{n-1} x_i^{k_i}$. Tekintsük $(k_0,\dots k_{n-1}) \in \mathbb{N}_q^n$-et a q-alapú számrendszerben felírt t egész szám számjegyeinek, ekkor $q^n > t = \sum_{i=0}^{n-1} k_i q^i \in \mathbb{N}$. Különböző $(k_0,\dots k_{n-1})$ különböző t-t ad, és minden $q^n > t \in \mathbb{N}$-hez van olyan $(k_0,\dots k_{n-1}) \in \mathbb{N}_q^n$, amely éppen t-t határozza meg, így kölcsönösen egyértelműen hozzárendelhetünk minden$(k_0,\dots k_{n-1}) \in \mathbb{N}_q^n$ -hez egy q^n-nél kisebb nemnegatív egész számot. Ha most megadunk egy $\mathbb{N}_{q^n} \to \mathbb{F}_q$ leképezést, akkor ezzel egyértelműen meghatároztunk egy $\mathbb{F}_q$ fölötti n-határozatlanú, minden határozatlanban legfeljebb $q-1$-edfokú polinomot, és ez visszafelé is igaz, vagyis kölcsönösen egyértelmű megfeleltetést létesítettünk $\mathbb{F}_q[x_{n-1},\dots,x_0]$ és az $\mathbb{F}_q$ fölötti q^n-dimenziós lineáris tér elemei között. Rendezzük most tetszőleges, de rögzített módon $\mathbb{F}_q$ elemeit, és rögzítsük az $\mathbb{F}_q$-t önmagába képező n-változós függvények változóinak sorrendjét is. Ekkor, az előbbiekhez hasonlóan, minden $\mathbb{F}_q^n \to \mathbb{F}_q$ függvény tekinthető az $\mathbb{F}_q$ fölötti q^n-dimenziós lineáris tér elemének, és a megfeleltetés ismét kölcsönösen egyértelmű. Polinomok összegében az együtthatók az összeadandó polinomok megfelelő kitevőhöz tartozó együtthatóinak összege, polinom konstansszorosában az együtthatók az eredeti polinom együtthatóinak ugyanazon konstansszorosai, így az együtthatók tere izomorf a polinomok terével. Ugyanígy látható be, hogy a polinomfüggvények az összeadással és konstanssal való szorzással olyan lineáris teret alkotnak, amely izomorf a függvényértékek előbb megadott sorrendjével előálló vektorok terével. Végül test fölötti polinomok esetén polinomok összegéhez tartozó polinomfüggvény a megfelelő polinomfüggvények összege, és hasonló igaz polinom konstansszorosára, így az $f \mapsto \hat{f}$ leképzés izomorfizmus az $\mathbb{F}_q$ fölötti n-határozatlanú, minden határozatlanban legfeljebb $q-1$-edfokú polinomok együtthatóiból álló vektorok és az $\mathbb{F}_q^n \to \mathbb{F}_q$ függvények függvényértékeiből alkotott vektorok lineáris tere között. Ez azt jelenti, hogy a függvényértékekből lineáris transzformációval is meghatározható a megfelelő polinom, és ez a transzformáció az ellenkező irányban is végrehajtható. Ezt írja le az alábbi tétel.

4.4. Tétel

Legyen $\mathbb{F}_q = \{a_i | q > i \in \mathbb{N}\}$ a q-elemű test, $n \in \mathbb{N}$, $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q$, és legyen $f \in \mathbb{F}_q[x_{n-1},\dots,x_0]$ olyan, hogy $\hat{f} = \varphi$. Ekkor

$$f = \sum_{i=0}^{q^n-1}\left(\left(\sum_{j=0}^{q^n-1} a_{i,j}^{(n)}\varphi(a_{j_{n-1}},\dots,a_{j_0})\right)\prod_{k=0}^{n-1} x_k^{i_k}\right),$$

ahol $i = \sum_{l=0}^{n-1} i_l q^l$, $j = \sum_{l=0}^{n-1} j_l q^l$, és $a_{i,j}^{(n)}$ egy $\mathbb{F}_q$ fölötti, q^n-edrendű kvadratikus $\mathbf{A}_q^{(n)}$ mátrix i-edik sorának j-edik oszlopában álló elem.

Δ

A tétel alábbi bizonyításában konkrétan is meghatározzuk a transzformációhoz tartozó mátrix komponenseit.

Bizonyítás:

$n = 0$-nál f konstans függvény, és $f = \hat{f}(\ \ ) = \varphi(\ \ ) = \sum_{i=0}^{q^0-1}\left(\left(\sum_{j=0}^{q^0-1} e\varphi(\ \ )\right)\prod_{k=0}^{0-1} x_k^{i_k}\right)$. A továbbiakhoz felhasználjuk, hogy tetszőleges $\mathbb{F}_q$ véges test, és bármely $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q$ függvény esetén $f = \sum_{\mathbf{u}\in\mathbb{F}_q^n}\left(\varphi(\mathbf{u})\prod_{i=0}^{n-1}(e-(x_i-u_i)^{q-1})\right)$ olyan polinom, amelyhez tartozó polinomfüggvény megegyezik φ-vel. Alkalmazzuk ezt először $n = 1$-re. Ekkor

$$\begin{aligned} f &= \sum_{j=0}^{q-1}\varphi(a_j)\left(e-(x_0-a_j)^{q-1}\right) \\ &= \sum_{j=0}^{q-1}\varphi(a_j)\left(e-\sum_{i=0}^{q-1}(-1)^{q-1-i}\binom{q-1}{i}a_j^{q-1-i}x_0^i\right) \\ &= \sum_{j=0}^{q-1}\varphi(a_j)\sum_{i=0}^{q-1}\left(\delta_{i,0}e+(-1)^{q-i}\binom{q-1}{i}a_j^{q-1-i}\right)x_0^i \\ &= \sum_{i=0}^{q-1}\sum_{j=0}^{q-1}\left(\delta_{i,0}e+(-1)^{q-i}\binom{q-1}{i}a_j^{q-1-i}\right)\varphi(a_j)\,x_0^i, \end{aligned}$$

és ha $a_{i,j}^{(1)} = \delta_{i,0}e+(-1)^{q-i}\binom{q-1}{i}a_j^{q-1-i}$, úgy

$$f = \sum_{i=0}^{q-1}\left(\sum_{j=0}^{q-1}a_{i,j}^{(1)}\varphi(a_j)\right)x_0^i = \sum_{i=0}^{q^1-1}\left(\sum_{j=0}^{q^1-1}a_{i,j}^{(1)}\varphi(a_j)\right)\prod_{k=0}^{1-1}x_k^{i_k}$$

Most tegyük fel, hogy egy pozitív egész n-re az $\mathbb{F}_q$ fölötti bármely n-változós φ függvény megegyezik az $f = \sum_{i=0}^{q^n-1}\left(\sum_{j=0}^{q^n-1}a_{i,j}^{(n)}\varphi(a_{j_{n-1}},\dots,a_{j_0})\right)\prod_{k=0}^{n-1}x_k^{i_k}$ n-határozatlanú polinom polinomfüggvényével, és legyen φ egy $n+1$-változós függvény. $q^{n+1} > i \in \mathbb{N}$ $i = i_n q^n + i'$ alakban írható, ahol $q^n > i' \in \mathbb{N}$ és $q > i_n \in \mathbb{N}$. $q^{n+1} > j \in \mathbb{N}$ hasonló módon írható a $j = j_n q^n + j'$ alakban. Vezessük be a $\varphi_{j_n}\left(a_{j'_{n-1}},\dots,a_{j'_0}\right) = \varphi(a_{j_n},a_{j_{n-1}},\dots,a_{j_0}) = \varphi_{j'}(a_{j_n})$ jelölést. Az indukciós feltétellel

$$\begin{aligned} f &= \sum_{j=0}^{q^{n+1}-1}\varphi(a_{j_n},a_{j_{n-1}},\dots,a_{j_0})\prod_{k=0}^{n}\left(e-(x_k-a_{j_k})^{q-1}\right) \\ &= \sum_{j_n=0}^{q-1}\left(\sum_{j'=0}^{q^n-1}\varphi_{j_n}\left(a_{j'_{n-1}},\dots,a_{j'_0}\right)\prod_{k=0}^{n-1}\left(e-\left(x_k-a_{j'_k}\right)^{q-1}\right)\right)\left(e-(x_n-a_{j_n})^{q-1}\right) \\ &= \sum_{j_n=0}^{q-1}\left(\sum_{i'=0}^{q^n-1}\left(\sum_{j'=0}^{q^n-1}a_{i',j'}^{(n)}\varphi_{j_n}\left(a_{j'_{n-1}},\dots,a_{j'_0}\right)\right)\prod_{k=0}^{n-1}x_k^{i'_k}\right)\left(e-(x_n-a_{j_n})^{q-1}\right). \end{aligned}$$

Az összegzés sorrendjének felcserélésével ebből azt kapjuk, hogy

$$f = \sum_{i'=0}^{q^n-1}\sum_{j'=0}^{q^n-1}a_{i',j'}^{(n)}\left(\sum_{j_n=0}^{q-1}\varphi_{j'}(a_{j_n})\left(e-(x_n-a_{j_n})^{q-1}\right)\right)\prod_{k=0}^{n-1}x_k^{i'_k},$$

és a belső összeget a korábbi eredmény alapján átírva

$$f=\sum_{i'=0}^{q^n-1}\sum_{j'=0}^{q^n-1}a_{i',j'}^{(n)}\left(\sum_{i_n=0}^{q-1}\left(\sum_{j_n=0}^{q-1}a_{i_n,j_n}^{(1)}\varphi_{j'}(a_{j_n})\right)x_n^{i_n}\right)\prod_{k=0}^{n-1}x_k^{i'_k}.$$

Az összegzések sorrendjének ismételt felcserélésével és tényezők sorrendjének módosításával végül

$$\begin{aligned}f&=\sum_{i_n=0}^{q-1}\sum_{i'=0}^{q^n-1}\sum_{j_n=0}^{q-1}\sum_{j'=0}^{q^n-1}\left(a_{i_n,j_n}^{(1)}a_{i',j'}^{(n)}\right)\varphi_{j'}(a_{j_n})\left(x_n^{i_n}\prod_{k=0}^{n-1}x_k^{i'_k}\right)\\&=\sum_{i=0}^{q^{n+1}-1}\left(\sum_{j=0}^{q^{n+1}-1}a_{i,j}^{(n+1)}\varphi\left(a_{j_n},a_{j_{n-1}},\dots,a_{j_0}\right)\right)\prod_{k=0}^{n}x_k^{i_k},\end{aligned}$$

ahol $a_{i,j}^{(n+1)}=a_{i_n,j_n}^{(1)}a_{i',j'}^{(n)}$.

□

Az eddigiek alapján $\mathbf{A}_q^{(0)}=(e)$-ből $\mathbf{A}_q^{(1)}$ felhasználásával iterációval sorban egymás után meg tudjuk határozni tetszőleges nemnegatív egész n-re $\mathbf{A}_q^{(n)}$-t. Az alábbi tétel szerint azonban $\mathbf{A}_q^{(1)}$ elemei az eredetileg megadott kifejezésnél lényegesen egyszerűbb szerkezetűek.

4.5. Tétel

Legyen p prímszám, $m\in\mathbb{N}^+$, $q=p^m$ és $\mathbb{F}_q=\{a_i|q>i\in\mathbb{N}\}$ a q-elemű test, ahol $a_0=0$. Ekkor a $q>i\in\mathbb{N}$ és $q>j\in\mathbb{N}$ indexre $a_{i,j}^{(1)}=\delta_{i,0}e-a_j^{q-1-i}$.

Δ

Bizonyítás:

$q>i\in\mathbb{N}$-re $\frac{\prod_{k=1}^{i}(q-k)}{\prod_{k=1}^{i}k}=\binom{q-1}{i}=c\in\mathbb{N}^+$, így $c\prod_{k=1}^{i}k=\prod_{k=1}^{i}(q-k)$. Ha $k=p^{r_k}u_k$, ahol $p\nmid u_k$, akkor $1\le k\le i<p^m$-ből $m>r_k\in\mathbb{N}$, azaz $m-r_k>0$, tehát $p^{m-r_k}-u_k\equiv-u_k\ (p)$. Ezt felhasználva

$$\begin{aligned}c\prod_{k=1}^{i}u_k&=c\prod_{k=1}^{i}\frac{k}{p^{r_k}}=\frac{1}{\prod_{k=1}^{i}p^{r_k}}c\prod_{k=1}^{i}k=\frac{1}{\prod_{k=1}^{i}p^{r_k}}\prod_{k=1}^{i}(q-k)\\&=\prod_{k=1}^{i}\frac{q-k}{p^{r_k}}=\prod_{k=1}^{i}(p^{m-r_k}-u_k)\equiv\prod_{k=1}^{i}(-u_k)=(-1)^i\prod_{k=1}^{i}u_k\ (p).\end{aligned}$$

$p\nmid u_k$-ból $\prod_{k=1}^{i}u_k$ relatív prím p-hez, tehát a fenti kongruencia osztható $\prod_{k=1}^{i}u_k$-val, és így $\binom{q-1}{i}=c\equiv(-1)^i\ (p)$. Ekkor $\binom{q-1}{i}e=(-1)^ie$ és $(-1)^{q-i}\binom{q-1}{i}a_j^{q-1-i}=(-1)^qa_j^{q-1-i}$. Ha q páratlan, akkor $(-1)^qe=-e$, míg $q=2^m$-nél $(-1)^qe=e=-e$, tehát bármely pozitív egész kitevős q prímhatványnál $\delta_{i,0}e+(-1)^{q-i}\binom{q-1}{i}a_j^{q-1-i}=\delta_{i,0}e-a_j^{q-1-i}$.

□

Ha u a test egy primitív eleme, akkor rendezhetjük úgy a test elemeit, hogy $q>j\in\mathbb{N}^+$-ra $a_j=u^{j-1}$. Ekkor $a_j=\left(1-\delta_{j,0}\right)u^{j-1}$ még $j=0$ esetén is teljesül.

$\mathbf{A}_q^{(n)}$-et tömörebb formában is meg tudjuk adni. Ha $\mathbf{A}$ egy $r \times s$- és $\mathbf{B}$ egy $m \times n$-méretű mátrix, akkor a két mátrix ebben a sorrendben vett $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$ **Kronecker-szorzata** olyan, $rm \times sn$-méretű mátrix, amelyben $c_{i_1 m+i_0, j_1 n+j_0} = a_{i_1,j_1} b_{i_0,j_0}$, vagyis egy olyan $r \times s$-méretű hipermátrix, amelynek i-edik sorában a j-edik elem $\mathbf{D}_{i,j} = a_{i,j}\mathbf{B}$. Könnyű ellenőrizni, hogy bármely két mátrixnak létezik a Kronecker-szorzata, ez a szorzás asszociatív, mindkét oldalról disztributív, de nem kommutatív. Legyen $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ és $\mathbf{D}$ ugyanazon test fölötti mátrix úgy, hogy $\mathbf{A}$ $\mathbf{C}$-vel és $\mathbf{B}$ $\mathbf{D}$-vel összeszorozható. Ekkor

$$((\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D}))_{i,k} = \sum_{j=0}^{s-1} \left(a_{i,j}\mathbf{B}\right)\left(c_{j,k}\mathbf{D}\right) = \left(\sum_{j=0}^{s-1} a_{i,j}c_{j,k}\right)(\mathbf{BD}) = (\mathbf{AC})_{i,k}(\mathbf{BD}),$$

és így $(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D}) = (\mathbf{AC})\otimes(\mathbf{BD})$. Ebből következik, hogy ha mind $\mathbf{A}$-nak, mind $\mathbf{B}$-nek van inverze, akkor $\mathbf{A}\otimes\mathbf{B}$ is invertálható, és $(\mathbf{A}\otimes\mathbf{B})^{-1} = \mathbf{A}^{-1}\otimes\mathbf{B}^{-1}$. Azt is könnyű belátni, hogy ha mindkét mátrix négyzetes, és valamelyikük nem invertálható, akkor ez igaz a Kronecker-szorzatukra is.

A Kronecker-szorzással az alábbi tételt kapjuk.

4.6. Tétel

Legyen $\mathbb{F}_q = \{a_i | q > i \in \mathbb{N}\}$, $a_0 = 0$, $n \in \mathbb{N}$, a $q^n > i \in \mathbb{N}$, $q^n > j \in \mathbb{N}$ indexekre $a_{i,j}^{(n)}$ az $\mathbb{F}_q$ fölötti q^n-edrendű $\mathbf{A}_q^{(n)}$ mátrix *i*-edik sorának *j*-edik eleme, $\mathbf{A}_q^{(0)} = (e)$ és $a_{i,j}^{(1)} = \delta_{i,0}e - a_j^{q-1-i}$. Ekkor $\mathbf{A}_q^{(n+1)} = \mathbf{A}_q^{(1)} \otimes \mathbf{A}_q^{(n)}$, $\mathbf{A}_q^{(n)}$ minden $n \in \mathbb{N}$-re reguláris, és $\mathbf{A}_q^{(0)^{-1}} = (e)$, $\left(\mathbf{A}_q^{(1)}\right)_{i,j}^{-1} = a_i^j$.

Δ

Bizonyítás:

$\mathbf{A}_q^{(0)} = (e)$, $a_{i,j}^{(1)} = \delta_{i,0}e - a_j^{q-1-i}$ és $a_{i,j}^{(n+1)} = a_{i_n q^n + i', j_n q^n + j'}^{(n+1)} = a_{i_n,j_n}^{(1)} a_{i',j'}^{(n)}$ (lásd a 4.4. és 4.5 Tételt), és az utóbbi egyenlőség mutatja, hogy $\mathbf{A}_q^{(n+1)} = \mathbf{A}_q^{(1)} \otimes \mathbf{A}_q^{(n)}$. $\mathbf{A}_q^{(0)^{-1}} = (e)^{-1} = (e)$, így már csak azt kell igazolnunk, hogy $\mathbf{A}_q^{(1)}$-nek van inverze, és $\left(\mathbf{A}_q^{(1)}\right)_{i,j}^{-1} = a_i^j$.

Legyen $\mathbf{B}$ q-adrendű mátrix, és a $q > i \in \mathbb{N}$, $q > j \in \mathbb{N}$ indexekre legyen $b_{i,j} = a_i^j$. Nézzük a $\mathbf{B}\mathbf{A}_q^{(1)}$ mátrixot. Ha $i = 0$, akkor $\sum_{j=0}^{q-1} b_{0,j} a_{j,k}^{(1)} = \sum_{j=0}^{q-1} a_0^j \left(\delta_{j,0}e - a_k^{q-1-j}\right) = e - a_k^{q-1} = \delta_{0,k}e$, vagyis $i = 0$ esetén $\left(\mathbf{B}\mathbf{A}_q^{(1)}\right)_{0,k} = \delta_{0,k}e$. A továbbiakban legyen $q > i \in \mathbb{N}^+$. Elsőként tekintsük a $k = 0$ esetet. Ekkor $\sum_{j=0}^{q-1} b_{i,j} a_{j,0}^{(1)} = \sum_{j=0}^{q-1} a_i^j \left(\delta_{j,0}e - a_0^{q-1-j}\right) = a_i^0 \cdot e - a_i^{q-1} = 0 = \delta_{i,0}e$, ami, az előbbi eredmény szerint, $i = 0$-nál is igaz. Ha $k \neq 0$, akkor létezik a_k^{-1}, $a_i^j a_k^{q-1-j} = \left(a_i a_k^{-1}\right)^j = a_l^j$, ahol $l \neq 0$, és

$$\sum_{j=0}^{q-1} a_i^j \left(\delta_{j,0}e - a_k^{q-1-j}\right) = a_i^0 \left(e - a_k^{q-1}\right) - \sum_{j=1}^{q-1} a_i^j a_k^{q-1-j} = -\sum_{j=1}^{q-1} \left(a_i a_k^{-1}\right)^j$$
$$= -\sum_{j=1}^{q-1} a_l^j = -\sum_{j=0}^{q-2} a_l^j = -\delta_{i,k}(q-1)e = \delta_{i,k}e,$$

ugyanis $-(q-1) \equiv 1\ (p)$, $i = k$ esetén $a_l = e$, és ha $a_l \neq e$, akkor $\sum_{j=0}^{q-2} a_l^j = \frac{a_l^{q-1} - e}{a_l - e} = 0$. Összefoglalva, minden $q > i \in \mathbb{N}$, $q > k \in \mathbb{N}$ indexre $\left(\mathbf{B}\mathbf{A}_q^{(1)}\right)_{i,k} = \delta_{i,k}e$, vagyis $\mathbf{B} = \mathbf{A}_q^{(1)^{-1}}$.

□

A speciális $q = 2$ esetben $a_0 = 0$, $a_1 = e$, vagyis $a_i = \left(1 - \delta_{i,0}\right)e$, és ezt alkalmazva

$$a_{i,j}^{(1)} = \delta_{i,0}e - a_j^{2-1-i} = \left(\delta_{i,0} - \left(1 - \delta_{j,0}\right)^{1-i}\right)e = \left(1 - \delta_{i,0}\delta_{j,1}\right)e,$$

tehát $\mathbf{A}_2^{(1)} = \begin{pmatrix} e & 0 \\ e & e \end{pmatrix}$. Ekkor $\mathbf{A}_2^{(n+1)} = \begin{pmatrix} \mathbf{A}_2^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}_2^{(n)} & \mathbf{A}_2^{(n)} \end{pmatrix}$ és $\mathbf{A}_2^{(1)^{-1}} = \mathbf{A}_2^{(1)}$, így $\mathbf{A}_2^{(n)^{-1}} = \mathbf{A}_2^{(n)}$.

Legyen most $\mathcal{R}$ olyan m-elemű kommutatív gyűrű, ahol $1 < m \in \mathbb{N}$, úgy, hogy $\mathcal{R}$ nem test. Ekkor $\mathcal{R}$-ben szükségszerűen van nullosztó. Legyen egy nullosztó u, és $0 \neq v \in R$ olyan, hogy $uv = 0$ (mivel u nullosztó, ilyen v létezik). Ekkor $f = u\prod_{a\in R\setminus\{v\}}(x_{n-1} - a)$ $\mathcal{R}$ fölötti olyan, n-határozatlanú, nemnulla polinom, amely minden határozatlanban legfeljebb $m - 1$-edfokú, és amelyhez tartozó polinomfüggvény a nullfüggvény. Ez azt jelenti, hogy van két olyan különböző, minden határozatlanban legfeljebb $m - 1$-edfokú, $\mathcal{R}$ fölötti, n-határozatlanú polinom, nevezetesen f és a nullpolinom, amelyekhez tartozó polinomfüggvény azonos leképezést valósít meg. Mivel az $\mathcal{R}$ fölötti, minden határozatlanban legfeljebb $m - 1$-edfokú, n-határozatlanú polinomok és az R^n-et R-be képező függvények száma egyaránt m^{m^n}, és az $f \mapsto \hat{f}$ leképezés nem injektív, ezért nem is szürjektív, vagyis nem lehet bármely $\varphi: R^n \to R$ leképezést egy polinomhoz tartozó polinomfüggvényként megadni.

Ha $\mathcal{R}$ nem egységelemes, akkor $x_{n-1} - a$ nem eleme $R[x]$-nek, így látszólag erre az esetre nem megfelelő az $f = u\prod_{a\in R\setminus\{v\}}(x_{n-1} - a)$ polinom. Valójában jobb a helyzet. Ha ugyanis elvégezzük a szorzást, akkor a szorzatpolinom minden tagjának együtthatója már olyan kifejezés, amely R-beli elemek szorzata, és ez eleme a gyűrűnek, tehát a polinom is benne van az $\mathcal{R}$ feletti polinomgyűrűben.

A megadott polinom csak formálisan n-határozatlanú, valójában csupán egyetlen határozatlant tartalmaz. Megadható ténylegesen *n* határozatlant tartalmazó nem nulla polinom, amely szintén rendelkezik azzal a tulajdonsággal, hogy a hozzá tartozó polinomfüggvény az azonosan nulla leképezés. Ilyen például az $f = u\prod_{a\in R\setminus\{v\}}(x_{n-1} - a)\prod_{k=0}^{n-2} x_k$ polinom.

Az m-elemű halmazt önmagába képező függvények, ahol m egy 1-nél nagyobb egész szám, az **m-értékű logikai függvény**ek, speciálisan az $m = 2$ esetben a **Boole-függvény**ek. Az előbbi eredmények szerint, ha m prímhatvány, és csak ekkor, az m-értékű logikai függvények megadhatóak polinomfüggvényként, és az átjárás a függvényértékek és a polinom között az előbb megadott mátrixszal is történhet. A Boole-függvények függvényértékkel való közvetlen megadása például a diszjunktív normál alak, ezen belül is például a kanonikus diszjunktív normál alak, azaz az 1 függvényértékhez tartozó **minterm**ek **diszjunkció**ja, **VAGY-kapcsolat**a. A minterm az összes változót egyszer és csak egyszer tartalmazó **konjunkció**, vagyis a változók **ÉS-kapcsolat**a, ahol egyes változók **negált**jukkal, azaz az ellentettjükkel, míg más változók az eredeti értékükkel, **ponált**an szerepelnek. n változónak összesen 2^n mintermje van, amelyeket sorba rendezhetünk oly módon, hogy először rögzítjük a változók sorrendjét, majd tekintjük azt a nemnegatív egész számot, amelynek kettes számrendszerbeli felírásában az i-edik jegy 0, ha a mintermben az i-indexű változó negált, egyébként ez a jegy 1. A megfelelő minterm $m_k^{(n)} = \wedge_{i=0}^{n-1}\left(\overline{a_i^{(k)}} \veebar x_i\right)$, ahol $a_i^{(k)}$ a k szám bináris felírásában az i-edik helyiértékhez tartozó jegy, a felülhúzás a negálás jele, míg $\veebar$ a **KIZÁRÓ VAGY** jele. Ekkor a függvény egy 2^n- hosszúságú $0 - 1$ sorozattal adható meg, amely egy 2^{2^n}-nél kisebb l nemnegatív egész számot ad a kettes számrendszerben, és ha ebben a sorozatban a k-adik jegy $c_k^{(l)}$, akkor $f^{(l)} = \vee_{k=0}^{2^n-1}\left(c_k^{(l)} \wedge m_k^{(n)}\right)$ a megfelelő függvény.

A Boole-függvény egy másik reprezentációja a polinommal való megadás, amelyet szokás **Zsegalkin-polinom**nak is nevezni. Ez olyan **monom**ok, azaz **egytagú**ak összege, amelyben minden határozatlan kitevője 0 vagy 1, és a 0-s kitevőhöz tartozó határozatlanokat nem írjuk ki. Ismét, ha $2^n > k \in \mathbb{N}$, és $k = \sum_{i=0}^{n-1} a_i^{(k)} 2^i$, akkor $S_k^{(n)} = \prod_{i=0}^{n-1}\left(\overline{a_i^{(k)}} \vee x_i\right) = \prod_{i=0}^{n-1} x_i^{a_i^{(k)}}$, továbbá amennyiben $l = \sum_{i=0}^{2^n-1} u_k^{(l)} 2^k$, akkor $f^{\langle l\rangle} = \sum_{k=0}^{2^n-1} u_k^{(l)} S_k^{(n)}$. Természetesen általában $f^{\langle l\rangle} \neq f^{(l)}$ (bár vannak olyan indexek, amelyeknél teljesül az egyenlőség), és a $c_k^{(l)}$ valamint az $u_k^{(l)}$ együtthatók által meghatározott

vektorok közötti kapcsolat többek között a korábban megadott $\mathbf{A}_2^{(1)} = \begin{pmatrix} e & 0 \\ e & e \end{pmatrix}$ illetve $\mathbf{A}_2^{(n+1)} = \begin{pmatrix} \mathbf{A}_2^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}_2^{(n)} & \mathbf{A}_2^{(n)} \end{pmatrix}$ mátrixszal adható meg (és azt is láttuk, hogy az ellenkező irányú transzformáció ugyanezen mátrixszal történik az $m = 2$, azaz a Boole-függvények esetén).

Azt azért fontos megjegyezni, hogy az egyszerű mátrixszorzással való átjárás számítástechnikailag csupán kis *m* és *n* értékek esetén járható út, hiszen az eljárás nem polinomiális futási idejű (a mátrixok és a vektorok m^n-méretűek). A számítási idő azonban lényegesen csökkenthető. Tekintsük az az $\mathbf{A}_q^{(1)} = \begin{pmatrix} e & \mathbf{0}^{(q-1)^T} \\ -\mathbf{e}_{q-2}^{(q-1)} & -\mathbf{B} \end{pmatrix}$ mátrixot, ahol $\mathbf{0}^{(q-1)}$ a $q-1$-dimenziós nullvektor, T a transzponálás jele, $\mathbf{e}_{q-2}^{(q-1)}$ az a $q-1$-dimenziós egységvektor, amelynél $\left(\mathbf{e}_{q-2}^{(q-1)}\right)_i = \delta_{i,q-2}e$ (az indexelést 0-val kezdve), végül $\mathbf{B}$ az $\mathbf{A}_q^{(1)}$ legfelső sorát és bal szélső oszlopát törölve kapott mátrix ellentettje. Ha $\mathbf{u}$ az $\mathbb{F}_q$ feletti q-dimenziós tér egy tetszőleges eleme, és $\mathbf{U} = \mathbf{A}_q^{(1)}\mathbf{u}$, továbbá $\tilde{\mathbf{u}}$ az $\mathbf{u}$-ból és $\tilde{\mathbf{U}}$ az $\mathbf{U}$-ból a 0-indexű komponens törlésével kapott $q-1$-dimenziós vektor, akkor $\tilde{\mathbf{U}} = -\left(u_0\mathbf{e}_{q-2}^{(q-1)} + \mathbf{B}\tilde{\mathbf{u}}\right)$. Ennek a vektornak a kiszámításához szükséges idő lényegében véve $\mathbf{B}\tilde{\mathbf{u}}$ kiszámításának futási idejével azonos. Legyen $\vec{\mathbf{B}}$ az a mátrix, amelyet $\mathbf{B}$-ből a sorok egy sorral való ciklikus lefelé mozgatásával kapunk, és legyen $\hat{\mathbf{U}} = \vec{\mathbf{B}}\tilde{\mathbf{u}}$. $\left(\vec{\mathbf{B}}\right)_{i,j} = -a_{(i-1) \bmod (q-1)+1,j+1} = a_{j+1}^{(q-1)-((i-1) \bmod (q-1)+1)} = \left(z^j\right)^{-i} = \left(z^{-i}\right)^j$ a test egy *z* primitív elemével. Ezzel $\hat{U}_i = \sum_{j=0}^{\tilde{n}-1}\left(z^{-i}\right)^j\tilde{u}_j$, ha $\tilde{n} = q-1 = n-1$, az $\tilde{\mathbf{u}}$ és $\hat{\mathbf{U}}$ vektorok komponenseinek száma. Ez azonban, amint azt majd a megfelelő fejezetben látjuk, azt jelenti, hogy $\hat{\mathbf{U}}$ az $\tilde{\mathbf{u}}$ vektor diszkrét Fourier-transzformáltja, és a diszkrét Fourier-transzformáció kiszámítására létezik gyors algoritmus, a gyors Fourier-transzformáció, az FFT. Mivel $\mathbf{A}_q^{(n+1)}$-et nagyrészt $\mathbf{A}_q^{(1)}$-ből hatványozással kapjuk, ezért megfelelő átalakításokkal az n-változós függvények esetén is alkalmazható az FFT, és így a lineáris transzformáció elfogadható futási idővel számolható, ha $q > 2$.

Sokszor fogjuk használni az $x^q - x = \prod_{u\in\mathbb{F}_q}(x-u)$ és a hasonló $x^{q-1} - e = \prod_{u\in\mathbb{F}_q^*}(x-u)$ összefüggést. Ennél valamivel általánosabb a következő tétel.

4.7. Tétel

Ha $f \in \mathbb{F}_q[x]$, akkor $f^q - f = \prod_{u\in\mathbb{F}_q}(f-u)$.

Δ

Bizonyítás:

$(fg)\circ h = (f\circ h)(g\circ h)$ ($\circ$ a polinomok kompozíciója), és ha $f = g$, akkor $f\circ h = g\circ h$ tetszőleges h polinommal, így

$$f^q - f = (x^q - x)\circ f = \left(\prod_{u\in\mathbb{F}_q}(x-u)\right)\circ f = \prod_{u\in\mathbb{F}_q}\left((x-u)\circ f\right) = \prod_{u\in\mathbb{F}_q}(f-u).$$

□

Lényeges lesz a továbbiakban az is, hogy q^m-elemű testen az $u \mapsto u^{q^n}$ megfeleltetés automorfizmus (és relatív automorfizmus a q-elemű résztestre vonatkozóan, lásd a 3.48. Kiegészítést). Ebből következik a két következő tétel.

4.8. Tétel

$t \in \mathbb{N}^+$-ra $f \in \mathbb{F}_{q^t}[x]$ akkor és csak akkor eleme $\mathbb{F}_q[x]$-nek, ha $f^q = f \circ x^q$.

Δ

Bizonyítás:

Legyen $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_{q^t}[x]$. a_i eleme $\mathbb{F}_{q^t}$-nek, így $f^q = \left(\sum_{i=0}^{n} a_i x^i\right)^q = \sum_{i=0}^{n} a_i^q (x^q)^i$, míg $f \circ x^q = \sum_{i=0}^{n} a_i (x^q)^i$. De két polinom pontosan akkor egyenlő, ha minden indexre az együtthatójuk azonos, azaz ha $n \geq i \in \mathbb{N}$-re $a_i = a_i^q$, és ez $\mathbb{F}_{q^t}$ elemei közül pontosan $\mathbb{F}_q$ elemeire igaz.

□

4.9. Tétel

Ha $\mathcal{L}|\mathbb{F}_q$, $f \in \mathbb{F}_q[x]$, és $\alpha \in L$ gyöke f-nek, akkor bármely $k \in \mathbb{N}$-re α^{q^k} is gyöke f-nek.

Δ

Bizonyítás:

$k = 0$-ra $\alpha^{q^k} = \alpha$, és α gyöke a polinomnak. Legyen $n \in \mathbb{N}$ és $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_q[x]$. Ekkor minden $n \geq i \in \mathbb{N}$-re $a_i \in \mathbb{F}_q$, és így $a_i^q = a_i$, továbbá $\mathbb{F}_q$-ban és annak bármely $\mathcal{L}$ bővítésében $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ L-beli a és b elemekkel. Most legyen $j \in \mathbb{N}$-re $\hat{f}\left(\alpha^{q^j}\right) = 0$. Ezzel $0 = 0^q = \left(\hat{f}\left(\alpha^{q^j}\right)\right)^q = \left(\sum_{i=0}^{n} a_i \left(\alpha^{q^j}\right)^i\right)^q = \sum_{i=0}^{n} a_i \left(\alpha^{q^{j+1}}\right)^i = \hat{f}\left(\alpha^{q^{j+1}}\right)$, tehát $\alpha^{q^{j+1}}$ is gyöke f-nek. ami igazolja a tételben megfogalmazott állításunkat.

□

Láthatóan q-hatvány-elemű testben a q^i-kitevős hatványok fontosak. Most ezeket vizsgáljuk.

4.10. Tétel

Legyen $\alpha \in \mathbb{F}_{q^t}$, továbbá $s = 1$, ha $\alpha = 0$, egyébként $s = o_n(q)$ (a q modulo n rendje), ahol n az α rendje. Ekkor $\alpha^{q^0}, \alpha^{q^1}, \ldots, \alpha^{q^{s-1}}$ páronként különböző, bármely $j \in \mathbb{N}$-re α^{q^j} az előbbi hatványok valamelyikével azonos, és az $i \in \mathbb{N}$, $j \in \mathbb{N}$ egészekre $\alpha^{q^i} = \alpha^{q^j}$ pontosan akkor igaz, ha $i \equiv j\ (s)$.

Δ

Bizonyítás:

$\alpha = 0$-ra az állítás nyilvánvaló, ezért legyen $\alpha \neq 0$, és $i \in \mathbb{N}$, $j \in \mathbb{N}$. Ekkor $\alpha^{q^i} = \alpha^{q^j}$ akkor és csak akkor igaz, ha $q^i \equiv q^j\ (n)$. n osztója az $\mathbb{F}_{q^t}$ multiplikatív csoportja rendjének, azaz $q^t - 1$-nek, így relatív prím q-hoz, ezért, ha $j \geq i$, az előbbi kongruencia ekvivalens $q^{j-i} \equiv 1\ (n)$-nel, és ez $i \equiv j\ (s)$-sel, ahol $s = o_n(q)$. Innen az is látszik, hogy $s > i \in \mathbb{N}$ kitevőkkel az α^{q^i} hatványok páronként különbözőek, és bármely α^{q^j} egy s-nél kisebb nemnegatív egész i kitevős α^{q^i}-vel azonos.

□

4.11. Definíció

$\alpha \in \mathbb{F}_{q^t}$ **($\mathbb{F}_q$-ra vonatkozó) ciklikus rendje** $s_\alpha^{(q)} = \min_{k \in \mathbb{N}^+} \left\{\alpha^{q^k} = \alpha\right\}$, ahol $t \in \mathbb{N}^+$.

Δ

Az előző tételben azt láttuk be, hogy egy $\mathcal{L}$ véges test minden elemének létezik és egyértelmű a test bármely $\mathcal{K}$ résztestére vonatkozó ciklikus rendje. Az is látszik, hogy ez a rend – eltekintve a prímtest elemeitől – attól is függ, hogy $\mathcal{L}$ mely résztestére vonatkoztatjuk. Erről is szól az alábbi tétel.

4.12. Tétel

1. Ha $\mathcal{L}$ a $\mathcal{K}$ véges test t-edfokú bővítése, és $\alpha \in L$, úgy α $\mathcal{K}$ feletti ciklikus rendje osztója t-nek, és a ciklikus rend akkor és csak akkor 1, ha $\alpha \in K$.

2. Ha f a q-elemű $\mathcal{K}$ test feletti n-edfokú polinom, α az f egy gyöke a $\mathcal{K}$ valamely bővítésében, és α $\mathcal{K}$-ra vonatkozó ciklikus rendje s, akkor $s \leq n$.

3. Ha az $\mathcal{M}$ véges test az $\mathcal{L}$ test m_2-fokú bővítése, és $\mathcal{L}$ a q-elemű $\mathcal{K}$ test m_1-efokú bővítése, továbbá az M valamely $u \neq 0$ elemének $\mathcal{K}$ feletti ciklikus rendje $s_u^{(q)} = s$, akkor u $\mathcal{L}$ feletti ciklikus rendje $s_1 = s_u^{(q^{m_1})} = \frac{s}{(s,m_1)} = o_s^+(m_1)$.

Δ

Bizonyítás:

1. Legyen $\mathcal{K}$ q-elemű test. $\mathcal{L}$ a $\mathcal{K}$ t-edfokú bővítése, ezért L elemeinek száma q^t, és $\alpha^{q^t} = \alpha$. Ez az előző tétel értelmében azt jelenti, hogy $t \equiv 0\ (s)$, azaz $s|t$, ahol $s = s_\alpha^{(q)}$. Az L-beli α akkor és csak akkor eleme K-nak, ha az előbbi oszthatóság $t = 1$ esetén is teljesül, és ez ekvivalens azzal a feltétellel, hogy s maga is 1.

2. Mivel $s > i \in \mathbb{N}$-re az α^{q^i}-k páronként különböző gyökei f-nek, és test fölötti polinomnak nem lehet a fokszámát meghaladó számú gyöke, ezért s valóban legfeljebb n lehet.

3. s a q modulo n rendje, így $q^r \equiv 1\ (n)$ akkor és csak akkor igaz egy pozitív egész r-rel, ha r osztható s-sel. Ha s_1 az u ciklikus rendje a q^{m_1}-elemű test fölött, akkor s_1 a legkisebb pozitív egész, amellyel $(q^{m_1})^k \equiv 1\ (n)$, vagyis s_1 a legkisebb k pozitív egész, amelyre km_1 osztható s-sel. Ha $s|km_1$, akkor $\frac{s}{(s,m_1)} \Big| k$, és a legkisebb ilyen k pozitív egész szám maga az osztó, azaz $\frac{s}{(s,m_1)}$.

□

Most rátérünk az irreducibilis polinomok vizsgálatára.

4.13. Tétel

Legyen $f \in \mathbb{F}_q[x]$ m-edfokú polinom. f akkor és csak akkor irreducibilis $\mathbb{F}_q$ fölött, ha van $\mathbb{F}_q$-nak olyan $\mathcal{L}$ bővítése, és L-ben olyan α, hogy $\hat{f}(\alpha) = 0$ és $s = s_\alpha^{(q)} \geq m$.

Δ

Bizonyítás:

Mivel f-nek van foka, ezért f nem a nullpolinom.

1. Tegyük fel, hogy f-nek $\mathbb{F}_q$ valamely bővítésében van gyöke. Mivel f nem a nullpolinom, ezért a gyök létezése azt jelenti, hogy a polinom legalább elsőfokú, így nem egység. Legyen a gyök α és $s \geq m$, továbbá $f = gh$ $\mathbb{F}_q$ fölötti g és h polinomokkal. Mivel $f \neq 0$, ennélfogva $g \neq 0 \neq h$. A feltétel szerint $\hat{g}(\alpha)\hat{h}(\alpha) = 0$, és test nullosztómentes, ezért $\hat{g}(\alpha)$ és $\hat{h}(\alpha)$ közül legalább az egyik 0. Az általánosság csorbítása nélkül feltehető, hogy például $\hat{g}(\alpha) = 0$. Ekkor α-val együtt $m > i \in \mathbb{N}$-re α^{q^i} is gyöke g-nek, és $s \geq m$ következtében ezek a gyökök páronként különbözőek, így g legalább m-edfokú, ennél magasabb fokú viszont nem lehet, mert osztója a nem nulla f-nek. Ez azzal jár, hogy h foka 0, hiszen test fölötti nem nulla polinomok szorzatának foka megegyezik a tényező-polinomok fokának összegével, vagyis h konstans, és természetesen nem nulla, ezért egység $\mathbb{F}_q$ fölött. Ez $m \geq 1$ következtében egyúttal azt is jelenti, hogy f felbonthatatlan.

2. Most legyen f felbonthatatlan $\mathbb{F}_q[x]$-ben. Ekkor $\deg(f) = m \geq 1$, és van $\mathbb{F}_q$-nak olyan $\mathcal{L}$ bővítése, amelyben van f-nek gyöke, mondjuk α. Ha α $\mathbb{F}_q$ fölötti ciklikus rendje s, akkor $\hat{f}(\alpha) = 0$-ból az $s > i \in \mathbb{N}$ egészekkel α^{q^i} páronként különböző gyöke f-nek. Legyen $g = \prod_{i=0}^{s-1}\left(x - \alpha^{q^i}\right)$. Ez a g $\mathcal{L}$ feletti polinom, és mivel s gyöke van, ezért a foka s. L elemeinek száma q egy pozitív egész kitevős hatványa, és α q^s-edik hatványa azonos a q^0-adik hatvánnyal, így

$$g^q = \left(\prod_{i=0}^{s-1}\left(x-\alpha^{q^i}\right)\right)^q = \prod_{i=0}^{s-1}\left(x^q-\alpha^{q^{i+1}}\right) = \prod_{i=0}^{s-1}\left(x^q-\alpha^{q^i}\right) = g\circ x^q,$$

tehát $g \in \mathbb{F}_q[x]$. α gyöke az $\mathbb{F}_q$ fölött irreducibilis f-nek, ezért f asszociáltja az α $\mathbb{F}_q$ fölötti minimál-polinomjának. $h \in \mathbb{F}_q[x]$-nek α akkor és csak akkor gyöke, ha $\mathbb{F}_q$ fölötti minimál-polinomja osztója h-nak, így f osztója g-nek. Ebből már következik, hogy $m = \deg(f) \leq \deg(g) = s$.

□

4.14. Következmény

1. $\mathbb{F}_q$ fölött irreducibilis m-edfokú polinom gyökének $\mathbb{F}_q$ fölötti ciklikus rendje m, így egy elemnek az őt tartalmazó test valamely résztestére vonatkozó ciklikus rendje megegyezik ugyanezen résztest fölötti minimál-polinomjának fokával;
2. $\mathbb{F}_q$ valamely bővítésében egy primitív elem ciklikus rendje azonos a bővítés fokával;
3. véges test feletti irreducibilis polinom gyökei egyszeresek.

Δ

Bizonyítás:

1. Korábban láttuk, hogy m-edfokú polinom gyökének ciklikus rendje nem nagyobb a polinom fokánál, az előző tételben pedig kiderült, hogy irreducibilis polinom gyökének ciklikus rendje legalább akkora, mint a polinom foka. A kettő együtt azt jelenti, hogy adott test felett irreducibilis polinom foka megegyezik egy gyökének ugyanezen testre vonatkozó ciklikus rendjével.
2. Primitív elem minimál-polinomjának foka azonos a bővítés fokával, így ez 1. alapján igaz.
3. A tétel szerint, ha f az $\mathbb{F}_q$ test fölött m-edfokú irreducibilis polinom, és a test egy alkalmas bővítésében α a polinom gyöke, akkor az α^{q^i} elemek $m > i \in \mathbb{N}$ esetén páronként különböző gyökök, a polinomnak van m különböző gyöke. De test fölötti nem nulla polinom gyökeinek száma multiplicitásukkal számolva megegyezik a polinom fokszámával, így ha valamelyik gyök többszörös lenne, akkor a gyököket multiplicitásukkal számolva f-nek több gyöke lenne m-nél, ami lehetetlen.

□

A $\mathbb{Q}$ feletti $x^3 - 2$ polinomnak egy valós és két komplex gyöke van. $\mathbb{Q}$-t a valós gyökkel bővítve a bővített test minden eleme valós, így ez a test nem tartalmazza a polinom másik két gyökét, a bővített test nem a polinom $\mathbb{Q}$ feletti felbontási teste. A fenti tétel szerint véges test esetén más a helyzet.

4.15. Tétel

Véges test egyszerű algebrai bővítése a bővítő elem minimál-polinomjának felbontási teste.

Δ

Bizonyítás:

Ha α az f $\mathbb{F}_q$ fölött felbonthatatlan m-edfokú polinom gyöke, akkor a felbontási test tartalmazza α-t és $\mathbb{F}_q$-t, tehát $\mathbb{F}_q(\alpha)$-t. Ugyanakkor minden $m > i \in \mathbb{N}$-re $\alpha^{q^i} \in \mathbb{F}_q(\alpha)$, tehát f minden gyöke eleme $\mathbb{F}_q(\alpha)$-nak, így a felbontási test része $\mathbb{F}_q(\alpha)$-nak, tehát a két test azonos.

□

4.16. Definíció

Ha $\alpha \in \mathbb{F}_{q^t}$, akkor $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{t-1}}$ az α $\mathbb{F}_q$**-ra vonatkozó konjugáltjai**.

Δ

4.17. Tétel

A konjugáltság ekvivalencia-reláció $\mathbb{F}_{q^t}$-ben, és a konjugáltak $\mathbb{F}_{q^t}^*$-beli rendje továbbá ciklikus rendje azonos. α egymással azonos konjugáltjainak száma $\frac{t}{s}$, ahol s az α $\mathbb{F}_q$ fölötti ciklikus rendje.

Δ

Bizonyítás:

Legyen α ciklikus rendje s, ekkor $s \leq t$, hiszen s osztója a nem nulla t-nek.

1. Jelölje az $\mathbb{F}_{q^t}$-beli α-ra és β-ra $\alpha \sim \beta$, hogy β az α konjugáltja. Ez bármely $\mathbb{F}_{q^t}$-beli rendezett párra vagy igaz, vagy nem, így $\sim$ binér reláció $\mathbb{F}_{q^t}$-ben.

A konjugáltság definíciójából közvetlenül látszik, hogy $\alpha \sim \alpha$, tehát $\sim$ reflexív.

Amennyiben $\alpha \sim \beta$ és $\beta \sim \gamma$, akkor $\beta = \alpha^{q^u}$ és $\gamma = \beta^{q^v}$, ahol u és v egyaránt t-nél kisebb nemnegatív egész, és helyettesítés után $\gamma = \left(\alpha^{q^u}\right)^{q^v} = \alpha^{q^{u+v}}$. De ha α $\mathbb{F}_q$ fölötti ciklikus rendje s, és $w = (u+v) \bmod s$, akkor $u + v \equiv w\ (s)$, tehát $\gamma = \alpha^{q^{u+v}} = \alpha^{q^w}$, továbbá $0 \leq w < s \leq t$, így γ az α $\mathbb{F}_q$ fölötti konjugáltja, $\alpha \sim \gamma$, a reláció tranzitív.

Az előbbi α-val és β-val legyen $v = (-u) \bmod s$. Ekkor $0 \leq v < s \leq t$ és $u + v \equiv 0\ (s)$, így $\beta^{q^v} = \left(\alpha^{q^u}\right)^{q^v} = \alpha^{q^{u+v}} = \alpha$, vagyis a reláció szimmetrikus is, tehát valóban ekvivalencia-reláció.

2. A rendek egyenlőségének bizonyításához a szimmetria miatt elegendő megmutatni, hogy ha $\alpha \neq 0$ és $\alpha \sim \beta$, akkor β rendje osztója α rendjének. De ha α rendje n, akkor tetszőleges $r \in \mathbb{N}$-re $(\alpha^r)^n = (\alpha^n)^r = e$, vagyis α^r rendje osztja n-et, és $\beta = \alpha^{q^u}$, így β rendje osztója n-nek, azaz α rendjének. Ha viszont a rendek megegyeznek, akkor a ciklikus rendek is azonosak, hiszen $s = o_n(q)$.

3. s osztója t-nek, és tetszőleges nemnegatív egész i-re és k-ra $\alpha^{q^i} = \alpha^{q^{i+ks}}$.

□

4.18. Következmény

Legyen α és β az $\mathbb{F}_{q^t}$ két eleme. Ekkor

1. α és β $\mathbb{F}_q$ fölötti minimál-polinomja pontosan akkor azonos, ha $\alpha \sim \beta$.

Ha $\alpha \sim \beta$, akkor

2. $f \in \mathbb{F}_q[x]$-re α pontosan akkor gyöke f-nek, ha β is gyöke a polinomnak;
3. α pontosan akkor primitív elem $\mathbb{F}_{q^t}$-ben, ha β is az.

Δ

Bizonyítás:

1. Ha $\alpha \sim \beta$, akkor $\beta = \alpha^{q^i}$, ahol $i \in \mathbb{N}$, így β gyöke α $\mathbb{F}_q$ fölötti minimál-polinomjának, $m = m_\alpha^{(q)}$-nak. Ez irreducibilis $\mathbb{F}_q$ fölött és főpolinom, tehát $m_\beta^{(q)} = m = m_\alpha^{(q)}$. Fordítva, ha β gyöke $m_\alpha^{(q)}$-nak, akkor $\beta = \alpha^{q^i}$ egy nemnegatív egész i-vel, hiszen $m_\alpha^{(q)}$ irreducibilis $\mathbb{F}_q$ fölött, így $\alpha \sim \beta$.

2. Tudjuk, hogy ha α gyök, akkor α^{q^i} is gyök, tehát α-val együtt valamennyi konjugáltja, így β is gyök. Mivel a konjugáltság ekvivalencia, és így szimmetrikus, ezért visszafelé is áll az állítás.

3. Nemnulla elem konjugáltja sem nulla. Konjugált elemek rendje megegyezik, és egy elem pontosan akkor primitív elem, ha a rendje $q^t - 1$, így ha α primitív elem, akkor β is az, és fordítva.

□

Fontos és közvetlen kapcsolat van egy test adott test feletti relatív automorfizmusai valamint a test elemeinek az adott test feletti konjugáltjai között.

4.19. Tétel

Legyen $\mathcal{L}$ a q-elemű $\mathcal{K}$ test t-edfokú bővítése. Az L α és β eleme akkor és csak akkor konjugált $\mathcal{K}$ fölött, ha van $\mathcal{L}$-nek olyan $\mathcal{K}$ fölötti σ relatív automorfizmusa, amellyel $\beta = \sigma(\alpha)$.

Δ

Bizonyítás:

Ha α és β konjugáltak $\mathcal{K}$ fölött, akkor $\beta = \alpha^{q^k}$ egy $0 \leq k < t$ egésszel. De $\alpha \mapsto \alpha^{q^k}$ a q-elemű test bármely bővítésében automorfizmus, amely az alaptest elemein az identikus leképezés.

Fordítva, legyen σ az $\mathcal{L}$ $\mathcal{K}$ feletti relatív automorfizmusa, és $\beta = \sigma(\alpha)$, továbbá az α $\mathcal{K}$ feletti minimál-polinomja $f = \sum_{i=0}^{n} c_i x^i$. Ekkor

$$0 = \sigma(0) = \sigma\left(\hat{f}(\alpha)\right) = \sigma\left(\sum_{i=0}^{n} c_i \alpha^i\right) = \sum_{i=0}^{n} c_i \big(\sigma(\alpha)\big)^i = \hat{f}\big(\sigma(\alpha)\big),$$

így $\sigma(\alpha)$ is gyöke f-nek. f irreducibilis (mert minimálpolinom felbonthatatlan), ezért a korábbiak alapján β az α egy q^k-kitevős hatványa, ahol $0 \leq k < s = \deg(f)$. De f foka az α ciklikus rendje, amely osztója a bővítés fokának, t-nek, így $s \leq t$, vagyis $0 \leq k < t$, β az α $\mathcal{K}$ fölötti konjugáltja.

□

A bizonyításban hivatkoztunk rá, hogy q-elemű $\mathcal{K}$ test bármely $\mathcal{L}$ bővítésében minden $k \in \mathbb{N}$-re $\alpha \mapsto \alpha^{q^k}$ az $\mathcal{L}$ $\mathcal{K}$ feletti relatív automorfizmusa. Belátjuk, hogy véges $\mathcal{L}$-re nincs is más lehetőség.

4.20. Tétel

Legyen az $\mathcal{L}$ véges test a q-elemű $\mathcal{K}$ test t-edfokú bővítése, és $\sigma: \alpha \mapsto \alpha^q$ az L elemeire. Ekkor az $\mathcal{L}$ $\mathcal{K}$ feletti relatív automorfizmusai t-rendű ciklikus csoportot alkotnak a σ generátorelemmel.

Δ

Bizonyítás:

$\sigma: \alpha \mapsto \alpha^q$ automorfizmusa $\mathcal{L}$-nek, és ha $\alpha \in K$, akkor $\alpha^q = \alpha$, ezért σ az $\mathcal{L}$ egy $\mathcal{K}$ feletti relatív automorfizmusa. Test relatív automorfizmusainak szorzata szintén relatív automorfizmus, és automorfizmusnak létezik inverze, amely ismét relatív automorfizmus, végül az identikus leképezés relatív automorfizmus, így ezek csoportot alkotnak. Legyen $\alpha \in L$. Ekkor $\sigma^0(\alpha) = \varepsilon(\alpha) = \alpha = \alpha^{q^0}$, ahol ε az identikus leképezés L-en. Mivel $\alpha^{q^{k+1}} = \left(\alpha^{q^k}\right)^q$ minden $k \in \mathbb{N}$-re, ezért, ha k-ra $\sigma^k(\alpha) = \alpha^{q^k}$, akkor $\sigma^{k+1}(\alpha) = \sigma\left(\sigma^k(\alpha)\right) = \left(\alpha^{q^k}\right)^q = \alpha^{q^{k+1}}$, vagyis minden $k \in \mathbb{N}$-nel $\sigma^{k+1}: \alpha \mapsto \alpha^{q^{k+1}}$.

Legyen u az $\mathcal{L}$ primitív eleme, és τ az $\mathcal{L}$ egy $\mathcal{K}$ feletti relatív automorfizmusa. A 4.19. Tétel szerint $\tau(u) = u^{q^k}$ egy $k \in \mathbb{N}$-nel. Amennyiben $\alpha \neq 0$, akkor $\alpha = u^i$ egy $q^t - 1 > i \in \mathbb{N}$ egésszel, és $\tau(\alpha) = \tau\big(u^i\big) = \big(\tau(u)\big)^i = \left(u^{q^k}\right)^i = \big(u^i\big)^{q^k} = \alpha^{q^k}$, továbbá $\tau(0) = 0 = 0^{q^k}$, vagyis $\tau = \sigma^k$, így beláttuk, hogy $\mathcal{L}$ bármely $\mathcal{K}$ feletti relatív automorfizmusa eleme a σ által generált ciklikus csoportnak.

u ciklikus rendje t, hiszen primitív elem ciklikus rendje azonos a bővítés fokával, így a t-nél kisebb kitevőkre $\sigma^i(u) = u^{q^i}$ páronként különböző, és a megfelelő σ^i automorfizmusok is páronként különbözőek, a σ által generált ciklikus csoport rendje legalább t. Másrészt az L bármely α elemével $\sigma^t(\alpha) = \alpha^{q^t} = \alpha = \sigma^0(\alpha)$, így $\sigma^t = \sigma^0 = \varepsilon$, és az identikus leképezés a csoport egységeleme, ami mutatja, hogy a csoport rendje legfeljebb t, tehát ez a rend pontosan t, így az $\mathcal{L}$ $\mathcal{K}$ feletti relatív automorfizmusai egy t-edrendű ciklikus csoportot alkotnak a σ generátorelemmel.

□

4.21. Definíció

Ha $\alpha \in \mathbb{F}_{q^t}$, akkor $\prod_{k=0}^{t-1}\left(x-\alpha^{q^k}\right)$ az α $\mathbb{F}_q$ **feletti karakterisztikus polinomja**.

Δ

A definíció szerint $\deg(f)=t$, bármely elem gyöke a saját karakterisztikus polinomjának, és két elem azonos test feletti karakterisztikus polinomja pontosan akkor azonos, ha konjugáltak.

4.22. Tétel

Legyen $\mathcal{L}$ a q-elemű $\mathcal{K}$ test t-edfokú bővítése, $\alpha \in L$, m az α $\mathcal{K}$ feletti minimál-polinomja, és f az α $\mathcal{K}$ feletti karakterisztikus polinomja. Ekkor $\alpha \in K[x]$, és $f=m^{\frac{t}{s}}$, ahol $s=\deg(m)$.

Δ

Bizonyítás:
α $\mathcal{K}$ feletti ciklikus rendje s, és s osztója t-nek, ezért

$$f=\prod_{k=0}^{t-1}\left(x-\alpha^{q^k}\right)=\prod_{j=0}^{\frac{t}{s}-1}\prod_{i=0}^{s-1}\left(x-\alpha^{q^{i+js}}\right)=\prod_{j=0}^{\frac{t}{s}-1}\left(\prod_{i=0}^{s-1}\left(x-\alpha^{q^i}\right)\right)=m^{\frac{t}{s}},$$

amiből következik, hogy f $\mathcal{K}$ feletti polinom.

□

4.23. Következmény

Ha $\mathcal{L}|\mathcal{K}$, L véges és $\alpha \in L$, akkor α $\mathcal{K}$ feletti konjugáltjainak összege és szorzata K-beli.

Δ

Bizonyítás:
A gyökök összege és szorzata a karakterisztikus polinom együtthatója, tehát K-beli.

□

Tudjuk, hogy a q^n-elemű test az $x^{q^n}-x \in \mathbb{F}_q[x]$ polinom $\mathbb{F}_q$ feletti felbontási teste, így maga a polinom is sok szempontból fontos. Most ennek a polinomnak vizsgáljuk néhány tulajdonságát.

4.24. Tétel

Az $\mathbb{F}_q$ fölött irreducibilis m-edfokú f polinom pontosan akkor osztója $x^{q^n}-x \in \mathbb{F}_q[x]$-nek, ha $m|n$, ahol $n \in \mathbb{N}$.

Δ

Bizonyítás:
Ha $n=0$, akkor $m|n$, másrészt $x^{q^n}-x$ a nullpolinom, amelynek osztója minden f polinom. Nézzük az $n \in \mathbb{N}^+$ esetet. Ha f irreducibilis, akkor a fokszáma, tehát m, nagyobb, mint 0. Legyen α az f egy gyöke. $f\left|x^{q^n}-x\right.$ pontosan akkor teljesül, ha $\alpha^{q^n}-\alpha=0$, vagyis ha $\alpha^{q^n}=\alpha$. Ez pontosan akkor igaz, ha $s|n$, ahol s az α $\mathbb{F}_q$ fölötti ciklikus rendje, és ha f irreducibilis $\mathbb{F}_q$ fölött, akkor $s=m$.

□

4.25. Tétel

$x^{q^n} - x = \prod_{f \in P_n^{(q)}} f$, ahol $P_n^{(q)}$ azon $\mathbb{F}_q$ fölött irreducibilis főpolinomok halmaza, amelyek fokszáma az n pozitív egész szám osztója.

Δ

Bizonyítás:

Legyen $f_n^{(q)} = x^{q^n} - x$. $f_n^{(q)'} = q^n x^{q^n - 1} - e = -e$, mert $f_n^{(q)} \in \mathbb{F}_q[x]$ és $\mathrm{char}(\mathbb{F}_q) | q$, így $f_n^{(q)}$-nak nincs többszörös gyöke, tehát többszörös faktora sem lehet. Az előző tétel szerint $P_n^{(q)}$ minden eleme osztója $f_n^{(q)}$-nak, és mivel ezek mindegyike irreducibilis, tehát páronként relatív prím, ezért a szorzatuk, g is osztója $f_n^{(q)}$-nak. Ha most t az $f_n^{(q)}$ valamely, $\mathbb{F}_q$ fölött irreducibilis főpolinom faktora, akkor csak egyszeres faktor lehet, és az előző tétel szerint eleme $P_n^{(q)}$-nek, vagyis a t-k szorzata, $f_n^{(q)}$, osztója g-nek, így $f_n^{(q)}$ és g asszociáltak. De mindkét polinom főpolinom, így meg is egyeznek.

□

4.26. Következmény

$\mathbb{F}_q$ fölött irreducibilis, n-edfokú főpolinomok száma $\frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$ (μ a Moebius-függvény).

Δ

Bizonyítás:

$q^n = \deg\left(x^{q^n} - x\right) = \deg\left(\prod_{f \in P_n^{(q)}} f\right) = \sum_{f \in P_n^{(q)}} \deg(f)$, ahol valamennyi f-re teljesül, hogy $\deg(f) | n$. Jelöljük a $P_n^{(q)}$-beli n-edfokú polinomok számát $N_n^{(q)}$-val. Ekkor $q^n = \sum_{d|n} d N_d^{(q)}$, vagyis q^n a $h(n) = n N_n^{(q)}$ számelméleti függvény összegzési függvénye, és így a Moebius-féle megfordítási összefüggéssel visszakapjuk h-t, ahonnan n-nel való osztás után a felírt egyenlőségre jutunk.

□

Sokszor van szükség irreducibilis polinomra. Kérdés, hogy egy véletlenül választott polinom milyen eséllyel irreducibilis. Nézzük meg, milyen arányban fordulnak elő az irreducibilis polinomok. Legyen ez az arány $p_n^{(q)}$. Tekintetbe véve, hogy n valódi osztója legfeljebb $\frac{n}{2}$, azt kapjuk, hogy

$$\begin{aligned} n N_n^{(q)} &= \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = q^n + \sum_{n > d | n} \mu\left(\frac{n}{d}\right) q^d \geq q^n + \sum_{n > d | n} (-1) q^d \\ &= q^n - \sum_{n > d | n} q^d \geq q^n - \sum_{k=1}^{\left\lfloor \frac{n}{2} \right\rfloor} q^k = q^n - q \frac{q^{\left\lfloor \frac{n}{2} \right\rfloor} - 1}{q-1} \geq q^n - q \frac{q^{\frac{n}{2}} - 1}{q-1} \\ &= q^n - \frac{(q-1)+1}{q-1}\left(q^{\frac{n}{2}} - 1\right) \geq q^n - \left(1 + \frac{1}{2-1}\right)\left(q^{\frac{n}{2}} - 1\right) \\ &= \left(q^n - 2q^{\frac{n}{2}} + 1\right) + 1 = \left(q^{\frac{n}{2}} - 1\right)^2 + 1. \end{aligned}$$

Az $\mathbb{F}_q$ fölötti n-edfokú főpolinomok száma q^n, így kapjuk, hogy

$$p_n^{(q)} = \frac{N_n^{(q)}}{q^n} \geq \frac{\frac{1}{n}\left(\left(q^{\frac{n}{2}} - 1\right)^2 + 1\right)}{q^n} = \frac{1}{n}\left(\left(1 - q^{-\frac{n}{2}}\right)^2 + q^{-n}\right) > \frac{1}{n}\left(1 - q^{-\frac{n}{2}}\right)^2.$$

Ha $n \geq 2$, akkor $1 - q^{-\frac{n}{2}} \geq 1 - \frac{1}{q} \geq \frac{1}{2}$, tehát $p_n^{(q)} > \frac{1}{4n}$, és ha $q^n \geq 12$, akkor $p_n^{(q)} > \frac{1}{2n}$. $1 - q^{-\frac{n}{2}}$ az n szigorúan monoton növekvő függvénye, és a határértéke a $+\infty$-ben 1, így $p_n^{(q)}$ alsó becslése $\frac{1}{n}$-hez tart. A másik oldalról viszont az n-edfokú irreducibilis főpolinomok szorzata osztója az $x^{q^n} - x$ polinomnak, így $nN_n^{(q)} \leq q^n$, tehát $p_n^{(q)} \leq \frac{1}{n}$.

Kissé eltérő számítással egy másik közelítést kaphatunk:

$$q^n = \sum_{d|n} dN_d^{(q)} = nN_n^{(q)} + \sum_{n>d|n} dN_d^{(q)} \leq nN_n^{(q)} + \sum_{p|n} \sum_{d|\frac{n}{p}} dN_d^{(q)}$$
$$= nN_n^{(q)} + \sum_{p|n} q^{\frac{n}{p}} \leq nN_n^{(q)} + \lfloor \log_2 n \rfloor q^{\lfloor \frac{n}{2} \rfloor},$$

ugyanis a kettős összegben ugyanazon irreducibilis polinomot esetleg többször is számba vesszük, a különböző prímosztók száma legfeljebb $\lfloor \log_2 n \rfloor$, és minden p-re $p \geq 2$. A fenti eredményből átrendezéssel kapjuk, hogy $nN_n^{(q)} \geq q^n - \lfloor \log_2 n \rfloor q^{\lfloor \frac{n}{2} \rfloor}$. Hasonlítsuk ezt össze a korábbi levezetés egy közbülső eredményével, ahol azt kaptuk, hogy $nN_n^{(q)} = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \geq q^n - q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1}$. Ez akkor és csak akkor ad jobb eredményt, mint a mostani, ha $q^n - q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1} \geq q^n - \lfloor \log_2 n \rfloor q^{\lfloor \frac{n}{2} \rfloor}$, azaz akkor és csak akkor, ha $q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1} \leq \lfloor \log_2 n \rfloor q^{\lfloor \frac{n}{2} \rfloor}$. Ez biztosan teljesül, ha $\frac{q}{q-1} q^{\lfloor \frac{n}{2} \rfloor} \leq \lfloor \log_2 n \rfloor q^{\lfloor \frac{n}{2} \rfloor}$, tehát, egyszerűsítve a pozitív $q^{\lfloor \frac{n}{2} \rfloor}$-vel, ha $\frac{q}{q-1} \leq \lfloor \log_2 n \rfloor$. De $q \geq 2$-ből $\frac{q}{q-1} \leq 2$, így, ha $2 \leq \lfloor \log_2 n \rfloor$, azaz ha $n \geq 8$, akkor a korábbi számítás közbülső eredménye adja a jobb becslést. Azt is könnyen be lehet látni, hogy páros n esetén, ha n legalább 4, akkor a korábbi végső becslés is jobb eredményt ad.

$\left(q^{\frac{n}{2}} - 1\right)^2 + 1 \geq 1 > 0$, így $N_n = \frac{1}{n}\left(\left(q^{\frac{n}{2}} - 1\right)^2 + 1\right) > 0$, ami azt mutatja, hogy véges test fölött bármely pozitív egész n-hez van az adott test fölött irreducibilis n-edfokú polinom, amit más úton már a 3.59. Következményben is igazoltunk (lásd a 67. oldalon).

A 4.13. Tétel megad egy szükséges és elégséges feltételt egy polinom irreducibilitására, ám ez inkább csak elvileg használható, hiszen a döntéshez ismerni kellene a polinom egy gyökét. Az alábbi tételben olyan feltételt adunk, amely a gyakorlatban is alkalmazható a felbonthatóság eldöntésére.

4.27. Tétel

Az $\mathbb{F}_q$ fölötti n-edfokú f polinom, ahol $2 \leq n \in \mathbb{N}^+$, akkor és csak akkor bontható fel $\mathbb{F}_q$ fölött, ha van olyan $\frac{n}{2} \geq i \in \mathbb{N}^+$, hogy $d_i = \left(f, x^{q^i} - x\right)$ legalább elsőfokú. Amennyiben $\hat{f}(0) \neq 0$, akkor a d_i polinomok helyett tekinthetjük a $\delta_i = \left(f, x^{q^i - 1} - e\right)$ polinomokat.

Δ

Bizonyítás:

Legyen f felbontható $\mathbb{F}_q[x]$-ben. Ekkor van olyan $\mathbb{F}_q$ fölött irreducibilis faktora, amelynek a fokszáma legfeljebb n fele . Ha g ilyen faktor, és $\deg(g) = u$, akkor g osztója f-nek és $x^{q^u} - x$-nek, így ezek legnagyobb közös osztójának is, a legnagyobb közös osztó nem konstans. Ha viszont a megadott korlátok közé eső u-ra d_u nem konstans, akkor van felbonthatatlan osztója, mondjuk g, ennek foka osztója az n-nél kisebb u-nak, tehát g valódi osztója f-nek, f felbontható.

Ha $\deg(f) \geq 2$, úgy f csak úgy lehet felbonthatatlan, ha x nem osztója, vagyis ha $\hat{f}(0) \neq 0$. Ekkor f és x relatív prímek, és mivel $x^{q^i} - x = x\left(x^{q^i-1} - e\right)$, ezért $\left(f, x^{q^i} - x\right) = \left(f, x^{q^i-1} - e\right)$.

□

A tételből következik, hogy ha f felbontható a q-elemű test fölött, akkor meg tudjuk határozni, hány különböző l-edfokú, $\mathbb{F}_q$ fölött irreducibilis faktora van, amint az alábbi eredmény mutatja.

4.28. Következmény

Legyen $f \in \mathbb{F}_q[x]$ felbontható $\mathbb{F}_q$ fölött és l a legkisebb pozitív egész, amelyre d_i legalább elsőfokú. Ekkor d_l az f páronként különböző, $\mathbb{F}_q$ fölött felbonthatatlan l-edfokú osztójának szorzata, és d_1 foka az f $\mathbb{F}_q$-beli különböző gyökeinek száma.

Δ

Bizonyítás:

$x^{q^l} - x$-nek, de akkor valamennyi osztójának, tehát d_l-nek is minden felbonthatatlan osztója egyszeres. Ha g az f egy l-edfokú irreducibilis osztója, akkor g osztója f-nek és osztója $x^{q^l} - x$-nek, tehát d_l-nek, és d_l minden g osztója, tehát minden felbonthatatlan osztója osztója f-nek, így már csak azt kell belátni, hogy d_l minden irreducibilis osztója l-edfokú. Legyen g foka m. $g|d_l \left| x^{q^l} - x \right.$, és g irreducibilis $\mathbb{F}_q$ fölött, ezért $\deg(g)|l$, tehát $m \leq l$. Ugyanakkor $g\left|x^{q^m} - x\right.$ és $g|d_l|f$, és akkor $g|d_m$. De l-nél kisebb t-re d_t konstans, vagyis nem lehet osztható a legalább elsőfokú g polinommal, ezért $m \geq l$, ennélfogva $m = l$.

u akkor és csak akkor f gyöke, ha $x - u$ osztója f-nek, és $x - u \in \mathbb{F}_q[x]$ akkor és csak akkor, ha $u \in \mathbb{F}_q$, tehát a polinom $\mathbb{F}_q$-beli különböző gyökei és elsőfokú faktorai kölcsönösen egyértelműen megfeleltethetőek egymásnak, így d_1 foka megegyezik f különböző gyökeinek számával.

□

Legyen $l > i \in \mathbb{N}$-re $r_i = 0$, $g_{l,1} = d_l$ és $r_l = 1$. Az előbbi eredmény alapján f-nek $\frac{\deg(d_l)}{l}$ páronként különböző l-edfokú irreducibilis faktora van. Ha $d_l = f$, akkor f minden irreducibilis faktora egyszeres és l-edfokú. Ellenkező esetben $f_l = \frac{f}{d_l}$-lel $\deg(f_l) = n - \deg(d_l) < n$, és $f = f_l d_l$, így f felbontása azonos f_l és d_l felbontásának szorzatával. f_l-nek nincs l-nél alacsonyabb fokú irreducibilis faktora, vagyis l-nél kisebb pozitív egész i-re $\left(f_l, x^{q^i} - x\right) = e$, így ezeket a legnagyobb közös osztókat felesleges kiszámítani. Ha f egy l-edfokú felbonthatatlan osztója többszörös faktora f-nek, akkor viszont $d_{2l} = \left(f_l, x^{q^l} - x\right) \neq e$, és d_{2l} minden irreducibilis osztója az f legalább kétszeres l-edfokú irreducibilis faktora. $g_{l,1}$-et elosztva d_{2l}-lel, és az így kapott hányadost írva $g_{l,1}$-be, a kapott $g_{l,1}$ az f olyan l-edfokú irreducibilis osztóinak szorzata, amelyek az eredeti polinomban első hatványon fordulnak elő. Legyen $g_{l,2} = d_{2l}$ és $f_{2l} = \frac{f_l}{d_{2l}}$. Ezek után ismét meghatározhatjuk az utóbbi hányados és $x^{q^l} - x$ legnagyobb közös osztóját. Ezt addig folytathatjuk, míg olyan polinomot nem kapunk, amely már relatív prím $x^{q^l} - x$-hez. A hányadospolinomok fokszáma szigorúan monoton csökken, ezért véges sok lépés után biztosan ilyen polinomot kapunk. Ha ez a polinom f_{tl}, akkor legyen $r_l = t - 1$, és legyen a polinom foka n_l. f_{tl}-nek már nincs olyan irreducibilis faktora, amelynek a foka legfeljebb l. Most meghatározzuk az l után következő legkisebb olyan $l < s \leq \frac{n_l}{2}$ kitevőt, amelyre $d_s = \left(f_{tl}, x^{q^s} - x\right) \neq e$. Ha ilyen nincs, akkor f_{tl} felbonthatatlan, ellenkező esetben d_s az f különböző s-edfokú irreducibilis osztóinak szorzata, így tovább folytathatjuk a korábban leírt eljárást. A végén minden pozitív egész l-re ismerjük, hogy f-nek hány különböző l-edfokú, a q-elemű test fölött irreducibilis faktora van, és ismerjük is minden l-re, és ezen belül minden j-re a j-edik hatványon előforduló faktorok egyszeres multiplicitású szorzatait,

ugyanis $f = \prod_{k=1}^{n} \prod_{i=1}^{r_k} g_{k,i}^{i}$. Ezt például kihasználhatjuk a véges test feletti polinom faktorizálásánál. Az eljárást az 1. algoritmus mutatja.

$u = f$
$n = \deg(f)$
$k = 1$
$h = x^q - x$
$j = 0$
ciklus amíg $k \leq \frac{n}{2}$
  $d = (u, h)$
  $m = \deg(d)$
  ha $m > 0$, akkor
    $j = j + 1$
    $g_{k,j} = d$
    ha $j = 1$, akkor
      $s = k$
    különben
      $g_{k,j-1} = \frac{g_{k,j-1}}{d}$
    elágazás vége
    $u = \frac{u}{d}$
    $n = n - m$
  különben
    $r_k = j$
    $k = k + 1$
    $h = x^{q^k} - x$
    $j = 0$
  elágazás vége
ciklus vége
ha $n = 0$, akkor
  $r_k = j$
különben ha $n = s$, akkor
  $g_{k,j} = \frac{g_{k,j}}{u}$
  $r_k = j + 1$
  $g_{k,r_k} = u$
különben
  ha $k = s$, akkor
    $r_k = j$
    $k = k + 1$
  elágazás vége
  ciklus $l = k$-tól $n - 1$-ig
    $r_l = 0$
  ciklus vége
  $g_{n1} = u$
  $r_n = 1$
elágazás vége
$f = \prod_{k=1}^{s} \prod_{l=1}^{r_k} g_{k,l}^{l}$

1. algoritmus

Mivel a felbonthatóság mindig adott testre vonatkozik, ezért érdemes megvizsgálni, hogy ha egy polinom felbonthatatlan egy test fölött, akkor hogyan viselkedik egy másik testhez viszonyítva.

4.29. Tétel

Ha f n-edfokú irreducibilis polinom a q-elemű $\mathcal{K}$ test fölött, és $\mathcal{L}$ a $\mathcal{K}$ m-edfokú bővítése, akkor f $d = (m, n)$, páronként különböző, $\mathcal{L}[x]$-ben irreducibilis polinom szorzata, és valamennyi faktor $\frac{n}{d}$-edfokú. Ha $\alpha \in L$ az f gyöke, akkor α^{q^u} és α^{q^v} pontosan akkor gyöke ugyanazon faktornak, ha $u \equiv v\ (d)$, így $d > i \in \mathbb{N}$-re az α^{q^i} gyökök a felbontás különböző polinomjainak gyökei.

Δ

Bizonyítás:

Legyen $\mathcal{M}$ az f $\mathcal{K}$ fölötti felbontási teste, és tegyük fel, hogy f a $\mathcal{K}$ test fölött irreducibilis, n-edfokú főpolinom (ez utóbbi feltétel semmiben nem korlátozza az általánosságot, hiszen a főegyüttható nem nulla, és így egység a test feletti polinomgyűrűben), továbbá α az f egyik M-beli gyöke. Mivel f n-edfokú, $\mathbb{F}_q$ fölött felbonthatatlan főpolinom, ezért $\mathcal{M}$ fölött $f = \prod_{i=0}^{n-1} \left(x - \alpha^{q^i}\right)$, és $j > i \in \mathbb{N}$ egészekre $\alpha^{q^i} = \alpha^{q^j} \Leftrightarrow i \equiv j\ (n)$. Legyen f felbontása $\mathcal{L}$ fölött $f = \prod_{i=0}^{r-1} g_i$. Nyilván teljesül, hogy f gyökeinek halmaza megegyezik a faktorok M-beli gyökei halmazának uniójával. f irreducibilis $\mathcal{K}$ fölött, így gyökei egyszeresek, amiből következik, hogy a g_i polinomok páronként különbözőek, tehát M-ben gyökeik halmaza páronként diszjunkt, másrészről egyik ilyen halmaz sem üres, hiszen irreducibilis polinom legalább elsőfokú, azaz, összefoglalóan, a g_i polinomok gyökeinek halmazai f gyökei halmazát partícionálják. Legyen u az $r > i \in \mathbb{N}$ indexek bármelyike, és β a g_u gyöke. Ekkor $\beta = \alpha^{q^k}$ alkalmas

$n > k \in \mathbb{N}$ egésszel. g_u $\mathcal{L}$ fölött felbonthatatlan polinom, ezért g_u valamennyi gyöke a β valamely $(q^m)^i = q^{mi}$ kitevős hatványa, vagyis $\alpha^{q^{k+mi}}$-alakú, és g_u foka a legkisebb pozitív egész t, amelyre teljesül a $k \equiv k + mt\ (n)$ kongruencia, ahonnan $\deg(g_u) = \frac{n}{d}$. Mivel ez független u-tól, ezért valamennyi faktor foka azonos, ahonnan azt is kapjuk, hogy a faktorok száma, r, éppen d.

A fentiek alapján α^{q^i} és α^{q^j} és akkor és csak akkor gyöke ugyanazon faktornak, ha egy w egésszel $j \equiv i + mw\ (n)$. Ilyen w pontosan akkor létezik, ha $j - i$ osztható m és n legnagyobb közös osztójával, azaz ha $i \equiv j\ (d)$, és így $d > i \in \mathbb{N}$ -re az α^{q^i} gyökök páronként különböző faktorhoz tartoznak.

□

A tételből közvetlenül kapjuk az alábbi eredményt.

4.30. Következmény

Véges $\mathcal{K}$ test felett irreducibilis n-edfokú polinom pontosan akkor felbonthatatlan a $\mathcal{K}$ m-edfokú $\mathcal{L}$ bővítése fölött, ha $(m, n) = 1$, és pontosan akkor elsőfokú polinomok szorzata $\mathcal{L}[x]$-ben, ha $n|m$.

Δ

n-edfokú irreducibilis polinom gyökével bővítve, a bővítés foka n, és ha n osztója m-nek, akkor az m-edfokú bővítés az n-edfokú bővítéssel kapott test bővítése, így természetes, hogy amennyiben m osztható n-nel, akkor az így bővített test felett a polinom elsőfokú tényezők szorzata.

A fejezet hátralévő részében polinomok reciprokával és a reciprok polinomokkal foglalkozunk.

4.31. Definíció

A $\mathcal{K}$ test feletti *n*-edfokú *f* polinom **reciproka**, illetve **duálisa** $f^* = x^n(f \circ x^{-1})$, míg $0^* = 0$.

Δ

4.32. Tétel

Ha $f \in K[x]$, akkor f^* is $\mathcal{K}$ feletti polinom. Amennyiben f^* $\mathcal{K}$ felett felbontható, akkor f is felbontható $\mathcal{K}$ felett, míg ha f felbontható $\mathcal{K}[x]$-ben, és $\hat{f}(0) \neq 0$, akkor f^* is reducibilis $\mathcal{K}$ fölött.

Δ

Bizonyítás:

$0^* = 0 \in K[x]$, így a továbbiakban legyen $0 \neq f = \sum_{i=0}^{n} a_i x^i$, ahol $a_n \neq 0$ (tehát $\deg(f) = n$). A bizonyításban a duálisra vonatkozó több, önmagában is fontos tulajdonságot látunk be.

a) $f^* = x^n(f \circ x^{-1}) = x^n \sum_{i=0}^{n} a_i x^{-i} = \sum_{i=0}^{n} a_i x^{n-i} = \sum_{i=0}^{n} b_i x^i$, ahol $b_i = a_{n-i}$, így f^* valóban $\mathcal{K}$ feletti polinom, és f^* akkor és csak akkor nulla, ha f a nullpolinom.

b) Legyen $f = gh$, és g és h foka rendre m és r, ekkor $n = m + r$. x felcserélhető az együtthatókkal, így $f^* = x^n(f \circ x^{-1}) = x^{m+r}\big((gh) \circ x^{-1}\big) = \big(x^m(g \circ x^{-1})\big)\big(x^r(h \circ x^{-1})\big) = g^* h^*$.

c) Ha $f = c \in K^* \subseteq K[x]$, akkor $\deg(f) = 0$, és $f^* = c^* = x^0(c \circ x^{-1}) = c$, míg $f = x$ esetén $\deg(f) = 1$, így $f^* = x^* = x(x \circ x^{-1}) = e$.

d) a) szerint f^* legfeljebb n-edfokú, és akkor és csak akkor n-edfokú, ha $0 \neq b_n = a_0 = \hat{f}(0)$.

e) $\hat{f}^*(0) = b_0 = a_n \neq 0$.

f) Ha $f = x^r g$, ahol $\hat{g}(0) \neq 0$, akkor b) és c) alapján $f^* = g^*$, ezért $(f^*)^* = (g^*)^*$. Most d)-ből g^* foka azonos g fokával, és így az a) ponthoz hasonlóan eljárva, és figyelembe véve e)-t kapjuk, hogy $(f^*)^* = g$. Ebből következik, hogy $(f^*)^*|f$.

g) Legyen f^* felbontható $\mathcal{K}$ felett, és $f^* = gh$, ahol g és h egyaránt legalább elsőfokú. Az e) pont alapján $\hat{f}^*(0) \neq 0$, és így $\hat{g}^*(0) \neq 0$ és $\hat{h}^*(0) \neq 0$, vagyis mind g^*, mind h^* legalább elsőfokú. Viszont $g^*h^* = (f^*)^* | f$, ami mutatja, hogy f is felbontható $\mathcal{K}$ fölött.

h) Ha f felbontható, és $\hat{f}(0) \neq 0$, akkor $f = gh$ olyan g és h polinomokkal, hogy mindkét polinom foka legalább 1, és $\hat{g}^*(0) \neq 0 \neq \hat{h}^*(0)$. Innen kapjuk, hogy $f^* = g^*h^*$, és mindkét tényező legalább elsőfokú, tehát f reciproka felbontható.

□

4.33. Tétel

$0 \neq f \in K[x]$-nek $\alpha \neq 0$ akkor és csak akkor k-szoros gyöke, ha α^{-1} az f^* k-szoros gyöke.

Δ

Bizonyítás:

Legyen először a nem nulla α az f k-szoros gyöke, ekkor $f = (x-\alpha)^k g$, $\hat{g}(\alpha) \neq 0$, és α-nak létezik inverze, így $f^* = (e-\alpha x)^k g^* = (-\alpha)^k (x-\alpha^{-1})^k g^*$, α inverze legalább k-szoros gyöke f duálisának. Amennyiben viszont $\hat{g}^*(\alpha^{-1}) = 0$, akkor $f^* = (x-\alpha^{-1})^{k+1} h$, innen az előbbi átalakításhoz hasonlóan eljárva kapjuk, hogy $(f^*)^* = (-(\alpha)^{-1})^{k+1}(x-\alpha^{-1})^{k+1}h^*$, és mivel $(f^*)^*$ osztója f-nek, ezért $f = (x-\alpha)^{k+1}u$, ami lehetetlen, hiszen ez azt jelentené, hogy α legalább $k+1$-szeres gyöke f-nek.

Fordítva, ha α^{-1} f^*-nak k-szoros gyöke, akkor az előbbiek szerint α pontosan k-szoros gyöke $(f^*)^*$-nak. De $f = x^r (f^*)^*$, ahol $r \in \mathbb{N}$, és $\alpha \neq 0$ (mert α^{-1} f^* gyöke), így α nem gyöke x^r-nek, ezért α multiplicitása f-ben és $(f^*)^*$-ban azonos, tehát α pontosan k-szoros gyöke f-nek.

□

Érdekesek és fontosak azok a polinomok, amelyek duálisa saját asszociáltjuk.

4.34. Definíció

A $\mathcal{K}$ test feletti f polinom **önduális** vagy **reciprok**, ha $f^* = cf$ egy K^*-beli c elemmel.

Δ

4.35. Tétel

A $\mathcal{K}$ test feletti nemnulla f polinomra az alábbi állítások ekvivalensek:

1. f önduális;
2. $f^* = f$ vagy $f^* = -f$;
3. ha α gyöke f-nek, akkor α és α^{-1} azonos multiplicitású gyöke a polinomnak.

Δ

Bizonyítás:

1. Legyen $f \neq 0$ önduális. Ekkor $\hat{f}(0) = c^{-1}\hat{f}^*(0) \neq 0$, így $(f^*)^* = f$. Ezt alkalmazva kapjuk, hogy $f = (f^*)^* = (cf)^* = cf^* = c(cf) = c^2 f$, és innen $c^2 = e$ (mert f nem nulla), vagyis c gyöke a $\mathcal{K}$ feletti $x^2 - e$ polinomnak. De ennek a polinomnak pontosan két megoldása van, e és $-e$ (ha a test karakterisztikája 2, akkor ez a két gyök azonos, vagyis ekkor egy darab kétszeres gyök van).

2. Ha $f^* = f$ vagy $f^* = -f$, és f nem a nullpolinom, akkor f konstans tagja nem nulla, így a 0 nem gyöke a polinomnak. Az előző tételben bebizonyítottuk, hogy egy polinom nem nulla gyökének multiplicitása és a gyök inverzének multiplicitása a reciprok polinomban azonos, az pedig nyilvánvaló, hogy egy polinomnak és ellentettjének a gyökei azonosak és ugyanolyan multiplicitásúak.

3. Ha f bármely gyöke és a gyök inverze azonos multiplicitású gyöke f-nek, akkor f és f^* gyökei a 4.33. Tétel szerint azonosak, és így egy konstans szorzótól eltekintve a polinom megegyezik a

reciprokával (mert ha két polinom gyökei multiplicitással együtt azonosak, akkor a két polinom csak egy nem nulla konstans szorzóban különbözik), tehát f önduális.

□

Ha $f \in K[x]$ önduális polinom, akkor $f = (x-e)^r(x+e)^s \prod_{i=1}^{t}\left((x-u_i)\left(x-u_i^{-1}\right)\right)^{m_i}$, ahol r, s, t és $t \geq i \in \mathbb{N}^+$-ra m_i nemnegatív egész szám valamint u_i a test 0-tól, e-től és $-e$-től különböző eleme. $(x-e)^* = -(x-e)$, $(x+e)^* = x+e$ és $\left((x-u_i)\left(x-u_i^{-1}\right)\right)^* = (x-u_i)\left(x-u_i^{-1}\right)$, ezért $f^* = (-1)^r f$, továbbá $\prod_{i=1}^{t}\left((x-u_i)\left(x-u_i^{-1}\right)\right)^{m_i}$ foka páros. $\hat{f}(v) = 0$ esetén legyen $f_v = \frac{f}{x-v}$. Ha $f^* = -f$, akkor e biztosan gyöke f-nek, és ekkor $f_e^* = f_e$, míg ha $\deg(f)$ páratlan, akkor e és $-e$ legalább egyike gyöke f-nek, és ha $f^* = cf$, akkor az előbbi esetben $f_e^* = (-c)f_e$, míg az utóbbi esetben $f_{-e}^* = cf_{-e}$. Azt könnyű megállapítani, hogy egy polinomnak gyöke-e e illetve $-e$, így, ha az eredeti polinomot mindig osztjuk a gyöktényezővel, akkor végül a $g = \prod_{i=1}^{t}\left((x-u_i)\left(x-u_i^{-1}\right)\right)^{m_i}$ polinomot kapjuk, amely az előbbiek szerint páros fokszámú, és $g^* = g$. A továbbiakban feltesszük, hogy $= \sum_{i=0}^{2m} a_i x^i$ már ilyen alakú, vagyis olyan önduális polinom, amelynek sem e, sem $-e$ nem gyöke. Ekkor $a_i = a_{2m-i}$, és ezt alkalmazva $f = \sum_{i=0}^{2m} a_i x^i = x^m\left(\sum_{i=0}^{m-1} a_i\left(x^{m-i} + x^{-(m-i)}\right) + a_m\right)$. Legyen $y = x + x^{-1}$. Ha $k \in \mathbb{N}$, akkor $\left(x^k + x^{-k}\right)(x + x^{-1}) = \left(x^{k+1} + x^{-(k+1)}\right) + \left(x^{k-1} + x^{-(k-1)}\right)$, és így $x^{k+1} + x^{-(k+1)} = \left(x^k + x^{-k}\right)(x + x^{-1}) - \left(x^{k-1} + x^{-(k-1)}\right)$. $x^0 + x^{-0} = 2e = 2y^0$, és hasonlóan, $x^1 + x^{-1} = x + x^{-1} = y = y^1$, vagyis $k = 0$ és $k = 1$ esetén $x^k + x^{-k}$ y k-adfokú polinomja. Tegyük fel, hogy ez igaz minden $n \geq i \in \mathbb{N}$ esetén, ahol n pozitív egész szám, és legyen i-re a megfelelő polinom f_i. Ekkor, az előző eredmények alapján,

$$x^{n+1} + x^{-(n+1)} = (x^n + x^{-n})y - \left(x^{n-1} + x^{-(n-1)}\right) = yf_n - f_{n-1},$$

és a felírásból láthatóan ez is az y $n+1$-edfokú polinomja, tehát $\sum_{i=0}^{m-1} a_i\left(x^{m-i} + x^{-(m-i)}\right) + a_m$ is polinomja y-nak, és a foka y-ban m. f reciprok polinom, így a 0 nem gyöke, tehát f akkor és csak akkor 0 egy u pontban, ha $\sum_{i=0}^{m-1} a_i\left(x^{m-i} + x^{-(m-i)}\right) + a_m$ értéke is 0 ugyanebben az u pontban. Ha a $g = \sum_{i=0}^{m-1} a_i f_{m-i} + a_m$ polinom egy gyöke v, akkor $v = x + x^{-1}$-ből megkapjuk f egy u gyökét: ez az előbbi kifejezésből az $x^2 - vx + e$ polinom gyöke lesz, azaz $u = \frac{v}{2e} \pm \sqrt{\left(\frac{v}{2e}\right)^2 - e}$, kivéve, ha a test karakterisztikája 2. Minden v-hez meghatározva u-t, megkapjuk f valamennyi gyökét, vagyis a $2m$-edfokú polinom gyökeit egy m-edfokú, és legfeljebb m különböző másodfokú polinom gyökeinek meghatározására vezettük vissza. Ez például azt jelenti, hogy reciprok polinomok esetén a komplex test fölötti legfeljebb 9-edfokú polinom gyökeit gyökképlettel tudjuk meghatározni.

Végül meghatározzuk a duálisok legnagyobb közös osztóját és legkisebb közös többszörösét.

4.36. Tétel

Ha $d = (f_i | n \geq i \in \mathbb{N}^+)$ és $t = [f_i | n \geq i \in \mathbb{N}^+]$, akkor az f_i-k duálisainak legnagyobb közös osztója d^*, és legkisebb közös többszöröse t^*.

Δ

Bizonyítás:

Ha minden i-re f_i a nullpolinom, akkor a legnagyobb közös osztó a nullpolinom, és ekkor igaz a legnagyobb közös osztóra vonatkozó állítás. Amennyiben a megadott polinomok között van nem nulla, akkor a legnagyobb közös osztó értékét nem befolyásolja nullpolinomok hozzávétele vagy elhagyása, így feltehetjük, hogy a megadott polinomok egyike sem nulla. Legyen δ a reciprok polinomok legnagyobb közös osztója. Mivel nemnulla polinom duálisa a nullában nem nulla, és δ osztója a duálisoknak, ezért $\hat{\delta}(0) \neq 0$, és így $(\delta^*)^* = \delta$. $n \geq i \in \mathbb{N}^+$-ra δ osztója f_i^*-nak, így δ^* osztója $(f_i^*)^*$-nak, ami viszont osztója f_i-nek, amiből következik, hogy δ^* osztója az f_i-k legnagyobb közös osztójának, azaz d-nek,

innen pedig kapjuk, hogy δ^* reciproka, vagyis δ osztója d^*-nak. Másrészről valamennyi $n \geq i \in \mathbb{N}^+$-ra d osztója f_i-nek, ezért d^* osztója f_i^*-nak, ami csak úgy lehetséges, ha egyben osztója az utóbbi polinomok legnagyobb közös osztójának, azaz δ-nak. Ez az előbbi oszthatósággal kiadja, hogy δ és d^* asszociáltak, és ha mindkettőt főpolinomnak választjuk, akkor meg is egyeznek.

Amennyiben az adott polinomok között előfordul a nullpolinom, akkor a legkisebb közös többszörös is nulla, másrészt a reciprokok között is fellép a nullpolinom, így a két legkisebb közös többszörös egybeesik. Legyen most az f_i-k halmaza olyan, amelyben nem szerepel a nullpolinom; a legkisebb közös többszörösre vonatkozó állítást indukcióval bizonyítjuk. Ha $n = 1$, akkor nyilvánvaló az egyenlőség. Ha $n = 2$, akkor $td = f_1 f_2$, amiből már adódik az állítás, hiszen d^* az f_1^* és f_2^* legnagyobb közös osztója. Végül $n \geq 2$-nél $[f_i | n \geq i \in \mathbb{N}^+] = \left[[f_i | n > i \in \mathbb{N}^+], f_n\right]$, így indukcióval minden $n \in \mathbb{N}^+$-ra igazoltuk a tétel legkisebb közös többszörösre vonatkozó részét.

□

5. Véges test feletti polinomok felbontása

Egy adott objektum felbontása kisebb összetevőkre, a dekompozíció, a faktorizáció abból a szempontból előnyös, hogy az egyszerűbb összetevők tulajdonságainak vizsgálata általában könnyebb, ugyanakkor ezen tulajdonságok ismeretében sok fontos információt ismerhetünk meg az eredeti, bonyolultabb objektumról. Test fölötti polinomok gyűrűt alkotnak, ahol a gyűrű euklideszi, tehát Gauss-gyűrű, és így az ilyen nem nulla polinomok lényegében véve egyértelműen írhatóak az adott test fölött felbonthatatlan polinomok szorzataként, ahol ezek a felbonthatatlan polinomok egyben prímek is a polinomgyűrűben. A felbontás ismeretében válaszolni tudunk különböző kérdésekre, például könnyedén meg tudjuk adni a polinom valamennyi osztóját. Az alábbiakban ismertetünk egy felbontási algoritmust, az úgynevezett **Berlekamp-algoritmus**t, azzal a megjegyzéssel, hogy léteznek más felbontási algoritmusok véges test feletti polinomokra, és léteznek a Berlekamp-algoritmusnak különböző módosításai is. A fejezetben az algoritmus lépései során előbukkanó kérdéseket többnyire a szükségesnél általánosabban vizsgáljuk.

Elsőként ismét emlékeztetünk néhány, a továbbiakban felhasznált tényre.

1. Ha $\mathcal{R}$ gyűrű, és $\mathcal{R}[x]$ az $\mathcal{R}$ fölötti x-határozatlanú polinomgyűrű, akkor $\mathcal{R}[x]$ tartalmaz egy, az $\mathcal{R}$-rel izomorf részgyűrűt, a konstans polinomok gyűrűjét. Ekkor $\mathcal{R}$ beágyazható a polinomgyűrűbe. A továbbiakban ennek megfelelően mindig feltesszük, hogy $\mathcal{R} \leq \mathcal{R}[x]$, ahol $\mathcal{R}$ elemei azonosak a megfelelő konstans polinomokkal.
2. $|R[x]| \geq |R| \geq 1$, és $|R[x]| = 1$ akkor és csak akkor, ha $|R| = 1$, vagyis ha $\mathcal{R}$ a nullgyűrű.
3. $\mathcal{R}[x]$ akkor és csak akkor kommutatív, ha $\mathcal{R}$ kommutatív, pontosan akkor nullosztómentes, ha $\mathcal{R}$ nullosztómentes (nullosztómentes gyűrűről feltesszük, hogy van legalább két eleme), így $\mathcal{R}[x]$ és $\mathcal{R}$ egyszerre integritási tartomány vagy nem integritási tartomány, és vagy mindkét gyűrű egységelemes, vagy egyik sem az, és ha egységelemes a két gyűrű, akkor az egységelemük azonos.
4. $\mathcal{R}[x]$ akkor és csak akkor Gauss-gyűrű, ha $\mathcal{R}$ Gauss-gyűrű (vagyis olyan egységelemes integritási tartomány, amelyben bármely nem nulla elem a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelműen írható véges sok, a gyűrűben irreducibilis elem szorzataként).
5. Ha $\mathcal{S}$ nullosztómentes gyűrű, és $\mathcal{R}$ az $\mathcal{S}$ legalább két elemet tartalmazó részgyűrűje, akkor a két gyűrű karakterisztikája azonos. Ebből következik, hogy ha $\mathcal{R}$ nullosztómentes, akkor $\mathcal{R}$ és $\mathcal{R}[x]$ karakterisztikája megegyezik.
6. Ha $\mathcal{R}$ integritási tartomány, $0 \neq u \in R$, $v \in R$ és $v|u$, akkor $v \neq 0$, és van olyan egyértelműen meghatározott $w \in R$, hogy $vw = u = wv$. Ekkor w sem a gyűrű nulleleme, és w-t a $w = \frac{u}{v}$ alakban írhatjuk.

Legyen $0 \neq f \in R[x]$, $\deg(f) = n \in \mathbb{N}^+$ és $f = \sum_{i=0}^{n} a_i x^i$. Ekkor $f' = \sum_{i=1}^{n} i a_i x^{i-1}$ legfeljebb $n-1$-edfokú, amint az az előbbi felírásból közvetlenül leolvasható. $\deg(f') < n-1$ csak akkor lehet, ha $na_n = 0$. Legyen $\mathcal{R}$ nullosztómentes, ekkor, tekintettel arra, hogy $a_n \neq 0$, $na_n = 0$ akkor és csak akkor teljesül, ha n osztható a gyűrű karakterisztikájával. Mivel n pozitív egész szám, ezért nem lehet osztható 0-val, tehát 0-karakterisztikájú gyűrű feletti pozitív fokszámú polinom deriváltjának foka pontosan eggyel kisebb, mint az eredeti polinom foka, és hasonló a helyzet, ha a prímkarakterisztikájú gyűrű karakterisztikája nem osztója a polinom fokának. Most legyen $\mathrm{char}(\mathcal{R}) = p \in \mathbb{N}^+$ és $p|n$, vagyis legyen $n = pm$, ahol m is pozitív egész. Ekkor $\delta(f) < n-1$, és akár $f' = 0$ is lehetséges. Legyen f olyan, hogy $f' = 0$. Ez csak úgy lehetséges, ha f minden olyan tagjának együtthatója 0, amelynek a foka nem osztható p-vel, vagyis ekkor $f = \sum_{k=0}^{m} a_{kp} x^{kp} = \sum_{k=0}^{m} b_k (x^p)^k = g \circ x^p$, ahol $b_k = a_{kp}$ és $g = \sum_{k=0}^{m} b_k x^k \in R[x]$. Ha minden $m \geq k \in \mathbb{N}$-re létezik olyan $c_k \in R$, hogy $c_k^p = b_k$, akkor $f = \sum_{k=0}^{m} b_k x^{kp} = \sum_{k=0}^{m} c_k^p (x^k)^p = \left(\sum_{k=0}^{m} c_k x^k\right)^p = h^p$ egy $h = \sum_{k=0}^{m} c_k x^k \in R[x]$ polnommal. Amennyiben R véges, vagyis $\mathcal{R}$ véges és nullosztómentes gyűrű (azaz $\mathcal{R}$ véges test), akkor az $u \mapsto u^p$ leképezés automorfizmus $\mathcal{R}$-en, tehát bijektív, és így minden R-beli elemnek van egy és csak egy p-edik gyöke magában R-ben. Ekkor $f' = 0$ esetén $f = h^p$, és ez fordítva is igaz, hiszen, ha f egy h polinom

p-edik hatványa, ahol a nem nulla p a gyűrű karakterisztikája, akkor $f' = ph^{p-1}h' = 0$. Általánosabban is, ha $f = g \circ x^p$, akkor $f' = (g' \circ x^p)px^{p-1} = 0$.

Megmutatjuk, hogy van olyan p prímkarakterisztikájú nullosztómentes gyűrű, ahol nem minden elemnek van p-edik gyöke. Legyen $\mathcal{K}$ tetszőleges p-karakterisztikájú test, és Θ egy, a $\mathcal{K}$ fölött transzcendens elem (vagyis olyan elem, amelyik egyetlen nem nulla, $\mathcal{K}$ feletti polinomnak sem gyöke; ilyen van, például $x \in K[x]$). Ekkor Θ^p is transzcendens $\mathcal{K}$ fölött. Ha ugyanis Θ^p gyöke egy $f \in K[x]$ polinomnak, akkor Θ gyöke a szintén $\mathcal{K}$ feletti $f \circ x^p$ polinomnak, és így f csupán a nullpolinom lehet. $K(\Theta^p) = \left\{\frac{\hat{f}(\Theta^p)}{\hat{g}(\Theta^p)} \middle| f \in K[x] \wedge 0 \neq g \in K[x]\right\}$, hiszen $K(\Theta^p)$ a $\mathcal{K}$ bővítése, tehát tartalmaznia kell K-t és tartalmaznia kell Θ^p-t, de akkor Θ^p minden nemnegatív egész kitevős hatványát, ezek K-beli elemmel való szorzatát és az ilyen szorzatok véges összegeit, vagyis Θ^p $\mathcal{K}$ feletti polinomjait. $\hat{f}(\Theta^p)$ akkor és csak akkor 0, ha maga az f polinom 0 (mert Θ^p transzcendens $\mathcal{K}$ fölött), és mivel $\mathcal{K}(\Theta^p)$ test, ezért $\frac{\hat{f}(\Theta^p)}{\hat{g}(\Theta^p)}$ is benne kell, hogy legyen, ha $g \neq 0$. Még azt kell belátni, hogy a polinom-műveletekkel $\left\{\frac{\hat{f}(\Theta^p)}{\hat{g}(\Theta^p)} \middle| f \in K[x] \wedge 0 \neq g \in K[x]\right\}$ test, vagyis nem üres, zárt a kivonásra, valamint a nem nulla elemekkel való osztásra. $0 = \frac{\hat{0}(\Theta^p)}{\hat{e}(\Theta^p)}$, a megadott halmaz nem üres. Legyen $\frac{\hat{f}_1(\Theta^p)}{\hat{g}_1(\Theta^p)}$ és $\frac{\hat{f}_2(\Theta^p)}{\hat{g}_2(\Theta^p)}$ a halmaz két eleme. Ekkor

$$\frac{\hat{f}_1(\Theta^p)}{\hat{g}_1(\Theta^p)} - \frac{\hat{f}_2(\Theta^p)}{\hat{g}_2(\Theta^p)} = \frac{\hat{f}_1(\Theta^p)\hat{g}_2(\Theta^p) - \hat{f}_2(\Theta^p)\hat{g}_1(\Theta^p)}{\hat{g}_1(\Theta^p)\hat{g}_2(\Theta^p)} = \frac{\hat{f}(\Theta^p)}{\hat{g}(\Theta^p)}$$

ahol $f = f_1g_2 - f_2g_1$ és $g = g_1g_2$. $g_1 \neq 0 \neq g_2$, ezért $g \neq 0$, így $\frac{\hat{f}(\Theta^p)}{\hat{g}(\Theta^p)} \in K(\Theta^p)$. Amennyiben $f_2 \neq 0$, akkor $\frac{\hat{f}_2(\Theta^p)}{\hat{g}_2(\Theta^p)} \neq 0$, és ekkor

$$\frac{\hat{f}_1(\Theta^p)}{\hat{g}_1(\Theta^p)}\left(\frac{\hat{f}_2(\Theta^p)}{\hat{g}_2(\Theta^p)}\right)^{-1} = \frac{\hat{f}_1(\Theta^p)}{\hat{g}_1(\Theta^p)}\frac{\hat{g}_2(\Theta^p)}{\hat{f}_2(\Theta^p)} = \frac{\widehat{f_1g_2}(\Theta^p)}{\widehat{g_1f_2}(\Theta^p)} = \frac{\hat{u}(\Theta^p)}{\hat{v}(\Theta^p)}$$

az $u = f_1g_2$ és $v = f_2g_1$ jelöléssel, és most ismét nem nulla a nevező, mert $f_2 \neq 0$. Ha a k egész számnak nem osztója p, akkor $\Theta^k \notin K(\Theta^p)$ Ezt elegendő pozitív kitevővel belátni, mert $\Theta^k \neq 0$, így Θ^k akkor és csak akkor eleme a testnek, ha Θ^{-k} benne van a testben. Tegyük ugyanis fel az állítás ellenkezőjét. Ekkor $\Theta^k = \frac{\hat{f}(\Theta^p)}{\hat{g}(\Theta^p)}$ egy $\mathcal{K}$ feletti f és nem nulla g polinommal, vagyis Θ gyöke a $h = f \circ x^p - x^k(g \circ x^p) \in K[x]$ polinomnak. De Θ $\mathcal{K}$ fölött transzcendens, így h csak a nullpolinom lehet. g nem a nullpolinom, így legalább egy együtthatója nem nulla. $x^k(g \circ x^p)$-ben csak olyan együttható lehet nullától különböző – és ilyen van –, amelynek az indexe kongruens k-val modulo p, vagyis ha l egy ilyen index, akkor $l \equiv k \not\equiv 0\ (p)$. Ugyanakkor $f \circ x^p$-ben csak a p-vel osztható kitevőhöz tartozó együtthatók lehetnek nullától különbözőek, tehát ha $x^k(g \circ x^p)$ i-edfokú tagjának együtthatója v_i, $f \circ x^p$-ben az i-edfokú tag együtthatója u_i, végül w_i a h i-indexű tagjának együtthatója, akkor $u_l = 0$ és $v_l \neq 0$, tehát $w_l = u_l - v_l = 0 - v_l = -v_l \neq 0$, ami nem lehet, mert $h = 0$. Az nyilvánvaló, hogy $\Theta^p \in K(\Theta)$, így $\mathcal{K}(\Theta)|\mathcal{K}(\Theta^p)$, és mivel az előbbiek szerint $\Theta \notin K(\Theta^p)$, $\mathcal{K}(\Theta^p)$ valódi részteste $\mathcal{K}(\Theta)$-nak. $\mathcal{K}(\Theta)$-n a $\varphi: u \mapsto u^p$ leképezés injektív homomorfizmus, és $\mathrm{Im}(\varphi)$ része $K(\Theta^p)$-nek, mert $\varphi(K) \subseteq K$ és Θ képe Θ^p, és a művelettartás következtében $\frac{\hat{f}(\Theta)}{\hat{g}(\Theta)}$ képe $\frac{\hat{f}_1(\Theta^p)}{\hat{g}_1(\Theta^p)} \in K(\Theta^p)$ egy f_1 és $g_1 \neq 0$ $\mathcal{K}$ feletti polinommal. Mivel a leképezés injektív, ezért egyetlen olyan elem van a bővebb testben, amelynek a képe Θ^p, és ez Θ, ám ez nincs benne $K(\Theta^p)$-ben, így Θ^p-nek nincs p-edik gyöke $K(\Theta^p)$-ben.

Az előbbiek szerint $\mathcal{K}(\Theta^p)$ valódi részteste $\mathcal{K}(\Theta)$-nak, és $\varphi: u \mapsto u^p$ bijektíven és művelettartóan képezi le $\mathcal{K}(\Theta)$-t $\mathcal{K}^{(1)}(\Theta^p)$-re, ahol $K^{(1)} = \varphi(K)$, vagyis $\mathcal{K}^{(1)}(\Theta^p)$ izomorf $\mathcal{K}(\Theta)$ egy valódi résztestével, tehát $\mathcal{K}(\Theta)$ izomorf önmagának egy valódi résztestével. Indukcióval innen azt kapjuk, hogy minden nemnegatív egész i-re $\mathcal{K}^{(i+1)}\left(\Theta^{p^{i+1}}\right) \neq \mathcal{K}^{(i)}\left(\Theta^{p^i}\right) \middle| \mathcal{K}^{(i+1)}\left(\Theta^{p^{i+1}}\right)$, ahol $K^{(0)} = K$ és $K^{(i+1)} = \varphi\left(K^{(i)}\right)$, és van $\mathcal{K}^{(i)}\left(\Theta^{p^i}\right)$-nek olyan valódi részteste, például $\mathcal{K}^{(i+1)}\left(\Theta^{p^{i+1}}\right)$, amely izomorf $\mathcal{K}^{(i)}\left(\Theta^{p^i}\right)$-vel, és akkor $\mathcal{K}(\Theta)$ egy valódi résztestével.

A most tárgyalt bővítéssel kapcsolatban még egy dolgot mutatunk, amely eltér az eddigiektől. A rövidség kedvéért vezessük be az $\mathcal{L} = \mathcal{K}(\Theta^p)$ jelölést. Θ gyöke a $0 \neq (x - \Theta)^p = x^p - \Theta^p \in L[x]$ polinomnak, amint az közvetlen behelyettesítéssel látható, így Θ algebrai $\mathcal{L}$ fölött, és az $\mathcal{L}$ fölötti minimál-polinomja osztója $x^p - \Theta^p$-nek, vagyis $m_\Theta^{(L)} = (x - \Theta)^r$ egy $p \geq r \in \mathbb{N}^+$ kitevővel. De $(x - \Theta)^r$ konstans tagja Θ^r vagy $-\Theta^r$, és ez a fentebbi eredményeink szerint csak akkor lehet benne az $\mathcal{L}$ testben, ha r osztható p-vel, ami csak úgy lehet, ha $r = p$, hiszen r a p-nél nem nagyobb pozitív egész. Ez azt jelenti, hogy az $\mathcal{L}$ test fölött irreducibilis, L-beli együtthatós $x^p - \Theta^p$

polinom gyökei p-szeresek, vagyis nem egyszeresek, szemben a nulla-karakterisztikájú, valamint a véges testekkel, ahol irreducibilis polinom minden gyöke egyszeres.

Visszatérve a polinom deriváltjához, legyen $f_0 = f$, valamilyen $k \in \mathbb{N}$-re és minden $k > i \in \mathbb{N}$-re $f_i' = 0$, $f_i = g_i \circ x^p$ és $f_{i+1} = g_i$, végül $f_k' \neq 0$. Ilyen k biztosan létezik, hiszen ha $\deg(f_i) = n_i$ a k-nál kisebb i indexre, akkor f_{i+1} foka $n_{i+1} = \frac{n_i}{p}$, és ez pozitív egész, mivel $n_0 = n > 0$. Legyen $p^r \parallel n$ (vagyis $p^r | n$, de $p^{r+1} \nmid n$), ekkor $k \leq r$, és ha $k < r$, akkor $\deg(f_k') < n_k - 1$, mert ekkor még $p | n_k$. Indukcióval könnyen belátható, hogy $f = f_0 = f_k \circ x^{p^k}$, és ha f_k minden együtthatójának van $\mathcal{R}$-ben p^k-adik gyöke (és véges R esetén ez igaz), akkor $f = g^{p^k}$ egy $\mathcal{R}$ fölötti g polinommal.

Ha a véges test feletti f polinomot faktorizáljuk, akkor elegendő az előbb g-vel jelölt polinomot felbontani, és minden faktornak a felbontásban szereplő kitevőjét szorozni p^k-val, így a továbbiakban feltesszük, hogy f deriváltja nem nulla. Ismét általánosabban kezdjük a vizsgálatot, azaz feltesszük, hogy f egy p-karakterisztikájú $\mathcal{R}$ Gauss-gyűrű feletti polinom. Legyen $f = g^t h$, ahol g irreducibilis a gyűrű fölött, t pozitív egész szám, és g nem osztója h-nak (és ekkor relatív prím h-hoz, hiszen g irreducibilis). f deriváltja $f' = g^{t-1}(tg'h + gh')$, ahonnan látjuk, hogy g legalább a $t-1$-edik hatványon van f'-ben. $g' \neq 0$, mert ellenkező esetben $g = g_1^p$, ahol g_1 legalább elsőfokú és $p > 1$, ám ekkor g felbontható. Ha $tg' \neq 0$, akkor tehát $p \nmid t$. g' foka kisebb g fokánál, ezért nem lehet osztható g-vel, és h sem többszöröse g-nek, így $g'h$ nem osztható g-vel, hiszen g irreducibilis, tehát prím a gyűrű fölött. Ekkor $tg'h$ sem osztható g-vel, ugyanis $p \nmid t$ -ből t és p relatív prímek (mert p prímszám), így alkalmas r és s egészekkel $1 = rt + sp$, majd $g'h = 1(g'h) = (rt + sp)g'h = r(tg'h)$. Ebben az esetben tehát pontosan $t-1$ a g kitevője f'-ben, mert a kéttagú $tg'h + gh'$-ben az egyik tag osztható g-vel, míg a másik tag nem. A másik esetben $tg' = 0$ (azaz p osztója t-nek), és $f' = g^t h'$, vagyis f'-ben g legalább a t-edik hatványon van (attól, hogy h nem osztható g-vel, még lehetséges, hogy a deriváltja többszöröse g-nek). Azt kaptuk tehát, hogy f'-ben g kitevője legalább $t-1$. Legyen d az f és f' legnagyobb közös osztója. f' nem nulla, és ekkor a foka kisebb, mint f foka, tehát d sem a nullpolinom, és alacsonyabb fokú, mint f. Mivel g az f polinomban a t-edik, míg a deriváltban legalább a $t-1$-edik hatványon áll, ezért d-ben g t-szer vagy $t-1$-szer fordul elő, és innen $\frac{f}{d}$-ben vagy nem szerepel g (akkor és csak akkor, ha $tg' = 0$), vagy pontosan egyszeres tényezője a hányadosnak, ennél fogva $\frac{f}{d}$ négyzetmentes. $f = \frac{f}{d} d$, így elegendő külön $\frac{f}{d}$-t és, ha nem konstans, akkor d-t faktorizálni. d faktorizálása azonos az eredeti f polinom felbontásával (azaz addig deriválunk, mígnem a derivált már nem a nullpolinom, stb.), és mivel d foka kisebb, mint f foka, ezért, ha $\frac{f}{d}$-t véges sok lépésben sikerül felbontanunk, akkor f-et is fel tudjuk bontani véges sok lépésben. A továbbiakban tehát olyan polinom felbontásával foglalkozunk, amelynek nincs többszörös faktora, vagyis amelyik négyzetmentes.

Legyen a q-elemű test fölötti, pozitív n fokszámú, négyzetmentes f főpolinom $\mathbb{F}_q$ fölötti felbontása $f = \prod_{i=1}^{k} g_i$, ahol k pozitív egész szám, és a g_i-k páronként különböző, $\mathbb{F}_q[x]$-ben irreducibilis főpolinomok (feltehetjük mind f-ről, mind a faktorairól, hogy főpolinomok, mert nem nulla konstans szorzó egység egy test fölötti polinomgyűrűben). Egyelőre sem k-t, sem a g_i-ket nem ismerjük, sőt, éppen az a célunk, hogy ezeket meghatározzuk. A felbontáshoz keresünk egy olyan, n-nél alacsonyabb fokú, nem konstans $h \in \mathbb{F}_q[x]$ polinomot, amelyre $h^q - h$ osztható f-fel, és minden $c \in \mathbb{F}_q$-ra meghatározzuk f és $h - c$ legnagyobb közös osztóját. Minden legalább elsőfokú legnagyobb közös osztó az f (nem feltétlenül irreducibilis) faktora. Ha a különböző ilyen faktorok száma k, akkor megkaptuk f irreducibilis faktorokra való felbontását. Ellenkező esetben választunk egy új h polinomot, és valamennyi előbbi faktorral ismét meghatározzuk az összes legnagyobb közös osztót minden $h - c$ polinommal, és így tovább. Megmutatjuk, hogy az eljárás véges sok lépés után befejeződik. Most még az sem világos, hogy egyáltalán létezik-e a feltételnek megfelelő h polinom, ha igen, akkor találunk-e az esetleges további fordulókban újabb polinomokat, ha a faktorok száma k, akkor megállhatunk-e, és egyáltalán, tudjuk-e, hogy mikor lehet leállni, hiszen ehhez ismerni kell az irreducibilis faktorok számát. A továbbiakban megmutatjuk, hogy mindegyik kérdésre megnyugtató választ tudunk adni.

Ha egy kommutatív gyűrű u és v elemének különbsége osztható a gyűrű w elemével, akkor azt is fogjuk írni, hogy $u \equiv v\ (w)$, és ilyenkor azt is mondjuk, hogy u **kongruens** v**-vel** modulo w. A kongruenciák összeadhatóak és szorozhatóak, és akkor hatványozhatóak is. Valóban, legyen $\mathcal{R}$ kommutatív gyűrű, $w \in R$, $n \in \mathbb{N}$ és $n > i \in \mathbb{N}$-re $u_i \in R$, $v_i \in R$ úgy, hogy $u_i \equiv v_i\ (w)$. Ekkor minden megadott i indexre $w|u_i - v_i$, és $\sum_{i=0}^{n-1} u_i - \sum_{i=0}^{n-1} v_i = \sum_{i=0}^{n-1}(u_i - v_i)$, így $\sum_{i=0}^{n-1} u_i - \sum_{i=0}^{n-1} v_i$ is többszöröse w-nek, tehát $\sum_{i=0}^{n-1} u_i \equiv \sum_{i=0}^{n-1} v_i\ (w)$. A szorzásnak a kongruenciával való kompatibilitását indukcióval látjuk be. $\prod_{i=0}^{-1} u_i = e \equiv e = \prod_{i=0}^{-1} v_i\ (w)$, $n = 0$-ra tehát igaz az állítás. Most tegyük fel, hogy $\prod_{i=0}^{n-1} u_i \equiv \prod_{i=0}^{n-1} v_i\ (w)$, és legyen u_n, v_n az R-nek a w modulus szerint kongruens két eleme. Ekkor $\prod_{i=0}^{n} u_i = \left(\prod_{i=0}^{n-1} u_i\right)u_n = uu_n$ az $u = \prod_{i=0}^{n-1} u_i$ jelöléssel, és hasonlóan, $\prod_{i=0}^{n} v_i = vv_n$, ahol $v = \prod_{i=0}^{n-1} v_i$. De $uu_n - vv_n = u(u_n - v_n) + (u - v)v_n$, és mindkét zárójeles tényező, de akkor a teljes kifejezés is osztható w-vel, azaz $\prod_{i=0}^{n} u_i = uu_n \equiv vv_n = \prod_{i=0}^{n} v_i\ (w)$, vagyis $n + 1$, ugyanazon modulus szerint páronként kongruens elem szorzata is kongruens a változatlan modulussal.

1. Legyen $\mathcal{R}$ kommutatív gyűrű, $\bigcup_{\gamma\in\Gamma} A_\gamma = A \subseteq R$, ahol Γ és az A_γ halmazok egyike sem üres, és tegyük fel, hogy minden A_γ halmaznak létezik d_γ legnagyobb közös osztója. Ilyen feltételekkel A-nak akkor és csak akkor létezik legnagyobb közös osztója, ha a részhalmazok legnagyobb közös osztóinak létezik a legnagyobb közös osztója, és ha létezik, akkor a két legnagyobb közös osztó – asszociáltságtól eltekintve – azonos. Legyen ugyanis az A elemeinek legnagyobb közös osztója d. d osztója A minden elemének, de akkor valamennyi γ-ra A_γ minden elemének, tehát minden γ -ra d_γ-nak, vagyis d közös osztója a d_γ legnagyobb közös osztóknak. Ha u is közös osztója a d_γ-knak, akkor u osztója minden A_γ összes elemének, és így az A mindegyik elemének, tehát osztója d-nek, amiből következik, hogy d legnagyobb közös osztója a részhalmazok legnagyobb közös osztóinak. Fordítva, tegyük fel, hogy létezik a d_γ-k legnagyobb közös osztója, és ez d. d az A minden elemének osztója, tehát közös osztója az A elemeinek. Legyen most u közös osztója az A-beli elemeknek. Ekkor u minden részhalmaz valamennyi elemének, tehát minden részhalmaz legnagyobb közös osztójának osztója, és akkor d-nek is, így d az A elemeinek legnagyobb közös osztója.

Legyen $\bigcup_{\gamma\in\Gamma} A_\gamma = U = \bigcup_{\delta\in\Delta} B_\delta$, ahol $\emptyset \neq U \subseteq R$, valamennyi részhalmaz tartalmaz legalább egy elemet, és minden részhalmaznak létezik a legnagyobb közös osztója. Ekkor vagy mind az A_γ-k, mind a B_δ-k legnagyobb közös osztóinak létezik legnagyobb közös osztója, vagy egyik sem létezik. Az előbbi esetben ez a két legnagyobb közös osztó – egy esetleges egységszorzótól eltekintve – azonos, hiszen mindkét legnagyobb közös osztó létezésének szükséges és elégséges feltétele, hogy U elemeinek létezzen a legnagyobb közös osztója, és ha ez létezik, akkor mindkét oldalon a részhalmazok legnagyobb közös osztóinak legnagyobb közös osztója lényegében véve – vagyis asszociáltságtól eltekintve – U legnagyobb közös osztójával azonos.

Az előbbi tulajdonság a legkisebb közös többszörösökre is igaz, hiszen csak mindenütt meg kell fordítani az oszthatóság irányát, és osztó helyett többszöröst kell írni.

Ha akár Γ, akár a Γ minden γ elemére A_γ üres, akkor $A \subseteq R$ is az üres halmaz. Az üres halmaz közös osztója és közös többszöröse a gyűrű valamennyi eleme. Mivel így a gyűrű nulleleme is közös osztó, és ennek egy és csak egy többszöröse van, önmaga, ezért az üres halmaznak mindig létezik a legnagyobb közös osztója, és ez a 0, ami egyben a teljes gyűrű legkisebb közös többszöröse is. Hasonlóan, az üres halmaz legkisebb közös többszöröse egyben a teljes gyűrű legnagyobb közös osztója, feltéve, hogy ez létezik. Ám olyan elem, amely a gyűrű minden elemét osztja, asszociáltaktól eltekintve az egységelem és csak az egységelem, tehát pontosan akkor van legkisebb közös többszöröse az üres halmaznak és legnagyobb közös osztója a teljes gyűrűnek, ha a gyűrű egységelemes, és ekkor ez a legkisebb közös többszörös illetve legnagyobb közös osztó az egységelem (illetve az asszociáltjai, az egységek).

Speciális esetként legyen v a kommutatív, egységelemes $\mathcal{R}$ gyűrű egy eleme, Γ nem üres indexhalmaz, és minden $\gamma \in \Gamma$-ra $u_\gamma \in R$. Ha a gyűrű egységelemes, akkor minden egyelemű halmaznak van legnagyobb közös osztója, a halmaz eleme, és $\big((u_\gamma, v)\big|\gamma \in \Gamma\big) = \Big(\big(u_\gamma\big|\gamma \in \Gamma\big), v\Big)$. Ha tehát az $\{u_\gamma|\gamma \in \Gamma\}$ halmaz valamely részhalmaza relatív prím, akkor az $\{(u_\gamma, v)|\gamma \in \Gamma\}$ halmaz megfelelő részhalmaza is relatív prím, és ekkor $\big((u_\gamma, v)\big|\gamma \in \Gamma\big) = e = \Big(\big(u_\gamma\big|\gamma \in \Gamma\big), v\Big)$. Ha tehát az u_γ-k között akár csak kettő (nem feltétlenül különböző) is relatív prím, akkor az $\big(u_\gamma, v\big)$ legnagyobb közös osztó(k) is

relatív prím(ek), és ha az u_γ-k páronként relatív prímek, akkor hasonló igaz az (u_γ, v) legnagyobb közös osztókra.

2. Gauss-gyűrű bármely részhalmazának létezik, és asszociáltságtól eltekintve egyértelmű a legnagyobb közös osztója és legkisebb közös többszöröse. Legyen $\mathcal{R}$ Gauss-gyűrű, Γ egy indexhalmaz, minden $\gamma \in \Gamma$-ra A_γ az R részhalmaza, $\Delta = \prod_{\gamma\in\Gamma} A_\gamma$, és minden $\delta \in \Delta$-ra $B_\delta = \mathrm{Im}(\delta)$. Megmutatjuk, hogy ekkor az A_γ-k legnagyobb közös osztói halmazának legkisebb közös többszöröse megegyezik a B_δ-k legkisebb közös többszöröseinek legnagyobb közös osztójával, és fordítva, az A_γ-k legkisebb közös többszöröseinek legnagyobb közös osztója azonos a B_δ-k legnagyobb közös osztóinak legkisebb közös többszörösével.

$\Delta = \prod_{\gamma\in\Gamma} A_\gamma$ az A_γ halmazok kiválasztási függvényeinek, azaz a Γ-t az $A = \bigcup_{\gamma\in\Gamma} A_\gamma$ -t tartalmazó tetszőleges halmazba képező olyan δ függvényeknek a halmaza, ahol minden $\gamma \in \Gamma$-ra $\delta(\gamma) \in A_\gamma$. Ha az A_γ halmazok legalább egyike az üres halmaz, akkor Δ is az üres halmaz, hiszen ha az A_γ-k között van üres halmaz, mondjuk $A_{\gamma^*} = \emptyset$, akkor Γ nem az üres halmaz, de ekkor γ^*-hoz nem tudunk hozzárendelni egyetlen elemet sem, így nincs kiválasztási függvény. Véges indexhalmaz esetén minden indexhez ki tudunk választani a hozzá tartozó nem üres halmazból egy elemet, de végtelen sok halmazból ez csak a kiválasztási axiómából következik, amely szerint nem üres halmazok tetszőleges rendszerének van kiválasztási függvénye. Ez azt jelenti, hogy a direkt szorzat akkor és csak akkor az üres halmaz, ha a szorzat legalább egy tényezője az üres halmaz. Most kérdés, hogy mi a helyzet, ha az indexhalmaz üres. Az üres halmazt bármely halmazba le tudjuk képezni, és tetszőleges halmaz esetén pontosan egy ilyen függvény van, az üres függvény, amelynek a képe is az üres halmaz, vagyis az üres halmaz elemeivel indexelt bármely halmazrendszer direkt szorzatának egy és csak egy eleme van, az üres függvény.

Először legyen $d_\gamma = (A_\gamma) = \mathrm{lnko} A_\gamma$, $D = \{d_\gamma | \gamma \in \Gamma\}$, $t = [D] = \mathrm{lkkt} D$, $t_\delta = [B_\delta] = \mathrm{lkkt} B_\delta$, $T = \{t_\delta | \delta \in \Delta\}$ és $d = (T) = \mathrm{lnko} T$. Belátjuk, hogy $t = d$.

Az előbbi eredményeket alkalmazva $\Gamma = \emptyset$ esetén $D = \emptyset$ és $T = \{\mathrm{lkkt}\emptyset\}$. Egyetlen elemet tartalmazó halmaz legnagyobb közös osztója a halmaz egyetlen eleme, így ez esetben $t = \mathrm{lkkt} D = \mathrm{lnko} T = d$. A másik speciális esetben, amikor a részhalmazok között előfordul az üres halmaz, akkor D-nek eleme az üres halmaz legnagyobb közös osztója, 0, így D legkisebb közös többszöröse, $t = 0$. Most $T = \emptyset$, és ennek a legnagyobb közös osztója 0, ismét teljesül a $t = d$ egyenlőség. Maradt az az eset, amikor az indexhalmaz nem üres, és valamennyi indexelt halmaznak van legalább egy eleme. Legyen γ a Γ és δ a Δ tetszőleges eleme. B_δ-nak van (egy és csak egy) A_γ-beli eleme. Ha ez a_γ, akkor $d_\gamma | a_\gamma | t_\delta$, vagyis minden d_γ osztója valamennyi t_δ-nak. Ez azt jelenti, hogy mindenegyes t_δ közös többszöröse D-nek, így többszöröse t-nek. Ez viszont azt jelenti, hogy t közös osztója T-nek, tehát osztója d-nek. De teljesül a fordított irányú oszthatóság is. Legyen ugyanis p a gyűrű olyan prímeleme, amelynek az l-edik hatványa osztója d-nek, ahol l pozitív egész szám. p^l mint d osztója osztója a T minden elemének. Ekkor van olyan $\gamma \in \Gamma$, hogy p^l közös osztója egy A_γ-nak. Ellenkező esetben ugyanis minden A_γ-ban lenne olyan elem, amely nem osztható ezzel a p-hatvánnyal. Ám ekkor annak a B_δ-nak, amelynek az elemei az előbbi elemek, egyetlen eleme sem osztható p^l-lel, innen a legkisebb közös többszöröse, és akkor a legkisebb közös többszörösök legnagyobb közös osztója, d sem osztható p^l-lel, ami ellent mond annak, hogy p^l osztja d-t. p^l tehát osztója D legalább egy elemének, így a D legkisebb közös többszörösének, t-nek. Ez viszont azt jelenti, hogy a d minden osztója t-nek is osztója, amiből következik, hogy d osztója t-nek, és mivel ez fordítva is igaz, ezért asszociáltaktól eltekintve $t = d$.

Az előbbi eredmények fordítva is igazak. Legyen most $t_\gamma = [A_\gamma] = \mathrm{lkkt} A_\gamma$, $T = \{t_\gamma | \gamma \in \Gamma\}$, $d = (T) = \mathrm{lnko} T$, $d_\delta = (B_\delta) = \mathrm{lnko} B_\delta$, $D = \{d_\delta | \delta \in \Delta\}$ és $t = [D] = \mathrm{lkkt} D$. Ekkor is teljesül a $t = d$ egyenlőség, amit ismét igazolunk.

$\Gamma = \emptyset$ esetén $T = \emptyset$ és $D = \{\mathrm{lnko}\emptyset\}$. Egyetlen elemet tartalmazó halmaz legkisebb közös többszöröse a halmaz egyetlen eleme, így ez esetben $d = \mathrm{lnko} T = \mathrm{lkkt} D = t$. A másik speciális esetben, amikor a részhalmazok között előfordul az üres halmaz, akkor T-nek eleme az üres halmaz legkisebb közös többszöröse, e, így T legnagyobb közös osztója $d = e$. Most $D = \emptyset$, és ennek a legkisebb közös többszöröse e, ismét teljesül a $t = d$ egyenlőség. Most legyen az indexhalmaz nem üres, és valamennyi indexelt halmaznak legyen legalább egy eleme. Legyen γ a Γ és δ a Δ tetszőleges eleme. A_γ-nak (egy és csak egy) eleme benne van B_δ-ban. Ha ez a_γ, akkor $d_\delta | a_\gamma | t_\gamma$, vagyis minden t_γ többszöröse valamennyi d_δ-nak. Ez azt jelenti, hogy mindenegyes d_δ közös osztója T-nek, így osztója d-nek. Ez viszont azt jelenti, hogy d közös többszöröse D-nek, tehát többszöröse t-nek. De t is többszöröse d-nek. Legyen ugyanis a pozitív egész kitevős p^l prímhatvány a d egy osztója. Ekkor osztója minden t_γ-nak, és így

minden A_γ legalább egy a_γ elemének. Ha most valamely B_δ minden eleme egy-egy ilyen a_γ, akkor p^l közös osztója ennek a B_δ-nak, így osztója ezen d_δ-nak, és ebből következően t-nek is, amiből már következik, hogy d osztója t-nek, t többszöröse d-nek.

A fentiek alapján $\left[\left(a_\gamma|\gamma\in\Gamma\right),b\right]=\left(\left[a_\gamma,b\right]|\gamma\in\Gamma\right)$ és $\left(\left[a_\gamma|\gamma\in\Gamma\right],b\right)=\left[\left(a_\gamma,b\right)|\gamma\in\Gamma\right]$, továbbá ha b osztója $\left[a_\gamma|\gamma\in\Gamma\right]$-nak, akkor $\left[\left(a_\gamma,b\right)|\gamma\in\Gamma\right]=b$. Gauss-gyűrűben páronként relatív prím elemek legkisebb közös többszöröse a szorzatuk, így, ha az a_γ-k páronként relatív prímek, akkor az előző pont alapján az $\left(a_\gamma,b\right)$-k is páronként relatív prímek, tehát $\prod_{\gamma\in\Gamma}\left(a_\gamma,b\right)=\left(\prod_{\gamma\in\Gamma}a_\gamma,b\right)$, és ha még az is teljesül, hogy $b\left|\prod_{\gamma\in\Gamma}a_\gamma\right.$, akkor $\prod_{\gamma\in\Gamma}\left(a_\gamma,b\right)=b$.

3. Legyen $\mathcal{R}$ főideálgyűrű, $n\in\mathbb{N}^+$, és $n\geq i\in\mathbb{N}^+$-ra $u_i\in R$ és $v_i\in R$ úgy, hogy a v_i-k páronként relatív prímek. Ekkor van R-nek olyan u eleme, hogy minden $n\geq i\in\mathbb{N}^+$ indexre $u\equiv u_i\ (v_i)$. Legyen ugyanis $v=\prod_{i=1}^n v_i$ és $V_i=\frac{v}{v_i}$. Az előző pont szerint $(V_i,v_i)=e$, míg a felírásból közvetlenül leolvasható, hogy ha $k\neq i$, akkor $v_k|V_i$. Tekintsük minden i-re a $V_ix\equiv e\ (v_i)$ kongruenciát. Ennek van megoldása, mert főideálgyűrűben a legnagyobb közös osztó felírható lineáris kombinációként, vagyis van a gyűrűben olyan r_i és s_i, amellyel $e=V_ir_i+v_is_i\equiv V_ir_i\ (v_i)$. Ekkor $u=\sum_{i=1}^n u_iV_ir_i$-ben a k-indexű kivételével minden tag osztható v_k-val, míg $u_kV_kr_k\equiv u_ke=u_k\ (v_k)$, és így $u\equiv u_k\ (v_k)$. Ha u' is a kongruencia-rendszer megoldása, akkor $u-u'\equiv 0\ (v_i)$ minden i-re, így minden v_i osztója $u-u'$-nek, tehát $u\equiv u'\ (v)$, mert v a v_k-k legkisebb közös többszöröse, hiszen páronként relatív prímek.

Egy kongruencia-rendszer nem feltétlenül oldható meg bármely Gauss-gyűrűben. Tekintsük például $\mathbb{Z}[x]$-et. $\mathbb{Z}$ Gauss-gyűrű, ezért Gauss-gyűrű $\mathbb{Z}[x]$ is. Ebben a gyűrűben felbonthatatlan, tehát prím a 2 és az x polinom, így relatív prímek is, hiszen nem asszociáltak. Ekkor nincs olyan $f\in\mathbb{Z}[x]$, amely 2-vel osztva 1-et, míg x-szel osztva 0-t adna maradékul, hiszen az előbbi feltételből a konstans tagja páratlan lenne, míg a másik feltételből következően a konstans tagja 0 kellene, hogy legyen.

4. Legyen $\mathcal{R}$ euklideszi gyűrű a φ normával. Ha bármely $v\in R$ és $0\neq u\in R$ elempárhoz egyetlen olyan $q\in R$, $r\in R$ létezik, amellyel $v=qu+r$, ahol $r=0$, vagy $r\neq 0$ és $\varphi(r)<\varphi(u)$ (ilyen például test fölötti egyhatározatlanú polinomgyűrű), akkor legyen $v\bmod u=r$. Könnyen belátható, hogy $(v\bmod u)\bmod u=v\bmod u$, továbbá $u|v-(v\bmod u)$, tehát $v\bmod u\equiv v\ (u)$. Azt is könnyű látni, hogy $v_1\equiv v_2\ (u)$ pontosan akkor igaz, ha $v_1\bmod u=v_2\bmod u$. Ha most a pozitív egész n-re és $n>i\in\mathbb{N}$-re $v_i\in R$, akkor $v_i\bmod u\equiv v_i\ (u)$-ból $\sum_{i=0}^{n-1}(v_i\bmod u)\equiv\sum_{i=0}^{n-1}v_i\ (u)$, és akkor, az előbbi eredmény alapján, $\sum_{i=0}^{n-1}(v_i\bmod u)\bmod u=\sum_{i=0}^{n-1}v_i\bmod u$, vagyis összeg maradéka megegyezik a maradékok összegének maradékával. Ugyanilyen módon kapjuk a szorzatra vonatkozó analóg állítást, azaz hogy szorzat maradéka megegyezik a maradékok szorzatának maradékával, matematikailag leírva tehát $\prod_{i=0}^{n-1}(v_i\bmod u)\bmod u=\prod_{i=0}^{n-1}v_i\bmod u$. Ha például $m\in\mathbb{N}^+$, akkor $(v^m-v)\bmod u=\left((v\bmod u)^m-(v\bmod u)\right)\bmod u$, másként írva $v^m-v\equiv w^m-w\ (u)$, ahol $w=v\bmod u$, és így v^m-v akkor és csak akkor osztható u-val, ha u osztója w^m-w-nek.

Mivel euklideszi gyűrű főideálgyűrű, ezért euklideszi gyűrűben egy kongruencia-rendszer megoldható, és ha a maradékos osztás maradéka egyértelmű, akkor a megoldások között pontosan egy olyan lesz, amely vagy 0, vagy a normája kisebb, mint a modulusok legkisebb közös többszörösének, azaz a szorzatuknak a normája.

5. Test feletti egyhatározatlanú polinomgyűrű euklideszi, tehát főideálgyűrű és Gauss-gyűrű, polinom foka az euklideszi norma, és a maradékos osztás maradéka egyértelmű, ezért ilyen gyűrűben az előbbi megállapítások érvényesek. Tetszőleges g és $f\neq 0$ polinom esetén $\delta(g\bmod f)<\deg(f)$. Ha c_1 és c_2 a test két különböző eleme, akkor $0\neq c_1-c_2$ konstans polinom, vagyis egység a polinomgyűrűben, következésképpen $g-c_1$ és $g-c_2$ relatív prímek. Legyen $\mathbb{F}_q$ a test, $0\neq f\in\mathbb{F}_q[x]$, $\deg(f)=n\in\mathbb{N}^+$ és $h\in\mathbb{F}_q[x]$. A 4.8. tétel szerint $h^q-h=\prod_{c\in\mathbb{F}_q}(h-c)$. Ezt alkalmazva

$$(f,h^q-h)=\left(f,\prod_{c\in\mathbb{F}_q}(h-c)\right)=\left(f,\left[h-c|c\in\mathbb{F}_q\right]\right)$$
$$=\left[(f,h-c)|c\in\mathbb{F}_q\right]=\prod_{c\in\mathbb{F}_q}(f,h-c),$$

és ha f osztója $h^q - h$-nak, akkor $f = (f, h^q - h) = \prod_{c \in \mathbb{F}_q} (f, h - c)$. Gyűrű elemeinek legnagyobb közös osztója nem változik, ha valamelyikükhöz hozzáadjuk valamely másiknak gyűrűbeli többszörösét, ezért, figyelembe véve, amit összeg és szorzat, valamint $v^m - v$ maradékáról láttunk, a fenti összefüggések akkor és csak akkor teljesülnek egy adott h polinommal, ha teljesülnek $h \bmod f$-fel, így feltehető, és fel is tesszük, hogy $\delta(h) < n$. Amennyiben f négyzetmentes, $f = \prod_{i=1}^{k} f_i$ az f irreducibilis faktorokra való felbontása $\mathbb{F}_q$ fölött és $h^q - h$ az f többszöröse, akkor minden $k \geq i \in \mathbb{N}^+$-hoz van egy és csak egy olyan $c_i \in \mathbb{F}_q$, hogy $f_i | h - c_i$, vagyis egy és csak egy $\mathbb{F}_q$-beli c_i-vel $h \equiv c_i \ (f_i)$. Egy i-től különböző j-re $f_j | h - c_i$ csak úgy lehetséges, ha f_j osztója $c_j - c_i$-nek, tehát ha $c_j = c_i$, és ekkor, és az előzőek szerint csak ekkor, $f_i | h - c_j$.

Az előbb azt láttuk, hogy ha f osztója $h^q - h$-nak, akkor h megoldása egy $X \equiv c_i \ (f_i)$ kongruencia-rendszernek. Ez fordítva is igaz. Ha ugyanis h az $\mathbb{F}_q$ fölötti olyan polinom, hogy megoldása az előbbi kongruencia-rendszernek valamilyen $(c_1, \dots, c_k)$ $\mathbb{F}_q$-beli k-assal, akkor $h^q \equiv c_i^q = c_i \equiv h \ (f_i)$, vagyis $h^q - h$ valamennyi f_i-vel, de akkor a szorzatukkal, f-fel is osztható. Mivel test feletti polinomgyűrű euklideszi, és a maradék az osztásnál egyértelmű, ezért bármely $(c_1, \dots, c_k)$ esetén van egy és csak egy olyan h megoldás, ahol $\delta(h) < \deg(f)$. Különböző $(c_1, \dots, c_k)$ rendszerhez különböző megoldás tartozik, mert ha $\left(c_1^{(1)}, \dots, c_k^{(1)}\right) \neq \left(c_1^{(2)}, \dots, c_k^{(2)}\right)$, akkor van olyan $k \geq l \in \mathbb{N}^+$ index, hogy $c_l^{(1)} \neq c_l^{(2)}$, és ha $h^{(1)} = h^{(2)}$, akkor $c_l^{(1)} \equiv h^{(1)} = h^{(2)} \equiv c_l^{(2)} \ (f_l)$, tehát $c_l^{(1)} \equiv c_l^{(2)} \ (f_l)$, ami lehetetlen, hiszen $c_l^{(1)} - c_l^{(2)} \neq 0$ konstans polinom, míg f_l legalább elsőfokú, hiszen irreducibilis. Mivel a c_i-k egymástól függetlenül választhatóak, és bármely választásnál van egy és csak egy legfeljebb $n-1$-edfokú megoldás, ezért pontosan q^k olyan, legfeljebb $n-1$-edfokú h polinom van $\mathbb{F}_q[x]$-ben, amelyre $h^q - h$ osztható f-fel. Az is igaz, hogy minden f_i, f_j párhoz, ahol $i \neq j$, van olyan h, hogy f_i, f_j a test különböző c elemével osztója $h - c$-nek. Láttuk ugyanis, hogy f_i és f_j pontosan akkor osztója a test ugyanazon c eleméhez tartozó $(f, h - c)$ legnagyobb közös osztónak, ha $h \equiv c_i = c \ (f_i)$ és $h \equiv c_j = c \ (f_j)$. Így, ha $c_i \neq c_j$, akkor az adott kongruencia-rendszer h megoldása szétválasztja a két irreducibilis faktort abban az értelemben, hogy a két polinom különböző legnagyobb közös osztónak lesz az osztója.

6. Most meg kellene határozni a q^k különböző h polinomot. Ezt megtehetnénk úgy, hogy meghatározzuk az előbbi kongruencia-rendszerek megoldásait, de ehhez ismerni kellene a modulusokat, és éppen ezeket nem ismerjük, hiszen a feladatunk ezek meghatározása. Azért vannak megoldások, amelyeket ismerünk, hiszen valamennyi konstans polinom megoldás, de ezek érdektelen megoldások, hiszen ekkor minden legnagyobb közös osztó vagy f (amikor h a nullpolinom), vagy az egységelem (amikor h a nullától különböző konstans polinom). A h polinomok meghatározása azért megoldható. Legyen $n > i \in \mathbb{N}$-re $x^{iq} \bmod f = q^{(i)} = \sum_{j=0}^{n-1} q_j^{(i)} x^j$, és legyen $\mathbf{Q}$ olyan $n \times n$-es mátrix, amelyben az $n > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$ indexekre $Q_{i,j} = q_j^{(i)}$. Legyen egy legfeljebb $n-1$-edfokú h polinom együtthatóinak vektora $\mathbf{h}$, és az ehhez tartozó sorvektor h^T. Ha $h = \sum_{i=0}^{n-1} h_i x^i$, akkor

7.

$$
\begin{aligned}
h^q \bmod f &= \sum_{i=0}^{n-1} h_i x^{qi} \bmod f = \sum_{i=0}^{n-1} h_i \left(x^{qi} \bmod f\right) \\
&= \sum_{i=0}^{n-1} h_i q^{(i)} = \sum_{i=0}^{n-1} h_i \sum_{j=0}^{n-1} q_j^{(i)} x^j = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} h_i q_j^{(i)} \right) x^j \\
&= \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} h_i Q_{i,j} \right) x^j = \sum_{j=0}^{n-1} (h^T \mathbf{Q})_j x^j,
\end{aligned}
$$

és $h = h^q \bmod f$ akkor és csak akkor teljesül, ha minden i-re $h_i^T = (h^T \mathbf{Q})_i$, azaz pontosan akkor, ha $h^T = h^T \mathbf{Q}$, ami ekvivalens a $h^T (\mathbf{Q} - \mathbf{I}_n) = 0^T$ feltétellel, ahol $\mathbf{I}_n$ az n-edrendű egységmátrix, és 0^T az n-dimenziós tér nullvektorához tartozó sorvektor. A keresett h polinomok tehát a $\mathbf{T} = \mathbf{Q} - \mathbf{I}_n$ mátrix nullterének vektoraihoz tartozó polinomok. (Mátrix sorvektorai által kifeszített tér nulltere azon vektorok összessége, amelyekhez tartozó sorvektorral a mátrixot balról szorozva a nullvektor sorvektorát

kapjuk. Ilyen vektor van, például a nullvektor, és ha két vektor rendelkezik az előbbi tulajdonsággal, akkor bármely lineáris kombinációjuk is ilyen tulajdonságú, vagyis ezek a vektorok lineáris teret alkotnak, a mátrix sorvektoraihoz tartozó nullteret. Ennek dimenziója a mátrix sorainak nullitása, ami megegyezik a sorok számának és a mátrix rangjának különbségével.) h meghatározása tehát egy n egyenletből álló, n-ismeretlenes homogén lineáris egyenletrendszer megoldása. Ebből az is látszik, hogy ha $\mathbf{T}$ rangja r, és így a nullitása $n-r$, akkor $k=n-r$, hiszen a q-elemű test fölötti s-dimenziós tér elemeinek száma q^s. A feladat megoldásához elegendő a nulltér egy bázisát meghatározni, mert ezek együttesen bármely két irreducibilis faktort szétválasztanak. Azt ugyanis már tudjuk, hogy bármely két különböző irreducibilis faktorhoz van olyan h, amely ezt a két faktort szétválasztja. Legyen $h=\sum_{l=1}^{k} a_l h^{(l)}$ egy őket szétválasztó polinom, ahol $h^{(l)}$ a nulltér egy bázisához tartozó polinom, míg a_l-ek a test elemei. Ha az állítással ellentétben nincs olyan bázisvektor, amelyhez tartozó polinom szétválasztja az előbbi két faktort, akkor minden l-re ez a két faktor ugyanazon $c^{(l)} \in \mathbb{F}_q$-hoz tartozó $\left(f, h^{(l)}-c^{(l)}\right)$ osztója, ám ekkor osztója $\left(f, \sum_{l=1}^{k} a_l\left(h^{(l)}-c^{(l)}\right)\right)=\left(f, h-\sum_{l=1}^{k} a_l c^{(l)}\right)$-nek, és $\sum_{l=1}^{k} a_l c^{(l)}$ is a test eleme, vagyis ekkor h sem választja szét a két faktort.

8. Mutatunk egy módszert, amellyel $\mathbf{T}$ nullterének egy bázisa meghatározható. Egy egységelemes integritási tartomány feletti kvadratikus $\mathbf{A}$ mátrix **redukált, trianguláris és idempotens**, röviden **RTI-mátrix**, ha

a) felső háromszögmátrix;
b) a főátló minden eleme 0 vagy a gyűrű egységeleme;
c) ha a főátlóban álló elem 0, akkor oszlopának minden eleme 0, míg ha a főátlóbeli elem a gyűrű egységeleme, akkor a sor minden más eleme 0.

A definícióból adódik, hogy a mátrix valóban trianguláris, és redukált a főátlóbeli elemekre, valamint a sorokra és oszlopokra kirótt feltételek miatt. Nézzük az idempotenciát. Azt kell belátnunk, hogy a fenti feltételeket kielégítő $\mathbf{A}$ mátrixra $\mathbf{A}^2=\mathbf{A}$. Mindenek előtt érdemes megfigyelni, hogy ha $a_{i,j}\neq 0$, akkor $a_{j,j}=e$ (mert különben a j-indexű oszlop minden eleme 0), és vagy $i=j$, vagy $i<j$ (mert $\mathbf{A}$ felső háromszögmátrix) és $a_{i,i}=0$ (mert $i<j$ miatt $a_{i,j}\neq 0$ nem a főátló eleme, és ha $a_{i,i}\neq 0$, akkor a sorában minden más elem 0). Ekkor $(\mathbf{A}^2)_{i,k}=\sum_{j=0}^{n-1} a_{i,j}a_{j,k}=a_{i,k}a_{k,k}=a_{i,k}$, mert $a_{i,j}a_{j,k}\neq 0$ akkor és csak akkor, ha $a_{i,j}\neq 0\neq a_{j,k}$, ami csak úgy lehet, ha $a_{j,j}=e$, és vagy $j=k$, vagy $j<k$ és $a_{j,j}=0$. De $0=a_{j,j}=e$ nem lehet, ezért $j=k$, vagyis az összegben legfeljebb csak a $j=k$ -hoz tartozó tag lehet nullától különböző, ezért igaz a $\sum_{j=0}^{n-1} a_{i,j}a_{j,k}=a_{i,k}a_{k,k}$ egyenlőség, és ha $a_{i,k}=0$, akkor $a_{i,k}a_{k,k}=0=a_{i,k}$, míg az ellenkező esetben $a_{k,k}=e$.

RTI-mátrix nullterének egy bázisát könnyű meghatározni. $\mathbf{A}^2=\mathbf{A}$-ból $(\mathbf{A}-\mathbf{I})\mathbf{A}=\mathbf{0}$, amiből következik, hogy $\mathbf{A}-\mathbf{I}$ sorai, és ekkor ezen sorok bármely lineáris kombinációja eleme $\mathbf{A}$ nullterének. Még azt kell belátni, hogy ezzel ki is merítettük a nullteret, amihez elegendő belátni, hogy $\mathbf{A}-\mathbf{I}$ rangja megegyezik $\mathbf{A}$ nullitásával.

Tekintsük elsőként az n-edrendű $\mathbf{A}$ mátrix rangját. Ha a főátlóban t számú elem 0, akkor a mátrixban t olyan oszlop van, amelynek minden eleme 0, így a mátrix rangja legfeljebb annyi, mint a főátlóban álló nem nulla elemek száma, vagyis $r(\mathbf{A})\leq n-t$. Ha a főátlóban $a_{i,i}=0$, akkor az i-indexű oszlop minden eleme 0, így elhagyva ezt az oszlopot, a mátrix rangja nem változik. Ha még az i-indexű sort is elhagyjuk, akkor olyan, ismét kvadratikus mátrixot kapunk, amely maga is RTI-mátrix. Ez valóban igaz. Az i-edik sor és i-edik oszlop az eredeti mátrixot négy részre osztja. A sor és oszlop törlésekor a bal felső rész helyben marad, a bal alsó rész egy sorral feljebb kerül, de ebben a részben minden elem 0, így az új mátrix bal oldali részében a főátló elemei megegyeznek az eredeti mátrix főátlóbeli elemeivel, így minden ilyen elem vagy 0, vagy az egységelem, míg az új főátló alatti elemek mindegyike most is 0. A jobb oldali részben minden elem eggyel balra kerül, vagyis az oszlopindexe eggyel csökken, míg a törölt sor alatti rész elemei a balra tolódás mellett eggyel feljebb kerülnek, vagyis a sorindexük is eggyel csökken. Ebből következik, hogy $\mathbf{A}$ főátlóbeli elemei a redukált mátrixban is a főátlóban állnak, és a főátló alatti minden elem most is 0. Még azt kell tekintetbe venni, hogy a módosítás során egy csupa 0-ból álló oszlop, ha nem töröltük, az új mátrixban is csak 0-kat tartalmaz, és ha egy sorban a főátlóban álló elem kivételével minden elem zérus volt, és a sort nem töröltük, akkor ugyanilyen tulajdonságú lesz

az új mátrixban is. Egy mátrixból egy sort törölve a rang legfeljebb csak csökkenhet, így az új mátrix rangja nem nagyobb, mint az eredeti mátrix rangja. Ezt az átalakítást addig végezzük, amíg a főátlóban van 0. Az eredményül kapott mátrix egy olyan felső háromszögmátrix, amelynek a főátlójában minden elem 0-tól különböző, így ennek a mátrixnak a rangja megegyezik a rendjével. De ez a rend azonos az eredeti mátrix főátlójában álló nem nulla elemek számával, vagyis $n-t$-vel. Mivel minden lépésben legfeljebb csak csökkenhetett a mátrix rangja, ezért az eredeti mátrix rangja ennél nem kisebb, tehát $r(\mathbf{A}) \geq n-t$, és ekkor $r(\mathbf{A}) = n-t$, hiszen a bekezdés elején láttuk, hogy $r(\mathbf{A}) \leq n-t$.

Az $\mathbf{A}-\mathbf{I}$ mátrix rangjának megállapítása az előbbi eredmény birtokában már könnyű. Mindenek előtt rögtön látjuk, hogy ez a mátrix is felső háromszögmátrix, hiszen csak a főátló elemei változtak. Ebben a mátrixban a főátló egy eleme $-e$, ha az eredeti mátrixban az ugyanezen pozícióban álló elem 0, és 0 az ellenkező esetben. Amennyiben most a főátló eleme 0, akkor ott az eredeti mátrixban *e* volt, és akkor ezen sor minden, nem a főátlóban álló eleme 0, így $\mathbf{A}-\mathbf{I}$ -ben egy olyan sor, ahol a főátlóban álló elem 0, csak 0-kból áll. Ha viszont az új mátrixban a főátlóbeli elem nem 0, akkor ott az eredeti mátrixban 0 állt, de akkor a megfelelő oszlop minden eleme is 0, tehát az új mátrixban ebben az oszlopban a főátlón kívüli minden elem 0. Azt látjuk, hogy $\mathbf{A}-\mathbf{I}$ soraira ugyanazon tulajdonság igaz, mint **A**-ban az oszlopokra, és hasonló a viszony $\mathbf{A}-\mathbf{I}$ oszlopai és **A** sorai között, azzal az egyetlen eltéréssel, hogy most a főátló nem 0 elemei nem a gyűrű egységelemével, hanem annak ellentettjével egyeznek meg. Ebből viszont az következik, hogy $\mathbf{A}-\mathbf{I}$ rangja is a főátlójában lévő nem nulla elemek számával azonos, ami viszont megegyezik az **A** főátlójában lévő nulla elemek számával, tehát valóban igaz, hogy **A** nullitása azonos $\mathbf{A}-\mathbf{I}$ rangjával.

Mivel $\mathbf{A}-\mathbf{I}$ rangja megegyezik a főátlójában álló nem nulla elemek számával, a többi sor viszont csak 0-t tartalmaz, így azt is kaptuk, hogy $\mathbf{A}-\mathbf{I}$ -ben azok és csak azok a sorok lineárisan függetlenek, amelyeknél a főátlóban álló elem különbözik 0-tól, vagyis ahol ez az elem $-e$.

Az **A** rangjára vonatkozó állítást formálisan is igazoljuk. Legyen az **A** mátrix i-edik sora a_i^T, ekkor $\left(\sum_{j=0}^{n-1} a_{i,j}a_j^T\right)_k = \sum_{j=0}^{n-1} a_{i,j}\left(a_j^T\right)_k = \sum_{j=0}^{n-1} a_{i,j}a_{j,k} = \mathbf{A}_{i,k}^2 = a_{i,k} = \left(a_i^T\right)_k$ bármely $n > k \in \mathbb{N}$ indexre. Korábban megmutattuk, hogy $a_{i,j} = a_{j,j}a_{i,j}$, így $\sum_{j=0}^{n-1} a_{i,j}a_j^T = \sum_{j=0}^{n-1} a_{i,j}\left(a_{j,j}a_j^T\right)$, vagyis $\mathbf{a}_i$ az $a_{j,j}\mathbf{a}_j$ vektorok, tehát azon $\mathbf{a}_j$ vektorok lineáris kombinációja, ahol $a_{j,j} \neq 0$. De ha $a_{j,j} \neq 0$, akkor $a_{j,j} = e$, és ekkor $a_{j,j}a_j^T = a_j^T = e_j^T$, ahol $\mathbf{e}_j$ a j-edik egységvektor. Ezen vektorok, és akkor az általuk meghatározott sorok lineárisan függetlenek, és az előbbiek szerint generálják a mátrix minden sorát, így a mátrix rangja megegyezik a főátlójában lévő nullától különböző elemek számával, vagyis a nullitása a főátlóban lévő 0-k száma.

Az előbbieket sorok helyett oszlopokra alkalmazva, a fentiekkel megegyező módon igazolhatjuk az $\mathbf{A}-\mathbf{I}$ rangjára vonatkozó állítást is.

Legyen most **U** tetszőleges mátrix, **V** egy olyan kvadratikus, reguláris mátrix, amellyel jobbról, és **u** olyan vektor, amelyhez tartozó sorvektorral balról szorozható **U** (vagyis **V** rendje megegyezik **U** oszlopainak számával, és **u** dimenziója **U** sorainak számával egyenlő). Ekkor $(u^T\mathbf{U})\mathbf{V} = u^T(\mathbf{UV}) = 0^T$ akkor és csak akkor igaz, ha $u^T\mathbf{U} = 0^T$, mert **V** reguláris, így **U** és **UV** nulltere azonos, tehát **U** nulltere helyett kereshetjük **UV** nullterét is. A **V**-vel való szorzás csak **U** oszlopainak manipulációja, így a nulltér meghatározásához bármilyen olyan átalakítást végezhetünk **U**-n, amely csak az oszlopait érinti és visszafordítható. Egy oszlop szorzása egy nem zérus elemmel és egy oszlopnak egy másik oszlophoz való hozzáadása invertálható műveletek, és invertálhatóak ezek bármilyen, tetszőleges sorrendben végrehajtott kombinációi, tehát például egy oszlop tetszőleges konstansszorosának egy másik oszlophoz való hozzáadása vagy két oszlop felcserélése. Megmutatjuk, hogy tetszőleges kvadratikus mátrix ilyen oszlop-transzformációkkal RTI-alakra hozható.

Az egyszerűség kedvéért úgy végezzük az átalakítást, hogy mindig csak az első sort manipuláljuk, és utána a sorokat ciklikusan egy pozícióval feljebb visszük. Ezt n-szer végezzük el, ahol n a mátrix rendje, vagyis a sorok száma. Mivel a sorok sorrendje nem változik, az n-edik lépés után a sorok az eredeti helyükön az eredeti sorrendben állnak, tehát, jóllehet a sorokat is mozgatjuk, de ezek hatása a végeredményben olyan, mintha semmilyen sorműveletet nem végeztünk volna. Ez a módszer viszont egyszerűbbé teszi az algoritmus leírását, és lényegesen egyszerűsíti a hardvert, ha az átalakítást célhardver végzi.

```
ciklus i-re 0-tól n − 1-ig
    t = −1
    ciklus j-re 0-tól n − 1-ig
        ha a_{0,j} ≠ 0, akkor
            ha t = −1 vagy a_{j,j} = 0, akkor
                t = j
            elágazás vége
            ha a_{j,j} = 0, akkor
                j = n − 1
            elágazás vége
        elágazás vége
    ciklus vége
    ha t > 0, akkor
        a 0- és a t-indexű oszlopok cseréje
    elágazás vége
    ha a_{0,0} ≠ 0, akkor
        ciklus j-re 1-től n − 1-ig
            a j-edik oszlopból a 0-dik oszlop a_{0,j}/a_{0,0}-szorosának kivonása
        ciklus vége
    elágazás vége
    a mátrix sorainak egy sorral való ciklikus feljebb tolása
    a mátrix oszlopainak egy oszloppal való ciklikus balra léptetése
ciklus vége
```

2. algoritmus

Az átalakítást a 2. algoritmus mutatja. Először, a bal felső sarokban álló elemmel kezdve, balról jobbra haladva megkeressük a legfelső sorban az első nem nulla elemet, amelynek oszlopában a főátlóban álló elem 0, illetve, ha ilyen nincs, akkor a legfelső sor első nullától különböző elemét. Ha ilyen sincs, akkor a legfelső sor minden eleme 0. Ellenkező esetben felcseréljük a bal szélső oszlopot az előbb talált elem oszlopával, utána a bal szélső oszlop megfelelő konstansszorosát kivonjuk az összes többi oszlopból úgy, hogy a mátrix felső sorában a bal szélső elem kivételével minden elem 0 legyen, végül a bal oldali oszlopot megszorozzuk a legfelső sorban álló elem inverzével. Ezek után, bármi is állt kezdetben a bal felső sarokban, a mátrix legfelső sorának minden eleme a bal szélső esetleges kivételével zérus, és a bal szélső elem, ha nem 0, akkor az egységelem. Amikor ezzel az átalakítással megvagyunk, akkor a mátrix minden elemét ciklikusan eggyel feljebb és egy pozícióval balra léptetjük, és ezt összesen n-szer végezzük el.

Megmutatjuk, hogy a külső ciklus k-adik lefutása után a mátrix alsó k sorában az utolsó k oszlopból álló k-adrendű mátrix RTI-alakú, és ugyanezen sorok első $n-k$ oszlopának minden eleme 0. Ez $k=0$ esetén nyilván igaz. Most tegyük fel, hogy adott $n > k \in \mathbb{N}$ esetén igaz az állításunk, és hajtsuk végre az algoritmus külső ciklusának magját egyszer, majd nézzük meg ekkor a mátrix utolsó $k+1$ sorát. Legyen $\mathbf{A}^{(k)}$ a k-adik lépés után a mátrix jobb alsó k-adrendű részmátrixa.

Amennyiben a legfelső sor minden eleme 0 volt, akkor mindössze annyi történt, hogy az utolsó k sor eggyel feljebb és ciklikusan eggyel balra mozdult, és legalulra bekerült a csupa 0-ból álló sor. A mozgás során $\mathbf{A}^{(k)}$ önmagán belül nem változott, de a végén kiegészült alul egy csupa 0-ból álló sorral és jobbról egy csupa 0-ból álló oszloppal. Az így kapott $k+1$-edrendű mátrix főátlójában továbbra is mindenütt 0 vagy e áll, a főátló alatti elemek mindegyike 0, és ha a főátlóban 0 áll, akkor az egész oszlop csak 0-t tartalmaz, míg az ellenkező esetben a főátlótól eltekintve a teljes sor 0-ból áll, vagyis a ciklus végén ez a $k+1$-edrendű $\mathbf{A}^{(k+1)}$ mátrix RTI-alakú, és az is igaz lesz, hogy az előtte álló valamennyi elem ezekben a sorokban 0, tehát öröklődött a kiinduló elrendezés.

Amennyiben volt a legfelső sorban nem zérus elem, akkor lehetséges, hogy oszlopot kellett cserélni. Ha igen, legyen ez a t-indexű oszlop. Ha $t < n-k$, vagy az oszlop utolsó k eleme 0, akkor a csere nem változtatja meg a mátrix utolsó k sorát. Ha viszont az utolsó k oszlop valamelyikével történik a csere, és ennek utolsó k eleme között van 0-tól különböző, akkor a főátlóban álló elem e, és a legfelső

sor első t elemének mindegyike 0. Most csere után $\mathbf{A}^{(k)}$-ban annyi változás lesz, hogy a kicserélt oszlop helyére egy csupa 0-ból álló oszlop kerül, így a módosult mátrix is RTI-alakú, míg $\mathbf{A}$ első oszlopának utolsó $n-t-1$ eleme az $\mathbf{A}^{(k)}$-ból kicserélt oszlop főátló alatti elemei lesznek, amelyek mindegyike 0. Látható, hogy a következő lépésben, amikor az első oszlop megfelelő konstansszorosait kivonjuk az egyes oszlopokból, csupán az esetleges csere legutolsó eseténél történhet változás az utolsó k sorban. De változás csak olyan oszlopban lehet, ahol a legfelső sor megfelelő eleme nem 0, tehát eleve csak a t-nél nagyobb indexű oszlopokban (a t-nél kisebb indexű oszlopok legfelső eleme ennél a cserénél 0 volt, míg a csere után ugyanez igaz a t-indexű oszlopra is), és az ilyen oszlopok utolsó k sorában is csak a főátló felett, mert a bal szélső oszlop egy konstansszorosát vonjuk le, de ennek a t-nél nagyobb indexű elemei, tehát $\mathbf{A}^{(k)}$-ban a kicserélt oszloptól jobbra eső oszlopokban minden, a főátlóba és az alá eső eleme 0, vagyis ezek az elemek nem változnak, így az oszlop-redukció után is a főátló minden eleme 0 vagy e és a főátló alatti minden elem 0 lesz. Még azt kell figyelembe vennünk, hogy $\mathbf{A}^{(k)}$-beli csupa 0-ból álló oszlop nem változik, mert ennek főátlójában 0 áll, így a legfelső sor megfelelő eleme is 0.

Láthatóan az esetleges oszlopcsere nem változtatott az utolsó k sor tulajdonságán, és ezek után a sorok illetve az oszlopok mozgatása során bekövetkező változás csak annyiban módosít azon, amit a csupa 0-ból álló legfelső sor esetén már megbeszéltünk, hogy most az új $\mathbf{A}^{(k+1)}$ jobb szélső oszlopában a főátlóbeli elem e lesz, tehát felette bármi állhat, attól még $\mathbf{A}^{(k+1)}$, tehát a ciklus n-edik lefutása után $\mathbf{A}^{(n)}$, vagyis a teljes mátrix RTI-mátrix lesz.

A 87. oldalon, a 4.28. Következmény bizonyítása után láttuk, hogy véges test fölötti f polinom felírható az $f = \prod_{k=1}^{n} \prod_{i=1}^{r_k} g_{k,i}^{i}$ alakban, ahol a $g_{k,i}$ polinom négyzetmentes, és minden faktorának foka pontosan k (így a számuk $\frac{\deg(g_{k,i})}{k}$). Ezek a $g_{k,i}$ polinomok könnyen meghatározhatóak, és utána f irreducibilis polinomok szorzatára való felbontásához elegendő a $g_{k,i}$ polinomokat faktorizálni.

6. Egységgyökök

Korábban már beláttuk, hogy véges test multiplikatív csoportja ciklikus. Most ismét foglalkozunk a kérdéssel, de a korábbinál részletesebben, és a tételre egy más bizonyítást mutatunk.

Ebben a részben p, ha mást nem mondunk, vagy prímszám, vagy $p = 0$.

6.1. Tétel

Legyen $\mathcal{S}$ egységelemes kommutatív félcsoport, e az egységelem, $n \in \mathbb{N}^+$, $T_n = \{s \in S | s^n = e\}$ és $T = \bigcup_{n\in\mathbb{N}^+} T_n$. Ekkor T_n és T az $\mathcal{S}$-beli szorzással csoport.

Δ

Bizonyítás:

$T_n \neq \emptyset$, mert $e^n = e$. Ha $n = 1$, akkor $T_n = \{e\}$, és ez az $\mathcal{S}$-beli szorzással csoport. Ha $n > 1$, és s és t a T_n elemei, akkor $(st)^n = s^n t^n = e \cdot e = e$, hiszen $\mathcal{S}$-ben a szorzás kommutatív, így T_n zárt az $\mathcal{S}$-beli szorzásra, vagyis az $\mathcal{S}$-beli szorzás T_n-re való megszorításával T_n az $\mathcal{S}$ részfélcsoportja. Ekkor $s^{n-1} \in T_n$ és $e = s^n = s^{n-1}s = ss^{n-1}$, így s-nek van inverze $\mathcal{S}$-ben, és ez az inverz is benne van T_n-ben, vagyis T_n csoport. $s^u = e$-ből következik $s^{uv} = e$, ezért $T_n \subseteq T_{mn}$ és $T_m \subseteq T_{mn}$. De T_n, T_m és T_{mn} csoport, tehát $T_m T_n^{-1} \subseteq T_{mn} T_{mn}^{-1}$, így az előzőek alapján T is csoport.

□

6.2. Következmény

Legyen $n \in \mathbb{N}^+$, és $\mathcal{R}$ kommutatív gyűrű az e egységelemmel. Ekkor az $\mathcal{R}$ feletti $x^n - e$ polinom R-beli gyökei csoportot alkotnak az $\mathcal{R}$-beli szorzással. Fordítva, az $\mathcal{R}$ kommutatív, egységelemes gyűrű multiplikatív félcsoportjában az e egységelemet tartalmazó m-elemű reguláris $\mathcal{S}$ részfélcsoport elemei gyökei az $\mathcal{R}$ feletti $x^m - e$ polinomnak.

Δ

Bizonyítás:

$x^n - e$ minden együtthatója 0, e illetve $-e$, így valamennyi együtthatója eleme R-nek, tehát a polinom $\mathcal{R}$ feletti. A gyűrű elemei a szorzással egy egységelemes, kommutatív $\mathcal{S}$ félcsoportot alkotnak. Legyen T az $\mathcal{R}$ feletti $x^n - e$ polinom R-beli gyökeinek halmaza. e gyöke a polinomnak, így T az R nem üres részhalmaza. Ha $u \in T$, akkor $u^n = e$, míg ha v az R olyan eleme, amelyre $v^n = e$, akkor v egy R-beli gyöke az $\mathcal{R}$ feletti $x^n - e$ polinomnak, így T pontosan azon R-beli elemek halmaza, amelyeknek az n-edik hatványa az $\mathcal{S}$ egységeleme. Ekkor, az előző tétel alapján T az $\mathcal{S}$-beli, tehát az $\mathcal{R}$-beli szorzással csoport.

Véges reguláris félcsoport csoport, így $\mathcal{S}$ m-edrendű csoport. m-edrendű csoport minden elemének m-edik hatványa a csoport egységeleme, ami a feltétel szerint megegyezik a gyűrű egységelemével, így $\mathcal{S}$ minden eleme gyöke az $\mathcal{R}$ feletti $x^m - e$ polinomnak.

□

6.3. Tétel

Legyen $\mathcal{R}$ egységelemes integritási tartomány, e az $\mathcal{R}$ egységeleme, p a gyűrű karakterisztikája és $n \in \mathbb{N}^+$. Ha $n = p^t m$, ahol t nemnegatív egész szám és m a p-vel nem osztható egész szám, akkor $x^n - e$ és $x^m - e$ gyökeinek halmaza azonos, $x^m - e$ gyökei egyszeresek és a számuk m, és $x^n - e$ gyökei p^t-szeresek. Az R-beli gyökök száma osztója m-nek.

Δ

Bizonyítás:
Az integritási tartomány bármely u elemével és tetszőleges l egész számmal $lu = 0$ akkor és csak akkor, ha vagy $u = 0$, vagy l osztható a gyűrű karakterisztikájával. Ekkor $(x^m - e)' = mx^{m-1}$-nek legfeljebb csak a 0 lehet gyöke, hiszen m nem osztható p-vel, de 0 nem gyöke $x^m - e$-nek, így ezen polinom gyökei egyszeresek. $x^n - e = x^{p^t m} - e = (x^m)^{p^t} - e^{p^t} = (x^m - e)^{p^t}$, amiből viszont a nullosztó-mentességgel következik, hogy a két polinom gyökeinek halmaza azonos, és $x^n - e$ minden gyöke p^t-szeres. Integritási tartomány feletti polinom gyökeinek száma nem lehet több a fokánál, és van olyan, az adott integritási tartományt tartalmazó test, amelyben a polinom elsőfokú tényezők szorzata, így $x^m - e$ gyökeinek száma m. Ezek a gyökök egy m-edrendű csoportot alkotnak az előbbi testben, és ennek a csoportnak egy részcsoportját alkotják az R-beli gyökök. Mivel véges csoport részcsoportjának rendje osztója a csoport rendjének, ezért az R-beli gyökök száma osztója m-nek.

□

6.4. Következmény

Integritási tartomány multiplikatív félcsoportjában bármely $n \in \mathbb{N}$-re legfeljebb egy n-edrendű, a nullelemet nem tartalmazó részfélcsoport van.

Δ

Bizonyítás:
Integritási tartomány multiplikatív félcsoportjának egy 0-t nem tartalmazó, véges részfélcsoportja csoport. Legyen $\mathcal{G}$ az $\mathcal{R}$ multiplikatív félcsoportjának egy, a 0-t nem tartalmazó n-edrendű részcsoportja, ahol n egy pozitív egész szám. Ekkor G minden g elemére $g^n = e$, vagyis mindegyik eleme gyöke az $\mathcal{R}$ feletti $x^n - e$ polinomnak. De ennek a polinomnak legfeljebb n különböző gyöke lehet, így nincs G-n kívül olyan elem, amelynek n-edik hatványa az egységelem, tehát nem lehet $\mathcal{R}$ multiplikatív csoportjában $\mathcal{G}$-től különböző n-edrendű részcsoport (mert ha lenne, akkor $\mathcal{G}$-nek és ennek a csoportnak együtt már n-nél több eleme lenne, és mindegyikük gyöke lenne az előbbi polinomnak).

□

A későbbiek kedvéért kihangsúlyozzuk, hogy integritási tartomány multiplikatív, a 0-t nem tartalmazó részfélcsoportjában még úgy sem lehet két különböző, azonos rendű részcsoport, hogy a két részcsoport izomorf.

6.5. Következmény

Egy testnek minden 1-nél nagyobb pozitív egész n-re legfeljebb egy n-elemű részteste lehet.

Δ

Bizonyítás:
Egy test és bármely résztestének karakterisztikája azonos, és nincs 0-karakterisztikájú véges test, vagyis 0-karakterisztikájú testnek nincs n-elemű részteste. Legyen a $\mathcal{K}$ test karakterisztikája a p prímszám. Ekkor $\mathcal{K}$-nak csak p^m-elemű véges részteste lehet, és ha maga $\mathcal{K}$ is véges, és elemeinek száma p^s, akkor m csak az s osztója lehet, és minden ilyen m-re van is $\mathcal{K}$-nak p^m-elemű részteste. Az n-elemű résztest minden nem nulla eleme gyöke a $\mathcal{K}$ feletti $x^{n-1} - e$ polinomnak, és a polinomnak más gyöke nincs, valamint $\mathcal{K}$-nak és minden résztestének a nulleleme azonos, továbbá test integritási tartomány, így a 6.4 Következmény alapján csak egyetlen ilyen részteste lehet a $\mathcal{K}$ testnek.

□

6.6. Tétel

Integritási tartomány multiplikatív félcsoportjának bármely, a nullát nem tartalmazó, véges részfélcsoportja ciklikus csoport.

Δ

Bizonyítás:

Legyen $\mathcal{R}$ az integritási tartomány. Integritási tartomány multiplikatív félcsoportjának a nullát nem tartalmazó részfélcsoportja reguláris félcsoport, és véges, reguláris félcsoport csoport. Ha e ennek a csoportnak az egységeleme, akkor e az egész gyűrű egységeleme, mivel a gyűrű nullosztómentes. Legyen $\mathcal{G}$ a csoport, és legyen a csoport rendje m. G tetszőleges a elemének d rendje osztója m-nek. Legyen $k \in \mathbb{N}$. Ekkor a^k is eleme G-nek, és $\left(a^k\right)^t = e$ akkor és csak akkor, ha $kt \equiv 0\ (d)$, vagyis ha $o_d^+(k) = \frac{d}{(k,d)} \Big| t$. Ebből a^k rendje $\frac{d}{(k,d)}$, azaz pontosan olyan k-ra lesz a^k d-edrendű, amelyre k relatív prím d-hez. A $d > k \in \mathbb{N}$ feltételt kielégítő egész kitevőkkel az a hatványai páronként különbözőek, minden egész kitevős hatványa a-nak ezek egyikével azonos, és $\left(a^k\right)^d = e$, ezért ezek az elemek gyökei az $\mathcal{R}$ feletti $x^d - e$ polinomnak. Mivel integritási tartomány feletti polinomnak nem lehet a fokánál több gyöke, és az a előbbi d hatványa a polinom d különböző gyöke, ezért más gyöke már nem lehet a polinomnak. Ezen gyökök közül $\varphi(d)$-számú lesz d-edrendű (φ az Euler-függvény). Az előbbiek alapján G elemeinek rendjei m pozitív egész osztói, és egy ilyen d osztóra vagy nincs, vagy pontosan $\varphi(d)$ különböző d-edrendű elem van $\mathcal{G}$-ben. Legyen $\psi(k)$ a pozitív egész számokon értelmezett olyan függvény, amelynek az értéke k-ban 1, ha van $\mathcal{G}$-ben k-adrendű elem, egyébként 0. Ekkor $m = \sum_{d|m} \psi(d)\varphi(d) \leq \sum_{d|m} \varphi(d) = m$, és $\varphi(d)$ minden d-re pozitív, így ψ az m minden d osztóján, és így m-nél is 1. Ez azt jelenti, hogy van $\mathcal{G}$-ben m-edrendű elem, mondjuk u. Az u által generált ciklikus csoport része $\mathcal{G}$-nek, és a csoportnak m eleme van, ezért $G = \langle u \rangle = \left\{u^k \middle| m > k \in \mathbb{N}\right\}$, $\mathcal{G}$ ciklikus csoport.

□

6.7. Következmény

Legyen $\mathcal{S}$ félcsoport és $\mathcal{R}$ integritási tartomány. $\mathcal{S}$ bármely véges homomorf képe R^*-ban ciklikus csoport, és minden pozitív egész n-re, a képelemek esetleges permutációjától eltekintve, $\mathcal{S}$-nek legfeljebb egy olyan φ homomorfizmusa van R^*-ba, ahol $0 \notin \mathrm{Im}(\varphi)$ és $|\mathrm{Im}(\varphi)| = n \in \mathbb{N}^+$. Ekkor, ha $\mathcal{S}$ véges csoport, és elemeinek a száma t, akkor n osztója t-nek.

Δ

Bizonyítás:

Félcsoport homomorf képe félcsoport, és a korábbiak szerint integritási tartomány multiplikatív félcsoportjának 0-t nem tartalmazó véges részfélcsoportja ciklikus csoport, így, ha $\mathrm{Im}(\varphi)$ véges, akkor ciklikus csoport. Szintén a korábbiak szerint, $\mathcal{R}$-nek legfeljebb egy n-edrendű részcsoportja van, így a képhalmaz egyértelmű. Az utolsó állítás következik abból, hogy csoport homomorf képe izomorf a leképezés magja szerinti faktorcsoporttal, a faktorcsoport rendje a mag indexének számossága, és ez véges csoport esetében osztója a csoport rendjének.

□

Nem feltétlenül különböző csoportoknak tehát egy integritási tartomány multiplikatív félcsoportjába való különböző olyan homomorfizmusainál, ahol a képhalmazok végesek, nem tartalmazzák a 0-t és a rendjük azonos, a képhalmazok meg is egyeznek, vagyis csak a képelemek sorrendjében lehet különbség.

A 6.6. Tételnek egy további, a véges testek szempontjából alapvető következménye, hogy véges test multiplikatív csoportja ciklikus. Ezt tételként is leírjuk.

6.8. Tétel

Véges test multiplikatív csoportja, és ennek minden részcsoportja, ciklikus.

Δ

Bizonyítás:
Véges test alaphalmaza és minden részhalmaza véges, így minden részcsoport – beleértve a nem valódi részcsoportot is – véges, ezért a tétel közvetlenül adódik a 6.6. Tételből.

□

Az előbbi tétel karakterizálja is a véges testeket, amint a következő tétel mutatja.

6.9. Tétel

Nullosztómentes gyűrű nem nulla elemeinek multiplikatív félcsoportja akkor és csak akkor ciklikus csoport, ha a gyűrű véges.

Δ

Bizonyítás:
Ha $\mathcal{R}$ véges, akkor test, így a multiplikatív csoportja az előző tétel szerint ciklikus.
Most legyen az $\mathcal{R}$ nullától különböző elemeinek multiplikatív félcsoportja ciklikus csoport, és legyen ennek a csoportnak egy generátoreleme u. Ha egy nullosztómentes gyűrű nem nulla elemei a szorzással csoportot alkotnak, akkor ferdetest, és ha a csoport ciklikus, akkor kommutatív, és a gyűrű test, így $\mathcal{R}$ test.
Ha $\mathrm{char}(\mathcal{R}) \neq 2$, akkor $u^0 = e \neq -e = u^k$ egy $k \neq 0$ egésszel, és $u^{2k} = e$. Ekkor $u^{-2k} = e$ is igaz, így feltehetjük, hogy $k > 0$. Ez viszont azt jelenti, hogy u rendje legfeljebb $2k$, tehát R véges.
Most legyen $\mathrm{char}(\mathcal{R}) = 2$. Mivel a test multiplikatív csoportja ciklikus az u generátorelemmel, ezért $\mathcal{R}$ részteste az $\mathcal{R}_P(u)$ testnek, ahol $\mathcal{R}_P$ az $\mathcal{R}$ prímteste, azaz a kételemű test. $u + e = u^k$ egy egész k-val, kivéve, ha $u + e = 0$. De ez utóbbi csak úgy lehet, ha $u = -e = e$, és ekkor $\mathcal{R}$ multiplikatív csoportja egyelemű, tehát $\mathcal{R}$ a kételemű, azaz véges test. Legyen tehát a továbbiakban $u \neq e$. k-ról feltehetjük, hogy nemnegatív. Ellenkező esetben ugyanis $(u^{-1})^{-k} = u^k = u + e = (u^{-1})^{-1} + e$, és innen $u^{-1} + e = (u^{-1})^{-k+1}$. De u^{-1} is generálja a csoportot, vagyis u helyett vehetjük u^{-1}-et, és ezzel az eredetihez hasonló egyenlőséget kapunk, de már pozitív kitevővel. k nem lehet 0 és nem lehet 1, mert az első esetben $u = 0$, míg a másodikban $e = 0$ lenne. u az $x^k + x + e$ polinom gyöke. Ez a polinom eleme a test prímteste feletti polinomgyűrűnek, így u algebrai a kételemű test fölött. Ekkor viszont $\mathcal{R}_P(u)$, és akkor az előbbiek szerint $\mathcal{R}$ is véges test.

□

Ciklikus csoport egyetlen elemmel generálható, így véges test multiplikatív csoportja is generálható a test egyetlen, nem nulla elemével. Korábban már definiáltuk az ilyen elemeket, a test **primitív elem**eit.

Általánosan is megvizsgáljuk egy test multiplikatív csoportjának véges részcsoportjait. Egy ilyen csoport ciklikus, és ha a rendje n, akkor minden eleme gyöke a test fölötti $x^n - e$ polinomnak.

6.10. Definíció

Legyen $\mathcal{K}$ test, e a $\mathcal{K}$ egységeleme, és $n \in \mathbb{N}^+$. $x^n - e \in K[x]$ $\mathcal{K}$ feletti felbontási teste **a** $\mathcal{K}$ **fölötti** n**-edik körosztási test**, és a polinomnak a felbontási testbeli gyökei a $\mathcal{K}$ **feletti** n**-edik egységgyökök**.

Δ

6.11. Megjegyzés

Mivel a $\mathcal{K}$ fölötti n-edik körosztási test felbontási test, ezért létezik és izomorfizmustól eltekintve egyértelmű, továbbá izomorf testek feletti n-edik körosztási testek izomorfak.

Δ

6.12. Jelölés

Legyen $\mathcal{K}$ test és $n \in \mathbb{N}^+$. Az izomorfizmustól eltekintve egyértelműen meghatározott $\mathcal{K}$ feletti n-edik körosztási testet $\mathcal{K}^{(n)}$, és az n-edik egységgyökök $\mathcal{K}^{(n)}$-beli halmazát $E^{(K,n)}$ jelöli.

Δ

$\mathcal{K}^{(n)}$ az $x^n - e$ $\mathcal{K}$ feletti felbontási teste, és $E^{(K,n)}$ a gyökök halmaza, így $\mathcal{K}^{(n)} = \mathcal{K}\left(E^{(K,n)}\right)$.

Legyen $\mathcal{K}$ p-karakterisztikájú test, e a test egységeleme, $n \in \mathbb{N}^+$ és $n = p^r m$, ahol $r \in \mathbb{N}$ és m a p-vel nem osztható pozitív egész. Ekkor a 6.3. Tétel szerint $E^{(K,n)} = E^{(K,m)}$ és $\mathcal{K}^{(n)} = \mathcal{K}^{(m)}$, továbbá $x^n - e$ minden gyöke p^r-szeres, $x^m - e$ valamennyi gyöke egyszeres a megfelelő felbontási test bármely bővítésében, végül 6.6. szerint $\mathcal{E}^{(K,m)}$ m-edrendű ciklikus csoport a $\mathcal{K}^{(n)}$-beli szorzással.

6.13. Definíció

Legyen $n \in \mathbb{N}^+$. Az $E^{(K,n)}$ u eleme **primitív n-edik (egység)gyök $\mathcal{K}$ fölött**, ha a rendje n.

Δ

A definíció és korábbi eredményeink alapján p-karakterisztikájú test fölött akkor és csak akkor van primitív n-edik egységgyök, ha p nem osztója n-nek. A definícióból az is következik, hogy q-elemű test primitív eleme primitív $q - 1$-edik egységgyök.

6.14. Tétel

(Primitív) n-edik egységgyök inverze (primitív) n-edik egységgyök.

Δ

Bizonyítás:

$x^n - e$ reciprok polinom, így nem gyöke a 0, és minden gyökének reciproka is gyöke a polinomnak. Mivel nem nulla elem reciprokának rendje azonos az adott elem rendjével, ezért igaz a primitív egységgyökre vonatkozó állítás is.

□

6.15. Következmény

Véges test primitív elemének reciproka primitív eleme a testnek.

Δ

Bizonyítás:

Test primitív eleme primitív egységgyök.

□

6.16. Tétel

Legyen $n \in \mathbb{N}^+$ és $u \in E^{(K,n)}$. u pontosan egy pozitív egész m-re $\mathcal{K}$ feletti primitív egységgyök, és ez az m nem osztható a test karakterisztikájával.

Δ

Bizonyítás:

Csoport elemének rendje egyértelmű, ezért minden egységgyök legfeljebb egy pozitív egész m-re lehet primitív m-edik egységgyök. Legyen $n \in \mathbb{N}^+$ és $u \in E^{(K,n)}$, ekkor $u^n = e$, vagyis u $\mathcal{K}^{(n)}$ multiplikatív csoportjának véges rendű eleme. Ha $|u| = m$, akkor $u^m = e$, így u gyöke a $\mathcal{K}$ feletti $x^m - e$

polinomnak, és a rendje m, tehát u egy $\mathcal{K}$ feletti primitív m-edik egységgyök. Mivel m a legkisebb azon k pozitív egész kitevők között, amelyekkel $u^k = e$, ezért m nem lehet osztható a test karakterisztikájával (hiszen ha $m = pm'$, akkor $u^{m'} = e$ és $m' < m$).

□

A primitív egységgyökök több különböző, az alábbiakban ismertetendő karakterisztikus tulajdonsággal rendelkeznek.

6.17. Tétel

Legyen $\mathcal{K}$ p-karakterisztikájú test, $p^r m = n \in \mathbb{N}^+$, ahol $r \in \mathbb{N}$ és $p \nmid m \in \mathbb{N}$, és legyen u egy $\mathcal{K}$ feletti m-edik egységgyök. Ekkor az alábbi állítások ekvivalensek:

1. u egy $\mathcal{K}$ feletti primitív m-edik egységgyök;
2. $u \in E^{(K,s)}$, ahol s pozitív egész szám, akkor és csak akkor, ha $m|s$;
3. $E^{(K,n)} = \langle u \rangle$;
4. $v \in E^{(K,n)}$ akkor és csak akkor primitív m-edik egységgyök $\mathcal{K}$ fölött, ha $v = u^k$, ahol $m > k \in \mathbb{N}^+$ és $(k, m) = 1 = (k, n)$.

Δ

Bizonyítás:

Ha u primitív m-edik egységgyök, akkor a rendje m, és csoport egy elemének valamely egész kitevős hatványa akkor és csak akkor egyenlő a csoport egységelemével, ha a kitevő osztható az elem rendjével, így 1-ből következik 2.

Most tegyük fel, hogy 2. teljesül. Ekkor m a legkisebb olyan pozitív egész, amely kitevős hatványa u-nak a csoport egységeleme, így u rendje m. Ekkor u-nak m különböző hatványa van, és minden l egész kitevővel $\left(u^l\right)^n = u^{nl} = u^{p^r ml} = (u^m)^{p^r l} = e$, vagyis $u^l \in E^{(K,n)}$. De $E^{(K,n)}$-nek m eleme van, éppen annyi, amennyi $\langle u \rangle$ rendje, így $E^{(K,n)} = \langle u \rangle$, tehát 2-ből következik 3.

$v \in E^{(K,n)} = \langle u \rangle$-ból $v = u^k$ egy $m > k \in \mathbb{N}$ kitevővel. Ekkor $|v| = \frac{m}{(k,m)}$, és v pontosan akkor primitív m-edik egységgyök, ha a rendje m. Ez akkor és csak akkor teljesül, ha k és m relatív prímek, ami azt jelenti, hogy 3-ból következik 4.

1 relatív prím minden egész számhoz, így m-hez is. Ha teljesül 4., akkor tehát $u = u^1$ $\mathcal{K}$ feletti primitív m-edik egységgyök, vagyis 4-ből megkapjuk 1-et.

□

A 2. ponttal ekvivalens állítás, hogy egy m-edik egységgyök pontosan akkor primitív m-edik egységgyök, ha m-nél kisebb pozitív egész t-re nem t-edik egységgyök. Valóban, egy elem rendje akkor és csak akkor m, ha m-edik hatványa az egységelem, és m a legkisebb ilyen pozitív egész, és egy elem egy hatványa pontosan akkor az egységelem, ha a kitevő osztható az elem rendjével.

6.18. Tétel

Legyen $\mathcal{K}$ p-karakterisztikájú test, $n \in \mathbb{N}^+$, és $n = p^r m$ a nemnegatív r és p-vel nem osztható m pozitív egésszel. A $\mathcal{K}$ fölötti primitív m-edik egységgyökök száma $\varphi(m)$, és ha u egy $\mathcal{K}$ feletti primitív m-edik egységgyök, akkor $\mathcal{K}^{(n)} = \mathcal{K}(u)$ és $x^m - e = \prod_{k=0}^{m-1}\left(x - u^k\right)$.

Δ

Bizonyítás:

$\mathcal{E}^{(K,m)}$ ciklikus csoport, ezért van m-edrendű eleme, például u. Ekkor u mindazon hatványa is generálja a csoportot, amelynek a kitevője relatív prím m-hez. Ezek a hatványok különbözőek, ha $m > k \in \mathbb{N}$, és más, ezektől különböző ilyen tulajdonságú elem nincs a csoportban, ezért a megfelelő tulaj-

donságú u-hatványok száma éppen $\varphi(m)$. $x^m - e$ gyökei egyszeresek és u hatványai, így igaz a szorzatalak. $\mathcal{K}^{(n)} = \mathcal{K}^{(m)}$, ez utóbbi viszont a legszűkebb olyan test, amely tartalmazza $\mathcal{K}$-t és a $\mathcal{K}$ feletti $x^m - e$ valamennyi gyökét. Ám $\mathcal{E}^{(K,m)}$ ciklikus, így ha $\mathcal{K}$ egy $\mathcal{L}$ bővítése tartalmazza $E^{(K,m)}$ egy g generátorelemét, akkor g minden hatványát, tehát $x^m - e$ valamennyi gyökét is tartalmazza, ezért $\mathcal{K}^{(n)} = \mathcal{K}(u)$.

□

A fenti eredményt egy speciális esetre alkalmazva kapjuk az alábbi tételt.

6.19. Tétel

q-elemű test primitív elemeinek száma $\varphi(q-1)$.

Δ

Bizonyítás:

q-elemű test multiplikatív csoportja $q-1$-edrendű ciklikus csoport, és ennek a csoportnak a generátorelemei, vagyis a primitív $q-1$-edik egységgyökök a primitív elemek.

□

Most legyen a csoport egy test feletti egységgyökök csoportja, és a testtel együtt tekintsük a művelettartó leképezést.

6.20. Tétel

Legyen $\mathcal{K}$ és $\mathcal{M}$ test és $n \in \mathbb{N}^+$. Pontosan akkor van olyan $\varphi: \mathcal{K}^{(n)} \to \mathcal{M}$ homomorfizmus, ahol $|\mathrm{Im}(\varphi)| > 1$, ha $M^{(n)} \subseteq M$ és létezik olyan $\mathcal{K}'$, hogy $\mathcal{M}|\mathcal{K}' \cong \mathcal{K}$. Ekkor $\mathcal{Im}(\varphi)$ és csak $\mathcal{Im}(\varphi)$ az $\mathcal{M}$ $\mathcal{K}'$-t tartalmazó és $\mathcal{K}^{(n)}$-nel izomorf részteste, és $\mathcal{Im}(\varphi) = \mathcal{K}'^{(n)} = \mathcal{K}'\left(E^{(M,n)}\right)$.

Δ

Bizonyítás:

Legyen $n = p^r m$, ahol $p = \mathrm{char}(\mathcal{K})$, $r \in \mathbb{N}$ és m a p-vel már nem osztható egész szám.

Testnek csak triviális ideáljai vannak, így test homomorfizmusa is csak triviális lehet, vagyis a képe vagy egyetlen elem, ami nem test, vagy izomorf az eredeti testtel. Ekkor φ $\mathcal{K}$-ra való megszorítása is izomorfizmus, így $\mathcal{K}$ képe az $\mathcal{M}$ egy $\mathcal{K}$-val izomorf részteste, és ez egyben $\mathcal{Im}(\varphi)$-nek is részteste. Az izomorfizmus során az n-edrendű egységgyökök csoportját is leképeztük M-be, és az izomorfizmus következtében a kép m-edrendű csoport, így a 6.6 tétel érelmében ez éppen $E^{(M,m)}$, amely azonban azonos $E^{(M,n)}$-nel. Mivel ez része M-nek, így $M^{(n)} \subseteq M$.

Fordítva, tegyük fel, hogy $\mathcal{M}$ tartalmaz $\mathcal{K}$-val izomorf $\mathcal{K}'$ résztestet, továbbá $M^{(n)} \subseteq M$. Ekkor $E^{(M,n)} \subseteq M$, és $E^{(M,n)}$ az $\mathcal{M}$ feletti $x^n - e_M$ polinom gyökeinek a halmaza. $\mathcal{K}'$ az $\mathcal{M}$ részteste, így $e_M = e_{K'}$, ezért $E^{(M,n)} = E^{(K',n)}$, $\mathcal{L} = \mathcal{K}'\left(E^{(M,n)}\right) = \mathcal{K}'^{(n)}$ és $\mathcal{M}|\mathcal{L}|\mathcal{K}'$. Mivel $\mathcal{K}$ és $\mathcal{K}'$ izomorf, ezért $\mathcal{K}^{(n)}$ és $\mathcal{L}$ is izomorf, tehát létezik a két test között izomorfizmus. Ha egy izomorfizmus φ, akkor $\mathrm{Im}(\varphi) = L$, tehát $\varphi: \mathcal{K}^{(n)} \to \mathcal{M}$ olyan homomorfizmus, hogy $\mathrm{Im}(\varphi)$ legalább kételemű.

Végül, ha $\mathcal{M}|\mathcal{L}'|\mathcal{K}'$ és $\mathcal{L}' \cong \mathcal{K}^{(n)}$, akkor $\mathcal{L}'$ tartalmaz m-edrendű csoportot. De ilyen csak egy van $(M^*;\cdot)$-ban, $\mathcal{E}^{(M,n)}$, így $\mathcal{L}' = \mathcal{K}'\left(E^{(M,n)}\right) = \mathcal{L}$, ami igazolja az egyértelműséget.

□

Megjegyezzük, hogy a tételben csupán az olyan, $\mathcal{K}^{(n)}$-nel izomorf résztest egyértelműségéről van szó, amely egy adott $\mathcal{M}$ test adott $\mathcal{K}'$ résztestének $\mathcal{M}$-beli bővítése. Egyrészt az egységgyököknek akárhány különböző reprezentációja lehetséges, és különböző reprezentációkkal bővítve $\mathcal{K}'$-t, bár a korábbiak alapján izomorf, de nyilván különböző, a $\mathcal{K}^{(n)}$-nel izomorf testeket kapunk. Másrészt $\mathcal{M}$ tartal-

mazhat több különböző, a $\mathcal{K}$-val izomorf résztestet, és ezek tetszőleges bővítése is különböző lesz. Például a komplex számok testének két különböző, bár (algebrailag) izomorf résztestét kapjuk, ha a racionális számok testét e-vel (a természetes logaritmus alapszámával) illetve π-vel bővítjük, és így különböző lesz az ezen testek fölötti azon test is, amelyet ebből a két testből valamely pozitív egész n-re az n-edik komplex egységgyökökkel való bővítéssel kapunk. Ha azonban a $\mathcal{K}$ test véges, akkor a 6.5 Következmény alapján $\mathcal{M}$-ben összesen is csak egyetlen, a $\mathcal{K}^{(n)}$-nel izomorf résztest van.

6.21. Következmény

1. Ha $\mathcal{M}|\mathcal{K}$, akkor $K^{(n)} = K\left(E^{(M,n)}\right)$, és ezzel a $K^{(n)}$-nel $\mathcal{M}^{(n)}\left|\mathcal{K}^{(n)}\right.$;
2. ha $\mathcal{M}|\mathcal{K}$, és σ az $\mathcal{M}^{(n)}$ egy $\mathcal{K}$ feletti relatív automorfizmusa, akkor $\sigma\left(K^{(n)}\right) = K^{(n)}$;
3. ha $\mathcal{L}$ p-karakterisztikájú test, és $\mathcal{K}_P = \mathbb{Q}$, ha $p = 0$, míg $\mathcal{K}_P = \mathbb{Z}_p$, amennyiben p prím, akkor létezik olyan $\varphi: \mathcal{K}_P^{(n)} \to \mathcal{L}^{(n)}$ injektív homomorfizmus, hogy u akkor és csak akkor s-edik egységgyök $\mathcal{K}_P$ felett, ha $\varphi(u)$ s-edik egységgyök $\mathcal{L}$ fölött.

Δ

Bizonyítás:

1. Ha $\mathcal{M}|\mathcal{K}$, akkor $\mathcal{M}^{(n)}|\mathcal{M}$-ből $\mathcal{M}^{(n)}|\mathcal{K}'$, ahol $\mathcal{K}' = \mathcal{K} \cong \mathcal{K}$, így alkalmazható az előző tétel, ami igazolja az állítást.
2. σ az n-edik egységgyököt n-edik egységgyökbe viszi, és mivel automorfizmus invertálható, ezért $\sigma\left(E^{(M,n)}\right) = E^{(M,n)}$, hiszen $\mathcal{M}^{(n)}$-ben csak egy n-edrendű csoport van.
3. $\mathcal{K}_P$ izomorf az $\mathcal{L}$ prímtestével, $\mathcal{L}_P$-vel, így $\mathcal{L}^{(s)}$ tartalmaz $\mathcal{K}_P^{(s)}$-sel izomorf résztestet.

□

Az előbbi következmény utolsó pontja azt jelenti, hogy tetszőleges test feletti bármely (primitív) n-edik egységgyök a prímtest felett is (primitív) n-edik egységgyök, tehát ismerve a prímtestek, vagyis a racionális számok $\mathbb{Q}$ teste és a prímmodulusú $\mathbb{Z}_p$ maradékosztály-gyűrűk feletti egységgyököket, lényegében véve már tetszőleges karakterisztikájú bármely test fölött is rendelkezünk az egységgyökökkel.

Az egységgyökök általában nincsenek benne a megadott testben, csupán annak valamely bővítésében. Ennek ellenére néhány egységgyök benne van az alaptestben, ilyen például a test egységeleme, hiszen egy test és bármely résztestének egységeleme azonos.

6.22. Tétel

Legyen $\mathcal{K}$ q-elemű test, n a q-hoz relatív prím pozitív egész szám, és u egy $\mathcal{K}$ fölötti primitív n-edik egységgyök. Ekkor u^k pontosan akkor eleme K-nak, ha $o_n^+(q-1) = \frac{n}{(q-1,n)} \Big| k$, és a K-beli n-edik egységgyökök az $\mathcal{E}^{(K,n)}$ egy $(q-1,n)$-edrendű, $\mathcal{K}$-beli ciklikus részcsoportját alkotják.

Δ

Bizonyítás:

u^k pontosan akkor eleme K-nak, ha $u^{qk} = \left(u^k\right)^q = u^k$. Mivel u primitív n-edik egységgyök, ezért a rendje n, így $u^{qk} = u^k$ ekvivalens a $qk \equiv k\ (n)$ kongruenciával, vagy ugyanezt másként írva, ha $(q-1)k \equiv 0\ (n)$. Ez pontosan azokra a k egészekre teljesül, amelyek oszthatóak $o_n^+(q-1)$-gyel, és az $n > k \in \mathbb{N}$ feltétellel az ilyen egészek száma $(q-1,n)$. Végül az $E^{(K,n)}$ K-beli elemeinek halmaza nem üres, hiszen az egységelem benne van, és ha két eleme benne van K-ban, akkor a szorzatuk és az inverzük is eleme K-nak, így ezek az elemek részcsoportot alkotnak $\mathcal{E}^{(K,n)}$-ben. Mivel ciklikus csoport minden részcsoportja ciklikus, ezért ez a részcsoport is ciklikus.

□

6.23. Tétel

Ha $\mathcal{K}$ p-karakterisztikájú test, ahol p prímszám, $q = p^s$ egy pozitív egész s-sel, és $\mathcal{L}$ egy q-elemű test, akkor $\mathcal{E}^{(K,q-1)} \cong (L^*;\cdot)$, és $\mathcal{K}^{(q-1)}$ tartalmaz $\mathcal{L}$-lel izomorf résztestet. Ha $\mathcal{K}$ az $\mathcal{L}$ részteste, akkor $\mathcal{K}^{(q-1)} \cong \mathcal{L}$, továbbá $\mathcal{L}$ minden primitív eleme, és csak ezek, $q-1$-edik primitív egységgyök $\mathcal{K}$ fölött.

Δ

Bizonyítás:

p és $q-1$ relatív prímek, így $\mathcal{E}^{(K,q-1)}$ egy $q-1$-edrendű ciklikus csoport, hasonlóan $(L^*;\cdot)$-hoz, így $\mathcal{E}^{(K,q-1)} \cong (L^*;\cdot)$. Mivel $\mathcal{K}$ nulleleme, valamint $E^{(K,q-1)}$ elemei gyökei a $\mathcal{K}$ prímteste feletti $x^q - x$ polinomnak, és az előbbi elemek száma q, ezért ezek az elemek a $\mathcal{K}^{(q-1)}$-beli műveletekkel egy q-elemű résztestet, vagyis $\mathcal{L}$-lel izomorf résztestet alkotnak.

$\mathcal{L}|\mathcal{K}$ esetén $\mathcal{K}^{(q-1)} = \mathcal{K}(L^*) \leq \mathcal{L}$, másrészt $L = L^* \cup \{0\} \subseteq L^* \cup K \subseteq K^{(q-1)}$, így $\mathcal{K}^{(q-1)} = \mathcal{L}$. Most u akkor és csak akkor $q-1$-edik primitív egységgyök a $\mathcal{K}$ test fölött, ha egyben $\mathcal{L}$ fölött is hasonló tulajdonságú, tehát ha a rendje $(L^*;\cdot)$-ban $q-1$. Ezek az elemek viszont éppen az $\mathcal{L}$ test primitív elemei.

□

A tétel azt fejezi ki, hogy minden véges test valamennyi nem nulla eleme valamilyen n-re n-edik, és így alkalmas m-re primitív m-edik egységgyök a test prímteste fölött.

Az alábbiakban egy fontos polinomot definiálunk.

6.24. Definíció

Legyen m a $\mathcal{K}$ test karakterisztikájával nem osztható pozitív egész szám, továbbá u egy $\mathcal{K}$ fölötti primitív m-edik egységgyök. Ekkor $\Phi^{(K,m)} = \prod_{\substack{m>k\in\mathbb{N} \\ (k,m)=1}} \left(x - u^k\right)$ a $\mathcal{K}$ **fölötti m-edik körosztási polinom**.

Δ

Látható, hogy az m-edik körosztási polinom gyökei a test feletti primitív m-edik egységgyökök, és csak ezek, és a polinom minden gyöke egyszeres. A definíció alapján azon és csak azon pozitív egész m-re létezik adott test fölötti m-edik körosztási polinom, amely nem osztható a test karakterisztikájával.

6.25. Tétel

Legyen $\mathcal{K}$ p-karakterisztikájú test, és m a p-vel nem osztható nemnegatív egész. Ekkor $\Phi^{(K,m)}$ egy $\mathcal{K}_P$ feletti $\varphi(m)$-edfokú főpolinom, és $x^m - e = \prod_{d|m} \Phi^{(K,d)}$, ahol $\mathcal{K}_P$ a $\mathcal{K}$ prímteste.

Δ

Bizonyítás:

$\varphi(m)$ a $\mathcal{K}$ feletti m-edik primitív egységgyökök, tehát a polinom gyökeinek száma, és így a körosztási polinom fokszáma, és a körosztási polinom főpolinomok szorzata, tehát maga is főpolinom.

Mivel m nem osztható p-vel, ezért $x^m - e$ gyökei egyszeresek, továbbá mindegyikük egy és csak egy pozitív egészre primitív egységgyök $\mathcal{K}$ fölött, és a megfelelő egész osztója m-nek, ami igazolja $x^m - e$ szorzatfelbontását. Azt kell még belátni, hogy a körosztási polinom együtthatói a prímtest elemei. Ezt indukcióval bizonyítjuk. 1 a p-vel nem osztható nemnegatív egész, tehát megfelel a tétel követelményeinek. Ekkor $x^m - e = x - e \in K_P[x]$, és $x - e = \Phi^{(K,1)}$, vagyis $m = 1$ esetén igaz az állítás. Tegyük fel, hogy már beláttuk a tétel igazságát minden, az $m > k \in \mathbb{N}^+$ feltételt kielégítő k egészre. Ekkor igaz lesz az állítás az m valamennyi valódi osztójára, így az $x^m - e$ és $\prod_{\substack{d|m \\ d<m}} \Phi^{(K,d)}$ $\mathcal{K}_P$ feletti polinomok, de akkor a hányadosuk, $\Phi^{(K,m)}$ is $K_P[x]$-beli.

□

6.26. Megjegyzés

1. Izomorf testek feletti, azonos m-hez tartozó m-edik körosztási testek izomorfak, és ez utóbbi izomorfizmusnál primitív m-edik egységgyök képe primitív m-edik egységgyök, ezért könnyen látható, hogy ha $\psi: \mathcal{K}_1^{(m)} \to \mathcal{K}_2^{(m)}$ a körosztási testek közötti izomorfizmus, és u a $\mathcal{K}_1$ fölötti primitív m-edik egységgyök, akkor $\Phi^{(K_2,m)} = \prod_{\substack{m>k\in\mathbb{N} \\ (k,m)=1}} \left(x - \left(\psi(u)\right)^k\right)$ a $\mathcal{K}_2$ fölötti m-edik körosztási polinom. Ebből kapjuk, hogy ha $\Phi^{(K_1,m)} = \sum_{i=0}^{\varphi(m)} c_i^{(1)} x^i$, akkor $\Phi^{(K_2,m)} = \sum_{i=0}^{\varphi(m)} c_i^{(2)} x^i = \sum_{i=0}^{\varphi(m)} \psi_K\left(c_i^{(1)}\right) x^i$, ahol ψ_K a ψ K_1-re való megszorítása, vagyis izomorf testek fölötti, azonos m-hez tartozó körosztási polinomok lényegében véve azonosak.

2. $\mathrm{char}(\mathcal{K}) = 0$ esetén $\mathcal{K}_P \cong \mathbb{Q}$, és így $\mathcal{K}_P$, és vele együtt $\mathcal{K}$ tartalmaz $\mathbb{Z}$-vel izomorf részgyűrűt. A körosztási polinom főpolinom, így a bizonyításból látható, hogy együtthatói $\mathbb{Z}$-ben vannak. Például a jól ismert n-edik komplex egységgyökök esetén a körosztási polinom egész együtthatós főpolinom.

3. Ha létezik $\Phi^{(K,n)}$, és $n > m|n$, akkor $\Phi^{(K,n)} \left| \frac{x^n-e}{x^m-e} \right.$ (láttuk a 39. oldalon, hogy ha $m|n$, akkor $x^m - e$ osztója $x^n - e$-nek, és $\frac{x^n-e}{x^m-e}$ jelölte a hányadost). Valóban, a megadott $m < n$ és $m|n$ feltétellel $(x^m - e)\Phi^{(K,n)} = \Phi^{(K,n)} \prod_{d|m} \Phi^{(K,d)} \left| \prod_{d|n} \Phi^{(K,d)} = x^n - e \right.$, és innen $x^m - e$-vel való osztással kapjuk az állított oszthatóságot.

Δ

Ha a körosztási polinomot a definíciója alapján szeretnénk meghatározni, akkor ehhez ismerni kellene egy primitív egységgyököt. A valóságban a helyzet általában fordított, egy primitív egységgyök meghatározásához megkeressük ennek a minimál-polinomját, amely viszont a körosztási polinom egy faktora. Szerencsére a körosztási polinomot igen könnyen elő tudjuk állítani.

6.27. Tétel

Ha $\mathcal{K}$ test, és $\mathrm{char}(\mathcal{K}) \nmid n \in \mathbb{N}^+$, akkor $\Phi^{(K,n)} = \prod_{d|n} \left(x^d - e\right)^{\mu\left(\frac{n}{d}\right)}$.

Δ

Bizonyítás:

Ez $x^n - e = \prod_{d|n} \Phi^{(K,d)}$-ből a megfordítási képlet multiplikatív alakjával adódik (lásd az 1.11. Tételt és 1.12. Kiegészítést a 12-13. oldalon).

□

Az 1.13. Megjegyzés alapján a $\Phi^{(K,n)}$ körosztási polinom meghatározása valóban igen egyszerű. Tekintsük n azon d osztóit, amelyekre $\mu(d) = 1$ illetve $\mu(d) = -1$. Ha $g = \prod_{\substack{d|n \\ \mu(d)=1}} \left(x^{\frac{n}{d}} - e\right)$ és $h = \prod_{\substack{d|n \\ \mu(d)=-1}} \left(x^{\frac{n}{d}} - e\right)$, akkor $\Phi^{(K,n)}$ az előbbi két polinom hányadosa, így $\Phi^{(K,n)}$ meghatározása $x^d - e$ alakú, igen egyszerű polinomok szorzásával és két polinom hányadosának a kiszámításával elvégezhető.

6.28. Tétel

Legyen $\mathcal{K}$ q-elemű test, $n \in \mathbb{N}^+$ a q-hoz relatív prím és $r = o_n(q)$. Ekkor $\Phi^{(K,n)}$ $\frac{\varphi(n)}{r}$-számú, páronként különböző, r-edfokú, $\mathcal{K}$ fölött irreducibilis polinom szorzata.

□

Bizonyítás:

Ha $\mathrm{char}(\mathcal{K}) = p$, akkor p prím, és q a p pozitív egész kitevős hatványa, ezért $(n, q) = 1$ következtében n és p relatív prímek, $\Phi^{(K,n)}$ létezik, és a fokszáma pozitív egész. Legyen $\Phi^{(K,n)}$ $\mathcal{K}$ feletti

felbontása irreducibilis polinomok szorzatára $\Phi^{(K,n)} = \prod_{i=1}^{s} m_i^{(K,n)}$. Az előzőek szerint $s \geq 1$. $\Phi^{(K,n)}$ gyökei egyszeresek, ezért az $m_i = m_i^{(K,n)}$ faktorok páronként különbözőek. m_i legalább elsőfokú, így van gyöke, és ez a gyök csak $\Phi^{(K,n)}$ valamelyik gyöke, tehát egy $\mathcal{K}$ felett primitív n-edik egységgyök lehet. Ha ez a gyök u, akkor m_i gyökei pontosan azok az u-hatványok, amelyeknél a kitevő q^j alakú, ahol $o_n(q) > j \in \mathbb{N}$, így a megfelelő faktor foka $o_n(q)$. Valamennyi primitív egységgyök gyöke egy és csak egy faktornak, ezért az előbbi megállapítás minden tényezőre érvényes, tehát ezek mindegyike $o_n(q)$-adfokú. $\Phi^{(K,n)}$ foka $\varphi(n)$, így a tényezők száma $\frac{\varphi(n)}{r}$, ahol r az egyes polinomok fokszáma.

□

6.29. Megjegyzés

A tételben lényeges, hogy a $\mathcal{K}$ test karakterisztikája nem 0, ugyanis majd bebizonyítjuk, hogy 0-karakterisztikájú test feletti körosztási polinom irreducibilis a prímtest fölött (tehát a komplex egységgyökök körosztási polinomjai egész együtthatós, a $\mathbb{Q}$ fölött felbonthatatlan, $\varphi(n)$-edfokú főpolinomok).

□

6.30. Következmény

Ha $\mathcal{K}$ egy p-karakterisztikájú, q-elemű test, $n = p^r n$, ahol r nemnegatív egész, és m a p-vel nem osztható pozitív egész, akkor $\mathcal{K}^{(n)}$ a $\mathcal{K}$ $o_m(q)$-fokú egyszerű bővítése.

Δ

Bizonyítás:

$\mathcal{K}^{(n)} = \mathcal{K}^{(m)} = \mathcal{K}(u)$ az u $\mathcal{K}$ feletti primitív m-edik egységgyökkel. Ez a $\mathcal{K}$ felett felbonthatatlan $o_m(q)$-adfokú polinom gyöke, ebből következik az állítás.

□

A körosztási polinom rendelkezik bizonyos szimmetriával, „elölről hátra” és „hátulról előre” olvasva lényegében véve (előjeltől eltekintve) azonos polinomot kapunk. Az ilyen polinomokat neveztük reciproknak vagy önduálisnak (4.34. Definíció a 89. oldalon), és láttuk, hogy ez pontosan akkor teljesült, amikor a polinom minden gyökének inverze is gyöke volt a polinomnak (azonos multiplicitással).

6.31. Tétel

Körosztási polinom önduális.

Δ

Bizonyítás

Ha k relatív prím n-hez, akkor $-k$ is az, így a körosztási polinom bármely gyökének inverze is gyök, továbbá minden gyök egyszeres.

□

Most megvizsgáljuk a 0-karakterisztikájú test fölötti körosztási polinomot.

6.32. Tétel

0-karakterisztikájú test fölötti körosztási polinom irreducibilis a test prímteste fölött.

Δ

Bizonyítás:

Azt már tudjuk, hogy 0-karakterisztikájú $\mathcal{K}$ test fölötti körosztási polinom lényegében véve egy $\mathbb{Z}$ fölötti főpolinom (lásd a 6.25. Tételt a 113. oldalon, és az utána következő 6.26. Megjegyzést), tehát

egyben egy racionális együtthatós főpolinom, és megegyezik a $\mathbb{Q}$ fölötti körosztási polinommal. A továbbiakban a $\mathbb{Q}$ fölötti m-edik körosztási polinomot a test feltüntetése nélkül, egyszerűen $\Phi^{(m)}$-mel jelöljük. Legyen f a $\Phi^{(m)}$ egy $\mathbb{Q}$ fölött irreducibilis főpolinom osztója, amelynek u egy gyöke. Tekintsünk egy tetszőleges, az m-hez relatív prím p prímszámot, és legyen u^p $\mathbb{Q}$ fölötti minimál-polinomja g. $\Phi^{(m)}$ egész együtthatós főpolinom, így van olyan $\mathbb{Q}$ fölötti irreducibilis polinomokra való felbontása, ahol minden faktor egész együtthatós főpolinom. f és g ilyen faktorok, mivel mind f, mind g irreducibilis főpolinom osztója a körosztási polinomnak. Ha $f \neq g$, akkor relatív prímek (mert mindkettő irreducibilis), így $fg\left|\Phi^{(m)}\right|x^m - 1$. Most legyen $\bar{f}$ és $\bar{g}$ azon $\mathbb{Z}_{\boldsymbol{p}}$ feletti polinom, amelynek együtthatói a megfelelő együtthatók által reprezentált modulo p maradékosztályok. Mivel $fg|x^m - 1$, ezért $\bar{f}\bar{g}\left|x^m - \bar{1}\right.$, ahol $\bar{1}$ a $\mathbb{Z}_{\boldsymbol{p}}$ egységeleme. u^p gyöke g-nek, tehát u gyöke $g \circ x^p$-nek és az u-t tartalmazó modulo p maradékosztály, $\bar{u}$, $\bar{g} \circ x^p = \bar{g}^p$-nek, tehát $\bar{g}$-nek. De u gyöke f-nek, és így $\bar{u}$ $\bar{f}$-nek is gyöke. Ekkor viszont $\bar{u}$ legalább kétszeres gyöke $\bar{f}\bar{g}$-nek, és ekkor $x^m - \bar{1}$-nek, ami lehetetlen, hiszen $(m, p) = 1$, amiből következik, hogy $x^m - \bar{1}$ gyökei egyszeresek.

Eddig azt láttuk be, hogy ha p az m-hez relatív prím prímszám, akkor u és u^p ugyanannak a faktornak a gyöke. Ebből indukcióval adódik, hogy ha u^p-nek és u^k-nak, ahol k relatív prím m-hez, közös a minimál-polinomja, akkor u-nak és u^{kp}-nek is azonos a minimál-polinomja. Ebből viszont következik, hogy a $\mathbb{Q}$ fölötti valamennyi primitív m-edik egységgyök minimál-polinomja azonos, tehát éppen a $\mathbb{Q}$ fölötti m-edik körosztási polinom, és így ez a polinom **Q** fölött felbonthatatlan.

□

A $\mathbb{Q}$ fölötti körosztási polinom minden együtthatója egész szám, ezért bármely q egész szám esetén $\widehat{\Phi}^{(m)}(q)$ egész szám. Mivel a komplex egységgyökök között csupán 1 és -1 valós, és az előbbi $m = 1$-re, az utóbbi pedig $m = 2$-re primitív egységgyök, ezért $m > 2$ esetén $\Phi^{(m)}$ minden gyöke komplex szám. De $\Phi^{(m)}$ valós együtthatós polinom, így $\Phi^{(m)}$ minden gyökével együtt annak konjugáltja is gyöke a polinomnak, és a két gyök különböző. Legyen most u tetszőleges valós szám (m továbbra is nagyobb, mint 2). Ekkor

$$\widehat{\Phi}^{(m)}(u) = \prod_{\substack{\frac{m}{2} > k \in \mathbb{N}^+ \\ (k,m)=1}} \left(u - \varepsilon_k^{(m)}\right)\left(u - \varepsilon_{m-k}^{(m)}\right) = \prod_{\substack{\frac{m}{2} > k \in \mathbb{N}^+ \\ (k,m)=1}} \left(u - \varepsilon_k^{(m)}\right)\left(u - \overline{\varepsilon_k^{(m)}}\right)$$
$$= \prod_{\substack{\frac{m}{2} > k \in \mathbb{N}^+ \\ (k,m)=1}} \left(u - \varepsilon_k^{(m)}\right)\overline{u - \varepsilon_k^{(m)}} = \prod_{\substack{\frac{m}{2} > k \in \mathbb{N}^+ \\ (k,m)=1}} \left|u - \varepsilon_k^{(m)}\right|^2 \in \mathbb{R}^+,$$

vagyis $m > 2$-nél $\Phi^{(m)}$ értéke minden valós u-ra pozitív valós szám. $\Phi^{(1)} = x - 1$ és $\Phi^{(2)} = x + 1$, és ezek is valósak minden valós helyen, de az előbbi csak $u > 1$, míg az utóbbi $u > -1$ esetén pozitív. Továbbra is valós u-val $\widehat{\Phi}^{(1)}(u) > 1$ akkor és csak akkor, ha $u > 2$, és $\widehat{\Phi}^{(2)}(u) > 1$ pontosan akkor, ha $u > 1$. Ha $m > 2$, akkor pedig $u \geq 2$ esetén biztosan igaz, hogy $\widehat{\Phi}^{(m)}(u) > 1$. Valóban, $m > 2$ esetén minden primitív m-edik egységgyök nem valós és abszolút értékben 1, így a képzetes része nem 0 és a valós része (még abszolút értékben is) kisebb, mint 1. Ekkor

$$\left|u - \varepsilon_k^{(m)}\right|^2 = \left(u - \mathrm{Re}\left(\varepsilon_k^{(m)}\right)\right)^2 + \left(-\mathrm{Im}\left(\varepsilon_k^{(m)}\right)\right)^2$$
$$> \left(u - \mathrm{Re}\left(\varepsilon_k^{(m)}\right)\right)^2 > (u-1)^2 \geq 1^2 = 1,$$

és $\widehat{\Phi}^{(m)}(u) = \prod_{\substack{\frac{m}{2} > k \in \mathbb{N}^+ \\ (k,m)=1}} \left|u - \varepsilon_k^{(m)}\right|^2 \geq \left|u - \varepsilon_1^{(m)}\right|^2 > (u-1)^2 \geq 1$. De ha $u \geq 1$ és $(u-1)^2 \geq 1$, akkor $(u-1)^2 \geq u - 1$, tehát $2 \leq q \in \mathbb{N}$ esetén $q - 1 < \widehat{\Phi}^{(m)}(q) \in \mathbb{N}$, ha $m > 1$.

Korábban (lásd a 3.2. Tételt a 44. oldalon) ismertettük Wedderburn tételét, amely szerint minden véges ferdetestben a szorzás kommutatív, minden véges ferdetest test. Ott a tételt nem bizonyítottuk, mert még nem is tudtuk bizonyítani, ugyanis nem álltak rendelkezésünkre olyan ismeretek, amelyekre, mint most majd látjuk, szükségünk van az állítás igazolásához. Magának a tételnek a belátásához azonban még további algebrai fogalmakat kell definiálnunk, és belátnunk bizonyos tulajdonságaikat.

6.33. Definíció

Legyen $\mathcal{S}$ félcsoport, és A az S részhalmaza. Ekkor

a) $N(A) = \{c \in S | cA = Ac\}$ az A **normalizátora**;
b) $C(A) = \{c \in S | \forall (a \in A): ca = ac\}$ az A **centralizátora**;
c) $C = \{c \in S | \forall (a \in S): ca = ac\}$ az $\mathcal{S}$ **centruma**[1].

Csoport és gyűrű normalizátora, centralizátora és centruma a csoport félcsoportjának illetve a gyűrű multiplikatív félcsoportjának normalizátora, centralizátora és centruma.

$C(\{a_1, \dots, a_n\})$ és $N(\{a_1, \dots, a_n\})$ helyett röviden $C(a_1, \dots, a_n)$-et és $N(a_1, \dots, a_n)$-et írunk.

Δ

6.34. Tétel

Ha $\mathcal{S}$ félcsoport és $A \subseteq S$, akkor

1. $u \in N(A)$ akkor és csak akkor, ha az A minden a eleméhez van olyan a_b és a_j elem A-ban, hogy $ua = a_b u$ és $au = ua_j$;
2. $C(A) \subseteq N(A)$, és ha $|A| = 1$, akkor $C(A) = N(A)$;
3. $C = C(S)$;
4. ha minden $\gamma \in \Gamma$-ra $A_\gamma \subseteq S$, akkor $C\left(\bigcup_{\gamma\in\Gamma} A_\gamma\right) = \bigcap_{\gamma\in\Gamma} C(A_\gamma)$;
5. $C(A) = \bigcap_{a\in A} C(a)$, így, ha $A \subseteq B \subseteq S$, akkor $C(B) \subseteq C(A)$;
6. az S minden A részhalmazára $C \subseteq C(A)$;
7. egységelem és zéruselem – ha létezik – eleme a centrumnak;
8. C, $C(A)$ és $N(A)$ zárt az $\mathcal{S}$-beli műveletre, $\mathcal{C} \leq \mathcal{C}(A) \leq \mathcal{N}(A) \leq \mathcal{S}$, és $A \subseteq B \subseteq S$ esetén $\mathcal{C}(B) \leq \mathcal{C}(A)$, feltéve, hogy a megfelelő halmaz nem üres;
9. ha c eleme a normalizátor, centralizátor és centrum valamelyikének, és létezik c inverze, akkor az inverz is eleme a megfelelő halmaznak;
10. $\mathcal{C}$ kommutatív;
11. $\mathcal{S}$ akkor és csak akkor kommutatív, ha $C = S$, és ekkor $C = C(A) = N(A) = S$;

ha $\mathcal{S}$ csoport, akkor

12. $\mathcal{C}$, $\mathcal{C}(A)$ és $\mathcal{N}(A)$ részcsoportok $\mathcal{S}$-ben, és 8. mint részcsoportokra is igaz;
13. $\mathcal{C} \lhd \mathcal{S}$
14. ha $\mathcal{A} \leq \mathcal{S}$, akkor $\mathcal{A} \lhd \mathcal{N}(A)$.

Δ

Bizonyítás:

1. $u \in N(A) \Leftrightarrow uA = Au \Leftrightarrow \forall (a \in A)\left((\exists (a_b \in A): ua = a_b u) \wedge \left(\exists \left(a_j \in A\right): au = ua_j\right)\right)$.
2. $C(A) \subseteq N(A)$ korlátlanul igaz, mert ha $c \in C(A)$, akkor minden $a \in A$-ra $ca = ac$, és így

$$cA = c\bigcup_{a\in A}\{a\} = \bigcup_{a\in A} c\{a\} = \bigcup_{a\in A}\{ca\} = \bigcup_{a\in A}\{ac\} = \bigcup_{a\in A}\{a\}c = \left(\bigcup_{a\in A}\{a\}\right)c = Ac.$$

[1] A centrummal foglalkoztuk a 24. oldalon, de most a többi definiált fogalommal együtt is megvizsgáljuk

Ha $n \in \mathcal{N}(A)$, akkor $nA = An$, tehát A valamennyi a eleméhez van olyan A-beli b, amellyel $na = bn$. De ha A-nak egyetlen eleme van, akkor $b = a$, ez az A összes (tudniillik egyetlen) elemére igaz, $n \in C(A)$, $N(A) \subseteq C(A)$, és a két halmaz egybeesik.

3. Ez közvetlen következménye a centralizátor és a centrum definíciójának.

4. $c \in C\left(\bigcup_{\gamma\in\Gamma} A_\gamma\right)$ akkor és csak akkor, ha minden $\gamma \in \Gamma$-ra és minden $a \in A_\gamma$-ra $ca = ac$, vagyis ha minden γ indexre $c \in C\left(A_\gamma\right)$, tehát ha $c \in \bigcap_{\gamma\in\Gamma} C\left(A_\gamma\right)$.

5. Az előző pont alapján $C(A) = C(\bigcup_{a\in A}\{a\}) = \bigcap_{a\in A} C(a)$, és szintén az előző pont szerint $C(B) = C(B \setminus A)\cap C(A\cap B) \subseteq C(A\cap B)$, és ha $A \subseteq B$, akkor $A\cap B = A$, tehát $C(B) \subseteq C(A)$.

6. $A \subseteq S$, tehát $C = C(S) \subseteq C(A)$ az előző pont eredményéből.

7. Az egységelem és a zéruselem definíciójából azonnal következik.

8. Azt már láttuk, hogy $C \subseteq C(A) \subseteq N(A) \subseteq S$. Legyen c és d a $C(A)$ eleme, és $a \in A$. Ekkor $(cd)a = c(da) = c(ad) = (ca)d = (ac)d = a(cd)$, tehát $cd \in C(A)$. Ha $A = S$, akkor $C(A)$ helyett kapjuk, hogy $\mathcal{C} \leq \mathcal{S}$. Most nézzük A normalizátorát. Ha a fenti egyenletsorban a-t A-val cseréljük ki, akkor kiadódik az $\mathcal{N}(A) \leq \mathcal{S}$ összefüggés. Végül, ha $\mathcal{K} \leq \mathcal{S}$, $\mathcal{L} \leq \mathcal{S}$ és $K \subseteq L$, akkor $\mathcal{K} \leq \mathcal{L}$ is igaz, hiszen $\mathcal{K} \leq \mathcal{S}$-ből $KK \subseteq K \subseteq L$ és $\mathcal{L}$ részfélcsoport, tehát félcsoport, így beláttuk a $\mathcal{C} \leq \mathcal{C}(A) \leq \mathcal{N}(A) \leq \mathcal{S}$ reláció-sort, valamint igazoltuk azt is, hogy $\mathcal{C}(B) \leq \mathcal{C}(A)$.

9. Ha c-nek létezik inverze, és $ca = ac$, akkor $ac^{-1} = c^{-1}a$, így ha c eleme C vagy $C(A)$ valamelyikének, akkor c^{-1} is benne van az adott halmazban. Amennyiben $c \in N(A)$, akkor

$$Ac^{-1} = (eA)c^{-1} = \left((c^{-1}c)A\right)c^{-1} = \left(c^{-1}(cA)\right)c^{-1} = \left(c^{-1}(Ac)\right)c^{-1}$$
$$= c^{-1}\left((Ac)c^{-1}\right) = c^{-1}\left(A(cc^{-1})\right) = c^{-1}(Ae) = c^{-1}A,$$

tehát c^{-1} is eleme a normalizátornak.

10. Mivel S bármely a eleme a C minden elemével felcserélhető, ezért ez érvényes a C-re szorítkozva is, tehát $\mathcal{C}$ kommutatív.

11. $\mathcal{S}$ akkor és csak akkor kommutatív, ha valamennyi eleme a félcsoport minden elemével felcserélhető, vagyis ha bármely eleme benne van a centrumban. Ekkor $\mathcal{C} \leq \mathcal{C}(A) \leq \mathcal{N}(A) \leq \mathcal{S} = \mathcal{C}$-ből kapjuk, hogy a megadott halmazok megegyeznek.

12. Csoport esetében a centrum nem üres, de akkor a többi halmaz sem üres. 8. szerint az egyes részhalmazok zártak a szorzásra, és 9. szerint az inverzre is, így mindegyik részcsoport, és a tartalmazások miatt igaz a részstruktúrákra vonatkozó állítás is.

13. $\mathcal{C}$ részcsoport, és a csoport tetszőleges c elemével $cC = Cc$, tehát $\mathcal{C}$ normálosztó.

14. Amennyiben $\mathcal{A} \leq \mathcal{S}$, akkor A-beli a-val $aA = A = Aa$, tehát $a \in N(A)$, $A \subseteq N(A)$, és mivel $\mathcal{A}$ részcsoportja $\mathcal{S}$-nek, ezért még inkább részcsoportja $\mathcal{N}(A)$-nak, $\mathcal{A} \leq \mathcal{N}(A)$. Vegyük $\mathcal{N}(A)$ tetszőleges n elemét. A definíció miatt $nA = An$, így $\mathcal{A} \lhd \mathcal{N}(A)$.

□

6.35. Definíció

Legyen $\mathcal{G}$ csoport, $\emptyset \neq A \subseteq G$ és c a G eleme. Ekkor cAc^{-1} az A (**c-vel vett**) **konjugáltja**, és A, valamint $B \subseteq G$ **konjugáltak**, ha van olyan $c \in G$, amellyel $cAc^{-1} = B$. Ha $A = \{g\}$, akkor cAc^{-1} helyett cgc^{-1}-et írunk, cgc^{-1} a g (c-vel vett) konjugáltja, és $h \in G$ pontosan akkor konjugáltja g-nek, ha $h = cgc^{-1}$ a G valamely c elemével.

Δ

6.36. Tétel

A konjugáltság ekvivalencia-reláció a $\mathcal{G}$ csoport nem üres részhalmazainak halmazán. Ha G véges, akkor $\emptyset \neq A \subseteq G$ különböző konjugáltjainak száma $|\mathcal{G}: \mathcal{N}(A)|$, míg a $g \in G$ elemmel konjugáltak száma $|\mathcal{G}: \mathcal{C}(g)|$. Ha c centrumelem, akkor a c-vel reprezentált osztály egyelemű.

Δ

Bizonyítás:

Legyen $\emptyset \neq U \subseteq G$, $V \subseteq G$, $u \in G$ és $v \in G$, ekkor $U \sim V$ és $u \sim v$, ha V az U-nak illetve v az u-nak konjugáltja. $eUe^{-1} = U$, tehát $U \sim U$, a reláció reflexív. Ha $U \sim V$, akkor valamely $g \in G$-vel $V = gUg^{-1}$. Ekkor $U = g^{-1}V(g^{-1})^{-1}$, és g^{-1} is a G eleme, vagyis $U \sim V$, $\sim$ szimmetrikus. Végül legyen az előbbieken túl $V \sim W$, ahol W is a G egy nem üres részhalmaza. Most a G egy h elemével $W = hVh^{-1}$, de akkor $W = h(gUg^{-1})h^{-1} = (hg)U(hg)^{-1}$, ami mutatja, hogy W konjugáltja U-nak, hiszen hg is benne van G-ben, így tehát a reláció tranzitív, és összességében ekvivalencia-reláció.

Mivel az elemek konjugálása az egyelemű részhalmazok konjugálása, és ha A-nak egyetlen eleme van, u, akkor minden $g \in G$-vel $gAg^{-1} = g\{u\}g^{-1} = \{gug^{-1}\}$, tehát a halmaz konjugáltja is egyelemű, ezért az elemek konjugáltsága is ekvivalencia-reláció.

$gAg^{-1} = hAh^{-1}$ akkor és csak akkor, amikor $(h^{-1}g)A = A(h^{-1}g)$, vagyis ha $h^{-1}g \in N(A)$, ami ekvivalens azzal a feltétellel, hogy g és h az $\mathcal{N}(A)$ szerinti ugyanazon bal oldali mellékosztályban vannak, így az A különböző konjugáltjait különböző $\mathcal{N}(A)$ szerinti mellékosztályokból vett elemekkel való konjugálással nyerjük, ezek száma pedig éppen $\mathcal{N}(A)$ $\mathcal{G}$-beli indexe. Ha A-nak egyetlen eleme van, és ez g, akkor $N(A) = C(g)$, és ekkor $|\mathcal{G}: \mathcal{N}(A)| = |\mathcal{G}: \mathcal{C}(g)|$.

Ha c a csoport centrumában van, akkor bármely G-beli d-vel $dcd^{-1} = cdd^{-1} = c$, tehát c valamennyi konjugáltja maga c, a c-vel reprezentált osztályban egyetlen elem van.

□

6.37. Definíció

Legyen $\mathcal{G}$ véges csoport, C a csoport centruma, $r \in \mathbb{N}$ a konjugálás legalább kételemű osztályainak és $r \geq i \in \mathbb{N}^+$-ra n_i az i-edik osztály elemeinek a száma. Ekkor $|G| = |C| + \sum_{i=1}^{r} n_i$ az **osztályegyenlet**.

Δ

6.38. Tétel

Legyen $\mathcal{F}$ ferdetest, C az $\mathcal{F}^*$ centruma, $C(g)$ az F^* g elemének $\mathcal{F}^*$-beli centralizátora. Ekkor $\mathcal{F}$ centruma $Z = C \cup \{0\}$, és $\mathcal{Z}$ az $\mathcal{F}$ részteste. $Z(g) = C(g) \cup \{0\}$ a g $\mathcal{F}$-beli centralizátora, ez az $\mathcal{F}$-nek Z-t tartalmazó részferdeteste, és $Z(0) = F$.

Δ

Bizonyítás:

C minden eleme felcserélhető F^* minden elemével és a 0-val, a 0 is felcserélhető F bármely elemével, így Z része $\mathcal{F}$ centrumának. Ugyanakkor, ha F^* valamely u eleme minden F-beli elemmel felcserélhető, akkor ez teljesül a multiplikatív csoport elemeire is, ezért $u \in C \subseteq Z$, Z a test centruma. Z-beli u és v elemekkel $(u - v)a = ua - va = au - av = a(u - v)$, Z zárt a kivonásra, és mivel C a szorzással kommutatív csoport, ezért $\mathcal{Z}$ résztest.

Legyen $0 \neq g$ az F egy eleme. $C \subseteq C(g)$, ezért $C \cup \{0\} \subseteq C(g) \cup \{0\}$. 0 minden elemmel, de akkor g-vel is felcserélhető, viszont a nem nulla v pontosan akkor cserélhető fel g-vel, ha $v \in C(g)$, $Z(g)$ a g centralizátora. Ismét igaz, hogy $\mathcal{C}(g)$ a szorzásra csoport, továbbá $C(g) \cup \{0\} = Z(g)$-beli u-val és v-vel $(u - v)g = ug - vg = gu - gv = g(u - v)$, és így $\mathcal{Z}(g)$ részferdetest $\mathcal{F}$-ben.

Mivel a nullelemmel F minden eleme felcserélhető, ezért igaz az utolsó egyenlőség is.

□

Most visszatérünk Wedderburn tételéhez.

Bizonyítás (***Wedderburn-tétel***)**:**

Az $\mathcal{F}$ véges ferdetest $\mathcal{Z}$ centruma résztest $\mathcal{F}$-ben, így ha Z-nek q eleme van, akkor F elemszáma q^m egy m természetes számmal. Hasonlóan, ha $0 \neq g$, és g-nek egynél több konjugáltja van, akkor $|Z(g)| = q^{m_i}$, feltéve, hogy g az i-edik osztály eleme (F véges, tehát véges sok az egynél több elemet

tartalmazó osztályok száma is). F^*-ban az osztályegyenlet $q^m - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^m-1}{q^{m_i}-1}$ (r az egynél több elemből álló osztályok száma). $\mathcal{F}$ akkor és csak akkor test, ha $r = 0$, ugyanis ez az ekvivalens megfelelője annak, hogy a szorzás a teljes testen kommutatív, azaz minden nem nulla elem benne van a multiplikatív csoport centrumában, ez viszont ugyanaz, mint az $m = 1$ feltétel.

Tegyük fel, hogy $m > 1$. Az egységelem C-nek eleme, ezért minden lehetséges i-re (és $r > 0$ esetén ilyen i van) $m_i < m$. $\frac{q^m-1}{q^{m_i}-1}$ egy $q^m - 1$-elemű csoport $q^{m_i} - 1$-elemű részcsoportjának indexe, tehát egész szám, $q^m - 1$ osztható $q^{m_i} - 1$-gyel, ami csak akkor lehet, ha $m_i | m$ (lásd a 39. oldalon).

Legyen $\Phi^{(m)}$ a $\mathbb{Q}$ fölötti m-edik körosztási polinom. $m_i | m$, tehát $x^{m_i} - 1 | x^m - 1$, és ekkor az is igaz, hogy $\frac{x^m-1}{x^{m_i}-1} \Big| x^m - 1$. Ha m_i valódi osztója m-nek, azaz $m_i < m$, akkor a $\Phi^{(m)} \Big| \frac{x^m-1}{x^{m_i}-1}$ reláció is igaz. Ezek az oszthatóságok tetszőleges egész helyettesítésekor is érvényesek, így például a q helyen is, vagyis $\widehat{\Phi}^{(m)}(q)$ osztója $q^m - 1$-nek és $\sum_{i=1}^{r} \frac{q^m-1}{q^{m_i}-1}$-nek, ezért $q - 1$-nek is. Ez azonban lehetetlen, hiszen korábban láttuk a 116. oldalon, hogy ha $m > 1$ és $q \geq 2$, akkor $\widehat{\Phi}^{(m)}(q) > q - 1$, az oszthatóság nem teljesülhet, m nem lehet 1-nél nagyobb. De ez azt jelenti, hogy a centrum maga a ferdetest, $\mathcal{F}$ kommutatív, azaz test.

□

Végül speciális polinomokat vizsgálunk.

6.39. Definíció

Legyen $\mathcal{S}$ félcsoport, $a \in S$ és $n \in \mathbb{N}^+$. a **n-edik hatvány(elem) $\mathcal{S}$-ben**, ha van S-nek olyan b eleme, amellyel $a = b^n$, ellenkező esetben a **nem n-edik hatvány(elem) $\mathcal{S}$-ben**. Ha a n-edik hatvány $\mathcal{S}$-ben, akkor az S azon b eleme(i), amely(ek) n-edik hatványa a, az a **$\mathcal{S}$-beli n-edik gyöke(i)**. $n = 2$ esetén az n-edik gyök az a **négyzetgyök**e, és ha a-nak van $\mathcal{S}$-ben négyzetgyöke, akkor a **négyzetelem** vagy **kvadratikus elem $\mathcal{S}$-ben**, ellenkező esetben a **nem kvadratikus eleme $\mathcal{S}$-nek**.

Δ

6.40. Tétel

(Bal oldali) neutrális elem és (bal oldali) zéruselem minden pozitív egész n-re n-edik hatvány. Ha $n \in \mathbb{N}^+$-hez az $\mathcal{S}$ kommutatív félcsoportban van n-edik hatvány, akkor az n-edik hatványok részfélcsoportot képeznek $\mathcal{S}$-ben. Egységelemes félcsoportban invertálható n-edik hatvány inverze is n-edik hatvány, így egységelemes kommutatív félcsoport invertálható n-edik hatványainak összessége részcsoport a félcsoportban.

Δ

Bizonyítás:

Nyilván minden elem $n = 1$-re n-edik hatvány. Ha e_b bal oldali neutrális eleme a félcsoportnak, akkor $e_b^2 = e_b \cdot e_b = e_b$, és ha egy pozitív egész n-re $e_b^n = e_b$, akkor $e_b^{n+1} = e_b \cdot e_b^n = e_b \cdot e_b = e_b$, vagyis e_b minden $n \in \mathbb{N}^+$-ra n-edik hatvány a félcsoportban. e_b helyett z_b-t írva, ahol z_b bal oldali zéruselem, kapjuk az ilyen elemekre vonatkozó állítást.

Legyen $S^{(n)}$ az S n-edik hatványainak összessége. Ha a és b az $S^{(n)}$ elemei, akkor S valamely alkalmas u és v elemével $a = u^n$ és $b = v^n$. Ekkor $ab = u^n v^n = (uv)^n = w^n \in S^{(n)}$, hiszen uv eleme S-nek, így $S^{(n)}$ az $\mathcal{S}$-beli művelet megszorításával részfélcsoportja $\mathcal{S}$-nek.

Ha van egységelem, akkor az előbbiek szerint $S^{(n)}$ nem üres. Legyen a egy invertálható n-edik hatvány. Ekkor $a = b^n$ az S egy b elemével, és $e = a^{-1}b^n = (a^{-1}b^{n-1})b$, valamint ehhez hasonlóan $e = b^n a^{-1} = b(b^{n-1}a^{-1})$, így b is invertálható. Ezzel $a^{-1} = (b^n)^{-1} = (b^{-1})^n$, tehát a^{-1} is n-edik hatványa egy S-beli elemnek, a^{-1} is n-edik hatvány S-ben. Ebből következik, hogy egységelemes kommutatív félcsoport invertálható n-edik hatványai csoportot képeznek a félcsoportban.

□

Ha m egy 1-nél nagyobb egész szám, akkor $\mathbb{Z}_m$ egységelemes kommutatív gyűrű, és a gyűrű multiplikatív félcsoportjában az m-hez relatív prímek által reprezentált osztályok csoportot alkotnak. Az n-hez relatív prím egész szám **kvadratikus maradék** modulo m, ha kvadratikus eleme $(\mathbb{Z}_m^*;\cdot)$-nak, ellenkező esetben n **kvadratikus nemmaradék** modulo m.

6.41. Tétel

Legyen $m \in \mathbb{N}^+$, $\mathcal{G}$ m-edrendű ciklikus csoport, a a csoport tetszőleges eleme és n egy pozitív egész szám. a-nak akkor és csak akkor van $\mathcal{G}$-ben n-edik gyöke, ha $a^{\frac{m}{(n,m)}} = e$, ahol e a csoport egységeleme, és ekkor a $\mathcal{G}$-beli gyökeinek száma (n,m). $\mathcal{G}$-ben $\frac{m}{(n,m)}$ n-edik hatvány van.

Δ

Bizonyítás:

Legyen u a csoport egy generátoreleme, ekkor $a = u^k$ egy $m > k \in \mathbb{N}$ kitevővel. Ha $v \in G$ a csoport olyan eleme a csoportnak, hogy $v^n = a$, akkor v is az u egy nemnegatív egész kitevős hatványa, $v = u^l$. a-nak tehát pontosan akkor van n-edik gyöke a csoportban, ha van olyan nem negatív egész l, hogy $u^k = a = v^n = \left(u^l\right)^n = u^{nl}$. Az $u^k = u^{nl}$ egyenlet az m-edrendű u elemmel akkor és csak akkor teljesül, ha $k \equiv nl\ (m)$, vagyis akkor és csak akkor, ha az $nx \equiv k\ (m)$ kongruenciának van megoldása. A kongruencia megoldhatóságának szükséges és elégséges feltétele az $(n,m)|k$ oszthatóság. Ez ekvivalens az $m \left| k\frac{m}{(n,m)} \right.$ oszthatósággal. $a^{\frac{m}{(n,m)}} = u^{k\frac{m}{(n,m)}}$ pontosan akkor azonos a csoport egységelemével, ha teljesül az előbbi oszthatóság, ami igazolja a tétel első állítását. De rögtön kapjuk a második állítás igazolását is, mert ha van a kongruenciának megoldása, akkor a megoldások száma éppen (n,m). Végül a akkor és csak akkor n-edik hatvány $\mathcal{G}$-ben, ha $a^{\frac{q-1}{(n,q-1)}} = e$. Ilyen a eleme biztosan van a csoportnak, például e, ezért az ilyen elemek száma $\left(\frac{m}{(n,qm)}, m\right) = \frac{m}{(n,m)}$, mivel $\frac{m}{(n,m)} \left| m. \right.$

□

Ha $\mathcal{K}$ test, akkor $(K^*;\cdot)$ kommutatív csoport, így a fentiek vizsgálhatóak ebben a struktúrában. Ehhez definiáljuk a binomokat (magyarul a kéttag-okat, a kéttagú kifejezéseket).

6.42. Definíció

Legyen $\mathcal{K}$ test, $a \in K^*$, $b \in K^*$, $n \in \mathbb{N}^+$ és $n > m \in \mathbb{N}$. Ekkor $bx^n + ax^m \in K[x]$ egy $\mathcal{K}$ **feletti binom**.

Δ

Ha egy binom gyökeit akarjuk meghatározni, akkor ehhez elegendő az $x^{n-m} + ab^{-1} = x^r - c$ polinom, hiszen test feletti polinomnak és egy nem nulla konstansszorosának gyökei – multiplicitással együtt – azonosak, ezért a továbbiakban az ilyen alakú binomokat nézzük.

6.43. Definíció

Legyen $x^n - a$ egy $\mathcal{K}$ feletti binom. K^* azon elemei, amelyekre van a polinmnak $\mathcal{K}$-ban gyöke, a K-**beli** n-**edik hatvány**ok, és az egyenlet K-beli valamennyi gyöke az a K-**beli** n-**edik gyöke**.

Δ

Értelemszerűen beszélünk a test azon elemeiről, amelyek nem n-edik hatványok, valamint a kvadratikus és a nem kvadratikus elemekről.

6.44. Tétel

Az $x^n - a \in \mathbb{F}_q[x]$ binomnak pontosan akkor van $\mathbb{F}_q$-ban gyöke, ha $a^{\frac{q-1}{(n,q-1)}} = e$, ahol e a test egységeleme, és ekkor $x^n - a$-nak $(n, q-1)$ gyöke van $\mathbb{F}_q$-ban. $\mathbb{F}_q$-ban $\frac{q-1}{(n,q-1)}$ n-edik hatvány van.

Δ

Bizonyítás:

Ha a testben van gyöke a polinomnak, mondjuk v, akkor $v^n = a \neq 0$, de ekkor v sem lehet a test nulleleme. $\mathbb{F}_q$ multiplikatív félcsoportjában a nullától különböző elemek egy $q-1$-edrendű ciklikus csoportot alkotnak, így a 6.41. tétel közvetlenül alkalmazható $m = q-1$-gyel.

□

Láthatóan a akkor és csak akkor n-edik hatvány $\mathbb{F}_q$-ban, ha $\frac{q-1}{(n,q-1)}$-edik egységgyöke a tetnek, és a 6.22. Tétel szerint az ilyen gyökök száma $\left(\frac{q-1}{(n,q-1)}, q-1\right) = \frac{q-1}{(n,q-1)}$, egyezésben a fenti eredménnyel.

6.45. Következmény

Ha q egy páratlan prímszám hatványa, akkor az $\mathbb{F}_q$-beli kvadratikus elemek és nem kvadratikus elemek száma egyaránt $\frac{q-1}{2}$, és minden kvadratikus elemnek pontosan két négyztegyöke van, míg páros q esetén a test minden nem nulla eleme kvadratikus, és minden ilyen elem két négyzetgyöke egybeesik.

Δ

Bizonyítás:

A fenti tétel eredményeit alkalmazzuk $n = 2$-vel. Páros q esetén $q-1$ páratlan, $(2, q-1) = 1$, amiből következik az ezen esetre vonatkozó állítás. A másik esetben $q-1$ páros, $(2, q-1) = 2$ és $\frac{q-1}{(2,q-1)} = \frac{q-1}{2}$, tehát a kvadratikus elemek száma $\frac{q-1}{2}$, a négyzetgyökök száma 2. Mivel a testnek $q-1$ nem nulla eleme van, ezért a nem kvadratikus elemek száma is $\frac{q-1}{2}$.

□

p-karakterisztikájú test esetén $(p > 0)$ az $a \mapsto a^p$ leképezés automorfizmus, tehát a test önmagára való bijekciója, így a páros q esete éppen ennek a bijekciónak felel meg.

Speciális eset, amikor $a = -e$, ahol e a test egységeleme. Páros q esetén ez nem jelent újdonságot, hiszen ez esetben $-e = e$, és így a polinom gyökei a testbeli egységgyökök. Páratlan elemszámú testről szól a következő eredmény.

6.46. Tétel

Legyen q páratlan prímhatvány, e a q-elemű test egységeleme és n egy pozitív egész szám, amelyre $2^k \| n$. Ekkor $-e$ akkor és csak akkor n-edik hatvány $\mathbb{F}_q$-ban, ha $2^{k+1} | q-1$.

Δ

Bizonyítás:

$-e$ pontosan akkor n-edik hatvány $\mathbb{F}_q$-ban, ha $e = (-e)^{\frac{q-1}{(n,q-1)}} = (-1)^{\frac{q-1}{(n,q-1)}} e$, vagyis akkor és csak akkor, ha $(-1)^{\frac{q-1}{(n,q-1)}} = 1$, vagyis, ha $\frac{q-1}{(n,q-1)}$ páros. Legyen $q-1 = 2^l r$ és $n = 2^k s$, ahol k pozitív és l nem negatív egész szám, és r valamint s páratlan pozitív egész számok. Ekkor n és $q-1$ legnagyobb közös osztója $d = 2^t(r,s)$, ahol t a k és l minimuma, és $\frac{q-1}{(n,q-1)} = 2^{l-t}\frac{r}{(r,s)}$. r, tehát (r,s) páratlan egész szám, így a hányadosuk is páratlan egész szám, és $l-t$ nemnegatív egész szám, ennél fogva

$\frac{q-1}{(n,q-1)}$ akkor és csak akkor páros, ha $l > t$, vagyis akkor és csak akkor, ha $l > k$. Ez viszont éppen azt jelenti, hogy $2^{k+1} | q-1$.

□

6.47. Következmény

Ha q páratlan prímhatvány, n pozitív egész szám és a az $\mathbb{F}_q$ egy n-edik hatványa, úgy $-a$ akkor és csak akkor n-edik hatvány $\mathbb{F}_q$-ban, ha $-e$ n-edik hatványa $\mathbb{F}_q$-nak.

Δ

Bizonyítás:
n-edik hatványok szorzata, valamint n-edik hatvány inverze is n-edik hatvány, és $-a = (-e)a$.

□

6.48. Következmény

Legyen p prímszám és $q = p^s$ egy potzitív egész s-sel. Ekkor $-e$ akkor és csak akkor kvadratikus elem $\mathbb{F}_q$-ban, ha $p = 2$, $p = 4k+1$ vagy $s = 2l$, ahol k és l pozitív egész szám. Amennyiben $-e$ nem kvadratikus eleme $\mathbb{F}_q$-nak, akkor a test bármely $a \neq 0$ elemére a és $-a$ egyike és csak egyike kvadratikus elem a testben, míg az ellenkező esetben vagy mindkét elem kvadratikus, vagy egyikük sem az.

Δ

Bizonyítás:
$n = 2$ esetén $-e$ akkor és csak akkor kvadratikus, ha vagy $e = -e$, vagyis ha $p = 2$, vagy ha 4 osztója $q-1$-nek. Ez utóbbi ekvivalens azzal, hogy $q = 4k+1$ egy pozitív egész k-val. $4k+1$-alakú egész szám minden pozitív egész kitevős hatványa ilyen alakú, míg egy $4k-1$-alakú számnak a páros kitevős és csak a páros kitevős hatványai ilyen alakú egészek.

Legyen $a = b^2$, ahol b az $\mathbb{F}_q$ egy nullától különböző eleme. Ha $-e$ kvadratikus elem, akkor $-a = (-e)a$ mint két kvadratikus elem szorzata maga is kvadratikus. Ellenkező esetben $-a$ nem lehet kvadratikus, mert $-e = (-a)a^{-1}$, a^{-1} kvadratikus, hiszen kvadratikus elem inverze, és ha $-a$ is kvadratikus lenne, akkor $-e$ is ilyen tulajdonságú eleme lenne a testnek. Mivel a testben pontosan a nem nulla elemek fele kvadratikus, ezért az előbbi eredménnyel együtt azt kaptuk, hogy a test egy nullától különböző eleme és ennek ellentettje közül pontosan az egyik kvadratikus a testben.

□

A fenti eredmény szerint nem minden véges testben oldható meg az $x^2 + e = 0$ egyenlet. Ugyanakkor igaz az alábbi állítás.

6.49. Tétel

Tetszőleges véges testben megoldható az $x^2 + y^2 + e = 0$ egyenlet.

Δ

Bizonyítás:
A q-elemű testben $\frac{q-1}{2}$ kvadratikus elem van, így a 0-val együtt $\frac{q+1}{2}$ olyan eleme van a testnek, amely valamely a elem négyzete. De ugyanennyi eleme van a $-b^2 - e$-alakú elemek halmazának. A két halmaz uniója $q+1$ elemű lenne, de a testnek összesen csak q eleme van, így az előbbi két halmaz nem lehet diszjunkt, van legalább egy közös elemük, mondjuk u. Van tehát olyan a és olyan b eleme a testnek, hogy $a^2 = u = -b^2 - e$, és ekkor $a^2 + b^2 + e = 0$.

□

7. Diszkrét Fourier-transzformáció

Elsőként két új gyűrűt definiálunk, amelyekre a diszkrét Fourier-transzformáció épül.

7.1. Tétel

Legyen $\mathcal{R} = (R; +, \cdot)$ gyűrű, $n \in \mathbb{N}^+$, $S = R^n$, és $\mathbf{u} \in S$, $\mathbf{v} \in S$. Ekkor az $(\mathbf{u} +_n \mathbf{v})_i = u_i + v_i$, $(\mathbf{u} \cdot_n \mathbf{v})_i = u_i \cdot v_i$ szabályokkal, ahol $n > i \in \mathbb{N}$, $\mathcal{S} = (S; +_n, \cdot_n)$ gyűrű.

Δ

Bizonyítás:

A gyűrűaxiómák minden komponensre külön-külön teljesülnek, mert ezeket a műveleteket egy gyűrűben végezzük, de akkor a teljes vektorra is teljesülnek, hiszen ezekre a műveletet komponensenként alkalmazzuk. A nullvektor minden komponense $\mathcal{R}$ nulleleme, míg az ellentett vektor i-edik komponense az i-edik komponens ellentettje.

□

7.2. Definíció

$\mathcal{S} = (R^n; +_n, \cdot_n)$ az $\mathcal{R}$ gyűrű n-**szeres direkt összege**.

Δ

7.3. Tétel

Legyen $\mathcal{R} = (R; +, \cdot)$ gyűrű, $n \in \mathbb{N}^+$, $\mathcal{S} = (R^n; +_n, \cdot_n)$, és $\tilde{R} = \{\tilde{r} \in R^n | \forall (n > i \in \mathbb{N}): \tilde{r}_i = r\}$. Ekkor $\varphi: r \mapsto \tilde{r}$ egy $R \to \tilde{R}$ izomorfizmus, és ha $\mathbf{u} \in R^n$, akkor $(\tilde{r} \cdot_n \mathbf{u})_i = r \cdot u_i$ és $(\mathbf{u} \cdot_n \tilde{r})_i = u_i \cdot r$ minden $n > i \in \mathbb{N}$-re.

Δ

Bizonyítás:

φ az R minden eleméhez $\tilde{R}$-nek pontosan egy elemét rendeli, ezért φ R-nek $\tilde{R}$-be való leképezése. Ha $r \neq s$, akkor $\varphi(r) \neq \varphi(s)$, tehát φ injektív, és bármely $\tilde{R}$-beli elem képelem, így φ szürjektív. $\tilde{R} \subseteq R^n$, és $\big(\varphi(r+s)\big)_i = r + s = \big(\varphi(r)\big)_i + \big(\varphi(s)\big)_i$, $\big(\varphi(r \cdot s)\big)_i = r \cdot s = \big(\varphi(r)\big)_i \cdot \big(\varphi(s)\big)_i$, ami igazolja a művelettartást, és így a bijektivitással az izomorfizmust, amiből adódik a műveleti zártság.

A definíció alapján $(\tilde{r} \cdot_n \mathbf{u})_i = \tilde{r}_i \cdot u_i = r \cdot u_i$, és hasonlóan igaz a másik egyenlőség.

□

7.4. Tétel

$\mathcal{R}$ és $\mathcal{S}$ egyszerre (bal oldali) egységelemes illetve kommutatív, és $\mathcal{S}$ pontosan akkor nullosztómentes, ha $n = 1$ és $\mathcal{R}$ nullosztómentes, vagy ha $\mathcal{R}$ a nullgyűrű.

Δ

Bizonyítás:

Legyen $e^{(b)}$ bal oldali egységelem $\mathcal{R}$-ben. Ekkor $\left(\widetilde{e^{(b)}} \cdot_n \mathbf{u}\right)_i = e^{(b)} \cdot u_i = u_i$ az S bármely $\mathbf{u}$ elemére, $\widetilde{e^{(b)}}$ bal oldali egységelem $\mathcal{S}$-ben. Ha viszont $\mathbf{e}^{(b)}$ bal oldali egységeleme $\mathcal{S}$-nek, akkor bármely R-beli u-hoz egy olyan S-beli $\mathbf{u}$-val, amelyben $u_0 = u$, $e_0^{(b)} \cdot u = \left(\mathbf{e}^{(b)} \cdot_n \mathbf{u}\right)_0 = (\mathbf{u})_0 = u$, $e_0^{(b)}$ az $\mathcal{R}$-ben bal oldali egységelem.

Ha $\mathcal{R}$ kommutatív, akkor tetszőleges S-beli $\mathbf{u}$, $\mathbf{v}$ vektorral $(\mathbf{u} \cdot_n \mathbf{v})_i = u_i \cdot v_i = v_i \cdot u_i = (\mathbf{v} \cdot_n \mathbf{u})_i$, az új gyűrű is kommutatív. Fordítva, ha $\mathcal{S}$ kommutatív, és u, v az R elemei, akkor bármely olyan $\mathbf{u}$ és $\mathbf{v}$ vektorral, ahol $u_0 = u$ és $v_0 = v$, írhatjuk, hogy $u \cdot v = (\mathbf{u} \cdot_n \mathbf{v})_0 = (\mathbf{v} \cdot_n \mathbf{u})_0 = v \cdot u$, ami mutatja, hogy az eredeti gyűrűben is felcserélhető bármely pár.

Nézzük az utolsó állítást. Ha $n = 1$, akkor R és S lényegében azonosak, így $\mathcal{R}$ és $\mathcal{S}$ egyszerre nullosztómentes, míg ha R-ben egyetlen elem van, akkor ez a nullelem, és most S is egyetlen elemből áll, $\mathcal{S}$ is nullgyűrű. A többi esetben n nagyobb 1-nél, és R-ben van nullától különböző elem, mondjuk a. Legyen $\mathbf{u}$ az a vektor, amelyben $u_0 = a$, az összes többi komponens 0, míg $\mathbf{v}$ olyan, amelyben $v_0 = 0$, $v_1 = a$, és minden más i-re v_i tetszőleges, ekkor láthatóan sem $\mathbf{u}$, sem $\mathbf{v}$ nem a nullvektor, vagyis nem nullák $\mathcal{S}$-ben, viszont a szorzatvektor valamennyi komponense 0, azaz maga $\mathbf{u} \cdot_n \mathbf{v}$ is $\mathbf{0}$.

□

7.5. Következmény

Legyen $\mathcal{R} = (R; +, \cdot)$ gyűrű, $n \in \mathbb{N}^+$, és $\mathcal{S} = (R^n; +_n, \cdot_n)$. Az $r \times_b \mathbf{u} = \tilde{r} \cdot_n \mathbf{u}$, $\mathbf{u} \times_j r = \mathbf{u} \cdot_n \tilde{r}$ szabállyal, ahol $r \in R$ és $\mathbf{u} \in R^n$, $\mathcal{S}$ kétoldali $\mathcal{R}$-modulus, amely pontosan akkor unitér, ha $\mathcal{R}$ egységelemes. $\mathcal{S}$ akkor és csak akkor algebra $\mathcal{R}$ fölött, ha $\mathcal{R}$ test, és ekkor az algebra rangja n.

Δ

Bizonyítás:

Az előbbiek szerint $\mathcal{R}$ és $\tilde{\mathcal{R}} \leq \mathcal{S}$ izomorf az $r \mapsto \tilde{r}$ megfeleltetéssel, így a 2.2. Tétel szerint $\mathcal{S}$ kétoldali $\mathcal{R}$ modulus a tételben megfogalmazott szabályokkal. $\mathcal{S}$ és $\mathcal{R}$ egyszerre egységelemes, és ha $\mathcal{R}$ egységeleme e, akkor $\tilde{e}$ egységelem $\mathcal{S}$-ben, a modulus unitér.

Ha $\mathcal{R}$ test, akkor egységelemes, tehát a modulus unitér. A szorzás kommutatív a testben, és a direkt összegben is teljesül a szorzás kommutativitása, így algebrát kapunk, ha viszont $\mathcal{R}$ csak ferdetest, akkor nem minden elemmel teljesül a felcserélhetőség. Legyen $n > i \in \mathbb{N}$-re $\mathbf{e}^{(i)} \in R^n$ olyan, hogy $e_j^{(i)} = \delta_{i,j} e$, ahol $n > j \in \mathbb{N}$. Ekkor $\mathbf{u} \in R^n$-nel $\mathbf{u} = \sum_{i=0}^{n-1} \left(c_i \times_b \mathbf{e}^{(i)}\right)$ pontosan akkor teljesül, ha minden $n > j \in \mathbb{N}$ indexre $u_j = \left(\sum_{i=0}^{n-1} \left(c_i \times_b \mathbf{e}^{(i)}\right)\right)_j = \sum_{i=0}^{n-1} \delta_{i,j} c_i = c_j$, vagyis $\left\{\mathbf{e}^{(i)} \middle| n > i \in \mathbb{N}\right\}$ $(R; +)$-nak mint $\mathcal{R}$ fölötti lineáris térnek bázisa, így az algebra rangja n.

□

7.6. Jelölés

Legyen $a \in \mathbb{R}$, $b \in \mathbb{R}^*$. Ekkor $a^{(b)} = a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor$.

Δ

Könnyen ellenőrizhető, hogy $0 \leq \frac{a^{(b)}}{b} < 1$, továbbá ha $i \in \mathbb{Z}$ és $n \in \mathbb{N}^+$, akkor $n > i^{(n)} \in \mathbb{N}$, és $i^{(n)} \equiv i \ (n)$, vagyis $i^{(n)}$ az i n-nel való osztásakor keletkező nemnegatív maradéka.

7.7. Definíció

Legyen $\mathcal{R}$ gyűrű, $n \in \mathbb{N}^+$, $\mathbf{u}$ és $\mathbf{v}$ az R^n elemei, és $w_i = \sum_{j=0}^{n-1} u_j v_{(i-j)^{(n)}}$ a $\mathbf{w}$ i-edik komponense. Ekkor $\mathbf{w} = \mathbf{u} * \mathbf{v}$ az **u és v (ciklikus) konvolúciója**. Ha $\mathbf{a}$ és $\mathbf{b}$ az R^{2n} olyan elemei, amelyek legalacsonyabb indexű n komponense azonos $\mathbf{u}$-val illetve $\mathbf{v}$-vel, és a többi komponensük 0, akkor az $\mathbf{a}$ és $\mathbf{b}$ – R^{2n}-beli – ciklikus konvolúciója az **u és v (lineáris) konvolúciója**, ezt $\mathbf{w} = \mathbf{u} \circ \mathbf{v}$ jelöli.

Δ

Látható, hogy a lineáris konvolúció az R^n-beli párokhoz R^{2n} egy elemét rendeli.

7.8. Tétel

Ha $\mathcal{R} = (R; +,\cdot)$ gyűrű, és $n \in \mathbb{N}^+$, akkor $\mathcal{T} = (R^n; +_n,*)$ is gyűrű, ahol a $\mathcal{T}$-beli $+_n$ a komponensenkénti $\mathcal{R}$-beli összeadás. Az $\bar{R} = \{\bar{r} \in R^n | n > i \in \mathbb{N}: r_i = \delta_{0,i} r\}$ halmaz a $\mathcal{T}$-nek $\mathcal{R}$-rel izomorf részgyűrűje, és ha $\mathbf{u} \in T$, akkor $(\bar{r} * \mathbf{u})_i = r \cdot u_i$ és $(\mathbf{u} * \bar{r})_i = u_i \cdot r$.

Δ

Bizonyítás:

Az összeadásra teljesülnek a feltételek. $*$ az R^n bármely két elemére értelmezett, az eredmény is n-komponensű, és valamennyi komponens az R egyértelműen meghatározott eleme, hiszen $\mathcal{R}$-beli szorzással és összeadással áll elő, így $*$ binér művelet R^n-en.

Most nézzük a műveleti tulajdonságokat.

$$\big((\mathbf{u} * \mathbf{v}) * \mathbf{w}\big)_i = \sum_{j=0}^{n-1} (\mathbf{u} * \mathbf{v})_j w_{(i-j)^{(n)}} = \sum_{j=0}^{n-1} \left(\sum_{k=0}^{n-1} u_k v_{(j-k)^{(n)}} \right) w_{(i-j)^{(n)}}$$
$$= \sum_{k=0}^{n-1} \left(u_k \sum_{j=0}^{n-1} v_j w_{((i-k)-j)^{(n)}} \right) = \sum_{k=0}^{n-1} u_k (\mathbf{v} * \mathbf{w})_{(i-k)^{(n)}} = \big(\mathbf{u} * (\mathbf{v} * \mathbf{w})\big)_i,$$

$$\big((\mathbf{u} +_n \mathbf{v}) * \mathbf{w}\big)_i = \sum_{j=0}^{n-1} (\mathbf{u} +_n \mathbf{v})_j w_{(i-j)^{(n)}} = \sum_{j=0}^{n-1} \big(u_j +_n v_j\big)_j w_{(i-j)^{(n)}}$$
$$= \sum_{j=0}^{n-1} u_j w_{(i-j)^{(n)}} + \sum_{j=0}^{n-1} v_j w_{(i-j)^{(n)}} = (\mathbf{u} * \mathbf{w} +_n \mathbf{v} * \mathbf{w})_i,$$

így $*$ asszociatív, és disztributív az összeadás fölött (a bal oldali disztributivitás bizonyítása hasonló).

Az nyilvánvaló, hogy $\bar{R} \subseteq R^n$, és $\varphi: r \mapsto \bar{r}$ bijekció R és $\bar{R}$ között, másrészt könnyen belátható, hogy $\overline{r + s} = \bar{r} +_n \bar{s}$ és $\overline{r \cdot s} = \bar{r} * \bar{s}$, tehát φ művelettartó, azaz $\mathcal{T}$ műveleteinek $\bar{R}$-re való megszorításával $\mathcal{R}$-rel izomorf részgyűrűt kapunk $\mathcal{T}$-ben. $(\bar{r} * \mathbf{u})_i = \sum_{j=0}^{n-1} \bar{r}_j u_{(i-j)^{(n)}} = \bar{r}_0 \cdot u_i = r \cdot u_i$, hiszen $\bar{r}_j$ legfeljebb csak $j = 0$ esetén nem 0, és a másik egyenlőség ugyanígy igazolható.

□

7.9. Tétel

$n \in \mathbb{N}^+$-ra az $\mathcal{R} = (R; +,\cdot)$ és $\mathcal{T} = (R^n; +_n,*)$ gyűrű egyszerre (bal oldali) egységelemes illetve kommutatív, és $\mathcal{T}$ pontosan akkor nullosztómentes, ha $n = 1$ és $\mathcal{R}$ nullosztómentes, vagy $\mathcal{R}$ nullgyűrű.

Δ

Bizonyítás:

Ha $e^{(b)}$ bal oldali egységelem $\mathcal{R}$-ben, akkor $\overline{e^{(b)}}_j v_{(i-j)^{(n)}}$ csupán $j = 0$ esetén különbözhet nullától, és ekkor az értéke v_i, tehát a konvolúció eredménye az eredeti $\mathbf{v}$ vektor, $\overline{e^{(b)}}$ balról egységelem. Most tegyük fel, hogy $\boldsymbol{\varepsilon}_b$ bal oldali egységelem $\mathcal{T}$-ben. Ekkor $\delta_{0,i} v = \bar{v}_i = (\boldsymbol{\varepsilon}_b * \bar{v})_i = \varepsilon_i^{(b)} v$, vagyis $\varepsilon_0^{(b)}$ bal oldali egységelem $\mathcal{R}$-ben.

$(\mathbf{u} * \mathbf{v})_i = \sum_{j=0}^{n-1} u_j v_{(i-j)^{(n)}} = \sum_{j=0}^{n-1} v_{(i-j)^{(n)}} u_j = \sum_{j=0}^{n-1} v_j u_{(i-j)^{(n)}} = (\mathbf{v} * \mathbf{u})_i$, ha $\mathcal{R}$ kommutatív, mert mialatt a j szummációs index 0-tól $n-1$-ig minden értéket egyszer és csak egyszer felvesz, ezalatt $(i-j)^{(n)}$ is ugyanezt teszi, és amikor v indexe j, akkor u indexe $i - j$ modulo n maradéka, tehát $\mathcal{T}$ is kommutatív. Ha viszont $*$ kommutatív, akkor ez igaz $\bar{\mathcal{R}}$-ban, és így a vele izomorf $\mathcal{R}$-ben is.

Az $n = 1$ illetve $|R| = 1$ eset hasonló a direkt összegnél látotthoz. Most legyen $n > 1$ és $|R| > 1$, továbbá $a \in R^*$. Ha $\mathbf{u}$ minden komponense a, míg $\mathbf{v}$ első két komponense a és $-a$, a többi 0, akkor

a két vektor egyaránt különbözik $\mathcal{T}$ nullelemétől, viszont a konvolúciójuk valamennyi komponense 0 lesz, tehát két nem nulla vektor szorzata nulla, az új gyűrű nem nullosztómentes.

□

A bizonyításban $\delta_{0,i}v = \bar{v}_i = (\boldsymbol{\varepsilon}_b * \bar{v})_i = \varepsilon_i^{(b)}v$ biztosan 0, ha $n > i \in \mathbb{N}^+$, vagyis $i \neq 0$, bármelyik eleme is legyen v az $\mathcal{R}$ gyűrűnek. Ebből azonban nem következik, hogy a nem nulla i indexekre $\varepsilon_i^{(b)} = 0$. Legyen $m = u^{t+1}v$, ahol t és v pozitív egész, míg u egynél nagyobb egész szám, és tekintsük az $u\mathbb{Z}_m$ gyűrűt (könnyű ellenőrizni, hogy ez valóban gyűrű). Ha α ennek egy eleme, akkor $\alpha = u\bar{r} = \overline{ur}$ egy $\mathbb{Z}_m$-beli $\bar{r}$-rel, és $\overline{u^tv} \cdot \alpha = \overline{u^tv} \cdot \overline{ur} = \overline{u^tvur} = \overline{u^{t+1}vr} = \overline{mr} = r\bar{m} = r\bar{0} = \bar{0}$, de $\overline{u^tv} \neq \bar{0}$, vagyis lehet egy nem zérógyűrűnek olyan nem nulla eleme, amellyel a gyűrű bármely elemét szorozva a nullát kapjuk. Általában, ha $\emptyset \neq X \subseteq R$, és a a gyűrű olyan eleme, hogy minden $r \in X$-re $ar = 0$, akkor a **bal oldali annullátor**a X-nek. Hasonlóan definiáljuk a **jobb oldali annullátor**t, és ha a egyszerre bal és jobb oldali annullátora az X halmaznak, akkor a **annullátor**a X-nek. Az X bal oldali annullátorainak B halmaza bal oldali ideálja a gyűrűnek, és ha X maga is bal oldali ideál, akkor B ideálja $\mathcal{R}$-nek. Ha a gyűrűben van jobb oldali egységelem, akkor az R olyan részhalmazának, amely tartalmaz legalább egy jobb oldali egységelemet, nem lehet a 0-n kívül más bal oldali annullátora, hiszen ha a bal oldali annullátor, és $e^{(j)}$ egy jobb oldali egységelem, akkor $0 = ae^{(j)} = a$.

Visszatérve a fenti tételhez, ha $\mathcal{R}$-ben van bal oldali egységelem, és van a nullától különböző bal oldali annullátor is, akkor $\mathcal{R}$ egy bal oldali egységeleméhez több különböző bal oldali egységelem tartozik $\mathcal{T}$-ben. Ha viszont $\mathcal{R}$ egységelemes, akkor az egyetlen bal oldali annullátor a 0, és így egy és csak egy bal oldali egységelem lesz $\mathcal{T}$-ben, amely egyben egységelem is, nevezetesen e, vagyis az az elem, amelynek a nulla-indexű komponense $\mathcal{R}$ egységeleme, és valamennyi további komponense 0.

7.10. Következmény

Legyen $\mathcal{R}$ gyűrű, $n \in \mathbb{N}^+$, és $r \times_b \mathbf{u} = \bar{r} * \mathbf{u}$, $\mathbf{u} \times_j r = \mathbf{u} * \bar{r}$, ahol $r \in R$ és $\mathbf{u} \in R^n$. Ekkor $\mathcal{T}$ kétoldali $\mathcal{R}$ modulus, amely akkor és csak akkor unitér, ha $\mathcal{R}$ egységelemes, és ez a modulus pontosan akkor algebra, ha $\mathcal{R}$ test, és ekkor az algebra rangja n.

Δ

Bizonyítás:

$\mathcal{R} \cong \bar{\mathcal{R}} \leq \mathcal{T}$ a $\varphi: r \mapsto \bar{r}$ szabállyal, így a 2.2. Tétel szerint $\mathcal{T}$ $\mathcal{R} - \mathcal{R}$ modulus. $\mathcal{T}$ pontosan akkor egységelemes, ha $\mathcal{R}$ egységelemes, és ekkor az $\mathcal{R}$ e egységelemének képe egységelem a $\mathcal{T}$ gyűrűben, a modulus unitér. Ha $\mathcal{R}$ ferdetest, és része $\mathcal{T}$ centrumának, akkor $\mathcal{R}$ kommutatív, vagyis test, és algebrát kapunk. Legyen $n > i \in \mathbb{N}$-re $\mathbf{e}^{(i)} \in R^n$ úgy, hogy $e_j^{(i)} = \delta_{i,j}e$, ha $n > j \in \mathbb{N}$. Ekkor $\mathbf{u} \in R^n$-re $\mathbf{u} = \sum_{i=0}^{n-1}\left(c_i \times_b \mathbf{e}^{(i)}\right)$ pontosan akkor teljesül, ha $u_j = \left(\sum_{i=0}^{n-1}\left(c_i \times_b \mathbf{e}^{(i)}\right)\right)_j = \sum_{i=0}^{n-1}\delta_{i,j}c_i = c_j$ minden $n > j \in \mathbb{N}$-re, vagyis $\left\{\mathbf{e}^{(i)} \middle| n > i \in \mathbb{N}\right\}$ az $(R; +)$ $\mathcal{R}$ fölötti vektortérnek bázisa, így az algebra rangja n.

□

A továbbiakban $+_n$ és $\cdot_n$ helyett $+$-t és $\cdot$-ot írunk (illetve az utóbbit el is hagyhatjuk).

7.11. Tétel

Legyen $n \in \mathbb{N}^+$, $\mathcal{K}$ test, továbbá $\mathbf{A}_z^{(K,n)}$ a K^n fölötti olyan n-edrendű kvadratikus mátrix, amelyben az $n > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$ indexekre $a_{i,j}^{(z)} = \left(z^{-i}\right)^j$, ahol $z \in E^{(K,n)}$. $\mathbf{A}_z^{(K,n)}$ szimmetrikus, és pontosan akkor van inverze, ha $|z| = n$, és ekkor $\mathbf{A}_z^{(K,n)^{-1}} = (ne)^{-1}\mathbf{A}_{z^{-1}}^{(K,n)}$ a test e egységelemével.

Δ

Ha nyilvánvaló, hogy melyik testről van szó, és mi az n értéke, akkor $\mathbf{A}_z^{(K,n)}$ helyett egyszerűen $\mathbf{A}_z$-t írunk, valamint a továbbiakban $\mathbf{A}_z^{(K,n)}$ mindig a fentebb definiált mátrixot jelöli.

Bizonyítás:

$a_{i,j}^{(z)} = \left(z^{-i}\right)^j = \left(z^{-j}\right)^i = a_{j,i}^{(z)}$, így $\mathbf{A}_z = \mathbf{A}_z^T$, tehát $\mathbf{A}_z$ szimmetrikus.

$\mathbf{A}_z$-ben a 0 indexű sor minden eleme e. Ha $t < n$, és z t-edik egységgyök, akkor $\mathbf{A}_z$-ben a t-edik sor megegyezik a 0. sorral, így a mátrix nem reguláris, tehát biztosan nem invertálható.

Legyen most $t = n$, azaz z primitív n-edik egységgyök. Ekkor

$$(\mathbf{A}_z \cdot \mathbf{A}_{z^{-1}})_{i,k} = \sum_{j=0}^{n-1} a_{i,j}^{(z)} a_{j,k}^{(z^{-1})} = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j \left(z^j\right)^k = \sum_{j=0}^{n-1} \left(z^{k-i}\right)^j = \sum_{j=0}^{n-1} \left(z^{(k-i)^{(n)}}\right)^j.$$

Jelöljük $(k-i)^{(n)}$-et m-mel. i és k korlátjaiból $-(n-1) \leq k-i \leq n-1$, így m akkor és csak akkor 0, ha $i = k$, vagyis $z^m = e$ pontosan akkor teljesül, ha $i = k$, és ekkor az összeg éppen ne. $i \neq k$ esetén $z^m - e \neq 0$, ugyanakkor $\sum_{j=0}^{n-1} \left(z^{(k-i)^{(n)}}\right)^j = \frac{(z^m)^n - e}{z^m - e} = 0$, vagyis $\mathbf{A}_z \cdot \mathbf{A}_{z^{-1}}$ főátlójában ne, azon kívül 0 áll, $\mathbf{A}_z \cdot \mathbf{A}_{z^{-1}} = (ne)\mathbf{I}_n$, ahol $\mathbf{I}_n$ a $\mathcal{K}^{(n)}$ fölötti n-edrendű egységmátrix. Végül, ha z primitív n-edik egységgyök, akkor n nem osztható a test karakterisztikájával, így ne nem a nullelem, tehát létezik az inverze, és akkor $\mathbf{A}_z((ne)^{-1}\mathbf{A}_{z^{-1}}) = \mathbf{I}_n$, ami éppen azt jelenti, hogy $(ne)^{-1}\mathbf{A}_{z^{-1}}$ inverze az eredeti $\mathbf{A}_z$ mátrixnak.

□

Most $\mathbf{A}_z$ segítségével kapcsolatot keresünk a K^n felett korábban konstruált két gyűrű között. Előtte azonban nézzük meg, hogy mi lesz az $\{\mathbf{A}_z\mathbf{u} | \mathbf{u} \in K^n\}$ halmaz. Legyen először $\mathbf{u}$ olyan, hogy valamennyi komponense 0, kivéve a 0-indexűt, amely a K test egy tetszőleges c elemével egyenlő. Ekkor $U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = u_0 = c$, így $K^n \subseteq \{\mathbf{A}_z\mathbf{u} | \mathbf{u} \in K^n\}$. Másodszor nézzük azt a vektort, amelynek ismét minden komponense 0, kivéve most az utolsót, az $n-1$ indexhez tartozót, amely ezúttal legyen a test egységeleme, azaz e. Ebben az esetben $U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = \left(z^{-i}\right)^{n-1} u_{n-1} = z^i e = z^i$, ami viszont azt mutatja, hogy $z^i \in \{(\mathbf{A}_z\mathbf{u})_i | \mathbf{u} \in K^n\}$, így egy olyan test, amely tartalmazza a képvektorok i-indexű komponenseit, biztosan tartalmazza $K\left(z^i\right)$-t. Ugyanakkor ebben a testben bármilyen $\mathbf{u} \in K^n$ esetén benne van $\sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j$, tehát $\mathcal{K}\left(z^i\right)$ a legszűkebb test, amely a képvektorok i-indexű elemeit tartalmazza. Ez igaz $i = 1$ esetén is, és mivel tetszőleges i egész szám esetén $K\left(z^i\right) \subseteq K(z)$, ezért minden olyan $\mathcal{L}$ test, amellyel $\{\mathbf{A}_z\mathbf{u} | \mathbf{u} \in K^n\} \subseteq L^n$, a $\mathcal{K}(z)$ bővítése, amely lehet éppen $\mathcal{K}(z)$ is.

Most legyen $\varphi: K^n \to L^n$ a $\varphi: \mathbf{u} \mapsto \mathbf{A}_z\mathbf{u}$ szabállyal, és legyen $|z| = m$. Ekkor $m|n$, és

$$U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = \sum_{j=0}^{n-1} \left(z^{-(i \bmod m)}\right)^j u_j = U_{i \bmod m},$$

$$U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = \sum_{j=0}^{n-1} \left(z^{-i}\right)^{j \bmod m} u_{m\left\lfloor \frac{j}{m} \right\rfloor + (j \bmod m)} = \sum_{j=0}^{m-1} \left(z^{-i}\right)^j \sum_{l=0}^{\frac{n}{m}-1} u_{lm+j}.$$

A fenti eredményből látszik, hogy ha $m < n$, akkor az $\mathbf{u} \mapsto \mathbf{A}_z\mathbf{u}$ megfeleltetés sem szürjektív, sem injektív (az első tulajdonság közvetlenül leolvasható, míg a másodikhoz legyen például $\mathbf{u}$ egyszer olyan, amelynek csak a 0-indexű komponense nem 0, és másodszor olyan, amelyben csak az m-indexű komponens különbözik nullától, és ez a komponens azonos az előbbi vektor 0-indexű komponensével).

7.12. Tétel

Legyen $n \in \mathbb{N}^+$, $\mathcal{K}$ test, $z \in E^{(K,n)}$, és $\mathcal{L}|\mathcal{K}(z)$. Ekkor $\mathbf{u} \mapsto \mathbf{A}_z\mathbf{u}$ egy $\varphi\colon (K^n;+,*) \to (L^n;+,\cdot)$ algebra-homomorfizmus, amely pontosan akkor izomorfizmus, ha $|z| = n$ és $L \subseteq K$.

Δ

Bizonyítás:

Azt már a tétel kimondása előtt beláttuk, hogy $\mathrm{Im}(\varphi) \subseteq \big(K(z)\big)^n$, és az is nyilván igaz, hogy K^n minden elemére $\mathbf{A}_z\mathbf{u}$ egyértelműen meghatározott, így φ valóban K^n-nek L^n-be való leképezése.

Nézzük először a művelettartást. $\mathbf{A}_z(a\mathbf{u}+b\mathbf{v}) = a(\mathbf{A}_z\mathbf{u}) + b(\mathbf{A}_z\mathbf{v})$, ahol a és b K, $\mathbf{u}$ és $\mathbf{v}$ K^n elemei, így φ modulus-homomorfizmus. Speciális esetként φ összegtartó, és

$$\begin{aligned}\big(\mathbf{A}_z(\mathbf{u}*\mathbf{v})\big)_i &= \sum_{j=0}^{n-1}\big(z^{-i}\big)^j(\mathbf{u}*\mathbf{v})_j = \left(\sum_{j=0}^{n-1}\big(z^{-i}\big)^j\sum_{k=0}^{n-1}u_k v_{(j-k)^n}\right)\\ &= \sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\Big(\big(z^{-i}\big)^k u_k\Big)\Big(\big(z^{-i}\big)^{(j-k)^{(n)}} v_{(j-k)^{(n)}}\Big)\\ &= \left(\sum_{k=0}^{n-1}\big(z^{-i}\big)^k u_k\right)\left(\sum_{j=0}^{n-1}\big(z^{-i}\big)^j v_j\right) = (\mathbf{A}_z\mathbf{u})_i(\mathbf{A}_z\mathbf{v})_i = \big((\mathbf{A}_z\mathbf{u})\cdot(\mathbf{A}_z\mathbf{v})\big)_i,\end{aligned}$$

így φ szorzattartó is, tehát a φ leképezés valóban algebra-homomorfizmus.

Legyen $|z| = m$. Izomorfizmushoz szükséges a bijekció, így L nem lehet bővebb $K(z) = K^{(m)}$-nél. Ha $m < n$, akkor láttuk, hogy a leképezés nem szürjektív, és így nem is izomorfizmus. A továbbiakban legyen $m = n$. Ekkor létezik $\mathbf{A}_z$ inverze, és $\mathbf{A}_z\mathbf{u}_1 = \mathbf{A}_z\mathbf{u}_2$ csak úgy lehetséges, ha $\mathbf{u}_1 = \mathbf{u}_2$, vagyis a leképezés biztosan injektív. Ha $\mathbf{U} \in K^{(n)^n}$-ben $U_l = \delta_{i,(l+1)^{(n)}}(ne)$, akkor $(\mathbf{A}_z^{-1}\mathbf{U})_i = z^i$, és ha a leképezés szürjektív, akkor az előbbi $\mathbf{U}$ is eleme a képhalmaznak, ami csak úgy lehetséges, ha $z \in K$. Ez mutatja, hogy izomorfizmushoz szükséges az $L \subseteq K(z) \subseteq K$ feltétel. Végül legyen $\mathbf{w}$ a $\mathcal{K}$ feletti tér egy eleme. Ekkor $\mathbf{A}_z^{-1}\mathbf{w} = (ne)^{-1}\mathbf{A}_{z^{-1}}\mathbf{w}$ is benne van K^n-ben, és így $\mathbf{w} = \mathbf{A}_z(\mathbf{A}_z^{-1}\mathbf{w})$, a hozzárendelés szürjektív is, és akkor φ bijektív, és a művelettartással együtt izomorfizmus.

□

7.13. Kiegészítés

Ha $z \in K$ primitív n-edik egységgyök, akkor $\mathbf{A}_z^{-1}(\mathbf{U}\cdot\mathbf{V}) = (\mathbf{A}_z^{-1}\mathbf{U}) * (\mathbf{A}_z^{-1}\mathbf{V})$.

Δ

Bizonyítás:

Ha z primitív n-edik egységgyök, akkor létezik $\mathbf{A}_z^{-1}$, és a tételben megadott leképezés bijektív és művelettartó, így a képelemek szorzatának egyértelmű őse a szintén egyértelmű ősök konvolúciója.

□

A továbbiakban általában $\mathbf{A}_z\mathbf{u}$-t $\mathbf{U}$, és ha $\mathbf{A}_z$-nek van inverze, akkor $\mathbf{A}_z^{-1}\mathbf{U}$-t $\mathbf{u}$ jelöli, továbbá ha a K^n-beli $\mathbf{u}$ vektorra $u^T = (u_0, \dots, u_{n-2}, u_{n-1})$, akkor $\mathbf{u}_{\rightarrow}$ az $u^T = (u_{n-1}, u_0, \dots, u_{n-2})$ által meghatározott vektor, $\mathbf{U}^{\rightarrow} = \mathbf{A}_z\mathbf{u}_{\rightarrow}$, és ha z primitív n-edik egységgyök, akkor $\mathbf{u}^{\rightarrow} = \mathbf{A}_z^{-1}\mathbf{U}_{\rightarrow}$. Kiterjesztve tetszőleges egész k-ra, $u^T_{\underrightarrow{(k)}} = \Big(u_{(0-k)^{(n)}}, \dots, u_{(n-1-k)^{(n)}}\Big)$, és ennek transzformáltja $\mathbf{U}^{\overrightarrow{(k)}}$. Könnyen látható, hogy $\mathbf{u}_{\underrightarrow{(k)}} = \Big(\mathbf{u}_{\underrightarrow{(k-1)}}\Big)_{\rightarrow}$. Az előbbihez hasonlóan definiáljuk $\mathbf{U}_{\underrightarrow{(k)}}$-t és $\mathbf{u}^{\overrightarrow{(k)}}$-t.

7.14. Tétel

Legyen $\mathcal{K}$ test, $z \in E^{(K,n)}$ és $\mathbf{u} \in K^n$. Ekkor

1. $\sum_{i=0}^{n-1} u_i = U_0$, és $\sum_{i=0}^{n-1} U_i = nu_0$, ha $|z| = n$;
2. ha $\mathbf{U} = \mathbf{A}_z\mathbf{u}$, akkor $\left(\mathbf{U}^{\overrightarrow{(k)}}\right)_i = \left(z^k\right)^{-i} U_i$, és ha $|z| = n$, akkor $\left(\mathbf{u}^{\overrightarrow{(k)}}\right)_i = \left(z^k\right)^i u_i$.

Δ

Bizonyítás:

1. $\sum_{i=0}^{n-1} u_i = \sum_{i=0}^{n-1} (z^{-0})^i u_i = U_0$, ami igazolja az első állítást. Ha viszont z primitív n-edik egységgyök, akkor $(ne)^{-1} \sum_{i=0}^{n-1} U_i = (ne)^{-1} \sum_{i=0}^{n-1} (z^0)^i U_i = u_0$, tehát $\sum_{i=0}^{n-1} U_i = nu_0$.
2. Közvetlenül látszik, hogy K^n-beli $\mathbf{v}$ vektorra $\left(\mathbf{v}_{\overrightarrow{(k)}}\right)_i = v_{(i-k)^{(n)}}$. Ebből és a definícióból

$$\left(\mathbf{U}^{\overrightarrow{(k)}}\right)_i = \left(\mathbf{A}_z \mathbf{u}_{\overrightarrow{(k)}}\right)_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j \left(\mathbf{u}_{\overrightarrow{(k)}}\right)_j = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_{(j-k)^{(n)}}$$
$$= \sum_{j=0}^{n-1} \left(z^{-i}\right)^{j+k} u_j = z^{-ki} \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = z^{-ki} U_i = \left(z^k\right)^{-i} U_i.$$

A másik összefüggés igazolása hasonló, figyelembe véve, hogy a megadott feltétellel $ne \neq 0$.

□

A fenti eredményből $k = 1$ esetén $(\mathbf{U}^{\rightarrow})_i = z^{-i} U_i$, és, ha létezik, akkor $(\mathbf{u}^{\rightarrow})_i = z^i u_i$.

Kérdés, hogyan változik $\mathbf{A}_z\mathbf{u}$, ha z helyett egy másik egységgyököt alkalmazunk. Absztrakt testben az azonos rendű egységgyökök között nincs különbség, így elvárható, hogy a transzformáció lényegében véve azonos marad, ha z-t egy vele azonos rendű egységgyökkel helyettesítjük.

7.15. Jelölés

Legyen $n \in \mathbb{N}^+$, $k \in \mathbb{N}$ és $\mathbf{u} \in K^n$. Ekkor $\mathbf{u}^{(k)} \in K^n$ jelöli azt a vektort, amelynek $n > i \in \mathbb{N}$-indexű komponense $u_i^{(k)} = \left(\mathbf{u}^{(k)}\right)_i = u_{(ki)^{(n)}}$.

Δ

7.16. Tétel

Tetszőleges egész k-ra $\mathbf{A}_{z^k}\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(k)}$, és ha z primitív n-edik egységgyök, akkor bármely y n-edik egységgyökhöz van olyan $k \in \mathbb{N}$, hogy $\mathbf{A}_y\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(k)}$.

Δ

Bizonyítás:

A transzformáció definícióját alkalmazva

$$\left(\mathbf{A}_{z^k}\mathbf{u}\right)_i = \sum_{j=0}^{n-1} \left(\left(z^k\right)^{-i}\right)^j u_j = \sum_{j=0}^{n-1} \left(z^{-ki}\right)^j u_j$$
$$= \sum_{j=0}^{n-1} \left(z^{-(ki)^{(n)}}\right)^j u_j = (\mathbf{A}_z\mathbf{u})_{(ki)^{(n)}} = \left((\mathbf{A}_z\mathbf{u})^{(k)}\right)_i.$$

Ha $|z| = n$, akkor minden n-edik egységgyök z egy n-nél kisebb nemnegatív egész kitevős hatványa, így valamilyen nemnegatív egész k-val $y = z^k$, és a fentiekből következik a második állítás.

□

7.17. Kiegészítés

Legyen $n \in \mathbb{N}^+$ és k az n-hez relatív prím egész. Ekkor $\mathbf{A}_z\mathbf{u}^{(k)} = (\mathbf{A}_z\mathbf{u})^{(k')}$, ahol $kk' \equiv 1\ (n)$.

Δ

Bizonyítás:

Ha k és n relatív prím, akkor a $kx \equiv 1\ (n)$ kongruencia megoldható, tehát k' létezik, és

$$\left(\mathbf{A}_z\mathbf{u}^{(k)}\right)_i = \sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_{(kj)^{(n)}} = \sum_{j=0}^{n-1}\left(z^{-i}\right)^{\left(k'j\right)^{(n)}} u_j$$
$$= \sum_{j=0}^{n-1}\left(z^{-\left(k'i\right)^{(n)}}\right)^j u_j = (\mathbf{A}_z\mathbf{u})_{\left(k'i\right)^{(n)}} = \left((\mathbf{A}_z\mathbf{u})^{(k')}\right)_i.$$

Ez a transzformált vektor minden komponensére igaz, tehát $\mathbf{A}_z\mathbf{u}^{(k)} = (\mathbf{A}_z\mathbf{u})^{(k')}$.

□

Ha k relatív prím n-hez, akkor $n > i \in \mathbb{N}$-re az $i \mapsto (ki)^{(n)}$ szabály az indexek permutációja, így a tétel azt jelenti, hogy különböző primitív n-edik egységgyökökkel végezve a leképezést, csupán a kép komponenseinek sorrendje más. Az alábbi következményre jutunk.

7.18. Következmény

Legyen $n \in \mathbb{N}^+$, és $\mathcal{L}$ olyan test, hogy $L^{(n)} \subseteq L$, σ az $\mathcal{L}$ automorfizmusa, és $\mathcal{K}$ az $\mathcal{L}$ legbővebb részteste, amelyen σ az identikus leképezés, $\boldsymbol{\sigma}$ a σ L^n-re való komponensenkénti kiterjesztése, és z primitív n-edik egységgyök. Ekkor

1. van olyan, az n-hez relatív prím $n > k \in \mathbb{N}$, hogy L^n-beli $\mathbf{u}$-ra $\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = \mathbf{A}_{z^k}\boldsymbol{\sigma}(\mathbf{u})$;
2. $\mathbf{u} \in K^n$ akkor és csak akkor, ha $\boldsymbol{\sigma}(\mathbf{U}) = \mathbf{U}^{(k)}$;
3. $\mathbf{u} \in K^n$-re $\mathbf{U}$ akkor és csak akkor K^n-beli, ha $\mathbf{u} = \mathbf{u}^{(k')}$, ahol $kk' \equiv 1\ (n)$ a fentebbi k-val, és ekkor $\mathbf{U} = \mathbf{U}^{(k)}$.

Δ

Bizonyítás:

1. Automorfizmusnál n-edik egységgyök képe n-edik egységgyök, primitív n-edik egységgyöké primitív n-edik egységgyök, így van olyan $n > k \in \mathbb{N}$, hogy $\sigma(z) = z^k$ és $(k, n) = 1$. Ekkor

$$\left(\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u})\right)_i = \sigma((\mathbf{A}_z\mathbf{u})_i) = \sigma\left(\sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j\right) = \sum_{j=0}^{n-1}\left(\left(\sigma(z)\right)^{-i}\right)^j \sigma(u_j)$$
$$= \sum_{j=0}^{n-1}\left(\left(z^k\right)^{-i}\right)^j \sigma(u_j) = \left(\mathbf{A}_{z^k}\boldsymbol{\sigma}(\mathbf{u})\right)_i,$$

és az előző tételből kapjuk az első állítást.

2. $\mathbf{u} \in K^n$ akkor és csak akkor teljesül, ha $\boldsymbol{\sigma}(\mathbf{u}) = \mathbf{u}$. Most egyrészről $\mathbf{U}^{(k)} = (\mathbf{A}_z\mathbf{u})^{(k)} = \mathbf{A}_{z^k}\mathbf{u}$, másrészt $\boldsymbol{\sigma}(\mathbf{U}) = \boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = \mathbf{A}_{z^k}\boldsymbol{\sigma}(\mathbf{u})$, ennélfogva pontosan akkor lesz $\mathbf{U}^{(k)} = \boldsymbol{\sigma}(\mathbf{U})$, amikor $\mathbf{A}_{z^k}\mathbf{u} =$

$\mathbf{A}_{z^k}\boldsymbol{\sigma}(\mathbf{u})$. z^k primitív n-edik egységgyök, tehát $\mathbf{A}_{z^k}$ invertálható, így az előbbi egyenlőség pontosan akkor igaz, ha $\mathbf{u} = \boldsymbol{\sigma}(\mathbf{u})$, vagyis $\mathbf{u} \in K^n$ és $\boldsymbol{\sigma}(\mathbf{U}) = \mathbf{U}^{(k)}$ ekvivalens feltételek

3. $\mathbf{U} \in K^n$ akkor és csak akkor teljesül, ha $\boldsymbol{\sigma}(\mathbf{U}) = \mathbf{U}$, tehát K^n-beli $\mathbf{u}$-val pontosan akkor, ha $\mathbf{A}_z\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(\boldsymbol{k})} = \mathbf{A}_z\mathbf{u}^{(k')}$, vagyis ha $\mathbf{u} = \mathbf{u}^{(k')}$, és ekkor $\mathbf{U} = \mathbf{A}_z\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(\boldsymbol{k})} = \mathbf{U}^{(k)}$.

□

Legyen először $\mathcal{L} = \mathbb{C}$ (a komplex számok teste) és $\sigma: a \mapsto \bar{a}$ ($\bar{a}$ szokásos módon az a konjugáltja). Ekkor $\mathcal{K} = \mathbb{R}$ (ahol $\mathbb{R}$ a valós számok teste), és az $\mathbf{u} \in \mathbb{R}^n$ feltételhez szükséges és elégséges a $\boldsymbol{\sigma}(\mathbf{U}) = \mathbf{U}^{(-1)}$ egyenlőség. Valóban, $z \mapsto \bar{z}$ bijektív és műveletartó $\mathbb{C}$-n, tehát automorfizmus, és $\mathbb{R}$ a $\mathbb{C}$ legbővebb olyan részteste, amelyben a konjugálás az identikus leképezés. z most n-edik komplex egységgyök, tehát $\bar{z} = z^{-1} = z^{n-1}$, ezért $k = n - 1$, és $(\mathbf{A}_z\mathbf{u})^{(n-1)} = (\mathbf{A}_z\mathbf{u})^{(-1)}$.

A második esetként legyen $\mathcal{L} = \mathbb{F}_{q^m}$, ahol $m \in \mathbb{N}^+$, $\sigma: a \mapsto a^{q^l}$ a pozitív egész l-lel, és legyen $d = (m, l)$. $\tilde{q} = q^d$-vel, $\tilde{m} = \frac{m}{d}$-vel és $\tilde{l} = \frac{l}{d}$-vel $\mathcal{L} = \mathbb{F}_{\tilde{q}^{\tilde{m}}}$, $\sigma: a \mapsto a^{\tilde{q}^{\tilde{l}}}$ és $(\tilde{m}, \tilde{l}) = \tilde{d} = 1$, így a továbbiakban feltesszük, hogy m és l relatív prímek. Ekkor $\mathcal{K} = \mathbb{F}_q$, és $\mathbf{u} \in K^n$ akkor és csak akkor teljesül, ha $\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = (\mathbf{A}_z\mathbf{u})^{(q^l)} = \mathbf{U}^{(q^l)}$. Ez azért igaz, mert q-elemű test bármely bővítésén $a \mapsto a^{q^l}$ automorfizmus, és ez z-t z^{q^l}-be viszi, továbbá ez a leképezés L elemei közül pontosan K elemeit hagyja helyben (mert $0 \neq u \in L$-re $u^{q^m-1} = e, u = u^{q^l}$ pontosan akkor igaz, ha $u^{q^l-1} = e$, és a két egyenlőség együtt akkor és csak akkor teljesül, ha $e = u^{(q^m-1, q^l-1)} = u^{q^{(m,l)}-1} = u^{q-1}$, azaz ha $u^q = u$), vagyis $\mathcal{K}$ az $\mathcal{L}$-ben foglalt maximális olyan résztest, amelyen a transzformáció megszorítása az identikus leképezés.

A speciális esetek jelentését közelebbről is megnézzük.

Ha $\mathbf{u}$ valós vektor, akkor $\overline{(\mathbf{A}_z\mathbf{u})_k} = (\mathbf{A}_z\mathbf{u})_{(-k)^{(n)}}$. Ebből következik, hogy $(\mathbf{A}_z\mathbf{u})_0$ valós, és 0-nál nagyobb, de n-nél kisebb i egészre $\overline{(\mathbf{A}_z\mathbf{u})_i} = (\mathbf{A}_z\mathbf{u})_{n-i}$ (tehát ha n páros, mondjuk $n = 2m$, akkor az m-edik komponens is valós), ami azt jelenti, hogy csupán $\left\lceil\frac{n+1}{2}\right\rceil$ komponens lehet független (esetleg még ennyi sem). Ez visszafelé is igaz, vagyis ha az $\mathbf{u}$ komplex vektor $\mathbf{U}$ transzformáltjának konjugáltja azonos $\mathbf{U}^{(-1)}$-gyel, akkor $\mathbf{u}$ valós. Ha $k = -1$, akkor k' is -1, vagyis $\mathbf{u} = \mathbf{u}^{(k')}$ most, mint az előbb $\mathbf{U}$-nál, azt jelenti, hogy $u_i = u_{(n-i) \bmod n}$. Valós $\mathbf{u}$ esetén ha ez teljesül, és csak ekkor, $\mathbf{U}$ minden komponense valós, és a vektor minden komponensére $U_i = U_{(n-i) \bmod n}$.

A véges testre vonatkozó eset azt jelenti, hogy ha a vektor komponensei a q-elemű testből vannak, akkor a transzformált vektor $\left(q^l i\right)^{(n)}$-indexű komponense az eredeti vektor i indexéhez tartozó komponensének q^l-edik hatványa. Legyen r_i a legkisebb pozitív egész, amelyre $i\left(q^l\right)^{r_i} \equiv i\ (n)$. q és n relatív prím, mert a test karakterisztikája nem osztója n-nek, így van ilyen r_i kitevő, nevezetesen $r_i = o_{o_n^+(i)}\left(q^l\right) = \frac{o_{o_n^+(i)}(q)}{\left(o_{o_n^+(i)}(q), l\right)} = o^+_{o_{o_n^+(i)}(q)}(l)$, és ha $l = 1$, akkor egyszerűbben $r_i = o_{o_n^+(i)}(q)$. Most $r_i > t \in \mathbb{N}$-re U_i meghatározza $\mathbf{U}\left(\left(q^l\right)^t i\right)^{(n)} = \left(q^{lt} i\right)^{(n)}$-indexű komponenseit. Ekkor

$$U_{\left(\left(q^l\right)^{r_i} i\right)^{(n)}} = U_i^{\left(q^l\right)^{r_i}} = \left(\sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j\right)^{\left(q^l\right)^{r_i}} = \sum_{j=0}^{n-1}\left(\left(z^{-i}\right)^j\right)^{\left(q^l\right)^{r_i}} u_j$$
$$= \sum_{j=0}^{n-1}\left(z^{-i\left(q^l\right)^{r_i}}\right)^j u_j = \sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j = U_i,$$

amint annak lennie is kell, hiszen $\left(\left(q^l\right)^{r_i} i\right)^{(n)} = i$. $U_i^{\left(q^l\right)^{r_i}} = U_i$ azt jelenti, hogy U_i eleme a $\left(q^l\right)^{r_i}$-elemű testnek, és mivel eleme a q^m-elemű testnek, ezért a két test metszetének is. Ennek mérete q^s, ahol $s = (m, lr_i) = (m, r_i)$ (mert $(m, l) = 1$).

Fordítva, ha **U**-ban minden $n > i \in \mathbb{N}$ indexre teljesül, hogy a $\left(q^l i\right)^{(n)}$ indexű komponens megegyezik U_i q^l-edik hatványával, akkor **u** a q-elemű $\mathcal{K}$ test n-szeres direkt összegéhez tartozó vektor.

Végül legyen **u** ismét $\mathbb{F}_q$ feletti. Most **U** akkor és csak akkor $\mathbb{F}_q^n$-beli, ha $u_i = u_{\left(q^{l'} i\right)^{(n)}}$, ahol l' az l ellentettje modulo $o_n(q)$, vagyis $l' = (-l) \bmod o_n(q)$, és ebben az esetben $U_i = U_{\left(q^l i\right)^{(n)}}$.

Lássunk egy példát. Legyen $q = 3, m = 3, l = 2$ és $n = 13$. Ekkor $q^m = 27$ és $(m, l) = (3,2) = 1$, vagyis $\mathcal{K} = \mathbb{F}_3$ és $\mathcal{L} = \mathbb{F}_{27}$. $n = 13|26 = 27 - 1$, így az is teljesül, hogy $L^{(n)} \subseteq L$. Most $q^l = 3^2 = 9$, azaz $\sigma(v) = v^9$ az L elemeire, és ha $v \in K$, akkor $\sigma(v) = v^9 = v$. Nézzük $13 > i \in \mathbb{N}$-re $\left(q^l i\right)^{(n)} = (9i)^{(13)}$-at:

i	0	1	2	3	4	5	6	7	8	9	10	11	12
$(9i)^{(13)}$	0	9	5	1	10	6	2	11	7	3	12	8	4

A táblázat alapján öt diszjunkt ciklus van:

$$\begin{array}{lllllllll} 0 & \to & 0 & & & & & & \\ 1 & \to & 9 & \to & 3 & \to & 1 & & \\ 2 & \to & 5 & \to & 6 & \to & 2 & & \\ 4 & \to & 10 & \to & 12 & \to & 4 & & \\ 7 & \to & 11 & \to & 8 & \to & 7 & & \end{array}$$

és ennek megfelelően kapjuk – az egyelemű osztályt elhagyva – a transzformált vektor komponenseit:

$$\begin{array}{lllllllll} U_1 & \to & U_9 = U_1^9 & \to & U_3 = U_9^9 = U_1^{81} = U_1^3 & \to & U_1 = U_3^9 = U_1^{27} = U_1 \\ U_2 & \to & U_5 = U_2^9 & \to & U_6 = U_5^9 = U_2^{81} = U_2^3 & \to & U_2 = U_6^9 = U_2^{27} = U_2 \\ U_4 & \to & U_{10} = U_4^9 & \to & U_{12} = U_{10}^9 = U_4^{81} = U_4^3 & \to & U_4 = U_{12}^9 = U_4^{27} = U_4 \\ U_7 & \to & U_{11} = U_7^9 & \to & U_8 = U_{11}^9 = U_7^{81} = U_7^3 & \to & U_7 = U_8^9 = U_7^{27} = U_7 \end{array}$$

A táblázat mutatja, hogy 0 kivételével minden i-re $r_i = 3$. Valóban: $o_n^+(i) = o_{13}^+(i) = \frac{13}{(13,i)} = 13$ valamennyi i-re, hiszen 13 prímszám. Ekkor mindegyik i-re r_i értéke azonos, elegendő $i = 1$-re meghatározni. $o_{13}(9)$ osztója $\varphi(13) = 12$-nek, ezért csak 1, 2, 3, 4, 6 és 12 lehet a rend. 1 csupán 1-nek a rendje. $9^2 = 81 \equiv 3 \not\equiv 1\ (13)$, tehát még 2 sem a keresett rend, ám $9^3 \equiv 9 \cdot 3 = 27 \equiv 1\ (13)$, így megkaptuk $r_1 = 3$-at, és akkor minden más, a 13-nál kisebb pozitív egész i-re $r_i = 3$-at. Ez egyben azt is jelenti, hogy U_0 kivételével a transzformált vektor mindegyik eleme a 27-elemű test bármely eleme lehet (míg U_0 szükségszerűen K-beli). Az, hogy minden ciklus (a 0-t tartalmazó kivételével) azonos hosszúságú, és a transzformált vektor minden eleme a teljes test bármely eleme lehet, nem általánosan igaz, csupán ennek a példának egy sajátsága.

Most $l' = (-l) \bmod o_n(q) = (-2) \bmod 3 = 1$, így ha $13 > i \in \mathbb{N}$-re $u_{(3i)^{(13)}} = u_i \in \mathbb{F}_3$, akkor $U_{(9i)^{(13)}} = U_i^9 = U_i \in \mathbb{F}_3$.

Lineáris térben definiálják vektorok skalárszorzatát. Mi ennek legegyszerűbb formáját adjuk meg, majd röviden megvizsgáljuk, hogy az eddigiek hogyan illeszkednek ehhez a skalárszorzathoz.

7.19. Definíció

Legyen $\mathcal{K}$ test, **u** és **v** a K^n két eleme, ahol $n \in \mathbb{N}^+$. Ekkor **u** és **v belső szorzata** vagy **skalárszorzata** $(\mathbf{u}, \mathbf{v}) = \sum_{i=0}^{n-1} u_i v_i$.

Δ

7.20. Tétel

Legyen $\mathcal{K}$ test, n pozitív egész szám, z $\mathcal{K}$ feletti primitív n-edik egységgyök, $\mathbf{u}$ és $\mathbf{v}$ a K^n két eleme, $\mathbf{w} = \mathbf{uv}$, k az n-hez relatív prím egész, és k' olyan egész, amelyre $kk' \equiv 1\ (n)$. Ekkor

a) $\left(\mathbf{u}^{(k)} * \mathbf{v}\right)_i = \left(\mathbf{u}, \left(\mathbf{v}^{(-k')}\right)_{\underrightarrow{(-i)}}\right)$;
b) $\left(\mathbf{u} * \mathbf{v}^{(-1)}\right)_0 = (\mathbf{u}, \mathbf{v}) = W_0$;
c) $(\mathbf{U}, \mathbf{v}) = (\mathbf{A}_z\mathbf{u}, \mathbf{v}) = (\mathbf{u}, \mathbf{A}_z\mathbf{v}) = (\mathbf{u}, \mathbf{V})$.

Δ

Bizonyítás:

a) $\left(\mathbf{u}^{(k)} * \mathbf{v}\right)_i = \sum_{j=0}^{n-1} u_{(kj)^{(n)}} v_{(i-j)^{(n)}} = \sum_{j=0}^{n-1} u_j v_{\left(i-k'j\right)^{(n)}}$, és a $\left(\mathbf{v}^{(-k')}\right)_{\underrightarrow{(-i)}}$ vektor j-indexű komponense éppen a $\mathbf{v}$ vektor $\left((-k'j)^{(n)} - (-i)\right)^{(n)} = (i - k'j)^{(n)}$ indexhez tartozó eleme.

b) Az előző pontból és a definíciókból közvetlenül kapjuk az $i = 0$, $k = -1$ értékekkel.

c) $(\mathbf{A}_z\mathbf{u}, \mathbf{v}) = (\mathbf{u}, \mathbf{A}_z^T\mathbf{v})$, és $\mathbf{A}_z^T = \mathbf{A}_z$, tehát $(\mathbf{U}, \mathbf{v}) = (\mathbf{u}, \mathbf{V})$.

□

7.21. Következmény

Legyen $\mathcal{K}$ test, n pozitív egész szám, z $\mathcal{K}$ feletti primitív n-edik egységgyök, és $\mathbf{u}$ és $\mathbf{v}$ a K^n két eleme. Ekkor $(\mathbf{U}, \mathbf{V}) = n\left(\mathbf{u}, \mathbf{v}^{(-1)}\right)$.

Δ

Bizonyítás:

$(\mathbf{U}, \mathbf{V}) = (\mathbf{U}, \mathbf{A}_z\mathbf{v}) = \left(\mathbf{u}, \mathbf{A}_z(\mathbf{A}_z\mathbf{v})\right) = \left(\mathbf{u}, \mathbf{A}_z\left(\mathbf{A}_{z^{-1}}\mathbf{v}^{(-1)}\right)\right) = \left(\mathbf{u}, n\mathbf{v}^{(-1)}\right) = n\left(\mathbf{u}, \mathbf{v}^{(-1)}\right)$.

□

Az előbbi következményből speciális esetként kapjuk, hogy $(\mathbf{U}, \mathbf{U}) = n\left(\mathbf{u}, \mathbf{u}^{(-1)}\right)$.

Legyen $\mathbf{v} = \bar{e}$. Ekkor $\mathbf{V} = \tilde{e}$, és $(\mathbf{U}, \mathbf{V}) = \sum_{i=0}^{n-1} U_i$, míg $\left(\mathbf{u}, \mathbf{v}^{(-1)}\right) = u_0$, vagyis $\sum_{i=0}^{n-1} U_i = nu_0$ a fenti következményt alkalmazva. Ugyanezt az eredményt kaptuk korábban a 131. oldalon.

Test fölötti legfeljebb $n-1$-edfokú polinomok n-dimenziós vektorteret alkotnak az összeadással és a test elemeivel való szorzással. A továbbiakban ezt a tényt alkalmazzuk.

7.22. Jelölés

Legyen $n \in \mathbb{N}^+$, $\mathcal{R}$ tetszőleges gyűrű, és $\mathbf{u} \in R^n$. Ekkor $u = \sum_{i=0}^{n-1} u_i x^i$.

Δ

7.23. Tétel

Legyen $n \in \mathbb{N}^+$, $\mathcal{K}$ test és $\mathbf{u} \in K^n$. Ekkor $U_i = \hat{u}\left(z^{-i}\right)$, és $u_i = (ne)^{-1}\hat{U}\left(z^i\right)$, ha $|z| = n$.

Δ

Bizonyítás:

$U_i = \sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j = \sum_{j=0}^{n-1} u_j\left(z^{-i}\right)^j = \hat{u}\left(z^{-i}\right)$. Ha z primitív n-edik egységgyök, akkor létezik $\mathbf{A}_z$ inverze, és az előbbihez hasonlóan kapjuk, hogy $u_i = (ne)^{-1}\hat{U}\left(z^i\right)$.

□

A tételből közvetlenül kapjuk az alábbi eredményt.

7.24. Következmény

Legyen $n \in \mathbb{N}^+$. $U_i = 0$ pontosan akkor igaz, ha $\hat{u}(z^{-i}) = 0$, és $|z| = n$ esetén $u_i = 0$ ekvivalens $\hat{U}(z^i) = 0$-val.

Δ

7.24. azt az igen fontos tényt mutatja, hogy a transzformált i-edik komponense pontosan akkor 0, ha a vektorhoz tartozó polinomnak gyöke z^{-i}, illetve, ha létezik az inverz transzformáció, úgy az eredeti vektor i-indexű tagja akkor és csak akkor 0, ha a transzformált vektor polinomjának gyöke z^i.

7.25. Tétel

Legyen $n \in \mathbb{N}^+$. Ekkor $\hat{U}(0) = \hat{u}(e)$ és $\overset{(k)}{\mathcal{U}\rightarrow} = \mathcal{U} \circ (z^{-k}x)$, és ha z primitív n-edik egységgyök, akkor $\hat{U}(e) = n\hat{u}(0)$ és $\overset{(k)}{u\rightarrow} = u \circ (z^k x)$.

Δ

Bizonyítás:

Tetszőleges $f = \sum_{i=0}^{n} f_i x^i$ polinom esetén $f_0 = \hat{f}(0)$ és $\hat{f}(e) = \sum_{i=0}^{n} f_i e^i = \sum_{i=0}^{n} f_i$, valamint $\sum_{i=0}^{n}(f_i c^i)x^i = \sum_{i=0}^{n} f_i (cx)^i = f \circ (cx)$.

□

Most meghatározzuk a ciklikus konvolúcióhoz tartozó polinomot.

7.26. Tétel

Legyen $n \in \mathbb{N}^+$, $\mathcal{R}$ egy egységelemes gyűrű, $\mathbf{u} \in R^n$, $\mathbf{v} \in R^n$, $\mathbf{w} = \mathbf{u} * \mathbf{v}$ és $\mathbf{g} = \mathbf{u} \circ \mathbf{v}$. Ekkor $g = uv$ és $w = g \bmod (x^n - e)$.

Δ

Bizonyítás:

$g = uv$ legfeljebb $2n-2$-edfokú, tehát egyben legfeljebb $2n-1$-edfokú polinom. Legyen a két polinom $u = \sum_{i=0}^{n-1} u_i x^i$ és $v = \sum_{i=0}^{n-1} v_i x^i$, ekkor $g_i = \sum_{j=0}^{i} u_j v_{i-j}$, ahol $2n > i \in \mathbb{N}$, és 0-nál kisebb illetve n-nél nem kisebb indexekre az u illetve v együtthatóit 0-nak tekintjük. Ekkor viszont $g_i = \sum_{j=0}^{i} u_j v_{i-j} = \sum_{j=0}^{2n-1} u_j v_{(i-j)^{(2n)}}$, azaz g_i **u** és **v** lineáris konvolúciójának i-edik komponense, így fennáll a $\mathbf{g} = \mathbf{u} \circ \mathbf{v}$ egyenlőség. Ugyanakkor

$$uv = \sum_{i=0}^{2n-1} g_i x^i = \sum_{i=0}^{n-1} g_i x^i + \sum_{i=n}^{2n-1} g_i x^i = \sum_{i=0}^{n-1} g_i x^i + x^n \sum_{i=0}^{n-1} g_{n+i} x^i = a + x^n b,$$

ahol $a = \sum_{i=0}^{n-1} g_i x^i$ és $b = \sum_{i=0}^{n-1} g_{n+i} x^i$. Látható, hogy $uv = a + x^n b = b \cdot (x^n - e) + (a + b)$, vagyis $w = a + b$, és w is maximum $n-1$-edfokú polinom, tehát az n-nél kisebb mindenegyes i indexre $w_i = a_i + b_i = (uv)_i + (uv)_{n+i}$. Beírva g megfelelő együtthatóit,

$$w_i = \sum_{j=0}^{i} u_j v_{i-j} + \sum_{j=0}^{n+i} u_j v_{(n+i)-j} = \sum_{j=0}^{i} u_j v_{i-j} + \sum_{j=i+1}^{n-1} u_j v_{n+i-j} = \sum_{j=0}^{n-1} u_j v_{(i-j)^{(n)}},$$

ugyanis ha $j \geq n$, akkor $u_j = 0$, és ha $j \leq i$, akkor $v_{(n+i)-j} = 0$, másrészt, ha $n > i \in \mathbb{N}$, akkor egyben $i \geq j \in \mathbb{N}$-re $n > i - j \in \mathbb{N}$, így $i - j = (i-j)^{(n)}$, és $i + 1 \leq j < n$-re $n > n + i - j \in \mathbb{N}$, tehát ebben az esetben $n + i - j = (i-j)^{(n)}$. $\sum_{j=0}^{n-1} u_j v_{(i-j)^{(n)}}$ viszont $\mathbf{u} * \mathbf{v}$ i-edik komponense.

□

A következő tételhez foglalkozzunk polinomok maradékával. Legyen f_1, f_2 és $s \neq 0$ egy $\mathcal{K}$ test feletti polinomok, $f = f_1 f_2$ és $f_2 \bmod s = g = g_1 g_2$, ahol g mindkét tényezője is $\mathcal{K}$ feletti polinom. Ha u az s gyöke a $\mathcal{K}$ egy $\mathcal{L}$ bővítésben, akkor

$$\begin{aligned}\hat{f}(u) &= \hat{f}_1(u)\hat{f}_2(u) = \hat{f}_1(u)\big(\hat{t}(u)\hat{s}(u) + \hat{g}(u)\big) \\ &= \hat{f}_1(u)\hat{g}(u) = \hat{f}_1(u)\hat{g}_1(u)\hat{g}_2(u),\end{aligned}$$

és ha $\hat{f}_1(u) \neq 0 \neq \hat{g}_1(u)$, úgy u akkor és csak akkor gyöke f-nek, ha $\hat{g}_2(u) = 0$. Legyen például $\mathcal{K}$ a q-elemű test, $f_1 = x^k$ és $g_1 = x^l$, továbbá $s = x^{q-1} - e$. Ekkor s-nek $\mathbb{F}_q$ nullától különböző elemei, és csak ezek a gyökei, és ezek egyike sem gyöke f_1-nek és g_1-nek, így minden $0 \neq u \in \mathbb{F}_q$-ra u akkor és csak akkor gyöke f-nek, ha gyöke g_2-nek

7.27. Tétel (Kőnig-Rados)

Legyen $f \in \mathbb{F}_q[x]$, $0 \neq f \bmod (x^{q-1} - e) = r = x^k g$, ahol $\hat{g}(0) \neq 0$, $g = \sum_{i=0}^{q-2} g_i x^i$, és $\mathbf{G}$ olyan mátrix, amelyben $G_{i,j} = g_{(j-i)^{(q-1)}}$ a $q - 1 > i \in \mathbb{N}$ és $q - 1 > j \in \mathbb{N}$ indexekre. Ekkor f $\mathbb{F}_q$-beli, páronként különböző nem nulla gyökeinek száma $(q-1) - r$, ahol r a $\mathbf{G}$ mátrix rangja.

Δ

Bizonyítás:

A tétel előtt látottak alapján f és g $\mathbb{F}_q^*$-beli gyökei azonosak. Legyen z $\mathbb{F}_q$ primitív eleme. Ekkor a $q-1$-edrendű $\mathbf{A}_z$ mátrix reguláris, így $\mathbf{G}$ és $\mathbf{H} = \mathbf{A}_z\mathbf{G}$ rangja azonos. Erre a $\mathbf{H}$-ra

$$H_{i,k} = \sum_{j=0}^{q-2} (\mathbf{A}_z)_{i,j}\, G_{j,k} = \sum_{j=0}^{q-2} \left(z^{-i}\right)^j g_{(k-j)^{(q-1)}} = \sum_{j=0}^{q-2} \left(z^{-i}\right)^{k-j} g_j = \hat{g}\left(z^i\right) \cdot \left(z^{-i}\right)^k,$$

vagyis $\mathbf{H}$-t úgy kapjuk $\mathbf{A}_z$-ből, hogy ez utóbbi i-edik sorának minden elemét megszorozzuk $\hat{g}\left(z^i\right)$-vel. Legyen g $\mathbb{F}_q^*$-beli, páronként különböző gyökeinek száma $q - 1 > t \in \mathbb{N}$, és tegyük fel, hogy a gyökök a $0 \leq i_0 < \cdots < i_{t-1} < q - 1$ kitevőkhöz tartoznak. Ekkor $\mathbf{H}$ ugyanezen indexű, és csak ezekhez az indexekhez tartozó sorai a nullvektorok. A többi sornak vegyük az első $q - 1 - t$ elemét. Ezek együttesen $\mathbf{H}$-nak egy $q - 1 - t$-edrendű részmátrixát alkotják. Ha D ennek a mátrixnak a determinánsa, és ennek u-adik sora az eredeti mátrixban az i_u indexű sor kezdő szakasza, akkor D pontosan akkor 0, ha D' is 0, ahol D'-t úgy kapjuk D-ből, hogy az u-adik sorából kiemeljük a nem nulla $\hat{g}\left(z^i\right)$-t. A kiemelés után viszont az u-adik sor v-edik eleme $\left(z^{-i_u}\right)^v$, azaz D' Vandermonde-típusú, és mivel z primitív $q - 1$-edik egységgyök, és az i_u-k páronként különböző, $q - 1$-nél kisebb, nemnegatív egészek, ezért $D' \neq 0$. Ám ez pontosan azt jelenti, hogy a $\mathbf{H}$ mátrix rangja $q - 1 - t$, és $(q-1) - r = t$, megegyezésben a gyökök számával.

□

A tételben az $r \neq 0$ feltétel nem jelent lényeges megszorítást. Ez a kikötés azt jelenti, hogy f nem osztható $x^{q-1} - e$-vel. Ellenkező esetben $\mathbb{F}_q^*$ valamennyi eleme gyöke f-nek, és ekkor természetesen más $\mathbb{F}_q^*$-beli gyöke nem lehet, vagyis eleve ismerjük f összes $\mathbb{F}_q^*$-beli gyökét.

Az alábbiakban definiáljuk a diszkrét Fourier-transzformációt.

7.28. Definíció

Legyen $n \in \mathbb{N}^+$, és $\mathcal{K}$ olyan test, hogy $K^{(n)} \subseteq K$, $\mathbf{u}$ és $\mathbf{U}$ K^n elemei, továbbá z egy $\mathcal{K}$ fölötti primitív n-edik egységgyök. Ekkor $\mathcal{F}_z(\mathbf{u}) = \mathbf{A}_z\mathbf{u}$ az $\mathbf{u}$ (z**-vel vett**) **diszkrét Fourier-transzformáltja**, míg $\mathcal{F}_z^{-1}(\mathbf{U}) = \mathbf{A}_z^{-1}\mathbf{U}$ az $\mathbf{U}$ (z**-vel vett**) **inverz diszkrét Fourier-transzformáltja**. Magát a transzformációt és inverzét **diszkrét Fourier-transzformáció**nak és **inverz diszkrét Fourier-transzformáció**nak mondjuk, és általában **DFT**-nek és **IDFT**-nek rövidítjük.

Ha $\mathbf{U} = \mathcal{F}_z(\mathbf{u})$, akkor $\mathcal{U}$ **az** u **polinomhoz tartozó Mattson-Solomon polinom.**

Δ

A diszkrét Fourier-transzformáció speciális esete az eddig tárgyalt problémáknak. A korábbi tételek alapján összefoglaljuk a legfontosabb tulajdonságait.

1. $\mathcal{F}_z^{-1}\big(\mathcal{F}_z(\mathbf{u})\big) = \mathbf{u}$ és $\mathcal{F}_z\big(\mathcal{F}_z^{-1}(\mathbf{U})\big) = \mathbf{U}$;
2. $\mathcal{F}_z(a\mathbf{u} + b\mathbf{v}) = a\mathcal{F}_z(\mathbf{u}) + b\mathcal{F}_z(\mathbf{v})$;
3. $\mathcal{F}_z(\mathbf{u} * \mathbf{v}) = \mathcal{F}_z(\mathbf{u}) \cdot \mathcal{F}_z(\mathbf{v})$ és $\mathcal{F}_z(\mathbf{u} \cdot \mathbf{v}) = (ne)^{-1}\big(\mathcal{F}_z(\mathbf{u}) * \mathcal{F}_z(\mathbf{v})\big)$.

A felsorolt összefüggések közül csupán az első új, ez viszont nyilvánvaló tényt fejez ki, hiszen a definíció alapján $\mathcal{F}_z^{-1}\big(\mathcal{F}_z(\mathbf{u})\big) = \mathbf{A}_z^{-1}(\mathbf{A}_z\mathbf{u}) = (\mathbf{A}_z^{-1}\mathbf{A}_z)\mathbf{u} = \mathbf{u}$, és a másik kifejezés ehhez hasonló.

7.29. Megjegyzés

A diszkrét Fourier-transzformáció többek között azt a kapcsolatot fejezi ki, amely szerint egy test feletti legfeljebb $n-1$-edfokú polinomot egyrészt megadhatjuk n együtthatójával, másrészt n páronként különböző helyen felvett helyettesítési értékével.

Ha megadunk egy polinomot a $\mathcal{K}$ test fölött, az egyértelműen meghatározza K bármely pontjában a helyettesítési értéket. Legyen $n \in \mathbb{N}^+$, $\mathbf{f}$ és $\mathbf{g}$ K^n, a és b K elemei, $\mathbf{h} = a\mathbf{f} + b\mathbf{g}$ és $\mathbf{w} = \mathbf{f} * \mathbf{g}$, továbbá $t = ff$. Ekkor a $\mathcal{K}$ feletti bármely z n-edik egységgyökkel és $n > i \in \mathbb{N}$ egésszel

$$\big(\mathbf{A}_z(a\mathbf{f} + b\mathbf{g})\big)_i = (\mathbf{A}_z\mathbf{h})_i = \hat{h}\big(z^{-i}\big) = a\hat{f}\big(z^{-i}\big) + bg\big(z^{-i}\big) = a(\mathbf{A}_z\mathbf{f})_i + b(\mathbf{A}_z\mathbf{g})_i,$$

$$\big(\mathbf{A}_z(\mathbf{f} * \mathbf{g})\big)_i = (\mathbf{A}_z\mathbf{w})_i = \hat{w}\big(z^{-i}\big) = \hat{t}\big(z^{-i}\big) = f\big(z^{-i}\big)g\big(z^{-i}\big) = (\mathbf{A}_z\mathbf{f})_i \cdot (\mathbf{A}_z\mathbf{g})_i.$$

Ha z egy n-nél kisebb m-re primitív m-edik egységgyök, akkor az $n > i \in \mathbb{N}$-re vett z^{-i} hatványok száma csak m, és m helyettesítési érték nem határozza meg az eredeti polinom n együtthatóját. Ha viszont $m = n$, akkor n különböző helyen ismerjük a polinom helyettesítési értékét, és ebből az interpolációs polinom egyértelműsége következtében megkapjuk a polinomot. A diszkrét Fourier-transzformáció tehát többek között azt jelenti, hogy ha egy legfeljebb $n-1$-edfokú polinom helyettesítési értékeit egy primitív n-edik egységgyök hatványainál adjuk meg, akkor az interpolációs polinomot egyszerűen egy mátrixszal való szorzás útján is megkapjuk, hiszen ha $\mathbf{U}$ az a vektor, amelynek i-edik komponense $u\big(z^{-i}\big)$, akkor a korábbi eredmények alapján $\mathbf{u} = \mathbf{A}_z^{-1}\mathbf{U}$.

Δ

A Fourier-transzformáció lényeges szerepet játszik jelanalízisben, digitális jelfeldolgozásban (**DSP** = **D***igital* **S***ignal* **P***rocessing*), például hang és kép feldolgozásában, jelátvivő berendezések vizsgálatában. A transzformáció alább ismertetendő gyorsításával sokjegyű számok szorzásának gyors algoritmusa létezik. Konkrét felhasználásával találkozunk bizonyos hibajavító kódok dekódolása során.

A DFT-hez hozzávetőlegesen n^2 szorzásra és körülbelül ugyanennyi összeadásra van szükség (minden komponens egy n-tagú összeg, ahol az összeg minden tagja egy szorzat). A következő tételben megadott, **FFT**-vel jelölt **gyors Fourier-transzformáció**val az elvégzendő műveletek száma $n \log n$ nagyságrendű lesz. A tételt igazoló eljárást a 3. algoritmus mutatja.

7.30. Tétel

Ha $n = n_0 n_1$, akkor az n-komponensű vektor diszkrét Fourier-transzformáltja $n(n_0 + n_1)$ nagyságrendű szorzással és $\max(n_0, n_1)$ tárigénnyel meghatározható.

Δ

Bizonyítás:

Minden $n > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$ egyértelműen írható $i = i_1 n_1 + i_0$ és $j = j_1 n_0 + j_0$ alakban, ahol $n_1 > i_0 \in \mathbb{N}$, $n_0 > i_1 \in \mathbb{N}$, $n_0 > j_0 \in \mathbb{N}$ és $n_1 > j_1 \in \mathbb{N}$. Ekkor

$$U_{i_1 n_1 + i_0} = U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = \sum_{j_1=0}^{n_1-1} \sum_{j_0=0}^{n_0-1} \left(z^{-(i_1 n_1 + i_0)}\right)^{j_1 n_0 + j_0} u_{j_1 n_0 + j_0}$$
$$= \sum_{j_0=0}^{n_0-1} \left((z^{n_1})^{-i_1} z^{-i_0}\right)^{j_0} \sum_{j_1=0}^{n_1-1} \left((z^{n_0})^{-i_0}\right)^{j_1} u_{j_1 n_0 + j_0} = \sum_{j_0=0}^{n_0-1} \left((z^{n_1})^{-i_1} z^{-i_0}\right)^{j_0} \tilde{u}_{i_0 n_0 + j_0},$$

ahol $\tilde{u}_{i_0 n_0 + j_0} = \sum_{j_1=0}^{n_1-1} \left((z^{n_0})^{-i_0}\right)^{j_1} u_{j_1 n_0 + j_0}$. Számítsuk ki egymás után rögzített j_0 mellett minden i_0-ra $\tilde{u}_{i_0 n_0 + j_0}$-t. Ehhez egy-egy adott j_0 mellett legfeljebb n_1^2 szorzás kell, és az eredeti tárolóhelyen túl még n_1 helyre van szükség. Ám a képletből látható, hogy miután az n_1 számú $\tilde{u}_{i_0 n_0 + j_0}$-t kiszámoltuk, a szintén n_1 darab eredeti $u_{j_1 n_0 + j_0}$-ra már nincs szükség, így ezek helyére tehetjük az új $\tilde{u}_{i_0 n_0 + j_0}$ komponenseket. Amikor minden j_0-ra meghatároztuk az új komponenseket, akkor az addigi szorzások száma összesen $n_0 n_1^2$, és van egy új n-méretű vektorunk. Most az előzőhöz hasonlóan rögzített i_0-ra kiszámítjuk az n_0 számú i_1-re az n_0 darab $U_{i_1 n_1 + i_0}$-t. Ehhez n_0 helyre és n_0^2, tehát az összes i_0-ra számolva $n_0^2 n_1$ szorzásra van szükség, így az előbbiekkel együtt összesen mintegy $n(n_0 + n_1)$ szorzást végeztünk.

$n = n_0 n_1 \geq 2n_1 \geq n_0 + n_1$ ha $n_1 \geq n_0 \geq 2$, azaz ha $n = n_0 n_1$ az n valódi felbontása, és ha $n_1 > 2$, akkor már $n > n_0 + n_1$, tehát a fenti algoritmussal kevesebb szorzásra van szükség, mint az eredeti transzformációnál.

□

```
FFT_alap(n, n0, n1, u(n))
        ciklus j0 = 0-tól n0 − 1-ig
                ciklus i0 = 0-tól n1 − 1-ig
                        v(i0) = Σ_{j1=0}^{n1−1} ((z^{n0})^{−i0})^{j1} u(j1 ∗ n0 + j0)
                ciklus vége
                ciklus i0 = 0-tól n1 − 1-ig
                        u(i0 ∗ n0 + j0) = (z^{−j0})^{i0} v(i0)
                ciklus vége
        ciklus vége
        ciklus i0 = 0-tól n1 − 1-ig
                ciklus i1 = 0-tól n0 − 1-ig
                        v(i1) = Σ_{j0=0}^{n0−1} ((z^{n1})^{−i1})^{j0} u(i0 ∗ n0 + j0)
                ciklus vége
                ciklus i1 = 0-tól n0 − 1-ig
                        u(i0 ∗ n0 + i1) = v(i1)
                ciklus vége
        ciklus vége
eljárás vége.
```

3. algoritmus

Az előző eredményből indukcióval kapjuk a következő tételt.

7.31. Tétel

Legyen $\mathcal{K}$ test és $\prod_{i=0}^{t-1} n_i = n$, ahol $t \in \mathbb{N}^+$ és $t > k \in \mathbb{N}$-re $1 < n_k \in \mathbb{N}^+$. Ekkor a $\mathcal{K}^n$ feletti diszkrét Fourier-transzformáció elvégezhető $n \sum_{i=0}^{t-1} n_i$ nagyságrendű szorzással és $\max_{t>i\in\mathbb{N}}\{n_i\}$-méretű memóriával.

Δ

A tételnek megfelelő egy lehetséges eljárást is megadtunk (4. algoritmus).

```
FFT(t, n( ), u( ))
    ciklus r = 0-tól t − 1-ig
        Zir = (z^{-1})^{n/n_{t-r-1}}
        ind2 = 0
        ciklus Î^(r) = 0-tól n/N_{t-r-1} − 1-ig
            I_r meghatározása
            ZIr = (z^{-1})^{I_r N_{t-r-1}}
            ind1 = ind2
            ciklus J_{t-r-1} = 0-tól N_{t-r-1} − 1-ig
                Zjr = ZIr
            ciklus i_r = 0-tól n_{t-r-1} − 1-ig
                    ind = ind1
                    s = u(ind)
                    Z = 1
                    ciklus j_{t-r-1} = 1-től n_{t-r-1} − 1-ig
                        ind = ind + N_{t-r-1}
                        Z = Z * Zjr
                        s = s + Z * u(ind)
                    ciklus vége
                    ũ(i_r) = s
                    Zjr = Zjr * Zir
                ciklus vége
                    ind = ind1
                u(ind) = ũ(0)
                ciklus i_r = 1-től n_{t-r-1} − 1-ig
                    ind = ind + N_{t-r-1}
                    u(ind) = ũ(i_r)
            ciklus vége
                ind1 = ind1 + 1
            ciklus vége
            ind2 = ind2 + N_{t-r}
        ciklus vége
    ciklus vége
    u( ) átrendezése
eljárás vége.
```

4. algoritmus

Bizonyítás:

Ha $t = 1$, akkor a transzformációhoz a megadott két kifejezés szerint n^2 műveletre és n-méretű tárra van szükség, míg $t = 2$ esetén az állítás azonos az előző tétel eredményével. Most tegyük fel, hogy egy $2 \leq t \in \mathbb{N}$-re igaz az állítás, és legyen $n = \prod_{i=0}^{t} n_i$. Ha $n' = \prod_{i=1}^{t} n_i$, akkor $n = n_0 n'$. Szintén az előző tétel alapján a transzformáció elvégezhető n_0 számú, n'-méretű vektoron végrehajtott Fourier-transzformációval, majd utána az így kapott n-méretű vektoron végzett $n_0^2 n'$-nagyságrendű szorzással.

Az indukciós feltevés szerint az n'-méretű vektoron végzett Fourier-transzformációhoz $n'\sum_{i=1}^{t-1} n_i$, tehát összesen $n_0^2 n' + n_0 n' \sum_{i=1}^{t-1} n_i = n\sum_{i=0}^{t-1} n_i$ szorzás kell a teljes transzformáció elvégzéséhez. Az n'-komponensű részekhez $\max_{t>i\in\mathbb{N}^+}\{n_i\}$-, míg az utolsó lépéshez n_0-méretű tárolóhelyre, így összességében $\max_{t>i\in\mathbb{N}}\{n_i\}$-re van szükség a transzformáláshoz.

□

Az eddigiekből könnyen megkapjuk a transzformáció algoritmusát. Legyen tehát $\prod_{i=0}^{t-1} n_i = n$, ahol $t \in \mathbb{N}^+$ és $t > k \in \mathbb{N}$-re $1 < n_k \in \mathbb{N}^+$, és vezessük be az $N_l = \prod_{k=0}^{l-1} n_k$, $N^{(l)} = \prod_{k=t-l}^{t-1} n_k$ jelölést a $t > l \in \mathbb{N}$ indexekre. Könnyen látható, hogy amennyiben $r + s \geq t$, ahol r és s egyaránt nemnegatív egész szám, akkor $n \big| N_r N^{(s)}$. Ha $n > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$, akkor mind i, mind j egyértelműen megadható az $i = \sum_{k=0}^{t-1} i_k N^{(k)}$ és $j = \sum_{k=0}^{t-1} j_k N_k$ alakban, ahol $n_{t-1-k} > i_k \in \mathbb{N}$ és $n_k > j_k \in \mathbb{N}$, és fordítva, az előbbi feltételt kielégítő i_k és j_k értékekkel egy és csak egy n-nél kisebb nemnegatív egész i és j adható meg. Tetszőleges $t \geq r \in \mathbb{N}$-re

$$i = \left(i \bmod N^{(r)}\right) + \left\lfloor \frac{i}{N^{(r)}} \right\rfloor N^{(r)} = \sum_{l=0}^{r-1} i_l N^{(l)} + N^{(r)} \sum_{l=r}^{t-1} i_l \frac{N^{(l)}}{N^{(r)}} = I_r + I^{(r)} N^{(r)},$$

valamint

$$j = (j \bmod N_r) + \left\lfloor \frac{j}{N_r} \right\rfloor N_r = \sum_{l=0}^{r-1} j_l N_l + N_r \sum_{l=r}^{t-1} j_l \frac{N_l}{N_r} = J_r + J^{(r)} N_r,$$

ahol $N^{(r)} > I_r \in \mathbb{N}$, $N_{t-r} = \frac{n}{N^{(r)}} > I^{(r)} \in \mathbb{N}$, $N_r > J_r \in \mathbb{N}$ és $N^{(t-r)} = \frac{n}{N_r} > J^{(r)} \in \mathbb{N}$, és az előbbi osztathatósággal $ij \equiv \left(I_r + I^{(r)} N^{(r)}\right) J_r + I_r J^{(r)} N_r \ (n)$. A 7.30. Tétel szerint, a mostani jelölésekkel,

$$U_{I_r + I^{(r)} N^{(r)}} = \sum_{J_{t-r}=0}^{N_{t-r}-1} \left(\left(z^{N^{(r)}}\right)^{-I^{(r)}} z^{-I_r} \right)^{J_{t-r}} \sum_{J^{(t-r)}=0}^{N^{(r)}-1} ((z^{N_{t-r}})^{-I_r})^{J^{(t-r)}} u_{J_{t-r} + J^{(t-r)} N_{t-r}}.$$

Tegyük fel, hogy már meghatároztuk minden J_{t-r}-re a $\sum_{J^{(t-r)}=0}^{N^{(r)}-1} ((z^{N_{t-r}})^{-I_r})^{J^{(t-r)}} u_{J_{t-r} + J^{(t-r)} N_{t-r}}$ értéket, és az eredményt (helyileg az eredetivel azonos) $\mathbf{u}^{(r)}$ tárolja úgy, hogy az $\tilde{I}^{(r)} = \sum_{l=0}^{r-1} i_l \frac{N_{t-1-l}}{N_{t-r}}$ jelöléssel

$$u^{(r)}_{J_{t-r} + \tilde{I}^{(r)} N_{t-r}} = \sum_{J^{(t-r)}=0}^{N^{(r)}-1} ((z^{N_{t-r}})^{-I_r})^{J^{(t-r)}} u_{J_{t-r} + J^{(t-r)} N_{t-r}}$$

($\tilde{I}^{(r)}$-et úgy kapjuk, hogy I_r számjegyeit – a hozzájuk tartozó súlyokkal együtt – fordított sorrendben írjuk). Ez megtehető, mert $\frac{N_{t-1-(l-1)}}{N_{t-1-l}} = n_{t-1-l}$ és $n_{t-1-l} > i_l \in \mathbb{N}$, tehát $\frac{N_t}{N_{t-r}} = \frac{n}{N_{t-r}} = N^{(r)}$, így adott r mellett minden $N^{(r)} > k \in \mathbb{N}$ pontosan egyféleképpen írható $\sum_{l=0}^{r-1} i_l \frac{N_{t-1-l}}{N_{t-r}}$ alakban, és ez a tartomány azonos az I_r illetve $J^{(t-r)}$ számok halmazával. Például ellenőrizhető, hogy

$$u_j^{(0)} = u^{(0)}_{J_t + \tilde{I}^{(0)} N_t} = \sum_{J^{(t)}=0}^{N^{(0)}-1} ((z^{N_t})^{-I_0})^{J^{(t)}} u_{J_t + J^{(t)} N_t} = \sum_{J^{(t)}=0}^{1-1} ((z^n)^{-0})^{J^{(t)}} u_{j + J^{(t)} \cdot n} = u_j$$

illetve

$$u_{\tilde{I}^{(t)}}^{(t)} = u_{J_0+\tilde{I}^{(t)}N_0}^{(t)} = \sum_{J^{(0)}=0}^{N^{(t)}-1} ((z^{N_0})^{-I_t})^{J^{(0)}} u_{J_0+J^{(0)}N_0} = \sum_{J^{(0)}=0}^{n-1} \left((z^1)^{-i}\right)^{J^{(0)}} u_{0+J^{(0)}\cdot 1} = U_i.$$

Ha most $0 \le r < t$, akkor $J_{t-r} = J_{t-r-1} + j_{t-r-1}N_{t-r-1}$, így

$$\begin{aligned} U_{I_r+I^{(r)}N^{(r)}} &= \sum_{J_{t-r}=0}^{N_{t-r}-1} \left(\left(z^{N^{(r)}}\right)^{-I^{(r)}} z^{-I_r}\right)^{J_{t-r}} u_{J_{t-r}+\tilde{I}^{(r)}N_{t-r}}^{(r)} \\ &= \sum_{J_{t-r-1}=0}^{N_{t-r-1}-1} \sum_{j_{t-r-1}=0}^{n_{t-r-1}-1} \left(\left(z^{N^{(r)}}\right)^{-I^{(r)}} z^{-I_r}\right)^{J_{t-r-1}+j_{t-r-1}N_{t-r-1}} u_{J_{t-r-1}+j_{t-r-1}N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}}^{(r)}. \end{aligned}$$

z kitevőjének ellentettje

$$\begin{aligned} \left(N^{(r)}I^{(r)} + I_r\right)\left(J_{t-r-1} + j_{t-r-1}N_{t-r-1}\right) &= \left(N^{(r+1)}I^{(r+1)} + I_{r+1}\right)\left(J_{t-r-1} + j_{t-r-1}N_{t-r-1}\right) \\ &\equiv \left(N^{(r+1)}I^{(r+1)} + I_{r+1}\right)J_{t-r-1} + I_{r+1}j_{t-r-1}N_{t-r-1}\ (n), \end{aligned}$$

és ezzel

$$U_{I_{r+1}+I^{(r+1)}N^{(r+1)}} = \sum_{J_{t-r-1}=0}^{N_{t-r-1}-1} \left(\left(\left(z^{N^{(r+1)}}\right)^{-I^{(r+1)}} z^{-I_{r+1}} \right)^{J_{t-r-1}} \times \sum_{j_{t-r-1}=0}^{n_{t-r-1}-1} ((z^{N_{t-r-1}})^{-I_{r+1}})^{j_{t-r-1}} u_{J_{t-r-1}+j_{t-r-1}N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}}^{(r)} \right).$$

A belső összeg kitevőjét kicsit átalakítjuk:

$$N_{t-r-1}I_{r+1} = i_r N_{t-r-1}N^{(r)} + N_{t-r-1}\sum_{l=0}^{r-1} i_l N^{(l)} = N_{t-r-1}\sum_{l=0}^{r} i_l N^{(l)} = i_r \frac{n}{n_{t-r-1}} + N_{t-r-1}I_r,$$

és helyettesítve kapjuk, hogy

$$\begin{aligned} &\sum_{j_{t-r-1}=0}^{n_{t-r-1}-1} ((z^{N_{t-r-1}})^{-I_{r+1}})^{j_{t-r-1}} u_{J_{t-r-1}+j_{t-r-1}N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}}^{(r)} \\ &\qquad = \sum_{j_{t-r-1}=0}^{n_{t-r-1}-1} \left(\left(z^{\frac{n}{n_{t-r-1}}}\right)^{-i_r} (z^{N_{t-r-1}})^{-I_r}\right)^{j_{t-r-1}} u_{J_{t-r-1}+j_{t-r-1}N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}}^{(r)}. \end{aligned}$$

Látható, hogy rögzített J_{t-r-1} és $\tilde{I}^{(r)}$ (és ekkor rögzített I_r) mellett a fenti kifejezés lényegében véve egy n_{t-r-1}-komponensű vektor diszkrét Fourier-transzformáltja, hiszen $z^{\frac{n}{n_{t-r-1}}}$ egy n_{t-r-1}-edik primitív egységgyök, csupán a $z^{-N_{t-r-1}I_r}$ úgynevezett *csavaró tényező* módosítja a megszokott számítást. Az előbbiekben rögzített J_{t-r-1} és $\tilde{I}^{(r)}$ indexekkel valamennyi $n_{t-1-r} > i_r \in \mathbb{N}$ indexre meghatározva $\tilde{u}_{i_r} = \sum_{j_{t-r-1}=0}^{n_{t-r-1}-1} \left(\left(z^{\frac{n}{n_{t-r-1}}}\right)^{-i_r} (z^{N_{t-r-1}})^{-I_r}\right)^{j_{t-r-1}} u_{J_{t-r-1}+j_{t-r-1}N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}}^{(r)}$ értékét, a korábbiakhoz hasonlóan az $u_{J_{t-r-1}+j_{t-r-1}N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}}^{(r)}$ komponensekre már nincs szükség, azok helyén tárolhatjuk a most kiszámított értékeket. Ha még azt is figyelembe vesszük, hogy

$$i_r N_{t-r-1} + \tilde{I}^{(r)} N_{t-r} = \left(i_r + \tilde{I}^{(r)} n_{t-r-1}\right) N_{t-r-1} = \left(i_r \frac{N_{t-r-1}}{N_{t-r-1}} + \sum_{l=0}^{r-1} i_l \frac{N_{t-1-l}}{N_{t-r}} n_{t-r-1}\right) N_{t-r-1}$$
$$= \left(i_r \frac{N_{t-r-1}}{N_{t-r-1}} + \sum_{l=0}^{r-1} i_l \frac{N_{t-1-l}}{N_{t-r-1}}\right) N_{t-r-1} = \sum_{l=0}^{r} i_l \frac{N_{t-1-l}}{N_{t-r-1}} N_{t-r-1} = \tilde{I}^{(r+1)} N_{t-r-1},$$

akkor az $\tilde{u}_{i_r}$ komponensekkel az új vektorban $u^{(r+1)}_{J_{t-r-1}+\tilde{I}^{(r+1)}N_{t-r-1}} = u^{(r+1)}_{J_{t-r-1}+i_r N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}} = \tilde{u}_{i_r}$ lehet. Végül így azt kaptuk, hogy ha $U_{I_r+I^{(r)}N^{(r)}} = \sum_{J_{t-r}=0}^{N_{t-r-1}} \left(\left(z^{N^{(r)}}\right)^{-I^{(r)}} z^{-I_r}\right)^{J_{t-r}} u^{(r)}_{J_{t-r}+\tilde{I}^{(r)}N_{t-r}}$, akkor

$$U_{I_{r+1}+I^{(r+1)}N^{(r+1)}} = \sum_{J_{t-r-1}=0}^{N_{t-r-1}-1} \left(\left(z^{N^{(r+1)}}\right)^{-I^{(r+1)}} z^{-I_{r+1}}\right)^{J_{t-r-1}} u^{(r+1)}_{J_{t-r-1}+\tilde{I}^{(r+1)}N_{t-r-1}},$$

ahol

$$u^{(r+1)}_{J_{t-r-1}+i_r N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}} = u^{(r+1)}_{J_{t-r-1}+\tilde{I}^{(r+1)}N_{t-r-1}} = \tilde{u}_{i_r}$$
$$= \sum_{j_{t-r-1}=0}^{n_{t-r-1}-1} \left(\left(z^{\frac{n}{n_{t-r-1}}}\right)^{-i_r} (z^{N_{t-r-1}})^{-I_r}\right)^{j_{t-r-1}} u^{(r)}_{J_{t-r-1}+j_{t-r-1}N_{t-r-1}+\tilde{I}^{(r)}N_{t-r}}.$$

A transzformáció során tehát t egymás utáni fordulóban rögzített J_{t-r-1} és ezen belül rögzített $\tilde{I}^{(r)}$ mellett elvégzünk egy, a csavaró tényezőtől eltekintve n_{t-r-1}-dimenziós diszkrét Fourier-transzformációt az előbbi rögzített értékek minden lehetséges értéke mellett. Mindezek alapján a transzformáció algoritmusa könnyen felírható (4. algoritmus).

Legyen például $t = 3$, $n_0 = 3$, $n_1 = 2$ és $n_2 = 2$, tehát $n = 12$. Ekkor $3 \geq r \in \mathbb{N}$, és

r	N_r	$N^{(r)}$
0	1	1
1	2	3
2	4	6
3	12	12

Először $u_j^{(0)} = u_j$-ből minden lehetséges $3 > i_0 \in \mathbb{N}$, $1 > I_0 \in \mathbb{N}$ és $4 > J_2 \in \mathbb{N}$-re kiszámítjuk $u_j^{(1)} = u^{(1)}_{J_2+4i_0+12\tilde{I}^{(0)}} = \sum_{j_2=0}^{2}\left((z^4)^{-i_0}(z^4)^{-I_0}\right)^{j_2} u^{(0)}_{J_2+4j_2+12\tilde{I}^{(0)}}$ értékét (I_r és $\tilde{I}^{(r)}$ kölcsönösen egyértelműen meghatározzák egymást). Az így elvégzett számítás eredményét az 1. táblázat mutatja.

A második fordulóban $u_j^{(2)} = u^{(2)}_{J_1+2i_1+4\tilde{I}^{(1)}} = \sum_{j_1=0}^{1}\left((z^6)^{-i_1}(z^2)^{-I_1}\right)^{j_1} u^{(1)}_{J_1+2j_1+4\tilde{I}^{(1)}}$, és a felvehető értékek tartománya rendre $2 > i_1 \in \mathbb{N}$, $3 > I_1 \in \mathbb{N}$ és $2 > J_1 \in \mathbb{N}$. Az új komponensek értékei a 2. táblázaton láthatóak.

Végül $u_j^{(3)} = u^{(3)}_{J_0+i_2+2\tilde{I}^{(2)}} = \sum_{j_0=0}^{1}\left((z^6)^{-i_2} z^{-I_2}\right)^{j_0} u^{(2)}_{J_0+j_0+2\tilde{I}^{(2)}}$, és $2 > i_2 \in \mathbb{N}$, $6 > I_2 \in \mathbb{N}$ és $1 > J_0 \in \mathbb{N}$. Most valamivel bonyolultabb a számítás, mint az előző két esetben, ugyanis I_2 és $\tilde{I}^{(2)}$ általában nem egyenlő. A definíció felhasználásával $\tilde{I}^{(2)} = \sum_{l=0}^{1} i_l \frac{N_{2-l}}{N_1} = n_1 i_0 + i_1 = 2i_0 + i_1$ valamint $I_2 = \sum_{l=0}^{1} i_l N^{(l)} = i_0 + n_2 i_1 = i_0 + 3i_1$. A számítást a 3. táblázat, az eredményt a 4. táblázat mutatja.

Még minden j-re meg kell határozni i-t, amellyel $u_j^{(3)} = U_i$. A számítás hasonló, mint a 3. táblázaton, hiszen $u_{\tilde{I}^{(t)}}^{(t)} = U_i = U_{I_t}$. Az indexek átszámítását és párosítását az 5. táblázat mutatja.

j	$\tilde{I}^{(0)}$	I_0	i_0	J_2	$u_j^{(1)}$
0	0	0	0	0	$u_0^{(0)} + u_4^{(0)} + u_8^{(0)}$
1				1	$u_1^{(0)} + u_5^{(0)} + u_9^{(0)}$
2				2	$u_2^{(0)} + u_6^{(0)} + u_{10}^{(0)}$
3				3	$u_3^{(0)} + u_7^{(0)} + u_{11}^{(0)}$
4			1	0	$u_0^{(0)} + z^{-4}u_4^{(0)} + z^{-8}u_8^{(0)}$
5				1	$u_1^{(0)} + z^{-4}u_5^{(0)} + z^{-8}u_9^{(0)}$
6				2	$u_2^{(0)} + z^{-4}u_6^{(0)} + z^{-8}u_{10}^{(0)}$
7				3	$u_3^{(0)} + z^{-4}u_7^{(0)} + z^{-8}u_{11}^{(0)}$
8			2	0	$u_0^{(0)} + z^{-8}u_4^{(0)} + z^{-4}u_8^{(0)}$
9				1	$u_1^{(0)} + z^{-8}u_5^{(0)} + z^{-4}u_9^{(0)}$
10				2	$u_2^{(0)} + z^{-8}u_6^{(0)} + z^{-4}u_{10}^{(0)}$
11				3	$u_3^{(0)} + z^{-8}u_7^{(0)} + z^{-4}u_{11}^{(0)}$

1. táblázat

j	$\tilde{I}^{(1)}$	I_1	i_1	J_1	$u_j^{(2)}$
0	0	0	0	0	$u_0^{(1)} + u_2^{(1)}$
1				1	$u_1^{(1)} + u_3^{(1)}$
2			1	0	$u_0^{(1)} + z^{-6}u_2^{(1)}$
3				1	$u_1^{(1)} + z^{-6}u_3^{(1)}$
4	1	1	0	0	$u_4^{(1)} + z^{-2}u_6^{(1)}$
5				1	$u_5^{(1)} + z^{-2}u_7^{(1)}$
6			1	0	$u_4^{(1)} + z^{-8}u_6^{(1)}$
7				1	$u_5^{(1)} + z^{-8}u_7^{(1)}$
8	2	2	0	0	$u_8^{(1)} + z^{-4}u_{10}^{(1)}$
9				1	$u_9^{(1)} + z^{-4}u_{11}^{(1)}$
10			1	0	$u_8^{(1)} + z^{-10}u_{10}^{(1)}$
11				1	$u_9^{(1)} + z^{-10}u_{11}^{(1)}$

2. táblázat

$\tilde{I}^{(2)}$		I_2	
0	$2 \cdot 0 + 0$	$0 + 3 \cdot 0$	0
1	$2 \cdot 0 + 1$	$0 + 3 \cdot 1$	3
2	$2 \cdot 1 + 0$	$1 + 3 \cdot 0$	1
3	$2 \cdot 1 + 1$	$1 + 3 \cdot 1$	4
4	$2 \cdot 2 + 0$	$2 + 3 \cdot 0$	2
5	$2 \cdot 2 + 1$	$2 + 3 \cdot 1$	5

3. táblázat

j	$\tilde{I}^{(2)}$	I_2	i_2	J_0	$u_j^{(3)}$
0	0	0	0	0	$u_0^{(2)} + u_1^{(2)}$
1			1	0	$u_0^{(2)} + z^{-6}u_1^{(2)}$
2	1	3	0	0	$u_2^{(2)} + z^{-3}u_3^{(2)}$
3			1	0	$u_2^{(2)} + z^{-9}u_3^{(2)}$
4	2	1	0	0	$u_4^{(2)} + z^{-1}u_5^{(2)}$
5			1	0	$u_4^{(2)} + z^{-7}u_5^{(2)}$
6	3	4	0	0	$u_6^{(2)} + z^{-4}u_7^{(2)}$
7			1	0	$u_6^{(2)} + z^{-10}u_7^{(2)}$
8	4	2	0	0	$u_8^{(2)} + z^{-2}u_9^{(2)}$
9			1	0	$u_8^{(2)} + z^{-8}u_9^{(2)}$
10	5	5	0	0	$u_{10}^{(2)} + z^{-5}u_{11}^{(2)}$
11			1	0	$u_{10}^{(2)} + z^{-11}u_{11}^{(2)}$

4. táblázat

$\tilde{I}^{(3)}$		I_3	
0	$4 \cdot 0 + 2 \cdot 0 + 0$	$0 + 3 \cdot 0 + 6 \cdot 0$	0
1	$4 \cdot 0 + 2 \cdot 0 + 1$	$0 + 3 \cdot 0 + 6 \cdot 1$	6
2	$4 \cdot 0 + 2 \cdot 1 + 0$	$0 + 3 \cdot 1 + 6 \cdot 0$	3
3	$4 \cdot 0 + 2 \cdot 1 + 1$	$0 + 3 \cdot 1 + 6 \cdot 1$	9
4	$4 \cdot 1 + 2 \cdot 0 + 0$	$1 + 3 \cdot 0 + 6 \cdot 0$	1
5	$4 \cdot 1 + 2 \cdot 0 + 1$	$1 + 3 \cdot 0 + 6 \cdot 1$	7
6	$4 \cdot 1 + 2 \cdot 1 + 0$	$1 + 3 \cdot 1 + 6 \cdot 0$	4
7	$4 \cdot 1 + 2 \cdot 1 + 1$	$1 + 3 \cdot 1 + 6 \cdot 1$	10
8	$4 \cdot 2 + 2 \cdot 0 + 0$	$2 + 3 \cdot 0 + 6 \cdot 0$	2
9	$4 \cdot 2 + 2 \cdot 0 + 1$	$2 + 3 \cdot 0 + 6 \cdot 1$	8
10	$4 \cdot 2 + 2 \cdot 1 + 0$	$2 + 3 \cdot 1 + 6 \cdot 0$	5
11	$4 \cdot 2 + 2 \cdot 1 + 1$	$2 + 3 \cdot 1 + 6 \cdot 1$	11

5. táblázat

Nézzük meg például, hogy mit kapunk U_9-re. Az eredeti definíció alapján $U_i = \sum_0^{n-1}\left(z^{-i}\right)^j u_j$-ből $n = 12$ és $i = 9$ helyettesítéssel

$$U_9 = u_0^{(0)} + z^{-9}u_1^{(0)} + z^{-6}u_2^{(0)} + z^{-3}u_3^{(0)} + u_4^{(0)} + z^{-9}u_5^{(0)} + z^{-6}u_6^{(0)} + z^{-3}u_7^{(0)} + u_8^{(0)} + z^{-9}u_9^{(0)} + z^{-6}u_{10}^{(0)} + z^{-3}u_{11}^{(0)},$$

míg a módosított számítással

$$\begin{aligned} U_9 &= u_3^{(3)} = u_2^{(2)} + z^{-9}u_3^{(2)} = \left(u_0^{(1)} + z^{-6}u_2^{(1)}\right) + z^{-9}\left(u_1^{(1)} + z^{-6}u_3^{(1)}\right) \\ &= \left(u_0^{(0)} + u_4^{(0)} + u_8^{(0)}\right) + z^{-9}\left(u_1^{(0)} + u_5^{(0)} + u_9^{(0)}\right) + z^{-6}\left(u_2^{(0)} + u_6^{(0)} + u_{10}^{(0)}\right) \\ &+ z^{-3}\left(u_3^{(0)} + u_7^{(0)} + u_{11}^{(0)}\right) \\ &= u_0^{(0)} + z^{-9}u_1^{(0)} + z^{-6}u_2^{(0)} + z^{-3}u_3^{(0)} + u_4^{(0)} + z^{-9}u_5^{(0)} + z^{-6}u_6^{(0)} + z^{-3}u_7^{(0)} \\ &+ u_8^{(0)} + z^{-9}u_9^{(0)} + z^{-6}u_{10}^{(0)} + z^{-3}u_{11}^{(0)}, \end{aligned}$$

ami megegyezik az előbbi eredménnyel.

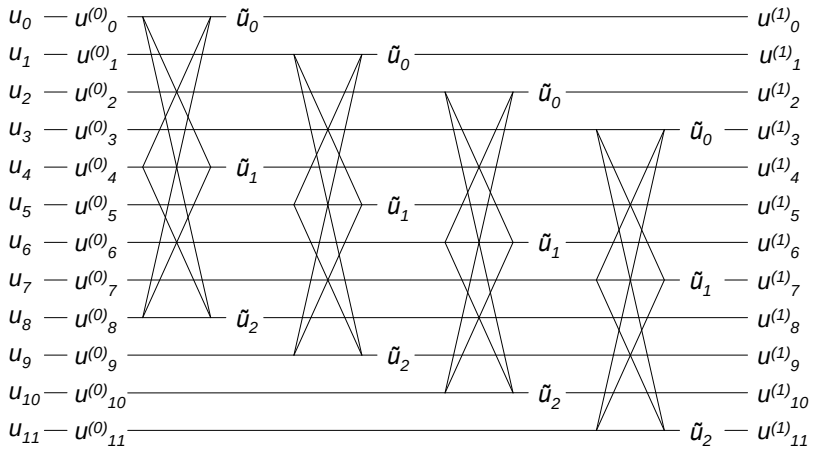
A gyors Fourier-transzformációt a 2. ábra - 4. ábra kicsit szemléletessé teszi. Az egész eljárást egyben az 5. ábra, míg U_9 kiszámítását a 6. ábra mutatja.

Ahhoz, hogy csökkenjen a szorzások száma, teljesülnie kell a $\prod_{k=0}^{t-1} n_k = n \geq \sum_{k=0}^{t-1} n_k$ feltételnek. Ez $t = 1$ esetén nyilvánvaló, míg $t = 2$ esetén ezt már igazoltuk, feltéve, hogy n mindkét faktora legalább 2. Innen pedig indukcióval egy $t \geq 2$-re

$$\prod_{k=0}^{t} n_k = n_t \prod_{k=0}^{t-1} n_k \geq n_t + \prod_{k=0}^{t-1} n_k \geq n_t + \sum_{k=0}^{t-1} n_k = \sum_{k=0}^{t} n_k,$$

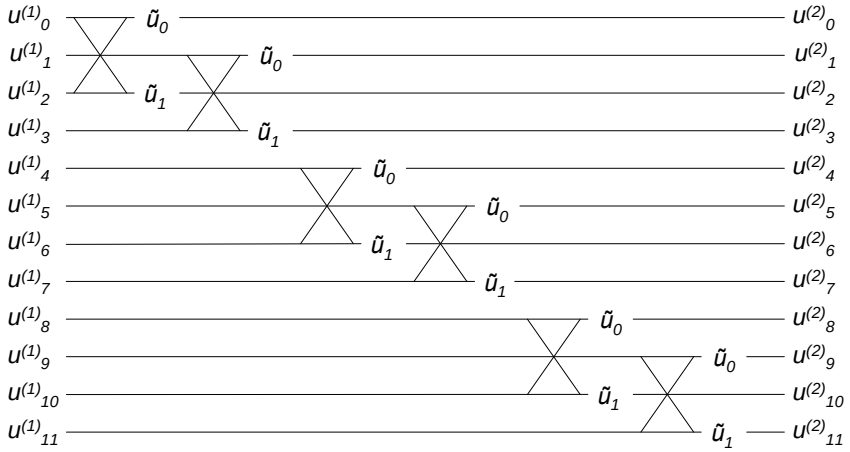
feltéve, hogy ismét minden faktor legalább 2.

A fenti számításoknál feltételeztük, hogy z hatványait nem kell számolni, azokat tároljuk a memóriában. Ha nem ez a helyzet, akkor a hatványokat előállító szorzásokat is figyelembe kell venni, ám ezek nagyságrendje hasonló az előbbi értékekhez.



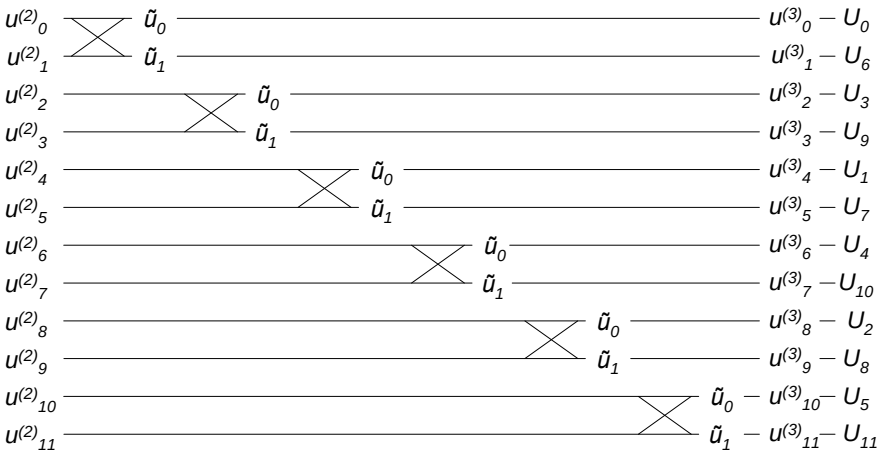
1. forduló

2. ábra



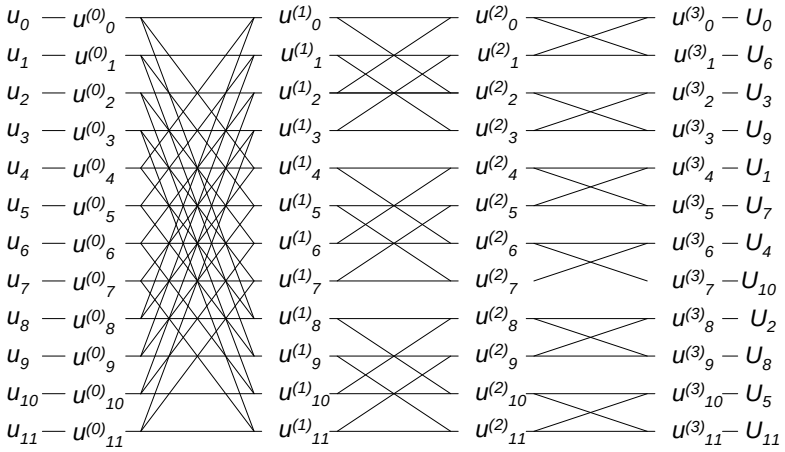
2. forduló

3. ábra



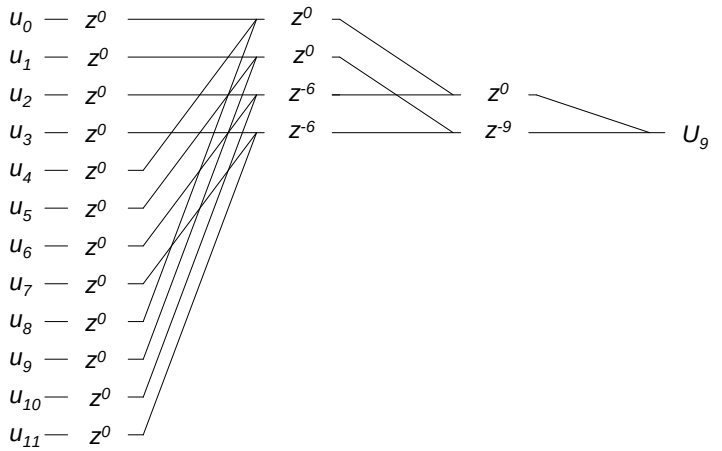
3. forduló

4. ábra



1-3. forduló

5. ábra



U_9 számítása

6. ábra

A számításhoz szükséges memória mérete is csökken. Míg az eredeti számításnál a transzformált vektor valamennyi komponensét az eredeti vektortól különböző helyen kell tárolni a számítások végéig, hiszen minden új komponens számításánál felhasználjuk az eredeti vektor mindenegyes komponensét, addig most csak $\tilde{u}$ komponenseit kell külön helyen tárolni, és amikor ennek az összes komponensét meghatároztuk, akkor ezek a komponensek már az eredeti vektor megfelelő helyére kerülhetnek, így a szükséges plusz tár mérete az $\tilde{u}$ maximális mérete. Ez viszont az i_s indexek maximuma, ami pedig az n_s faktorok maximuma.

A tételből következik, hogy ha n a t darab – nem feltétlenül különböző – p_i prím szorzata, akkor a diszkrét Fourier-transzformáció elvégezhető $n\sum_{i=0}^{t-1} p_i$ szorzással, és a szükséges tároló mérete $\max_{t>i\in\mathbb{N}}\{p_i\}$. Ha $n = p^t$, akkor a szükséges szorzások száma $tnp = pn\log_p n \sim n\log_p n$, és a többletmemória nagysága p, így a futási idő nagyjából $\frac{n}{\log_p n}$-szeres mértékben csökken, és ennek csupán egy p-méretű többletmemória az ára. $p = 2$ esetén a szorzások száma $n\log_2 n$, és ez már viszonylag kis t esetén is lényegesen kisebb, mint n^2. Például $t = 10$ mellett $n = 1024$, így az arány kisebb, mint 1% (10 az 1024-hez).

A gyors Fourier-transzformáció lehetővé teszi a konvolúció gyors kiszámítását is. Egy korábbi tétel alapján $\mathbf{u} * \mathbf{v} = \mathcal{F}_z^{-1}\big(\mathcal{F}_z(\mathbf{u})\mathcal{F}_z(\mathbf{v})\big)$. A bal oldal meghatározásához nagyságrendileg n^2 szorzás kell, míg a jobb oldal kiszámításához körülbelül $3n\sum_{i=0}^{t-1} n_i + n = n\big(3\sum_{i=0}^{t-1} n_i + 1\big)$ szorzásra van szükség, amely $3\sum_{i=0}^{t-1} n_i < n$ esetén nem nagyobb n^2-nél. Ha $t = 1$, akkor $3\sum_{i=0}^{t-1} n_i = 3n > n$. Most legyen $n = uv$. $uv > 3(u+v)$ pozitív u-val és v-vel pontosan akkor teljesül, ha $v > 3$ és $u > \frac{3v}{v-3}$. Ez biztosan igaz, ha $u \geq 7$ és $v \geq 6$, sőt, ekkor már $3\sum_{i=0}^{t-1} n_i + 1 < n$ is igaz. Legyen most $t > t' \in \mathbb{N}$-nel $u = \prod_{i=0}^{t'-1} n_i$ és $v = \prod_{i=t'}^{t-1} n_i$ az előbbi feltételnek megfelelő felbontása n-nek, és legyen az n valamennyi faktora legalább 2. Ekkor, figyelembe véve a korábbi eredményeket is,

$$\prod_{i=0}^{t-1} n_i = \prod_{i=0}^{t'-1} n_i \prod_{i=t'}^{t-1} n_i > 3\prod_{i=0}^{t'-1} n_i + 3\prod_{i=t'}^{t-1} n_i \geq 3\sum_{i=0}^{t'-1} n_i + 3\sum_{i=t'}^{t-1} n_i = 3\sum_{i=0}^{t-1} n_i,$$

vagyis a **gyors konvolúció** jobb, mint az eredeti eljárás.

A fenti gondolatoknál mindenütt a szorzások számát becsültük, de a szükséges összeadások, valamint értékadások száma is hasonló nagyságrendű, és a szorzás időigénye általában lényegesen meghaladja a másik két művelet elvégzéséhez szükséges időt, így a teljes futási idő lényegében véve azonos az előbbiekben meghatározott értékkel. A diszkrét Fourier-transzformáció gyakorlati alkalmazhatóságát éppen az tette lehetővé, hogy a futási idejét a gyors Fourier-transzformáció segítségével sikerült elfogadható nagyságúra redukálni. A 140. oldalon megadott algoritmus mutatja, hogy a gyors Fourier-transzformációt megvalósító program egy egyszerű, nem bonyolult program, könnyen programozható.

8. Polinomok rendje

Véges test feletti sorozatok periodikusságával kapcsolatban fontos a polinomok rendje.

8.1. Tétel

Ha $f \in \mathbb{F}_q[x]$, $\hat{f}(0) \neq 0$ és $\deg(f) = m$, ahol $m \in \mathbb{N}^+$, akkor van olyan $q^m - 1 \geq r \in \mathbb{N}^+$ egész, hogy $f | x^r - e$.

Δ

Bizonyítás:

$\mathbb{F}_q[x]/(f)$ (ahol (f) az f által generált ideál) nullától különböző elemeinek száma $q^m - 1$. Mivel $\hat{f}(0) \neq 0$, ezért x nem osztója f-nek, x irreducibilis polinom $\mathbb{F}_q$ fölött, tehát x és f, ennélfogva tetszőleges $i \in \mathbb{N}$-re x^i és f relatív prímek, így $x^i \not\equiv 0\ (f)$, $\mathbb{F}_q[x]/(f)$ x^i-vel reprezentált osztálya nem a nullelem a maradékosztály-gyűrűben. Ha $q^m - 1 \geq i \in \mathbb{N}$, akkor az ilyen kitevőjű x-hatványok száma q^m, több, mint a nem nulla elemek száma, ezért van legalább egy olyan i és j egész számpár, hogy $q^m - 1 \geq j > i \in \mathbb{N}$, és amelyre $x^i \equiv x^j\ (f)$, vagyis $f \left| x^j - x^i = x^i\left(x^{j-i} - e\right) \right.$ teljesül. Mivel x^i és f relatív prímek, ezért $f \left| x^{j-i} - e \right.$, és a korlátokat figyelembe véve $q^m - 1 \geq j - i \in \mathbb{N}^+$.

□

8.2. Definíció

Legyen $x^i g = f \in \mathbb{F}_q[x]$, ahol $i \in \mathbb{N}$ és $\hat{g}(0) \neq 0$, továbbá $r = \min_{k \in \mathbb{N}^+}\{g | x^k - e\}$. Ekkor r az f **polinom rendje**, **periódusa** vagy **exponense**, jele $o(f)$.

Δ

8.3. Tétel

Tetszőleges $0 \neq f \in \mathbb{F}_q[x]$ polinomnak van egyértelműen meghatározott rendje. Ha $f = x^i g$, ahol $i \in \mathbb{N}$, akkor $o(f) = o(g)$, és ha $\hat{g}(0) \neq 0$, továbbá $\deg(g) = m$, akkor $t \geq o(f) \in \mathbb{N}^+$ úgy, hogy $t = \max\{1, q^m - 1\}$.

Δ

Bizonyítás:

Az $\mathbb{F}_q[x]$-beli tetszőleges nem nulla polinom felírható $x^i g$ alakban alkalmas nemnegatív egész i-vel és $\mathbb{F}_q$ fölötti g polinommal, amelyre $\hat{g}(0) \neq 0$. Az első tétel szerint van olyan pozitív egész k, amelyre g osztója az $x^k - e$ polinomnak, ezért a definícióban megadott halmaz a pozitív egész számok halmazának nem üres részhalmaza, amelyben $\mathbb{N}^+$ jólrendezettsége folytán van egyértelműen meghatározott legkisebb elem, így f-nek van egyértelmű rendje. A következő állítás a definíció közvetlen következménye, az utolsó pedig a definíciónak és az első tételnek azzal a kiegészítéssel, hogy amennyiben g egy nem nulla konstans polinom, akkor a foka 0, viszont a rend definíciójában pozitív egészek minimuma áll, és a test tetszőleges nem nulla eleme osztója az $x - e$ polinomnak, ekkor tehát a rend 1.

□

8.4. Tétel

Legyen $f \in \mathbb{F}_q[x]$, $\hat{f}(0) \neq 0$ és $c \in \mathbb{N}^+$. Ekkor f akkor és csak akkor osztója az $x^c - e$, polinomnak, ha $o(f) | c$.

Δ

Bizonyítás:

$\hat{f}(0) \neq 0$-t azért kell kikötni, mert ellenkező esetben vagy $f = 0$, és így $o(f)$ nem definiált, vagy nem lehet osztója $x^c - e$-nek egyetlen pozitív egész c-re sem. Legyen $o(f) = r$. A rend definíciója és $\hat{f}(0) \neq 0$ alapján $f|x^r - e$, így f akkor és csak akkor osztója $x^c - e$-nek, ha osztója $x^r - e$ és $x^c - e$ legnagyobb közös osztójának. A 39. oldalon foglalkoztunk $x^m - e$ és $x^n - e$ legnagyobb közös osztójával, és láttuk, hogy $(x^m - e, x^n - e) = x^{(m,n)} - e$. $(m, n) \leq m$, és itt egyenlőség akkor és csak akkor teljesül, ha m osztója n-nek. r pozitív egész, ezért $d = (r, c)$ is pozitív egész szám. Mivel r az f rendje, ezért f csak akkor lehet osztója $x^d - e$-nek, ha $d \geq r$, másrészt d nem nagyobb r-nél, így pontosan akkor osztója f $x^d - e$-nek, ha $d = r$, tehát akkor és csak akkor, ha r osztója c-nek.

□

8.5. Tétel

Ha f egy m-edfokú irreducibilis polinom a q-elemű test fölött, $\hat{f}(0) \neq 0$, és α az f egy gyöke a felbontási testben, akkor f rendje megegyezik α rendjével a q^m-elemű test multiplikatív csoportjában.

Δ

Bizonyítás:

$\hat{f}(0) \neq 0$ biztosítja, hogy $\alpha \neq 0$, ezért van olyan pozitív egész i kitevő, amellyel $\alpha^i = e$. Legyen f rendje r, α multiplikatív rendje s. $\alpha^s = e$ következtében α gyöke az $x^s - e$ polinomnak, tehát $f|x^s - e$, így az előző tétel szerint $r|s$. Másrészt $f|x^r - e$ maga után vonja, hogy α gyöke az $x^r - e$ polinomnak, így $\alpha^r - e = 0$, azaz $\alpha^r = e$, ami pedig akkor és csak akkor teljesül, ha $s|r$. Mivel r és s egyaránt pozitív egész, a kölcsönös oszthatóság pontosan azt jelenti, hogy $r = s$.

□

8.6. Következmény

p-karakterisztikájú $\mathbb{F}_q$ test fölött irreducibilis, m-edfokú f polinomra $r|q^m - 1$, és $(r, p) = 1$, ahol $r = o(f)$.

Δ

Bizonyítás:

$\hat{f}(0) = 0$ az irreducibilitás miatt csupán $f = cx$ esetén lehetséges, ahol $c \in \mathbb{F}_q^*$. Ekkor $r = 1$, és 1 minden egésznek osztója, és minden egészhez relatív prím. f $\mathbb{F}_q$ fölötti felbontási teste $\mathbb{F}_{q^m}$, ezért $f|x^{q^m} - x$, és ha $\hat{f}(0) \neq 0$, akkor $f|x^{q^m-1} - e$, innen pedig $r|q^m - 1$, tehát most is teljesül az oszthatóság. De $q = p^n$ egy n pozitív egésszel, ezért $q^m - 1$ relatív prím p-hez, és ekkor $q^m - 1$ minden osztója is relatív prím p-hez.

□

8.7. Tétel

Az $\mathbb{F}_q$ fölötti normált m-edfokú, r-edrendű irreducibilis polinomok száma $r \geq 2$ és $m = o_r(q)$ esetén $\frac{\varphi(r)}{m}$, $m = 1 = r$ mellett 2, egyébként 0.

Δ

Normált polinom a főpolinom más megnevezése, azaz olyan polinom, amelynek főegyütthatója, vagyis legmagasabb fokú tagjának együtthatója a test (vagy gyűrű) egységeleme.

Bizonyítás:

Legyen f tetszőleges nem nulla polinom, akkor ez egyértelműen írható $x^i g$ alakban nemnegatív egész i-vel és olyan g-vel, amelyre $\hat{g}(0) \neq 0$. Ha f irreducibilis, akkor ez csak úgy lehet, ha $i = 1$ és $g = c \neq 0$ egy $\mathbb{F}_q^*$-beli c-vel, vagy ha $i = 0$, tehát $f = g$, $\hat{f}(0) \neq 0$, és $\deg(f) \geq 1$. $\hat{f}(0) \neq 0$ és

$\deg(f) > 1$ esetén f rendje legalább 2, hiszen legalább másodfokú polinom nem lehet osztója $x - e$-nek, ezért elsőrendű polinom nem lehet elsőfokúnál magasabb fokú. Konstans polinom nem irreducibilis, így $o(f) = 1$ irreducibilis polinommal csak $\deg(f) = 1$ esetén lehetséges. Minden elsőfokú polinom irreducibilis; az elsőfokú normált polinomok $x - c$ alakúak, ahol c a test tetszőleges eleme. Ha $c = 0$, akkor $f = x$, és x rendje 1, és ekkor $m = 1 = r$. $x - e = e(x - c) + (c - e)$, ezért $x - e$ akkor és csak akkor osztható $x - c$-vel, ha $c = e$, és így $x - e$ az egyetlen olyan polinom, amelyre $r = 1$ és $\hat{f}(0) \neq 0$, ezért $r = 1$ csak $m = 1$ mellett lehetséges irreducibilis normált polinomokkal, és ilyen tényleg 2 van (mármint olyan irreducibilis normált polinom, amelynek a rendje 1). A továbbiakban legyen $r \geq 2$. Ha f egy r-edrendű irreducibilis főpolinom, akkor bármely α gyöke $\mathbb{F}_q$ fölötti primitív r-edik egységgyök, f osztója az $\mathbb{F}_q$ fölötti r-edik körosztási polinomnak, és fordítva, ezen körosztási polinom minden irreducibilis főpolinom osztója egy $\mathbb{F}_q[x]$-beli r-edrendű normált irreducibilis polinom. Ezek foka egységesen $m = o_r(q)$, és a számuk $\frac{\varphi(r)}{m}$, ugyanakkor, ha egy $2 \leq r \in \mathbb{N}$-re $m \neq o_r(q)$, akkor látjuk, hogy nincs olyan $\mathbb{F}_q$ fölötti polinom, amelynek rendje r és a foka m.

□

8.8. Tétel

Ha g a p karakterisztikájú $\mathbb{F}_q$ test fölötti irreducibilis polinom, $\hat{g}(0) \neq 0$, és $f = g^n$, ahol n egy pozitív egész szám, továbbá t olyan egész szám, hogy $p^{t-1} < n \leq p^t$, akkor $o(f) = p^t o(g)$.

Δ

Bizonyítás:

Az nyilvánvaló, hogy $t \geq 0$, hiszen $p > 1$ miatt $p^{-1} < 1 \leq n$. Legyen $o(g) = v$ és $o(f) = u$. $\hat{g}(0) \neq 0$-ból következik, hogy $\hat{f}(0) \neq 0$, tehát $f | x^u - e$. Mivel $g | f$, ezért $g | x^u - e$, amiből következik, hogy $v | u$. $f = g^n | (x^v - e)^n \big| (x^v - e)^{p^t} \big| x^{vp^t} - e$, ezért $u | vp^t$, és ez $v | u$-val azt adja, hogy $u = vp^t$ egy $t \geq s \in \mathbb{N}$ egésszel. Mivel g irreducibilis, ezért $(v, p) = 1$, ennél fogva $x^v - e$ gyökei egyszeresek, de akkor $x^u - e = (x^v - e)^{p^s}$ mindenegyes gyöke pontosan p^s-szeres. Mivel g^n osztója $x^u - e$-nek, ezért $x^u - e$ gyökei legalább n-szeresek, tehát $n \leq p^s$, ami t választása folytán azonos a $t \leq s$ feltétellel, így a korábbi egyenlőtlenséggel együtt $s = t$, és $u = p^t v$.

□

8.9. Tétel

Ha $g_0, \ldots, g_{s-1}$ nem nulla polinomok a q-elemű test fölött, és $s > i \in \mathbb{N}$-re $\hat{g}_i(0) \neq 0$, akkor legkisebb közös többszörösük rendje megegyezik a rendek legkisebb közös többszörösével.

Δ

Bizonyítás:

Legyen $o(g_i) = n_i$, a polinomok legkisebb közös többszöröse g, ennek rendje n, és a rendek legkisebb közös többszöröse t. Ekkor valamennyi lehetséges i indexre $n_i | t$, és akkor $g_i | x^t - e$, így $g | x^t - e$, és $n | t$. Viszont megint minden $s > i \in \mathbb{N}$-re $g_i | g | x^n - e$, ahonnan az $n_i | n$ oszthatóságot kapjuk. ekkor t osztója n-nek, és t és n pozitív egész, tehát t és n megegyezik.

□

8.10. Következmény

Ha $g_0, \ldots, g_{s-1}$ páronként relatív prím nem nulla polinomok a q-elemű test fölött, és g szorzatukra $\hat{g}(0) \neq 0$, akkor g rendje megegyezik a g_i-k rendjének legkisebb közös többszörösével.

Δ

Bizonyítás:

$\hat{g}(0) \neq 0$-ból $\hat{g}_i(0) \neq 0$, és relatív prímek legkisebb közös többszöröse a szorzatuk.

□

8.11. Tétel

Legyen $\mathrm{char}(\mathbb{F}_q) = p$, $0 \neq f = ax^k \prod_{i=0}^{s-1} f_i^{n_i} \in \mathbb{F}_q[x]$, ahol $s > i \in \mathbb{N}$-re $n_i \in \mathbb{N}^+$, $\hat{f}_i(0) \neq 0$ és az f_i-k páronként különböző, $\mathbb{F}_q$ fölött irreducibilis polinomok, $k \in \mathbb{N}$, $a \in \mathbb{F}_q$, r az $o(f_i) = r_i$-k legkisebb közös többszöröse, $n = \max_{s>i\in\mathbb{N}}\{n_i\}$ és $t = \min_{t\in\mathbb{N}}\{p^t \geq n\}$. Ekkor $o(f) = p^t r$.

Δ

Bizonyítás:

t-ről tudjuk, hogy nemnegatív egész. $a \in \mathbb{F}_q^*$, ezért egység $\mathbb{F}_q[x]$-ben, tehát $a^{-1}f$ és f ugyanazon polinomok osztói, így a rendjük megegyezik, továbbá a rend nem függ x^k-tól sem. Az f_i-k páronként relatív prímek, a hatványaik is azok, továbbá a 0 nem gyökük, ezért a szorzatuk rendje megegyezik a rendjeik legkisebb közös többszörösével. Mindegyik rend p egy hatványának és a megfelelő f_i rendjének a szorzata. Ez utóbbi relatív prím p-hez, így a legkisebb közös többszörös p maximális kitevőjű hatványának és az f_i-k rendje legkisebb közös többszörösének szorzata, a p kitevője viszont a polinom kitevőjének monoton növekvő függvénye.

□

8.12. Tétel

Nem nulla polinom rendje megegyezik reciprokának rendjével.

Δ

Bizonyítás:

Legyen $f = x^i g$, ahol $i \in \mathbb{N}$ és $\hat{g}(0) \neq 0$. Ekkor $f^* = g^*$ és $o(f) = o(g)$, így elég azt belátni, hogy g és g^* rendje azonos. Ha g rendje r, akkor $g|x^r - e$, azaz $x^r - e = ug$ egy u polinommal, és innen $u^* g^* = (ug)^* = (x^r - e)^* = e - x^r = -e(x^r - e)$, tehát g^* osztja $x^r - e$-t, és így g^* rendje, r^* is osztója r-nek. Hasonló módon $(g^*)^*$ rendje osztója r^*-nak, és mivel $(g^*)^* = g$, ezért $r|r^*$, vagyis r és r^* kölcsönösen osztják egymást, ami pozitív egészek esetén csak egyenlőséggel lehetséges, márpedig r és r^* egyaránt pozitív egész, így $r = r^*$.

□

8.13. Definíció

Ha f az $\mathbb{F}_{q^m}$ egy primitív elemének $\mathbb{F}_q$ fölötti minimál-polinomja, akkor f **primitív polinom** $\mathbb{F}_q$ **fölött**.

Δ

8.14. Tétel

Az $\mathbb{F}_q[x]$-beli m-edfokú f főpolinom rendje pontosan akkor $q^m - 1$, ha $q = 2$ és $f = x$, vagy f primitív polinom $\mathbb{F}_q$ fölött.

Δ

Bizonyítás:

Ha $q = 2$ és $f = x$, akkor $o(f) = 1$ és $m = 1$, vagyis $q^m - 1 = 1$, míg m-edfokú primitív polinom egyben m-edfokú irreducibilis polinom is, így a rendje megegyezik bármely gyökének rendjével, amely a definíció alapján $q^m - 1$, hiszen a gyök a test primitív eleme.

Nézzük a fordított irányt. Legyen $f = x^k g$, ahol $k \in \mathbb{N}$ és $\hat{g}(0) \neq 0$. Amennyiben $k = m$, akkor $o(f) = o(g) = 1$, és $1 = q^m - 1$ akkor és csak akkor igaz, ha $q^m = 2$, azaz pontosan akkor, ha $q = 2$ és $m = 1$, vagyis amikor f a kételemű test fölötti polinom és $f = x$. Hasonlóan kapjuk, hogy $m > k \in \mathbb{N}^+$ esetén $o(f) = o(g) \leq q^{m-k} - 1 < q^m - 1$, ezért a továbbiakban legyen $m > k = 0$. Ha $f = f_1 f_2$, ahol f_1 foka $m > m_1$, f_2 foka $m > m_2$, és a két polinom relatív prím, akkor

$$o(f) = [o(f_1), o(f_2)] \leq o(f_1)o(f_2) \leq (q^{m_1} - 1)(q^{m_2} - 1) < (q^{m_1} - 1)q^{m_2}$$
$$= q^{m_1+m_2} - q^{m_2} = q^m - q^{m_2} \leq q^m - 2 < q^m - 1,$$

míg ha f egy g irreducibilis, a nullában nem 0 polinom r-edik hatványa, ahol $1 < r \in \mathbb{N}$, és p a test karakterisztikája, akkor $p|o(f) \leq q^m - 1$, ám p nem osztója $q^m - 1$-nek, így f rendje ismét kisebb, mint $q^m - 1$. Végül, ha f irreducibilis, de nem primitív, akkor a rendje a gyökének a q^m-elemű testbeli rendjével azonos, ami ismét kisebb, mint $q^m - 1$, hiszen ez a gyök nem primitív elem.

□

9. Elem nyoma; linearizált és affin polinomok

9.1. Definíció

Legyen $\mathcal{L}$ a q-elemű $\mathcal{K}$ test m-edfokú bővítése, és $\alpha \in \mathcal{L}$. Ekkor $\sum_{i=0}^{m-1} \alpha^{q^i}$ az α $\mathcal{K}$ **feletti nyoma**, amit $\mathrm{Tr}_{L|K}(\alpha)$ vagy $\mathrm{S}_{L|K}(\alpha)$ jelöl. Ha $\mathcal{K}$ prímtest, akkor egyszerűen $\mathrm{Tr}_L(\alpha)$-t vagy $\mathrm{S}_L(\alpha)$-t írunk, ez α **abszolút nyoma**. Ha nyilvánvaló, hogy mely testekről van szó, akkor az elem nyomát röviden $\mathrm{Tr}(\alpha)$-val vagy $\mathrm{S}(\alpha)$-val jelöljük.

Δ

S a német *Spur*, míg Tr az angol *trace* szó alapján jelöli a testbeli elem nyomát. Mi a továbbiakban a rövidebb S jelölést alkalmazzuk.

9.2. Tétel

Legyen $\mathcal{L}$ a q-elemű $\mathcal{K}$ test m-edfokú bővítése, α és βaz L, c a K tetszőleges eleme. Ekkor

1. $\mathrm{S}(\alpha+\beta) = \mathrm{S}(\alpha) + \mathrm{S}(\beta)$;
2. $\mathrm{S}(c\alpha) = c\mathrm{S}(\alpha)$;
3. $\mathrm{S}(c) = mc$;
4. $\mathrm{S}(\alpha^q) = \mathrm{S}(\alpha)$;
5. S az $\mathcal{L}$-nek mint $\mathcal{K}$ feletti lineáris térnek $\mathcal{K}$-ra mint a $\mathcal{K}$ test feletti vektortérre való lineáris leképezése.

Δ

Bizonyítás:

A $\sigma_i: L \to L$ leképezés, ahol $\sigma_i(\alpha) = \alpha^{q^i}$, bármely nemnegatív egész i-re az $\mathcal{L}$ test automorfizmusa, amely a $\mathcal{K}$ test elemein az identikus leképezés, ezért igaz az 1., 2. és 3. állítás. $\alpha^{q^m} = \alpha$, innen $\sum_{i=0}^{m-1}(\alpha^q)^{q^i} = \sum_{i=1}^{m} \alpha^{q^i} = \sum_{i=0}^{m-1} \alpha^{q^i}$, ami igazolja 4.-et.

Az első két állítás biztosítja, hogy a nyom az $\mathcal{L}$ vektortérnek $\mathcal{L}$ vektortérbe való lineáris leképezése. Ismét $\alpha^{q^m} = \alpha$-ra hivatkozva $\left(\mathrm{S}(\alpha)\right)^q = \left(\sum_{i=0}^{m-1} \alpha^{q^i}\right)^q = \sum_{i=1}^{m} \alpha^{q^i} = \sum_{i=0}^{m-1} \alpha^{q^i} = \mathrm{S}(\alpha)$ mutatja, hogy ez a leképezés valójában K-ba történik. Azt kell még bizonyítani, hogy ez a leképezés egyben szürjektív is. Ehhez elegendő azt belátni, hogy van olyan L-beli α elem, amelynek nem 0 a nyoma, ebből már következik a szürjektivitás.

Valóban, 0 nyoma 0. Most tegyük fel, hogy létezik olyan α elem L-ben, amelynek nem nulla a nyoma. Legyen $\mathrm{S}(\alpha) = a \in K^*$, és b a K^* tetszőleges eleme. Mivel K^* csoport a szorzással, így biztosan van olyan K^*-beli c elem, amellyel fennáll a $ca = b$ egyenlőség, és így $\mathrm{S}(c\alpha) = c\mathrm{S}(\alpha) = ca = b$, azaz b is egy L-beli elem nyoma, b is benne van a leképezés képterében. Lássuk tehát be ilyen α létezését. Legyen $\beta \in L$, és $\mathrm{S}(\beta) = 0$. Ekkor $0 = \sum_{i=0}^{m-1} \beta^{q^i}$, tehát β gyöke a q^{m-1}-edfokú $f = \sum_{i=0}^{m-1} x^{q^i}$ polinomnak. Ennek a polinomnak legfeljebb q^{m-1} különböző gyöke van, ugyanakkor L elemeinek száma q^m, és mivel $q > 1$, ezért $q^m > q^{m-1}$, van olyan L-beli elem, amely nem gyöke az f polinomnak, tehát amelynek a nyoma nem a test nulleleme.

□

9.3. Tétel

Legyen az $\mathcal{L}$ véges test a $\mathcal{K}$ test bővítése, $\alpha \in L$ tetszőleges rögzített elem, és $\mathbf{T}_\alpha$ az L elemein értelmezett olyan szabály, hogy az L bármely β elemére $\mathbf{T}_\alpha(\beta) = \mathrm{S}(\alpha\beta)$. Ekkor $\alpha = 0$ esetén $\mathbf{T}_\alpha = \mathbf{0}$,

egyébként $\mathbf{T}_\alpha$ az $\mathcal{L}$-nek mint $\mathcal{K}$ test feletti vektortérnek a $\mathcal{K}$ vektortérre való lineáris leképezése. Különböző L-beli α-hoz az $\mathcal{L}$ különböző, $\mathcal{K}$-ba való lineáris leképezése tartozik, és az $\mathcal{L}$ vektortér bármely, a $\mathcal{K}$ vektortérbe való $\mathbf{T}$ lineáris leképezéséhez van olyan L-beli α, hogy $\mathbf{T} = \mathbf{T}_\alpha$.

Δ

Bizonyítás:

$\alpha\beta$ az L eleme, a nyom az L minden elemére értelmezett, egyértelmű, és értéke K-beli, tehát $\mathbf{T}_\alpha$ valóban L-nek K-ba való leképezése. Ha $\alpha = 0$, akkor $\alpha\beta = 0$, és $\mathbf{T}_\alpha(\beta) = \mathrm{S}(\alpha\beta) = \mathrm{S}(0) = 0$ az L minden elemére, tehát $\mathbf{T}_\alpha = \mathbf{0}$. Ellenkező esetben, ha β végigfut L elemein, akkor $\alpha\beta$ is felveszi L minden elemét, ezért a leképezés K-ra történik. A nyom lineáris leképezés, így K-beli b, c és L-beli β, γ elemekkel $\mathbf{T}_\alpha(b\beta + c\gamma) = \mathrm{S}\big(\alpha(b\beta + c\gamma)\big) = b\mathrm{S}(\alpha\beta) + c\mathrm{S}(\alpha\gamma) = b\mathbf{T}_\alpha(\beta) + c\mathbf{T}_\alpha(\gamma)$, tehát $\mathbf{T}_\alpha$ egy $\mathcal{L} \to \mathcal{K}$ lineáris szürjektív leképezés.

Ha a és b a K, α és β az L eleme, akkor

$$\begin{aligned}\big(a\mathbf{T}_\alpha + b\mathbf{T}_\beta\big)(\gamma) &= a\mathbf{T}_\alpha(\gamma) + b\mathbf{T}_\beta(\gamma) = \mathrm{S}\big((a\alpha)\gamma\big) + \mathrm{S}\big((b\beta)\gamma\big) \\ &= \mathrm{S}\big((a\alpha + b\beta)\gamma\big) = \mathbf{T}_{a\alpha+b\beta}(\gamma).\end{aligned}$$

Ha $\alpha \neq \beta$, akkor létezik $\alpha - \beta$-nak inverze, $(\alpha - \beta)^{-1}$. Legyen $\delta \in L^*$ olyan, hogy $\mathrm{S}(\delta) \neq 0$, és legyen ezzel a δ-val $\gamma = (\alpha - \beta)^{-1}\delta$. Ekkor $\mathbf{T}_\alpha(\gamma) - \mathbf{T}_\beta(\gamma) = \mathbf{T}_{\alpha-\beta}(\gamma) = \mathrm{S}\big((\alpha - \beta)\gamma\big) = \mathrm{S}(\delta) \neq 0$, $\mathbf{T}_\alpha(\gamma) \neq \mathbf{T}_\beta(\gamma)$, és így $\mathbf{T}_\alpha$ és $\mathbf{T}_\beta$ különböző leképezések. Végül nézzük az utolsó állítást. Legyen K elemeinek száma q, a bővítés foka m, ekkor $\mathcal{L}$-nek van m elemű bázisa $\mathcal{K}$ fölött. Egy lineáris transzformációt egyértelműen meghatároz, ha megadjuk egy bázis elemeinek a képét. Bármely báziselemnek egymástól függetlenül q különböző képe lehet, tehát összesen q^m különböző lineáris $\mathcal{L} \to \mathcal{K}$ leképezés definiálható. De éppen ennyi a $\mathbf{T}_\alpha$-k száma is, tehát ez a rész is igaz.

□

A fenti tételből következik, hogy $\mathcal{L}$-nek $\mathcal{K}$-ba való bármely nem nulla homomorfizmusa epimorfizmus.

9.4. Tétel

Ha $\mathcal{M}$ véges test, $\mathcal{M}|\mathcal{L}|\mathcal{K}$, és $\alpha \in \mathcal{M}$, akkor $\mathrm{S}_{M|K}(\alpha) = \mathrm{S}_{L|K}\left(\mathrm{S}_{M|L}(\alpha)\right)$.

Δ

Bizonyítás:

$\mathrm{S}_{M|L}(\alpha) \in L$, így létezik $\mathrm{S}_{L|K}\left(\mathrm{S}_{M|L}(\alpha)\right)$. Ha $[\mathcal{L}:\mathcal{K}] = m$ és $[\mathcal{M}:\mathcal{L}] = n$, úgy $[\mathcal{M}:\mathcal{K}] = mn$, és

$$\mathrm{S}_{L|K}\left(\mathrm{S}_{M|L}(\alpha)\right) = \sum_{i=0}^{m-1}\left(\sum_{j=0}^{n-1}\alpha^{(q^m)^j}\right)^{q^i} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha^{q^{mj+i}} = \sum_{k=0}^{mn-1}\alpha^{q^k} = \mathrm{S}_{M|K}(\alpha),$$

ahol q a K elemeinek száma, ugyanis mialatt i 0-tól $m-1$-ig és j 0-tól $n-1$-ig megy, $k = mj + i$ pontosan egyszer felveszi a $0 \leq t < mn$ intervallum minden egész elemét.

□

9.5. Tétel

Ha $\mathcal{L}_1$ a $\mathcal{K}$ véges test n_1-edfokú, és $\mathcal{L}_2$ egy n_2-edfokú bővítése, n_1 és n_2 relatív prímek, és $\mathcal{M}$ a $\mathcal{K}$ $\mathcal{L}_1$-et és $\mathcal{L}_2$-t tartalmazó $n = n_1n_2$-edfokú bővítése, továbbá α_1 az $\mathcal{L}_1$ és α_2 az $\mathcal{L}_2$ test eleme, akkor $\mathrm{S}_{M|K}(\alpha_1\alpha_2) = \mathrm{S}_{L_1|K}(\alpha_1)\mathrm{S}_{L_2|K}(\alpha_2)$.

Δ

Bizonyítás:

Mivel n_1 és n_2 relatív prím, ezért tetszőleges $0 \leq k < n_1 n_2$ egészhez van egy és csak egy olyan $(i_1, i_2) \in \mathbb{N}^2$ számpár, amellyel $i_1 < n_1$, $i_2 < n_2$, $i_1 \equiv k\ (n_1)$ és $i_2 \equiv k\ (n_2)$. Ekkor $\alpha_1^{q^{i_1}} = \alpha_1^{q^k}$ és $\alpha_2^{q^{i_2}} = \alpha_2^{q^k}$, tehát $\alpha_1^{q^{i_1}} \alpha_2^{q^{i_2}} = \alpha_1^{q^k} \alpha_2^{q^k} = (\alpha_1 \alpha_2)^{q^k}$. Ezt felhasználva

$$\mathrm{S}_{L_1|K}(\alpha_1)\mathrm{S}_{L_2|K}(\alpha_2) = \left(\sum_{i_1=0}^{n_1-1} \alpha_1^{q^{i_1}}\right)\left(\sum_{i_2=0}^{n_2-1} \alpha_2^{q^{i_2}}\right) = \sum_{i_1=0}^{n_1-1}\sum_{i_2=0}^{n_2-1} \alpha_1^{q^{i_1}} \alpha_2^{q^{i_2}}$$
$$= \sum_{k=0}^{n_1 n_2-1} (\alpha_1 \alpha_2)^{q^k} = \mathrm{S}_{M|K}(\alpha_1 \alpha_2).$$

□

9.6. Következmény

Legyen az $i = 1$ és $i = 2$ indexekre $\mathcal{L}_i$ a $\mathcal{K}$ test n_i-edfokú bővítése, $n = [n_1, n_2]$, $d = (n_1, n_2)$, továbbá $\mathcal{M}_n$ és $\mathcal{M}_d$ a $\mathcal{K}$ n-edfokú és d-edfokú bővítése úgy, hogy $\mathcal{M}_n|\mathcal{L}_i|\mathcal{M}_d|\mathcal{K}$, és végül legyen $\alpha_i \in L_i$. Ekkor $\mathrm{S}_{M_n|K}(\alpha_1\alpha_2) = \mathrm{S}_{M_d|K}\left(\mathrm{S}_{L_1|M_d}(\alpha_1)\mathrm{S}_{L_2|M_d}(\alpha_2)\right)$.

Δ

Bizonyítás:

Mivel $d|n_i|n$, így létezik a $\mathcal{K}$-nak olyan $\mathcal{M}_n$ és $\mathcal{M}_d$ bővítése, amellyel $\mathcal{M}_n|\mathcal{L}_i|\mathcal{M}_d|\mathcal{K}$. $\mathcal{L}_i$ az $\mathcal{M}_d$ test $\frac{n_i}{d}$-edfokú bővítése. $\frac{n_1}{d}$ és $\frac{n_2}{d}$ relatív prímek, és $\mathcal{M}_n$ az $\mathcal{M}_d$-nek $\frac{n}{d} = \frac{\frac{n_1 n_2}{d}}{d} = \frac{n_1}{d} \cdot \frac{n_2}{d}$-edfokú bővítése, így a 9.5. Tétel szerint $\mathrm{S}_{M_n|M_d}(\alpha_1\alpha_2) = \mathrm{S}_{L_1|M_d}(\alpha_1)\mathrm{S}_{L_2|M_d}(\alpha_2)$. A 9.4. Tételt alkalmazva pedig azt kapjuk, hogy $\mathrm{S}_{M_n|K}(\alpha_1\alpha_2) = \mathrm{S}_{M_d|K}\left(\mathrm{S}_{M_n|M_d}(\alpha_1\alpha_2)\right) = \mathrm{S}_{M_d|K}\left(\mathrm{S}_{L_1|M_d}(\alpha_1)\mathrm{S}_{L_2|M_d}(\alpha_2)\right)$.

□

A továbbiakban az előbbi eredményeket részben általánosítjuk. Először a lineáris algebra néhány fogalmát tekintjük át.

Legyen $\mathcal{V}$ egy $\mathcal{K}$ test feletti lineáris tér, és $\mathcal{W}$ a $\mathcal{V}$ egy lineáris altere. Ha $\mathbf{u}$ a V egy eleme, akkor $\mathbf{u} + W$ a $\mathcal{W}$ (**u szerinti**) **eltoltja**, és $\mathbf{u} + W$ a $\mathcal{V}$ egy **affin altere**. $\mathbf{v} \in V$ akkor és csak akkor eleme $\mathbf{u} + W$-nek, ha $\mathbf{v} - \mathbf{u} \in W$, és ekkor $\mathbf{u} + W = \mathbf{v} + W$, vagyis az eltolt bármely elemével reprezentálható. Ugyanazon lineáris altér szerinti két eltolt vagy egybeesik, vagy diszjunkt, és nyilván egyik eltolt sem üres, így az eltoltak a tér elemeinek egy osztályozását adják. A V tetszőleges $\mathbf{u}$ és $\mathbf{v}$, valamint a K tetszőleges c elemével $(\mathbf{u} + W) + (\mathbf{v} + W) = (\mathbf{u} + \mathbf{v}) + W$ és $c(\mathbf{u} + W) = (c\mathbf{u}) + W$, így a $\mathcal{W}$ szerinti affin alterek egy lineáris teret alkotnak. Ez a lineáris tér a $\mathcal{V}$ lineáris tér $\mathcal{W}$ altér szerinti **faktortere**, amelyet $\mathcal{V}/\mathcal{W}$ jelöl. Ha $\mathcal{V}$ véges dimenziós tér, akkor $\dim_K \mathcal{V} = \dim_K \mathcal{W} + \dim_K \mathcal{V}/\mathcal{W}$. Amennyiben φ a $\mathcal{K}$ test feletti $\mathcal{V}_1$ lineáris térnek a $\mathcal{K}$ test feletti $\mathcal{V}_2$ lineáris térbe való művelettartó leképezése, és a leképezés magja, vagyis a leképezés nulltere $\mathcal{W}_1$, továbbá a leképezés képe $\mathcal{W}_2$, akkor az előbbi $\mathcal{V}_1$-nek, az utóbbi $\mathcal{V}_2$-nek altere, és $\mathcal{W}_2 \cong \mathcal{V}_1/\mathcal{W}_1$.

Ha $\varphi: \mathcal{V}_1 \to \mathcal{V}_2$ lineáris leképezés, és $\mathbf{v}$ V_2 tetszőleges eleme, akkor az $\mathbf{u} \mapsto \varphi(\mathbf{u}) + \mathbf{v}$ szabály a $\mathcal{V}_1$-nek $\mathcal{V}_2$-be való **affin leképezése**. Affin leképezések szorzata, azaz kompozíciója affin, ugyanis ha $\psi_1 = \varphi_1 + \mathbf{v}_1$ és $\psi_2 = \varphi_2 + \mathbf{v}_2$, ahol φ_1 és φ_2 lineáris leképezés, akkor

$$(\psi_2 \circ \psi_1)(\mathbf{u}) = \psi_2\big(\psi_1(\mathbf{u})\big) = \varphi_2(\varphi_1(\mathbf{u}) + \mathbf{v}_1) + \mathbf{v}_2$$
$$= \varphi_2\big(\varphi_1(\mathbf{u})\big) + (\varphi_2(\mathbf{v}_1) + \mathbf{v}_2) = (\varphi_2 \circ \varphi_1)(\mathbf{u}) + (\varphi_2(\mathbf{v}_1) + \mathbf{v}_2),$$

és az affin leképezések kompozíciója, mint bármely leképezések kompozíciója, asszociatív, így egy adott lineáris tér önmagába való affin leképezései a kompozícióval félcsoportot alkotnak. Az identikus leképezés lineáris, tehát affin, így van mind bal, mind jobb oldali semleges elem, amely egybeesik, ha a két tér azonos, és a kompozíció jobbról disztributív az összeadásra nézve, mert

$$\begin{aligned}\big((\psi_2+\psi_3)\circ\psi_1\big)(\mathbf{u}) &= \psi_2\big(\psi_1(\mathbf{u})\big)+\psi_3\big(\psi_1(\mathbf{u})\big)\\ &= (\psi_2\circ\psi_1)(\mathbf{u})+(\psi_3\circ\psi_1)(\mathbf{u}) = \big((\psi_2\circ\psi_1)+(\psi_3\circ\psi_1)\big)(\mathbf{u}).\end{aligned}$$

A bal oldali disztributivitás általában nem teljesül, mert az affin leképezés nem összegtartó, ugyanis általában, felhasználva, hogy a lineáris leképezés összegtartó,

$$\begin{aligned}\psi(\mathbf{u}_1+\mathbf{u}_2) &= \varphi(\mathbf{u}_1+\mathbf{u}_2)+\mathbf{v} = \varphi(\mathbf{u}_1)+\varphi(\mathbf{u}_2)+\mathbf{v} \neq \varphi(\mathbf{u}_1)+\varphi(\mathbf{u}_2)+2\mathbf{v}\\ &= (\varphi(\mathbf{u}_1)+\mathbf{v})+(\varphi(\mathbf{u}_2)+\mathbf{v}) = \psi(\mathbf{u}_1)+\psi(\mathbf{u}_2),\end{aligned}$$

Ha a leképezés lineáris, akkor igaz a bal oldali disztributivitás is, vagyis a lineáris tér önmagába való lineáris leképezései a leképezések összeadásával mint összeadással és a kompozícióval mint szorzással gyűrűt alkotnak, ez a lineáris tér **endomorfizmus-gyűrű**je.

Affin leképezés skalárszorosa is affin, így egy lineáris tér önmagába való affin leképezései a tér összes leképezésének terében egy alteret alkotnak, mint ahogy lineáris teret alkotnak a tér önmagába való lineáris leképezései is. Ez azt jelenti, hogy a lineáris tér önmagába való lineáris leképezései, vagyis endomorfizmusai algebrát alkotnak a teret meghatározó test fölött. Ha a tér n-dimenziós, akkor az endomorfizmusok algebrájának rangja n^2.

Lineáris altér lineáris altere lineáris altere az eredeti térnek, és hasonló igaz affin alterekre is, továbbá ha két altér közül az egyik része a másiknak, akkor az előbbi egyben altere is az utóbbinak.

9.7. Definíció

$L=\sum_{i=0}^{n} a_i x^{q^i} \in \mathbb{F}_{q^m}$ egy $\mathbb{F}_{q^m}$ **fölötti q-polinom** vagy $\mathbb{F}_{q^m}$ **fölötti linearizált polinom**. Ha L egy $\mathbb{F}_{q^m}$ fölötti q-polinom, és $u \in \mathbb{F}_{q^m}$, akkor $A=L-u$ $\mathbb{F}_{q^m}$ **fölötti affin q-polinom** vagy **q-affin polinom**, és L az A **linearizált része**.

Δ

Az $\mathbb{F}_{q^m}$ fölötti linearizált illetve affin q-polinomok halmazát $\mathfrak{L}^{(q^m)}[x]$-szel és $\mathfrak{A}^{(q^m)}[x]$-szel fogjuk jelölni, és ha nyilvánvaló, hogy mely test feletti polinomokról van szó, akkor a testre való utalást elhagyjuk, tehát ekkor a megfelelő jelölések $\mathfrak{L}[x]$ és $\mathfrak{A}[x]$.

A definícióból rögtön látszik, hogy $\alpha \in \mathbb{F}_{q^m}$ $\mathbb{F}_q$ fölötti nyoma az $\mathbb{F}_{q^m}$ fölötti $L=\sum_{i=0}^{m-1} x^{q^i}$ q-polinom α helyen vett helyettesítési értéke, vagyis ha L az előbbi polinom, akkor $\mathrm{S}_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)=\hat{L}(\alpha)$. Az is közvetlenül leolvasható, hogy affin q-polinomok összege affin q-polinom és q-polinomok összege q-polinom. Az előbbi megállapítások azonban a szorzásra nem érvényesek, például az x és az x^q linearizált – tehát affin q- – polinomok szorzata x^{q+1}, és nincs olyan nemnegatív egész i, amellyel $q+1=q^i$ (mert $q>1$, így $q^1=q<q+1<q+q=2q\le q\cdot q=q^2$, és ha $0\le u<v$, ahol u és v tetszőleges valós szám, akkor $q^u<q^v$). Igaz azonban az alábbi állítás.

9.8. Tétel

$\mathcal{A}^{(q^m)}[x]=\big(\mathfrak{A}^{(q^m)}[x],+,\circ\big)$-ben $\big(\mathfrak{A}^{(q^m)}[x],\circ\big)$, ahol $\circ$ a kompozíció, egységelemes, nem kommutatív félcsoport, és $\circ$ jobbról disztributív $+$ fölött. $\mathfrak{L}^{(q^m)}[x]$ az $\mathfrak{A}^{(q^m)}[x]$ mindkét előbbi műveletére zárt részhalmaza, továbbá $\mathcal{L}^{(q^m)}[x]=\big(\mathfrak{L}^{(q^m)}[x],+,\circ\big)$-ben a kompozíció balról is disztributív az összeadás fölött, így $\mathcal{L}^{(q^m)}[x]$ a megadott két művelettel egységelemes gyűrű, amely nullosztómentes, és akkor és csak akkor kommutatív, ha $m=1$.

$f \mapsto f^{q^l}$ minden $l \in \mathbb{N}$-re injektív leképezés $\mathcal{A}^{(q^m)}[x]$-en, amelyre $\mathcal{L}^{(q^m)}[x]$ zárt.

Δ

A halmazokhoz hasonlóan, ha lehet, a struktúrák jelölésénél is elhagyjuk a test megjelölését.

Bizonyítás:

Egy test legalább két elemet tartalmazó egységelemes, kommutatív, nullosztómentes gyűrű, így $(\mathbb{F}_{q^t};\circ)$ egységelemes félcsoport, amely jobbról disztributív a polinomok összeadására nézve, és ha $f \neq 0 \neq g$, akkor $f \circ g \neq 0$ (lásd a 2.39. Tételt a 40. oldalon). Az egységelem az x polinom, és ez q-polinom, hiszen $x = x^1 = x^{q^0}$, így azt kell csak bizonyítani, hogy affin q-polinomok kompozíciója affin q-polinom, q-polinomok kompozíciója q-polinom, a kompozíció még az affin q-polinomok körében is akkor és csak akkor kommutatív, ha $m = 1$ és a polinom linearizált, és végül, hogy a linearizált polinomok körében a kompozíció nullosztómentes és balról is disztributív az összeadás fölött.

Legyen $f = \sum_{i=0}^{n_f} a_i x^{q^i}$ és $g = \sum_{i=0}^{n_g} b_i x^{q^i}$ $\mathbb{F}_{q^m}$ fölötti polinom. Ekkor

$$f \circ g = \sum_{i=0}^{n_f} a_i \left(\sum_{j=0}^{n_g} b_j x^{q^j} \right)^{q^i} = \sum_{i=0}^{n_f} \left(\sum_{j=0}^{n_g} a_i b_j^{q^i} \right) x^{q^{i+j}} = \sum_{k=0}^{n_f+n_g} \left(\sum_{j=0}^{k} a_j b_{k-j}^{q^j} \right) x^{q^k} \in \mathfrak{L}[x],$$

$$f \circ (g+h) = \sum_{i=0}^{n_f} a_i (g+h)^{q^i} = \sum_{i=0}^{n_f} a_i g^{q^i} + \sum_{i=0}^{n_f} a_i h^{q^i} = f \circ g + f \circ h,$$

tehát linearizált polinomok kompozíciója linearizált polinom, és balról is teljesül a disztributivitás.

Ha $A_1 \in \mathfrak{A}[x]$, $A_2 \in \mathfrak{A}[x]$, akkor $A_1 = L_1 - u_1$, $A_2 = L_2 - u_2$ valamilyen $\mathfrak{L}[x]$-beli L_1, L_2 polinomokkal és $\mathbb{F}_{q^m}$-beli u_1, u_2 elemekkel, így

$$\begin{aligned} A_1 \circ A_2 &= (L_1 - u_1) \circ (L_2 - u_2) = L_1 \circ (L_2 - u_2) - u_1 \\ &= L_1 \circ L_2 - \left(\hat{L}_1(u_2) + u_1 \right) = L - u, \end{aligned}$$

ahol $L = L_1 \circ L_2 \in \mathfrak{L}[x]$ és $u \in \mathbb{F}_{q^m}$, tehát $A_1 \circ A_2 \in \mathfrak{A}[x]$. $x^2 \circ (ax) = a^2 x^2$ és $(ax) \circ x^2 = a x^2$, és ez a két polinom akkor és csak akkor egyenlő, ha $a = a^2$, vagyis ha $a(e-a) = 0$, tehát ha $a = 0$ vagy $a = e$. Ha $m > 1$, akkor a testnek biztosan van az előbbi két elemtől különböző eleme, így a kompozíció még a q-polinomok körében sem kommutatív, és $u_1 \circ u_2 = u_1$, míg $u_2 \circ u_1 = u_2$, tehát általában az affin q-polinomok körében még az $\mathbb{F}_q$ fölötti polinomokra sem teljesül a felcserélhetőség. Azonban $m = 1$ esetén a test minden elemének q^j-kitevős hatványa bármely nemnegatív egész j-re önmaga, így

$$\sum_{j=0}^{k} a_j b_{k-j}^{q^j} = \sum_{j=0}^{k} a_j b_{k-j} = \sum_{j=0}^{k} b_{k-j}\, a_j = \sum_{j=0}^{k} b_j a_{k-j} = \sum_{j=0}^{k} b_j a_{k-j}^{q^j},$$

tehát a kompozíció ebben az esetben, azaz az $\mathbb{F}_q$ fölötti q-polinomokra kommutatív.

Legyen $L = \sum_{i=0}^{n} a_i x^{q^i}$, $u \in \mathbb{F}_{q^m}$ és $A = L - u$. Ekkor

$$A^{q^l} = (L-u)^{q^l} = L^{q^l} - u^{q^l} = \left(\sum_{i=0}^{n} a_i x^{q^i} \right)^{q^l} - v = \sum_{i=0}^{n} a_i^{q^l} x^{q^{i+l}} - v = \sum_{i=0}^{n} b_{i+l} x^{q^{i+l}} - v,$$

ahol $b_{i+l} = a_i^{q^l} \in \mathbb{F}_{q^m}$ és $v = u^{q^l} \in \mathbb{F}_{q^m}$, tehát $A^{q^l} \in \mathfrak{A}[x]$, és ha $u = 0$, akkor $v = u^{q^l} = 0$, így $\mathfrak{L}[x]$ zárt a q^l-kitevős hatványozásra.

□

q-polinomok illetve affin q-polinomok kompozícióját **szimbolikus szorzás**nak, a kompozíció eredményét **szimbolikus szorzat**nak is fogjuk mondani, és ha $h = g \circ f$, ahol f és g linearizált polinom vagy mindkettő affin q-polinom, akkor azt mondjuk, hogy f **szimbolikusan osztja** h-t, vagy másként, hogy f **szimbolikusan osztója** h-nak illetve f **szimbolikus osztója** h-nak. Ha f szimbolikusan osztja h-t, akkor g a h és f **szimbolikus hányados**a (h és f sorrendje ez esetben lényeges).

Bizonyos esetekben a szimbolikus osztás visszavezethető a polinomok közönséges osztására. Ehhez új fogalmat vezetünk be.

9.9. Definíció

Legyen $F = \sum_{i=0}^{n} a_i x^{q^i}$ egy $\mathbb{F}_{q^m}$ fölötti q-polinom és $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_{q^m}[x]$. Ekkor F és f q-**asszociáltak**, f az F **konvencionális asszociáltja**, míg F az f **linearizált asszociáltja.** A q^m-elemű test fölötti q-asszociáltságot $\sim_{q^m}$ jelöli.

Δ

A q-asszociáltság által összetartozó párokat általában az ábécé ugyanazon betűjével fogjuk jelölni, a konvencionális q-asszociáltat kisbetűvel, míg a párját a megfelelő nagybetűvel.

Az nyilvánvaló, hogy a q-asszociáltak egyik tagja egyértelműen meghatározza a másik tagot. Az is könnyen látható, hogy összeg q-asszociáltja a q-asszociáltak összege, viszont ez szorzásra általában csak akkor igaz, ha a polinomok a q-elemű test fölöttiek, ugyanis az f és g polinom szorzatában a k-adfokú tag együtthatója $\sum_{j=0}^{k} a_j b_{k-j}$, míg F és G szimbolikus szorzatában az ugyanezen indexhez tartozó tag, tehát a q^k-adfokú tag együtthatója $\sum_{j=0}^{k} a_j b_{k-j}^{q^j}$, azt pedig tudjuk, hogy $b = b^q$ akkor és csak akkor igaz, ha $b \in \mathbb{F}_q$. Ekkor viszont az is igaz, hogy $F \circ G \sim_q fg = gf \sim_q G \circ F$, amit korábban már a 9.8. Tételben beláttunk. Igazoltuk tehát az alábbi tételt.

9.10. Tétel

Az $F \mapsto f$ megfeleltetés izomorfizmus $\mathcal{L}^{(q)}[x]$ és $\mathbb{F}_q[x]$ között.

Δ

Ennek a tételnek egyszerű következménye az alábbi.

9.11. Következmény

$\mathcal{L}^{(q)}[x]$ euklideszi gyűrű.

Δ

Bizonyítás:
Test fölötti polinomgyűrű euklideszi gyűrű, de akkor a vele izomorf bármely gyűrű is euklideszi gyűrű.

□

Ha $f = \sum_{i=0}^{n} a_i x^{q^i} - u \; \mathbb{F}_{q^m}$ fölötti affin q-polinom, és $a_n \neq 0$ ($n = 0$ esetén $a_n - u \neq 0$), akkor azt mondjuk, hogy f **affin fok**a n, és ezt úgy fogjuk jelölni, hogy $\mathrm{afdeg}(f) = n$, illetve, ha $f = 0$ is lehetséges, akkor használjuk az $\mathrm{af}\delta(f) \leq n$ jelölést.

Nézzük most a q-elemű test fölötti q-polinomok szimbolikus osztását. Ha $F \neq 0$ és H az előbbi test fölötti q-polinom, és a q-asszociáltakkal $h = gf + r$, ahol $\delta(r) < \deg(f)$, akkor $H = G \circ F + R$ és $\mathrm{af}\delta(R) = \delta(r) < \deg(f) = \mathrm{afdeg}(f)$, így F akkor és csak akkor szimbolikus osztója H-nak, ha f

osztója h-nak. Ezt $F|_\circ H$-val fogjuk jelölni. A q-elemű test fölötti q-polinomok kompozíciójának kommutativitásával ez egyben azt is jelenti, hogy ha F szimbolikusan osztja H-t, és a szimbolikus hányados G, akkor G is szimbolikus osztója H-nak.

Mint láttuk, linearizált polinomok szorzata általában nem linearizált, ám igaz az alábbi állítás.

9.12. Tétel

Ha F és H $\mathbb{F}_q$ fölötti q-polinom, és a q-asszociáltjuk rendre f és h, akkor az alábbi állítások ekvivalensek:

- $f|h$
- $F|H$
- $F|_\circ H$.

Δ

Bizonyítás:
$f|h$ akkor és csak akkor, ha $h = gf$, ami pontosan akkor igaz, ha $H = G \circ F$, vagyis ha $F|_\circ H$, így már csak azt kell igazolni, hogy ebben az esetben, és csak ekkor, az $F|H$ oszthatóság is igaz. Legyen először $H = G \circ F$. Ekkor G linearizált polinom, és $H = \sum_{i=0}^{n} g_i F^{q^i} = F \sum_{i=0}^{n} g_i F^{q^i-1} = Ft$, ahol t is egy $\mathbb{F}_q$ fölötti (de általában nem linearizált) polinom, így F osztója H-nak. Fordítva, tegyük fel, hogy $F|H$, és legyen $h = gf + r$ olyan g és r $\mathbb{F}_q$ fölötti polinomokkal, hogy $\delta(r) < \deg(f)$. Ekkor $H = G \circ F + R$ és $\mathrm{af}\delta(r) = \delta(r) < \deg(f) = \mathrm{afdeg}(f)$. De az előbb láttuk, hogy $F|G \circ F$, a feltétel alapján pedig $F|H$, amiből következik, hogy $F|R$, ami a fokszámok következtében csak úgy lehetséges, ha $R = 0$, vagyis ha $H = G \circ F$, azaz ha $F|_\circ H$.

□

Test fölötti polinomfüggvény az adott testet önmagába képező függvény. Nem túlságosan meglepő módon affin q-polinomok illetve linearizált polinomok esetén ez a leképezés speciális alakot ölt.

9.13. Tétel

Legyen A egy $\mathbb{F}_{q^m}$ fölötti affin q-polinom. Ekkor az $a \mapsto \hat{A}(a)$ leképezés $\mathbb{F}_{q^m}$-nek egy önmagába való affin leképezése, amely lineáris leképezés, ha A linearizált polinom. Kölcsönösen egyértelmű megfeleltetés adható az $\mathbb{F}_{q^m}$ fölötti, legfeljebb $m-1$ affinfokú q-affin polinomok és az $\mathbb{F}_{q^m}$-et önmagába képező affin leképezések között, ahol a q-polinomok és a lineáris leképezések egymásnak felelnek meg.

Δ

Bizonyítás:
Az első állításnál elegendő a lineáris részre vonatkozó állítást bizonyítani, hiszen ha $A = L - u$, akkor $a \in \mathbb{F}_{q^m}$-re $\hat{A}(a) = \hat{L}(a) - u$. Legyen u_1 és u_2 az $\mathbb{F}_{q^m}$ és c_1 valamint c_2 az $\mathbb{F}_q$ eleme, továbbá $L = \sum_{i=0}^{n} a_i x^{q^i}$. Ekkor

$$\hat{L}(c_1u_1 + c_2u_2) = \sum_{i=0}^{n} a_i (c_1u_1 + c_2u_2)^{q^i} = c_1 \sum_{i=0}^{n} a_i {u_1}^{q^i} + c_2 \sum_{i=0}^{n} a_i {u_2}^{q^i}$$
$$= c_1\, \hat{L}(u_1) + c_2\, \hat{L}(u_2).$$

A q^m-elemű test fölötti két, legfeljebb $q^m - 1$-edfokú polinomhoz tartozó polinomfüggvény akkor és csak akkor azonos, ha a két polinom is azonos, hiszen egyenlőség esetén a test valamennyi, tehát q^m elemén azonos a két leképezés értéke, és $q^{m-1} \leq q^m - 1$, így különböző, legfeljebb $m-1$ affinfokú affin q-polinomhoz különböző, a testet önmagába képező affin leképezés tartozik, tehát az affin

q-polinomot a megfelelő affin leképezéshez rendelő leképezés injektív. A legfeljebb $m-1$ affinfokú affin q-polinomok linearizált részében az együtthatók száma m, mindegyik együttható a test bármely eleme lehet, végül a konstans tagot is tetszőlegesen választhatjuk a testből, így az ilyen polinomok száma összesen $(q^m)^m q^m = q^{m(m+1)}$, és ezek közül $(q^m)^m = q^{m^2}$ a linearizált polinom. A testet önmagába képező affin leképezések egy $m \times m$-es mátrixszal és egy m-elemű vektorral adhatóak meg, és mind a mátrix, mind a vektor elemei egyaránt a q-elemű test elemei, így az affin leképezések száma $q^{m^2} q^m = q^{m(m+1)}$, a lineáris leképezések száma pedig q^{m^2}, hiszen ezek esetén az eltolást megadó vektor a nullvektor. Láthatóan a polinomok és a leképezések száma megegyezik, így az injektív leképezés egyben szürjektív, tehát bijektív is.

□

Szükségünk lesz egy speciális alakú mátrix determinánsának ismeretére.

9.14. Tétel

Legyen $n \in \mathbb{N}^+$ és $\boldsymbol{A}$ $\mathbb{F}_{q^m}$ fölötti n-edrendű kvadratikus mátrix, ahol az $n > i \in \mathbb{N}$, $n > j \in \mathbb{N}$ indexekre $(\boldsymbol{A})_{i,j} = \beta_i^{q^j}$ az $\mathbb{F}_{q^m}$ β_i elemeivel. Ekkor $\det(\boldsymbol{A}) = \beta_0 \prod_{i=0}^{n-2} \prod_{\mathbf{c} \in \mathbb{F}_q^{i+1}} \left(\beta_{i+1} - \sum_{j=0}^{i} c_j \beta_j\right)$, és a determináns akkor és csak akkor 0, ha a β_i elemek mint az $\mathbb{F}_q$ test fölötti $\mathbb{F}_{q^m}$ lineáris tér elemei lineárisan összefüggőek.

Δ

Bizonyítás:

Elsőként megmutatjuk, hogy egy $(\mathbf{u}_0, \dots, \mathbf{u}_{n-1})$ vektorrendszer akkor és csak akkor lineárisan összefüggő, ha van olyan $n > k \in \mathbb{N}$ index, hogy $\mathbf{u}_k$ lineárisan függ az $(\mathbf{u}_0, \dots, \mathbf{u}_{k-1})$ rendszertől. Ha a megadott vektorrendszer lineárisan összefüggő, akkor van olyan, nem csupa 0-ból álló, $\mathbb{F}_q$-beli együtthatórendszer, hogy $\sum_{i=0}^{n-1} c_i \mathbf{u}_i = \mathbf{0}$. Legyen $k = \max_{n > i \in \mathbb{N}} \{c_i \neq 0\}$. Ez a maximum létezik, mert a feltétel értelmében van olyan $n > i \in \mathbb{N}$ index, hogy $c_i \neq 0$. Ekkor $\mathbf{0} = \sum_{i=0}^{n-1} c_i \mathbf{u}_i = \sum_{i=0}^{k} c_i \mathbf{u}_i$-ból $\mathbf{u}_k = \sum_{i=0}^{k-1} \left(c_k^{-1} c_i\right) \mathbf{u}_i$, ugyanis $c_k \neq 0$, így létezik az inverze.

Az előbbiekből következik a tételnek azon állítása, hogy $\det(\boldsymbol{A})$ pontosan akkor 0, ha a mátrixot generáló β_i elemek rendszere lineárisan összefüggő, azzal a kiegészítő megjegyzéssel, hogy egyetlen elemből álló vektorrendszer akkor és csak akkor lineárisan összefüggő, ha a rendszer egyetlen eleme a nullvektor.

Most nézzük a determináns értékére vonatkozó állítást. A bizonyítást indukcióval végezzük. Ha $n = 1$, akkor $\boldsymbol{A} = (\beta_0)$, $\det(\boldsymbol{A}) = \beta_0$, és $\beta_0 \prod_{i=0}^{1-2} \prod_{\mathbf{c} \in \mathbb{F}_q^{i+1}} \left(\beta_{i+1} - \sum_{j=0}^{i} c_j \beta_j\right) = \beta_0$, mert egy olyan szorzat értéke, ahol a felső határ eggyel kisebb az alsó határnál, e-vel egyenlő, ahol e a test egységeleme, vagyis ekkor teljesül az egyenlőség. Most tegyük fel, hogy valamely $n \in \mathbb{N}^+$-ra teljesül a tételben leírt egyenlőség, és nézzük az $n+1$-edrendű $\boldsymbol{A}^{(n+1)}$ mátrixot. Legyen ennek bal felső n-edrendű részmátrixa $\boldsymbol{A}^{(n)}$, $\det\left(\boldsymbol{A}^{(n)}\right) = D^{(n)}$ és $\det\left(\boldsymbol{A}^{(n+1)}\right) = D^{(n+1)}$. Tekintsük az

$$\mathbf{U}(x) = \begin{pmatrix} \beta_0 & \beta_0^q & \cdots & \beta_0^{q^{n-1}} & \beta_0^{q^n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \cdots & \beta_{n-1}^{q^{n-1}} & \beta_{n-1}^{q^n} \\ x & x^q & \cdots & x^{q^{n-1}} & x^{q^n} \end{pmatrix}$$

mátrixot, és legyen ennek deteminánsa $D(x)$. Az utolsó sor szerint kifejtve, a mátrix determinánsa $D = D^{(n)} x^{q^n} + \sum_{i=0}^{n-1} a_i \, x^{q^i}$. Ennek a polinomnak minden együtthatója $\mathbb{F}_{q^m}$ eleme, hiszen a mátrix minden eleme, az utolsó sor elemeitől eltekintve, az előbbi testben van, és mind $D^{(n)}$, mind az a_i együtthatók a mátrix elemeiből vett szorzatok összege, tehát szintén az adott test eleme, így D egy $\mathbb{F}_{q^m}$ fölötti q-

polinom. Bármely $n > i \in \mathbb{N}$ esetén $\widehat{D}(\beta_i) = 0$, hiszen $\widehat{D}(\beta_i)$ annak a mátrixnak a detrerminánsa, amelyet $\mathbf{U}(x)$-ből úgy kapunk, hogy az utolsó sorban x helyére β_i-t teszünk, de akkor olyan mátrrixot kapunk, amelynek két sora azonos. Tekintsük a β_i-k által kifeszített lineáris teret. Az előbbi tétel szerint linearizált polinomhoz tartozó polinomfüggvény összegtartó, így ha $\beta = \sum_{j=0}^{n-1} c_j\beta_j$ ennek a térnek egy eleme, akkor $\widehat{D}(\beta) = \sum_{j=0}^{n-1} c_j\widehat{D}(\beta_i) = 0$. Ez azt jelenti, hogy a β_i-k által generált lineáris tér minden eleme gyöke a D polinomnak. Ha a β_i-k lineárisan függetlenek, akkor a tér n-dimenziós, és mivel az együtthatók a q-elemű test elemei, így a tér elemeinek száma, vagyis a polinom gyökeinek száma q^n, ami megegyezik a polinom fokával. Ezek szerint ha a β_i-k lineárisan függetlenek, akkor az előbbi tér elemei, és csak ezek a polinom gyökei, és minden ilyen gyök egyszeres, így a polinom gyöktényezős felírása $D = D^{(n)}\prod_{\mathbf{c}\in\mathbb{F}_q^n}\left(x - \sum_{j=0}^{n-1} c_j\beta_j\right)$. De ez a felírás akkor is érvényes, ha a mátrixot generáló elemek lineárisan összefüggőek. Ha ugyanis valamilyen $\mathbf{c} \in \mathbb{F}_q^n$ együttható-rendszerrel $\sum_{j=0}^{n-1} c_j\beta_j = 0$, akkor valamennyi $n > i \in \mathbb{N}$-re $0 = 0^{q^i} = \left(\sum_{j=0}^{n-1} c_j\beta_j\right)^{q^i} = \sum_{j=0}^{n-1} c_j\beta_j^{q^i}$, és ha $\mathbf{c} \neq \mathbf{0}$, azaz a β_i-k lineárisan összefüggőek, akkor mind $\mathbf{U}(x)$, mind $\boldsymbol{A}^{(n)}$ sorai lineárisan összefüggőek, tehát $D = 0 = D^{(n)}$, de akkor $D = 0 = 0 \cdot \prod_{\mathbf{c}\in\mathbb{F}_q^n}\left(x - \sum_{j=0}^{n-1} c_j\beta_j\right) = D^{(n)}\prod_{\mathbf{c}\in\mathbb{F}_q^n}\left(x - \sum_{j=0}^{n-1} c_j\beta_j\right)$, vagyis minden esetben teljesül a $D = D^{(n)}\prod_{\mathbf{c}\in\mathbb{F}_q^n}\left(x - \sum_{j=0}^{n-1} c_j\beta_j\right)$ felírás. Innen viszont azt kapjuk, hogy $\det\left(\boldsymbol{A}^{(n+1)}\right) = D^{(n+1)} = \widehat{D}(\beta_n) = D^{(n)}\prod_{\mathbf{c}\in\mathbb{F}_q^n}\left(\beta_n - \sum_{j=0}^{n-1} c_j\beta_j\right)$, míg az indukciós feltevés alapján $D^{(n)} = \beta_0\prod_{i=0}^{n-2}\prod_{\mathbf{c}\in\mathbb{F}_q^{i+1}}\left(\beta_{i+1} - \sum_{j=0}^{i} c_j\beta_j\right)$, tehát $D^{(n+1)} = \beta_0\prod_{i=0}^{n-1}\prod_{\mathbf{c}\in\mathbb{F}_q^{i+1}}\left(\beta_{i+1} - \sum_{j=0}^{i} c_j\beta_j\right)$.

□

Egy lineáris leképezés magja, vagyis nulltere lineáris altere az értelmezési tartománynak. Ha $\mathcal{A}$ affin leképezés, akkor $\mathcal{A} = \mathcal{L} - \mathbf{u}$ egy $\mathcal{L}$ lineáris leképezéssel és a képtér egy $\mathbf{u}$ elemével. Amennyiben $\mathcal{L}\mathbf{x}_1 - \mathbf{u} = \mathcal{A}\mathbf{x}_1 = \mathbf{0} = \mathcal{A}\mathbf{x}_2 = \mathcal{L}\mathbf{x}_2 - \mathbf{u}$, akkor $\mathcal{L}(\mathbf{x}_2 - \mathbf{x}_1) = \mathbf{0}$, tehát az értelmezési tartomány azon elemei, amelyek képe egy affin leképezésnél a képtér nulleleme, az értelmezési tartomány affin alterét képezik.

$\mathbb{F}_{q^m}$ m-dimenziós lineáris tér az $\mathbb{F}_q$ test fölött, továbbá $\mathbb{F}_{q^m}$ elemein az $u \mapsto u^q$ leképezés automorfizmus, amely az identikus leképezés $\mathbb{F}_q$-n, tehát az $\mathbb{F}_{q^m}$ egydimenziós alterén.

9.15. Definíció

Legyen $\mathcal{M}$ az $\mathbb{F}_{q^s}$ mint az $\mathbb{F}_q$ test fölötti lineáris tér lineáris altere. $\mathcal{M}$ egy ($\mathbb{F}_{q^s}$-**beli**) q-**modulus**, ha $M^q = \{u^q | u \in M\} \subseteq M$.

Δ

9.16. Tétel

Legyen $0 \neq f \in \mathbb{F}_{q^m}[x]$, $\mathbb{F}_{q^s}$ az f $\mathbb{F}_{q^m}$ fölötti felbontási testét tartalmazó test. f akkor és csak akkor q-affin polinom, ha minden gyöke azonos multiplicitású, ez a többszörösség q egy nemnegatív egész kitevős hatványa, és a gyökök M halmaza $\mathbb{F}_{q^s}$-nek mint $\mathbb{F}_q$ fölötti lineáris térnek affin altere. f pontosan akkor linearizált, ha ez az altér lineáris, és a linearizált f főpolinom pontosan akkor eleme $\mathbb{F}_q[x]$-nek, ha $\mathcal{M}$ q-modulus.

Δ

Bizonyítás:

Affin leképezésnél azon elemek, amelyek képe a képtér nulleleme, affin alteret alkotnak, amely lineáris altér, ha a leképezés lineáris. Ebből következik, hogy q-affin polinomok gyökeinek halmaza affin altér, amely lineáris, ha a polinom linearizált. Legyen $f = \sum_{i=0}^{n} a_i x^{q^i}$ és $g = f - u$ az $\mathbb{F}_{q^m}$ egy u elemével, és legyen $n \geq k \in \mathbb{N}$ olyan, hogy $k > i \in \mathbb{N}$-re $a_i = 0$, de $a_k \neq 0$. $f \neq 0$, így van ilyen k. Ekkor

$$f=\sum_{i=0}^{n}a_i x^{q^i}=\sum_{i=k}^{n}a_i^{q^{km}}x^{q^i}=\sum_{i=0}^{n-k}a_{i+k}^{q^{k(m-1)+k}}x^{q^{i+k}}=\left(\sum_{i=0}^{n-k}a_{i+k}^{q^{k(m-1)}}x^{q^i}\right)^{q^k}=h^{q^k},$$

ahol $h=\sum_{i=0}^{n-k}a_{i+k}^{q^{k(m-1)}}x^{q^i}=\sum_{i=0}^{n-k}b_i x^{q^i}$ és $b_0\neq 0$, és $g=f-u=h^{q^k}-u^{q^{km}}=t^{q^k}$ a $t=h-v$, $v=u^{q^{k(m-1)}}\in\mathbb{F}_{q^m}$ jelöléssel. $b_0\neq 0$-ból $t'=h'=b_0\neq 0$, így a derivált polinomnak nincs gyöke, tehát közös gyöke sem lehet az eredeti polinommal, amiből következik, hogy mind h, mind t minden gyöke egyszeres, vagyis q^0-szoros, és f valamint g minden gyöke q^k-szoros.

Most legyen $\mathcal{C}$ az $\mathbb{F}_{q^s}$ mint $\mathbb{F}_q$ fölötti lineáris tér affin altere. Ekkor $C=c+B$, ahol $c\in\mathbb{F}_{q^s}$ és $\mathcal{B}$ az $\mathbb{F}_{q^s}$ lineáris altere. $f=(\prod_{v\in C}(x-v))^{q^l}=\left(\prod_{b\in B}\big((x-c)-b\big)\right)^{q^l}=(\prod_{b\in B}(y-b))^{q^l}=g^{q^l}$ olyan $\mathbb{F}_{q^s}$ fölötti polinom, amelynek minden gyöke q^l-szeres, és amely q-affin, ha g linearizált. Az rögtön látszik, hogy $f=g$ pontosan akkor teljesül, ha $c=0$, azaz ha $C=B$, tehát ha $\mathcal{C}$ lineáris altér. Legyen $\mathcal{B}$ r-dimenziós, és $b_0,\dots,b_{r-1}$ a $\mathcal{B}$ bázisa. Ekkor $g=\prod_{\mathbf{a}\in\mathbb{F}_q^r}\left(y-\sum_{i=0}^{r-1}a_i b_i\right)=D^{(r)^{-1}}D$, ahol $D^{(r)}$ és D a 9.14. Tétel bizonyításában látható determináns és polinom, és D q-polinom.

q^m-elemű testen nemnegatív egész l-lel a q^l-kitevős hatványozás injektív, tehát szürjektív is, így, ha $\mathcal{M}$ q-modulus, akkor $M^q=M$. $\mathbb{F}_q$ fölötti polinom q-adik hatványa is gyöke a polinomnak, tehát a gyökök halmaza q-modulus. Ha egy főpolinom minden gyökének q-adik hatványa is gyöke a polinomnak, akkor $f^q=(\prod_{u\in M}(x-u))^q=\prod_{u\in M}(x^q-u^q)=\prod_{u\in M}(x^q-u)=f\circ x^q$, és ez azt jelenti, hogy $f\in\mathbb{F}_q[x]$.

□

Legyen $A=L-u$ $\mathbb{F}_{q^m}$ fölötti q-affin polinom, és keressük az $\hat{A}(x)=v$ egyenlet $\mathbb{F}_{q^s}$-beli megoldásait, ahol $\mathbb{F}_{q^s}$ az $\mathbb{F}_{q^m}$ egy bővítése és v az $\mathbb{F}_{q^m}$ eleme. A feladat ekvivalens egy $B=L-w$ q-affin polinom adott testbeli gyökeinek keresésével. Legyen $b_0,\dots,b_{s-1}$ az $\mathbb{F}_{q^s}$ egy $\mathbb{F}_q$ fölötti bázisa. Az $\mathbb{F}_{q^s}$ a eleme akkor és csak akkor gyöke a B polinomnak, ha

$$\begin{aligned}w^T b=\sum_{j=0}^{s-1}w_j b_j=w=\hat{L}(a)=\hat{L}\left(\sum_{i=0}^{s-1}a_i b_i\right)=\sum_{i=0}^{s-1}a_i\hat{L}(b_i)\\=\sum_{i=0}^{s-1}a_i\sum_{j=0}^{s-1}B_{i,j}b_j=\sum_{j=0}^{s-1}\left(\sum_{j=0}^{s-1}a_i B_{i,j}\right)b_j=(a^T\mathbf{B})b,\end{aligned}$$

ahol $B_{i,j}$ az $\hat{L}(b_i)$ j-edik komponense a $b_0,\dots,b_{s-1}$ bázisban való felírásában. De $\mathbf{b}$ elemei lineárisan függetlenek, így $w^T b=(a^T\mathbf{B})b$ akkor és csak akkor teljesül, ha $w^T=a^T\mathbf{B}$, és ez egy lineáris egyenletrendszer, amely homogén, ha $w=0$, így q-affin illetve linearizált polinomok gyökeinek meghatározását visszavezettük a sokkal egyszerűbb lineáris egyenletrendszer megoldására.

Az előbbi módszer kevés többletmunkával $\mathbb{F}_{q^m}$ fölötti tetszőleges $f\neq 0$ polinom $\mathbb{F}_{q^s}$-beli gyökeinek meghatározására is alkalmazható. Ehhez nem kell mást tennünk, mint keresni egy $\mathbb{F}_{q^m}$ fölötti olyan A affin q-polinomot, amely osztható f-fel. Ekkor ugyanis f minden gyöke gyöke A-nak, így meghatározva A gyökeit, behelyettesítéssel megállapíthatjuk, hogy ezek közül melyek gyökei f-nek. A kérdés csupán az, hogy mindig találunk-e alkalmas q-affin polinomot. A válasz pozitív. Legyen f n-edfokú, és tekintsük $n>i\in\mathbb{N}$-re az $r_i=x^{q^i}\bmod f$ polinomokat. Ezen polinomok mindegyike legfeljebb $n-1$-edfokú, így $r_i=\sum_{i=0}^{n-1}r_{i,j}x^j$. Keressünk olyan $c_0,\dots,c_{n-1}$ $\mathbb{F}_q$-beli nem csupa 0 együtthatókat, amelyekkel $\sum_{i=0}^{n-1}c_i r_i=u$ konstans polinom, vagyis amellyel minden $n>j\in\mathbb{N}^+$-ra teljesül, hogy $\sum_{i=0}^{n-1}c_i r_{i,j}=0$. Ez egy $n-1$ egyenletből álló, n-ismeretlenes homogén lineáris egyenletrendszer, így biztosan van nem triviális megoldása. Ekkor

$$u = \sum_{i=0}^{n-1} c_i r_i = \sum_{i=0}^{n-1} c_i \left(x^{q^i} \bmod f \right) = \sum_{i=0}^{n-1} c_i x^{q^i} \bmod f,$$

ami azt jelenti, hogy az $A = \sum_{i=0}^{n-1} c_i x^{q^i} - u$ q-affin polinom osztható f-fel. Feltehetjük, hogy A főpolinom, mert q-affin polinom konstansszorosa is affin q-polinom. Egy ilyen, f-fel osztható A affin q-polinom az f **affin többszöröse**, és ha a homogén lineáris egyenletrendszerünknek több lineárisan független megoldása van, akkor a legalacsonyabb fokszámú A polinom az f **legkisebb affin többszöröse**.

A másod-, harmad- és negyedfokú egyenletekre létező megoldóképletek illetve általános megoldási módszerek bármely test felett alkalmazhatóak, kivéve a 2- és harmad- és negyedfokú egyenletek esetén még a 3-karakterisztikájú testeket. Az előbb ismertetett módon azonban véges test esetén ezek a problémák is általános eszközökkel kezelhetőek.

Ha adott egy $A = L - u \in \mathcal{A}^{(q^m)}[x]$ polinom, akkor természetes kérdés, vajon hol helyezkednek el a polinom gyökei. Legyen $B = M - v$ is $\mathbb{F}_{q^m}$ fölötti affin q-polinom. A akkor és csak akkor osztója B-nek, ha minden gyöke egyben B-nek is gyöke. De q-affin polinom gyökei a gyököt tartalmazó test mint lineáris tér affin alterét alkotják, és affin altér részhalmaza, amely maga is affin altér, affin altere az őt tartalmazó altérnek. Affin q-polinom gyökeinek különbsége gyöke a polinom linearizált részének, és a szűkebb altérbeli különbségek egyben a bővebb altérben is az adott vektorok különbségei, így, ha A osztója B-nek, akkor L is osztója M-nek. Ez visszafelé általánosan nem igaz, igaz viszont abban az esetben, amikor van a testnek olyan r eleme, amellyel $u = \hat{L}(r)$ és $v = \hat{M}(r)$, hiszen ekkor $A = L - u = L - \hat{L}(r) = L \circ (x - r) = L \circ y$, és ugyanígy, $B = M \circ y$. Mármost A akkor és csak akkor osztója $x^{q^m} - x$-nek, ha minden gyöke benne van $\mathbb{F}_{q^m}$-ben. Az alábbi tételből következik, hogy ez ekvivalens azzal, hogy van $\mathbb{F}_{q^m}$-nek olyan r eleme, amellyel $u = \hat{L}(r)$, míg, ha ilyen elem nincs, akkor A-nak nincs gyöke a q^m-elemű testben.

9.17. Tétel

Legyen L egy $\mathbb{F}_{q^m}$ fölötti linearizált főpolinom, amely osztója az $x^{q^m} - x$ polinomnak. Ekkor van olyan, egyértelműen meghatározott, $\mathbb{F}_{q^m}$ fölötti L_1 q-polinom, amely szintén főpolinom és osztója $x^{q^m} - x$-nek, és az alábbi állítások ekvivalensek:

1. $L_1 \circ L = x^{q^m} - x$;
2. $L \circ L_1 = x^{q^m} - x$;
3. $A = L - u$-nak akkor és csak akkor van gyöke $\mathbb{F}_{q^m}$-ben, ha $\hat{L}_1(u) = 0$;
4. $A_1 = L_1 - u$-nak pontosan akkor van gyöke $\mathbb{F}_{q^m}$-ben, ha $\hat{L}(u) = 0$.

Δ

Bizonyítás:

Ha $L \left| x^{q^m} - x \right.$, akkor minden gyöke $\mathbb{F}_{q^m}$-ben van és egyszeres, és $L \in \mathfrak{Q}^{(q^m)}[x]$ következtében a különböző gyökök összessége $\mathbb{F}_{q^m}$-nek mint lineáris térnek lineáris alterét alkotják. Legyen r az altér dimenziója, és legyen ennek az altérnek mint $\mathbb{F}_q$ fölötti lineáris térnek egy bázisa $b_0, \dots, b_{r-1}$. Bázis elemei lineárisan függetlenek, és lineárisan független rendszer kiegészíthető a tér egy bázisává, így vannak $\mathbb{F}_{q^m}$-nek olyan $b_r, \dots, b_{m-1}$ elemei, hogy $b_0, \dots, b_{r-1}, b_r, \dots, b_{m-1}$ a teljes térnek, vagyis $\mathbb{F}_{q^m}$-nek egy $\mathbb{F}_q$ fölötti bázisa. A $b_0, \dots, b_{r-1}$, valamint a $b_r, \dots, b_{m-1}$ elemek által kifeszített térnek egyetlen közös eleme a 0, és együtt a teljes teret generálják, így a tér bármely w eleme egy és csak egyféleképpen írható $u + v$ alakban, ahol u a $b_0, \dots, b_{r-1}$ által generált U altérnek (vagyis az L gyökterének) eleme, míg $v \in V$, ahol V a további bázisvektorok generátuma. Ekkor

$$x^{q^m}-x=\prod_{w\in\mathbb{F}_{q^m}}(x-w)=\prod_{v\in V}\prod_{u\in U}\big(x-(v+u)\big)$$
$$=\prod_{v\in V}\left(\prod_{u\in U}\big((x-v)-u\big)\right)=\prod_{v\in V}\big(L\circ(x-v)\big)=\prod_{v\in V}\Big(L\circ x-\hat{L}(v)\Big).$$

Mivel $\hat{L}$ a test önmagába való lineáris leképezése, továbbá V-beli $0\neq v$-re $\hat{L}(v)\neq 0$, tehát L a V különböző elemeit a test különböző elemeibe viszi, ezért $V'=\{\hat{L}(v)|v\in V\}$ is $\mathbb{F}_{q^m}$ $m-r$-dimenziós lineáris altere, így $\prod_{v\in V}\left(x-\hat{L}(v)\right)=L_1$ egy $\mathbb{F}_{q^m}$ fölötti, az $x^{q^m}-x$-et osztó linearizált főpolinom, és

$$L_1\circ L=\left(\prod_{v\in V}\left(x-\hat{L}(v)\right)\right)\circ L=\prod_{v\in V}\left(L-\hat{L}(v)\right)=x^{q^m}-x.$$

L_1 egyértelmű, mert nem nulla polinomok kompozíciója nem lehet a nullpolinom, és L_1 minden gyöke az $\mathbb{F}_{q^m}$ eleme, így a polinom osztója $x^{q^m}-x$-nek. Most nézzük a négy állítást.

Az első állítás L_1 konstrukciójából világos, hiszen $L_1\circ L=x^{q^m}-x$.

$(L\circ L_1)\circ L=L\circ(L_1\circ L)=L\circ\left(x^{q^m}-x\right)=L\circ x^{q^m}-L=L^{q^m}-L=\left(x^{q^m}-x\right)\circ L$, és ebből, ismét azért, mert nem nulla polinomok kompozíciója nem lehet a nullpolinom, $L\circ L_1=x^{q^m}-x$.

$0=\hat{A}(v)=\hat{L}(v)-u$ akkor és csak akkor, ha $\hat{L}(v)=u$, és $\hat{L}(v)=u$ pontosan akkor teljesül, ha $\hat{L}_1(u)=\hat{L}_1\left(\hat{L}(v)\right)=L_1\circ(L\circ v)=(L_1\circ L)\circ v=\left(x^{q^m}-x\right)\circ v=v^{q^m}-v$. $v^{q^m}-v=0$ viszont az $\mathbb{F}_{q^m}$ és csak az $\mathbb{F}_{q^m}$ elemeire teljesül, így akkor és csak akkor van A-nak gyöke $\mathbb{F}_{q^m}$-ben, ha $\hat{L}_1(u)=0$, és ekkor A minden gyöke benne van ebben a testben, vagyis egymást kizáró módon A-nak vagy minden gyöke $\mathbb{F}_{q^m}$-beli, vagy nincs gyöke ebben a testben.

A negyedik állítás abból következik, hogy $L_1\circ L=L\circ L_1$, és mindkét polinom az $x^{q^m}-x$-et osztó főpolinom.

□

Abban a speciális esetben, amikor $L\in\mathbb{F}_q[x]$, és l az L, l_1 az L_1 q-asszociáltja, akkor könnyen meg tudjuk határozni L ismeretében L_1-et, hiszen ekkor $l_1 l$ az $x^{q^m}-x$ q-asszociáltja, ami x^m-e, vagyis ekkor l_1 az x^m-e és l hányadosa (ami létezik a 9.12. Tétel szerint), és L_1 ennek a hányadospolinomnak a linearizált q-asszociáltja.

10.Rekurzív sorozatok

10.1. Definíció

A nem üres S halmaz fölötti **s** sorozat **periodikus t-től a p periódussal**, ha $p \in \mathbb{N}^+$, $t \in \mathbb{N}$ és $\forall(i \in \mathbb{N}): s_{t+i+p} = s_{t+i}$. k_p **a p-hez tartozó küszöbindex**, ha **s** k_p-től p szerint periodikus és vagy $k_p = 0$ vagy $s_{k_p-1+p} \neq s_{k_p-1}$; az előbbi esetben **a sorozat tisztán periodikus a p periódussal**. Az **s** sorozat **periodikus**, ha van legalább egy periódusa. A periodikus **s** sorozat **minimális periódus**a p, ha periódusa a sorozatnak, és a sorozat bármely p' periódusára $p \leq p'$.

Egy sorozat **k-tól s-sorozat**, ha a $k \in \mathbb{N}$ indextől kezdve valamennyi tagja s, és **k-tól konstans sorozat**, ha valamilyen s-re k-tól s-sorozat; ha az előbbi k minimális a mondott tulajdonságra, akkor k a **küszöb**, vagyis **s** a k küszöbtől s-sorozat illetve a k küszöbtől konstans sorozat. Amennyiben $k = 0$, akkor egyszerűen **s-sorozat**ot illetve **konstans sorozat**ot mondunk. Abban az esetben, ha S-ben van nullelem, és az s-sorozatban s a nullával azonos, akkor használjuk a **nullsorozat** elnevezést is.

Δ

A definícióból látszik, hogy minden konstans sorozat periodikus, és minimális periódusa 1.

10.2. Tétel

k-tól a p periódussal periodikus sorozat minden $l \in \mathbb{N}^+$-ra lp szerint periodikus k-tól. Ha egy sorozat a k_1 küszöbtől a p_1 és a k_2 küszöbtől a p_2 periódussal periodikus, akkor $k_1 = k = k_2$, és a sorozat a k küszöbtől periodikus a $d = (p_1, p_2)$ periódussal.

Δ

Bizonyítás:

$l = 1$-re $lp = p$, és p periódusa a sorozatnak. Ha pedig egy pozitív egész l-lel lp periódus, akkor $s_{k+i+(l+1)p} = s_{k+i+lp+p} = s_{k+i+p+lp} = s_{k+i+lp} = s_{k+i}$, így $(l+1)p$ is periódus.

Legyen $k_2 \geq k_1$, ekkor van olyan $q \in \mathbb{N}^+$, hogy $k_1 + qp_1 \geq k_2$. Most a sorozat $k_1 + qp_1$-től periodikus p_2-vel, és $s_{k_1+i+p_2} = s_{k_1+i+p_2+qp_1} = s_{k_1+qp_1+i+p_2} = s_{k_1+qp_1+i} = s_{k_1+i+qp_1} = s_{k_1+i}$, tehát a sorozat k_1-től periodikus a p_2 periódussal, így $k_1 \geq k_2$, ennélfogva $k_1 = k_2$.

$(p_1, p_2) = d = u_1p_1 + u_2p_2$, ahol u_1 és u_2 egész szám. Mivel a két periódus pozitív, ezért a legnagyobb közös osztójuk is pozitív, és ekkor a két együttható legalább egyike, mondjuk u_1 pozotív egész. Ebből $s_{k+i} = s_{k+i+u_1p_1} = s_{k+i+u_1p_1+u_2p_2} = s_{k+i+d}$, vagyis d is periódusa a sorozatnak.

□

10.3. Tétel

Periodikus sorozatnak létezik egyértelműen meghatározott minimális periódusa és minden periódusához egyértelmű küszöbindexe. $p' \in \mathbb{N}^+$ akkor és csak akkor periódusa a sorozatnak, ha $p|p'$, ahol p a minimális periódus, és ekkor a p-hez és p'-höz tartozó k illetve k' küszöbindex megegyezik.

Δ

Bizonyítás:

Periodikus sorozatnak van periódusa és ez pozitív egész szám, vagyis ekkor a periódusok halmaza $\mathbb{N}^+$ nem üres részhalmaza. Ebben a halmazban van legkisebb elem, ami – ha létezik – egyértelmű, ez igazolja, hogy periodikus sorozatnak van egyértelműen meghatározott minimális periódusa.

Most legyen p a minimális periódus. Van olyan nemnegatív egész t, hogy minden $i \in \mathbb{N}$-re $s_{t+i+p} = s_{t+i}$. Legyen $K = \{j \in \mathbb{N} | \forall(i \in \mathbb{N}): s_{j+i+p} = s_{j+i}\}$. $\emptyset \neq K \subseteq \mathbb{N}$, hiszen $t \in K$, így létezik K-

ban legkisebb elem, mondjuk k. Ekkor minden nemnegatív egész i-re $s_{k+i+p} = s_{k+i}$, tehát k-tól periodikus a sorozat a p periódussal. Ha k nem nulla, akkor $s_{k-1+p} \neq s_{k-1}$, mert ellenkező esetben még $k-1$ is eleme lenne K-nak, így k minden esetben küszöbindex. Ez a küszöbindex egyértelmű, mert ha k' küszöbindex, akkor $k' \in K$, tehát $k \leq k'$, és $k < k'$ nem lehet, mert $k < k'$ esetén már $k'-1$-től is periodikus a sorozat a p periódussal.

Az előző tétel szerint p minden pozitív egész többszöröse is periódusa a sorozatnak. Másrészt, ha p' is periódusa ugyanezen sorozatnak, akkor $d = (p, p')$ is periódus. $p > 0$-ból és $d|p$-ből $d \leq p$, ugyanakkor $d \leq p$, hiszen p a minimális periódus, így $p = d|p'$. Szintén az előző tételből az is következik, hogy a p'-höz tartozó küszöbindex azonos a p periódus küszöbinedexével.

□

10.4. Következmény

Ha **s** periodikus k-tól a p periódussal, és $i \equiv j\ (p)$, ahol $i \in \mathbb{N}$ és $j \in \mathbb{N}$, akkor $s_{k+i} = s_{k+j}$.

Δ

Bizonyítás:

Az általánosság csorbítása nélkül tekinthetjük úgy, hogy $i \leq j$. Ha $i \equiv j\ (p)$, akkor alkalmas q nemnegatív egész i-vel $j = i + qp$, és ekkor $s_{k+j} = s_{k+i+qp} = s_{k+i}$.

□

Az előzőek szerint periodikus sorozat küszöbindexe minden periódus esetén azonos, így egy periodikus sorozat a periódustól függetlenül tisztán periodikus vagy nem tisztán periodikus. Ennek a ténynek felel meg az alábbi definíció.

10.5. Definíció

Egy periodikus sorozatnak a periódustól független küszöbindexe **a sorozat küszöbindexe**. Egy periodikus sorozat **tisztán periodikus**, ha a küszöbindexe 0.

Δ

10.6. Definíció

A nem üres S halmaz feletti **s** sorozat m**-edrendű rekurzív sorozat**, ha $m \in \mathbb{N}$, és létezik olyan $\varphi: S^m \to S$, hogy minden $i \in \mathbb{N}$-re $s_{i+m} = \varphi(s_i, \dots, s_{i+m-1})$. φ **a rekurziós összefüggés**, **rekurziós kapcsolat** vagy **rekurziós szabály**, és m **a rekurzió rendje**. Egy sorozat **rekurzív**, ha legalább egy m-re m-edrendű rekurzív sorozat; a rekurzió **minimális rendje** m, ha a sorozat m-edrendű rekurzív sorozat, de m-nél kisebb nemnegatív egész m'-re nem m'-rendű rekurzív sorozat.

$s^{(i)} = (s_i, \dots, s_{i+m-1})$ az m-edrendű rekurzív sorozat i**-edik állapota**, és $s^{(0)}$ a **kezdő állapot**.

Δ

10.7. Tétel

Rekurzív sorozat minimális rekurziós rendje létezik és egyértelmű, és ha ez m, akkor **s** minden $m \leq m' \in \mathbb{N}$-re m'-rendű rekurzív.

Δ

Bizonyítás:

Ha a sorozat rekurzív, akkor a rekurziós rendek halmaza a nemnegatív egész számok halmazának nem üres részhalmaza, így tartalmaz egyértelműen meghatározott legkisebb elemet, és ez maga is rekurziós rendje a sorozatnak. Legyen m az előbbiek szerint létező minimális rekurziós rend, φ a hozzá tartozó rekurziós összefüggés, m' az m-nél nem kisebb nemnegatív egész, és $\varphi': S^{m'} \to S$, ahol

$\varphi'(u_0, \dots, u_{m'-m-1}, u_{m'-m}, \dots, u_{m'-1}) = \varphi(u_{m'-m}, \dots, u_{m'-1})$, ha $(u_0, \dots, u_{m'-1}) \in S^{m'}$. Most bármely $i \in \mathbb{N}$ esetén $s_{i+m'} = \varphi(s_{i+m'-m}, \dots, s_{i+m'-1}) = \varphi'(s_i, \dots, s_{i+m'-m-1}, s_{i+m'-m}, \dots, s_{i+m'-1})$, hiszen $m' \geq m$ következtében $m' - m \geq 0$, vagyis a sorozat m' renddel is rekurzív.

□

10.8. Tétel

Rekurzív sorozat k-adik állapota, ahol k nemnegatív egész szám, egyértelműen meghatározza a sorozatot a k indextől kezdve.

Δ

Bizonyítás:

Ha **s** m-edrendű rekurzív sorozat a φ rekurzióval, és adott $s^{(k)} = (s_k, \dots, s_{k+m-1})$, a k-adik állapot, akkor ismert a sorozat s_k-val kezdődő m egymás utáni eleme. Legyen $t \in \mathbb{N}$, és tegyük fel, hogy már ismertek a sorozat elemei s_k-tól $s_{k+t+m-1}$-ig. Ekkor $s_{k+t+m} = \varphi(s_{k+t}, \dots, s_{k+t+m-1})$, vagyis ismert a sorozat $k + t + m$ -indexű eleme is, így az indukció mutatja, hogy a sorozat valamennyi eleme ismert a k indextől kezdve.

Δ

10.9. Következmény

Rekurzív sorozat kezdő állapota egyértelműen meghatározza a sorozatot.

Δ

Bizonyítás:

Az előbbi tételből kapjuk $k = 0$-val.

□

10.10. Tétel

Ha i nemnegatív egész, j az i-nél nagyobb egész, és az m-edrendű rekurzív sorozat i-edik és j-edik állapota megegyezik, akkor a sorozat i-től periodikus a $j - i$ periódussal.

Δ

Bizonyítás:

Amennyiben $(s_i, \dots, s_{i+m-1}) = s^{(i)} = s^{(j)} = (s_j, \dots, s_{j+m-1})$, akkor a jelölt állapotokat követő elemekre $s_{i+m} = \varphi(s_i, \dots, s_{i+m-1}) = \varphi(s_j, \dots, s_{j+m-1}) = s_{j+m}$, tehát a megadott állapotokra következő állapotokra $s^{(i+1)} = (s_{i+1}, \dots, s_{i+m}) = (s_{j+1}, \dots, s_{j+m}) = s^{(j+1)}$, és ha valamilyen nemnegatív egész t-re $s^{(i+t)} = s^{(j+t)}$, akkor hasonlóan kapjuk, hogy $s^{(i+t+1)} = s^{(j+t+1)}$, így minden nemnegatív egész l-re $s_{i+l+(j-i)} = s_{j+l} = s_{i+l}$, vagyis a sorozat i-től periodikus a $j - i$ periódussal.

Δ

10.11. Tétel

Ha az S feletti **s** sorozat t-től periodikus a p periódussal, akkor **s** $t + p$-edrendű rekurzív sorozat. Fordítva, ha S elemeinek száma q, és **s** rekurzív sorozat az m minimális renddel, akkor a sorozat periodikus, és $p \leq p + k \leq q^m$, ahol p a minimális periódus és k a küszöbindex.

Δ

Bizonyítás:

Először legyen $\varphi: S^{t+p} \to S$ olyan, hogy $\varphi(w_0, \dots, w_t, \dots, w_{t+p-1}) = w_t$ az S elemeiből álló bármely rendezett $t+p$ -esre. Ez S^{t+p}-nek S-be való leképezése, hiszen S^{t+p} minden eleméhez S egy és csak egy elemét rendeli. Most $s_{i+t+p} = s_{t+i+p} = s_{t+i} = s_{i+t} = \varphi(s_i, \dots, s_{i+t}, \dots, s_{i+t+p-1})$ tetszőleges nemnegatív egész i-re, ami azt jelenti, hogy a sorozat $t+p$ renddel rekurzív.

Másodszor legyen a sorozat m-edrendű rekurzív sorozat. Ha S elemeinek száma q, akkor a lehetséges állapotok száma nem lehet nagyobb q^m-nél, ezért van olyan $0 \le i < j \le q^m$ nemnegatív egész, amellyel $s^{(i)} = s^{(j)}$. Ekkor a 10.10. Tétel szerint a $j - i = p'$ jelöléssel a sorozat i-től biztosan periodikus a p periódussal, tehát $k + p \le i + p' = i + j - i = j \le q^m$. Ez minden rekurziós rendre, tehát a minimális rendre is igaz. Végül a küszöbindex nemnegatív, így nyilván $p \le k + p$.

□

10.12. Definíció

Legyen $b \in \mathbb{N}$ és $d \in \mathbb{N}^+$. A $\mathbf{t} = \mathbf{s}^{(b)}$ sorozat az $\mathbf{s}$ sorozat b-**eltoltja**, ha $t_i = s_{i+b}$ minden i indexre, és $\mathbf{u} = \mathbf{s}^{[d]}$ az $\mathbf{s}$ d-**decimáltja**, ha valamennyi nemnegatív egész i-re $u_i = s_{di}$.

Δ

10.13. Tétel

Legyen k és b nemnegatív és p pozitív egész. Ha $\mathbf{s}$ a k küszöbtől periodikus a p periódussal, akkor $\mathbf{s}^{(b)}$ periodikus a $k' = \max\{0, k-b\}$ küszöbtől a p periódussal. Fordítva, ha $\mathbf{s}^{(b)}$ a k küszöbtől periodikus a p periódussal, akkor $\mathbf{s}$ periodikus $k+b$-től a p periódussal, és ha $k > 0$, akkor $k+b$ az $\mathbf{s}$ sorozat küszöbindexe.

Δ

Bizonyítás:

$k' = \max\{0, k-b\} \ge k - b$, így $k' + b \ge k$, és $\mathbf{s}$ k-tól periodikus, így minden nemnegatív egész i-vel $s^{(b)}_{k'+i+p} = s_{k'+i+p+b} = s_{(k'+b)+i+p} = s_{(k'+b)+i} = s_{k'+i+b} = s^{(b)}_{k'+i}$, tehát $\mathbf{s}^{(b)}$ periodikus k'-től a p periódussal. Ha $k' = 0$, akkor k' nyilván küszöbindex, míg ha $k' = k - b$, és az eltolt sorozat küszöbindexe, $k^{(b)}$, kisebb, mint k', akkor $\mathbf{s}$ periodikus $k^{(b)} + b < k' + b = k - b + b = k$-tól, ami nem lehetséges.

Ha minden $i \in \mathbb{N}$-re $s^{(b)}_{k+i+p} = s^{(b)}_{k+i}$, akkor $s_{(k+b)+i+p} = s_{k+i+p+b} = s^{(b)}_{k+i+p} = s^{(b)}_{k+i} = s_{k+i+b} = s_{(k+b)+i}$, ami pontosan azt jelenti, hogy $\mathbf{s}$ $k+b$-től periodikus a p periódussal. Legyen az eltolt sorozat küszöbindexe pozitív. Ez azt jelenti, hogy $s_{(k+b)-1+p} = s_{k-1+p+b} = s^{(b)}_{k-1+p} \ne s^{(b)}_{k-1} = s_{k-1+b} = s_{(k+b)-1}$, és az eredeti sorozat küszöbindexe $k+b$.

□

A fenti tétel értelmében egy periodikus sorozat bármely eltoltjának minimális periódusa azonos az eredeti sorozat minimális periódusával.

10.14. Következmény

Ha $\left(\mathbf{s}^{(b)}\right)^{(b')} = \mathbf{s}$ egy b és b' nemnegatív egésszel, amelyek közül legalább az egyik pozitív, akkor $\mathbf{s}$ tisztán periodikus a $b + b'$ periódussal. Fordítva, ha $\mathbf{s}$ tisztán periodikus a p periódussal, akkor minden $b \in \mathbb{N}^+$-hoz van olyan $p > b' \in \mathbb{N}$, hogy $\mathbf{s}$ b-eltoltjának b'-eltoltja $\mathbf{s}$.

Δ

Bizonyítás:

a) A tétel első felében megfogalmazott feltétel szerint $b + b'$ pozitív egész, és tetszőleges nemnegatív egész i-re $s_i = \left(\left(\mathbf{s}^{(b)}\right)^{(b')}\right)_i = s^{(b)}_{i+b'} = s_{i+(b+b')}$, így **s** tisztán periodikus a $b + b'$ periódussal.

b) Legyen $b' = p\left\lceil\frac{b}{p}\right\rceil - b$. Ekkor egyrészt $0 = p\frac{b}{p} - b \le p\left\lceil\frac{b}{p}\right\rceil - b = b' < p\left(\frac{b}{p} + 1\right) - b = p$, másrészt $\left(\left(\mathbf{s}^{(b)}\right)^{(b')}\right)_i = s_{i+(b+b')} = s_{i+\left\lceil\frac{b}{p}\right\rceil \cdot p} = s_i$ minden nemnegatív egész i-re teljesül, ami éppen a tisztán periodikusság feltétele.

□

10.15. Tétel

k-tól a p periódussal periodikus **s** sorozat d-decimáltja periodikus $\left\lceil\frac{k}{d}\right\rceil$-től a $\frac{p}{(d,p)}$ periódussal.

Δ

Bizonyítás:

$d \cdot \left\lceil\frac{k}{d}\right\rceil \ge k$, ezért bármely nemnegatív egész i-re

$$s^{[d]}_{\left\lceil\frac{k}{d}\right\rceil + i + \frac{p}{(d,p)}} = s_{d\cdot\left(\left\lceil\frac{k}{d}\right\rceil + i + \frac{p}{(d,p)}\right)} = s_{d\cdot\left\lceil\frac{k}{d}\right\rceil + d\cdot i + d\cdot\frac{p}{(d,p)}} = s_{d\cdot\left\lceil\frac{k}{d}\right\rceil + d\cdot i + \frac{d}{(d,p)}p}$$
$$= s_{d\cdot\left\lceil\frac{k}{d}\right\rceil + d\cdot i} = s_{d\cdot\left(\left\lceil\frac{k}{d}\right\rceil + i\right)} = s^{[d]}_{\left\lceil\frac{k}{d}\right\rceil + i}.$$

□

Megjegyezzük, hogy a d-decimált periodikusságából nem következik az eredeti sorozat periodikussága. Ha például **s**-ben s_i akkor és csak akkor e, ha $i = dj$ vagy $i = \frac{(j+1)j}{2}d + 1$, ahol $j \in \mathbb{N}$, egyébként 0, akkor a d-decimált a konstans e-sorozat, és így periodikus. Ám az eredeti sorozat nem az, hiszen a sorozatban a 0-kon kívül egyedülálló e-k illetve két egymás mellett álló e-k fordulnak elő, és ez utóbbiak közötti távolság $\frac{(j+2)(j+1)}{2}d - \frac{(j+1)j}{2}d = (j+1)d$, ami szigorúan monoton nő.

10.16. Tétel

m-edrendű rekurzív sorozat b-eltoltja is m-edrendű rekurzív sorozat. Visszafelé, ha a b-eltolt m-edrendű rekurzív sorozat, akkor az eredeti sorozat $m + b$-edrendű rekurzív sorozat.

Δ

Bizonyítás:

a) $s^{(b)}_{i+m} = s_{i+m+b} = \varphi(s_{i+b}, \dots, s_{i+m-1+b}) = \varphi\left(s^{(b)}_i, \dots, s^{(b)}_{i+m-1}\right)$;

b) Legyen $\varphi'(w_0, \dots, w_{b-1}, w_b, \dots, w_{m-1+b}) = \varphi(w_b, \dots, w_{m-1+b})$ az eltolt sorozat φ rekurziójához. Ekkor

$$s_{i+(m+b)} = s_{i+m+b} = s^{(b)}_{i+m} = \varphi\left(s^{(b)}_i, \dots, s^{(b)}_{i+m-1}\right) = \varphi(s_{i+b}, \dots, s_{i+m-1+b})$$
$$= \varphi'(s_i, \dots, s_{i+b-1}, s_{i+b}, \dots, s_{i+m-1+b}).$$

□

10.17. Tétel

Véges halmaz felett rekurzív sorozat d-decimáltja is rekurzív.

Δ

Bizonyítás:
Véges halmaz felett rekurzív sorozat periodikus, így d-decimáltja periodikus, tehát rekurzív.

□

A tétel állítása visszafelé nem feltétlenül igaz. Korábban már beláttuk, hogy nem periodikus sorozat decimáltja lehet periodikus, tehát rekurzív, ugyanakkor az eredeti sorozat biztosan nem rekurzív, ha a tagjai egy véges halmaz elemei, hiszen a feltétel szerint az eredeti sorozat nem periodikus.
A tétel nem igaz, ha a sorozat elemeinek halmaza végtelen. Legyen $d = \varphi(a, b, c)$ olyan, hogy

ha $b = c$ akkor
  $d = 1$
különben ha $c = 1$ akkor
  $d = b + 1$
különben ha $b = 1$, akkor
  $d = 2$
különben ha $c = 0$, akkor
  $d = a$
különben ha $b = 0$, akkor
  $d = a + 1$
különben
  $d = 0$
elágazás vége,

és legyen a sorozat első három eleme $s_0 = 1$, $s_1 = 2$ és $s_2 = 2$. A sorozat 3-decimáltja egy olyan sorozat, amelyben minden k nemnegatív egészre egy 1-est k egymás utáni 0 követ. A teljes sorozatban a 3-decimáltak után álló elem $k + 2$, míg az ez után állónál kettővel kisebb szám azt mutatja, hogy a k darab nullából hányadik következik (az első 1-esnél az értéke 0). A sorozat megadásából következik, hogy rekurzív. Ugyanakkor a 3-decimáltat nem tudjuk rekurzióval előállítani, hiszen m-edrendű rekurziónál az utolsó m elem határozza meg a következő elemet, de a 3-decimáltban tetszőleges nemnegatív egész m-re a sorozat egy kezdeti véges szakaszától eltekintve van m egymás után következő 0, és bármilyen hosszúságú nullsorozatot is követ egy 1-es, ám m darab egymás utáni 0-ból nem lehet meghatározni, hogy a soron következő elem 0 vagy 1 lesz-e.

A továbbiakban speciális rekurzív sorozatokat vizsgálunk.

10.18. Definíció

Ha $\mathcal{R} = (R; +, \cdot)$ gyűrű, $m \in \mathbb{N}$, és minden nemnegatív egész i-re $s_{i+m} = \sum_{j=0}^{m-1} c_j s_{i+j} + c$ R-beli c_j és c elemekkel, akkor **s** ($\mathcal{R}$ **feletti**) (m-edrendű) **lineáris rekurzív sorozat**, és ha $c = 0$, akkor a sorozat egy ($\mathcal{R}$ **feletti**) (m-edrendű) **homogén lineáris rekurzív sorozat**

Δ

Ha a gyűrűben van bal oldali egységelem, akkor a fentebb definiált két sorozat között nincs lényeges különbség, ekkor ugyanis igaz az alábbi tétel.

10.19. Tétel

Ha e_b bal oldali egységelem az $\mathcal{R} = (R; +, \cdot)$ gyűrűben, és **s** egy m-edrendű lineáris rekurzív sorozat, akkor **s** lényegében véve egy $m + 1$-edrendű homogén lineáris rekurzív sorozat.

Δ

Bizonyítás:

$s_{i+m+1} = \sum_{j=0}^{m-1} c_j s_{i+j+1} + c = \sum_{j=1}^{m} c_{j-1} s_{i+j} + c$, és ebből kivonva s_{i+m}-et majd átrendezve $s_{i+(m+1)} = (e_b + c_{m-1}) s_{i+m} + \sum_{j=1}^{m-1} (c_{j-1} - c_j) s_{i+j} + (-c_0) s_{i+0} = \sum_{j=0}^{m} c'_j s_{i+j}$ a $c'_m = e_b + c_{m-1}$, $c'_j = c_{j-1} - c_j$, ha $m > j \in \mathbb{N}^+$ és $c'_0 = -c_0$ jelöléssel.

□

A két sorozat között van némi különbség. Az eredeti sorozat m-edrendű, tehát első m elemét szabadon választhatjuk, az utána következőket, és így s_m-et azonban már nem. A módosított sorozat $m+1$-edrendű, így ebben s_m is szabadon választható lenne, ha ez a sorozat nem az előbbi sorozathoz tartozna, nem azzal kellene megegyeznie. Most azonban ez az elem nem választható tetszés szerint, hiszen meg kell, hogy egyezzen az eredeti, nem feltétlenül homogén sorozat m-indexű elemével. Ebből az is következik, hogy a tétel az ellenkező irányban általában nem igaz. Ha például egy $m+1$-edrendű homogén lineáris rekurzív sorozat első $m+1$ eleme azonos és nem 0, azaz minden $m \geq i \in \mathbb{N}$-re $s_i = s \neq 0$, és a rekurziót megadó $s_{i+m+1} = \sum_{j=0}^{m} c_j s_{i+j}$ összefüggés olyan, hogy $\left(\sum_{j=0}^{m} c_j\right) s \neq s$, akkor ez az $m+1$-edrendű homogén lineáris rekurzív sorozat nem generálható egy m-edrendű lineáris rekurzióval. Ha ugyanis az $s_{i+m} = \sum_{j=0}^{m-1} c'_j s_{i+j} + c$ lineáris rekurzió ugyanazt a sorozatot generálja, mint az eredetileg adott homogén lineáris rekurzió, akkor

$$s_{m+1} = \sum_{j=0}^{m} c_j s_j = \sum_{j=0}^{m} c_j s = \left(\sum_{j=0}^{m} c_j\right) s \neq s = s_m$$
$$= \sum_{j=0}^{m-1} c'_j s_j + c = \sum_{j=0}^{m-1} c'_j s + c = \sum_{j=0}^{m-1} c'_j s_{j+1} + c = s_{m+1}$$

ami nyilván ellentmondás.

A fenti tétel miatt, ha egy gyűrűben van bal oldali egységelem, és így egységelemes gyűrűben is, elegendő a homogén eset vizsgálata.

10.20. Megjegyzés

Látható, hogy m-edrendű homogén lineáris rekurzív sorozat a nullsorozat, ha $m = 0$, és a sorozat m-től a nullsorozat, ha $m > 0$ és minden c_i nulla. Ha viszont $m > 0$ mellett $c_{m-1} = e$, és minden $m - 1 > i \in \mathbb{N}$ indexre $c_i = 0$, akkor **s** $m-1$-től konstans sorozat, és $m = 1$ esetén konstans sorozat.

Δ

10.21. Tétel

Bal oldali egységelemes gyűrű feletti periodikus sorozat homogén lineáris rekurzív sorozat.

Δ

Bizonyítás:

Ha **s** küszöbindexe k és minimális periódusa p, akkor minden $i \in \mathbb{N}$ -re

$$s_{i+k+p} = s_{k+i+p} = s_{k+i} = s_{i+k} = e_b s_{i+k} = \sum_{j=0}^{k+p-1} c_j s_{i+j},$$

ahol e_b a bal oldali egységelem, $c_k = e_b$, és minden más t-re $c_t = 0$.

□

10.22. Definíció

Egy gyűrű feletti **s** sorozat **generátorfüggvény**e $S = \sum_{i=0}^{\infty} s_i x^i$. Ha $f = \sum_{i=0}^{m} c_i x^i$ a gyűrű feletti főpolinom, akkor az $s_{i+m} = \sum_{j=0}^{m-1}(-c_j)s_{i+j}$ rekurzióval generálható sorozatok halmaza $\Omega(f)$, és ha **s** eleme az $\Omega(f)$ halmaznak, úgy f az **s sorozat karakterisztikus polinomja**.

Δ

Ha a gyűrűben van bal oldali egységelem, akkor az $s_{i+m} = \sum_{j=0}^{m-1}(-c_j)s_{i+j}$ rekurzióval megadott m-edrendű homogén lineáris rekurzív sorozat a $c_m = e_b$ választással átírható a $\sum_{j=0}^{m} c_j s_{i+j} = 0$ egyenlőségbe. Innen visszafelé azt kapjuk, hogy ha az adott gyűrű feletti **s** homogén lineáris rekurzív sorozat karakterisztikus polinomja $\sum_{i=0}^{m} c_i x^i$, akkor bármely nemnegatív egész i-re $\sum_{j=0}^{m} c_j s_{i+j} = 0$.

10.23. Tétel

Ha $\mathcal{R}$ egységelemes gyűrű, $f \in R[x]$ n-edfokú főpolinom, és $T = \{\tau \in R[x] | \delta(\tau) < n\}$, akkor $\tau \mapsto (f^*)^{-1}\tau$ a $\mathcal{T}$ unitér jobb oldali $\mathcal{R}$ modulus $\Omega(f)$-re való izomorf leképezése.

Δ

Bizonyítás:

Legyen $f = \sum_{i=0}^{m} c_i x^i$ főpolinom, és tekintsünk egy T-beli τ polinomot. f főegyütthatója, és így f^* konstans tagja egységelem, tehát egyben egység $\mathcal{R}$-ben, ezért f^* egység a formális hatványsorok gyűrűjében, ennélfogva van inverze. $S = (f^*)^{-1}\tau$ egy T-beli τ polinommal akkor és csak akkor, ha f^*S egy legfeljebb $n-1$-edfokú polinom, vagyis akkor és csak akkor, ha az f^*S hatványsor n-nél nem kisebb indexű minden együtthatója 0. Ha $n \le i$, akkor $f_i^* = 0$, így az n-nél nem kisebb indexekre $(f^*S)_i = \sum_{j=0}^{i} f_j^* s_{i-j} = \sum_{j=0}^{n} f_j^* s_{i-j} = \sum_{j=0}^{n} c_{n-j} s_{i-j} = \sum_{j=0}^{n} c_j s_{i-n+j}$, tehát az $n \le i \in \mathbb{N}$ indexekre $(f^*S)_i = 0$ pontosan akkor igaz, ha minden ilyen i indexre $\sum_{j=0}^{n} c_j s_{i-n+j} = 0$, vagyis akkor és csak akkor, ha tetszőleges nemnegatív egész i-re $\sum_{j=0}^{n} c_j s_{i+j} = 0$. Ez viszont akkor és csak akkor teljesül, ha $S \in \Omega(f)$. Ez azt jelenti, hogy $\tau \mapsto (f^*)^{-1}\tau$ a T-nek $\Omega(f)$-be való leképezése.

$(f^*)^{-1}\tau_1 = (f^*)^{-1}\tau_2$-t balról f^*-gal szorozva $\tau_1 = \tau_2$, ezért a leképezés injektív. Megmutatjuk, hogy a szürjektivitás is teljesül. Ha $S \in \Omega(f)$, akkor $\sum_{j=0}^{n} c_j s_{i+j} = 0$. Ebből $n \le i \in \mathbb{N}$ esetére kapjuk, hogy $(f^*S)_i = \sum_{j=0}^{i} f_j^* s_{i-j} = \sum_{j=0}^{n} f_j^* s_{i-j} = \sum_{j=0}^{n} c_{n-j} s_{i-j} = \sum_{j=0}^{n} c_j s_{i-n+j} = 0$, f^*S-ben az n-nél nem kisebb indexekhez tartozó minden tag nulla, így f^*S egy legfeljebb $n-1$-edfokú polinom.

A fentiek szerint $\tau \mapsto (f^*)^{-1}\tau$ egy $T \to \Omega(f)$ bijekció. Ha τ_1 és τ_2 $\mathcal{R}$ feletti legfeljebb $n-1$-edfokú polinom, és c_1, c_2 R eleme, akkor $(f^*)^{-1}(\tau_1 c_1 + \tau_2 c_2) = ((f^*)^{-1}\tau_1)c_1 + ((f^*)^{-1}\tau_2)c_2$, ami mutatja a művelettartást, és a bijekcióval az izomorfizmust.

□

10.24. Következmény

Legyen f $\mathcal{K}$ test feletti n-edfokú főpolinom. Ekkor $\Omega(f)$ n-dimenziós lineáris tér $\mathcal{K}$ felett, és ha $|K| = q$, akkor $|\Omega(f)| = q^n$.

Δ

Bizonyítás:

A $\mathcal{K}$ test feletti legfeljebb $n-1$-edfokú polinomok n-dimenziós lineáris teret alkotnak a test felett, de ekkor a vele izomorf $\Omega(f)$ is hasonló tulajdonságú.

Ha $|K| = q$, akkor a τ-polinomok száma q^n.

□

10.25. Tétel

Ha $\mathbf{s} \in \Omega(f)$, ahol f m-edfokú, $\mathbb{F}_q$ fölött irreducibilis főpolinom, $\hat{f}(0) \neq 0$, és α az f gyöke, akkor $s_i = \mathrm{S}_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\tau\alpha^i)$ a q^m-elemű test alkalmas τ elemével. Amennyiben f primitív polinom, és $\mathbf{s}$ nem a nullsorozat, akkor $s_i = \mathrm{S}(\alpha^{r+i})$ (ahol $\mathrm{S} = \mathrm{S}_{\mathbb{F}_{q^m}|\mathbb{F}_q}$) valamilyen $0 \leq r < q^m - 1$ egésszel.

Δ

Bizonyítás:

$\hat{f}(0) \neq 0$ biztosítja, hogy $\alpha \neq 0$, míg az irreducibilitás alapján a polinom foka, m, nagyobb nullánál. f irreducibilis m-edfokú polinom $\mathbb{F}_q$ fölött, így $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$, és α első m hatványa (α^0-val kezdve) az $\mathbb{F}_{q^m}$ mint $\mathbb{F}_q$ fölötti m-dimenziós tér bázisa. Van egy és csak egy olyan $\mathbf{T}_\tau: \mathbb{F}_{q^m} \to \mathbb{F}_q$ lineáris leképezés, amely α^i-t s_i-be képezi valamennyi $m > i \in \mathbb{N}$ indexre, ehhez a leképezéshez viszont létezik az egyértelműen meghatározott $\tau \in \mathbb{F}_{q^m}$, amellyel $\mathbf{T}_\tau(\alpha^i) = \mathrm{S}(\tau\alpha^i)$.

Az eddigiek alapján $m > i \in \mathbb{N}$-re $s_i = \mathrm{S}(\tau\alpha^i)$. Most legyen $u_i = \mathrm{S}(\tau\alpha^i)$ minden nemnegatív egész i-re. Ez mindenesetre egy $\mathbb{F}_q$ fölötti sorozat, amelynek első m eleme egybeesik $\mathbf{s}$ első m elemével. Legyen az eredeti sorozat karakterisztikus polinomja $f = x^m + \sum_{j=0}^{m-1} c_j x^j$, ekkor a rekurziós összefüggés $c_m = e$-vel $\sum_{j=0}^{m} c_j s_{t+j} = 0$. De $\sum_{j=0}^{m} c_j u_{t+j} = \sum_{j=0}^{m} c_j \mathrm{S}(\tau\alpha^{t+j}) = \mathrm{S}(\tau\alpha^t \sum_{j=0}^{m} c_j \alpha^j) = 0$, hiszen $\sum_{j=0}^{m} c_j \alpha^j = 0$, mert α gyöke a polinomnak, és nulla nyoma 0. Ez azt jelenti, hogy minden i-re u_i az $s_0, \dots, s_{m-1}$ kezdőértékekkel az f polinom által generált m-edrendű rekurzív sorozat i-edik tagja. De m-edrendű rekurzív sorozatot első m eleme egyértelműen meghatározza, így $s_i = u_i = S(\tau\alpha^i)$.

Végül, ha f primitív, akkor α primitív elem $\mathbb{F}_{q^m}$-ben, és $\mathbb{F}_{q^m}^*$ minden eleme, így τ is α hatványa egy $q^m - 1 > r \in \mathbb{N}$ kitevővel. Most $\tau \neq 0$, mert különben $\mathbf{s}$ a nullsorozat a tételben megadott kikötéssel ellentétben.

□

10.26. Definíció

s minimál-polinomja m, ha $S \in \Omega(m)$, és $S \in \Omega(f)$ csak $\deg(m) \leq \deg(f)$ esetén lehet.

Δ

10.27. Tétel

Test fölötti $\mathbf{s}$ homogén lineáris rekurzív sorozatnak van egyértelműen meghatározott minimálpolinomja, és ha ez m, akkor S akkor és csak akkor eleme $\Omega(f)$-nek, ha $m|f$.

Δ

Bizonyítás:

Test fölötti homogén lineáris rekurzív sorozatnak van karakterisztikus polinomja, és ez főpolinom, így a sorozatot generáló karakterisztikus polinomok halmaza nem üres. Főpolinom nem lehet a nullpolinom, és nem nulla polinom fokszáma nemnegatív egész szám, ezért a sorozathoz tartozó karakterisztikus polinomok fokszámainak halmaza a nemnegatív egész számok halmazának, tehát egy jólrendezett halmaznak nem üres részhalmaza. Ekkor az előbbi halmazban van egyértelműen meghatározott legkisebb elem, és van olyan karakterisztikus polinom, amelynek ez a fokszáma, így egy homogén lineáris rekurzív sorozatnak van minimál-polinomja. Ha igaz az oszthatóságra vonatkozó állítás, és m mellett t is minimálpolinom, akkor a kölcsönös oszthatóság miatt m és t asszociáltak, és mivel minimálpolinom főpolinom, ezért a két polinom meg is egyezik. Azt kell tehát megmutatni, hogy egy minimálpolinom osztója a sorozat karakterisztikus polinomjainak, de csak az ilyen főpolinomoknak.

Legyen $\mathcal{K}$ a test, és $m = x^{l_m} m_{(1)}$ a sorozat minimál-polinomja, ahol $l_m \in \mathbb{N}$ és $\hat{m}_{(1)}(0) \neq 0$. m főpolinom, tehát nem a nullpolinom, így ilyen $m_{(1)}$ polinom létezik, és m egyértelműen meghatározza

mind $m_{(1)}$-et, mind l_m-et. $S \in \Omega(m)$, tehát $S = \frac{\tau^{(m)}}{m^*}$ egy $\mathcal{K}$ feletti $\tau^{(m)}$ polinommal úgy, hogy $\delta(\tau^{(m)}) < \deg(m)$. Ha $d = (\tau^{(m)}, m^*)$, akkor d osztója m^*-nak, így $\hat{d}(0)\big|\hat{m}^*(0) = e$, tehát d konstans tagja nem nulla, és ekkor $(d^*)^* = d$ és $\deg(d) = \deg(d^*)$. Nemnulla legnagyobb közös osztó csupán asszociált, azaz egy nem nulla konstans szorzó erejéig egyértelmű, legyen ezért d konstans tagja e, ekkor d^* főpolinom. $d|m^*$-ból egyrészt $d^*\big|(m^*)^* = m_{(1)}$, másrészt $\frac{m}{d^*}$ is főpolinom. Visszatérve S-hez,

$$S = \frac{\tau^{(m)}}{m^*} = \frac{\frac{\tau^{(m)}}{d}}{\frac{m^*}{d}} = \frac{\frac{\tau^{(m)}}{d}}{\left(\frac{m}{d^*}\right)^*},$$

valamint

$$\delta\left(\frac{\tau^{(m)}}{d}\right) = \delta(\tau^{(m)}) - \deg(d) < \deg(m) - \deg(d) = \deg(m) - \deg(d^*) = \deg\left(\frac{m}{d^*}\right),$$

tehát $S \in \Omega\left(\frac{m}{d^*}\right)$. m az S minimál-polinomja, és az előbbiek alapján $\frac{m}{d^*}$ karakterisztikus polinomja S-nek, ezért $\deg(m) \le \deg\left(\frac{m}{d^*}\right) = \deg(m) - \deg(d^*) = \deg(m) - \deg(d)$, vagyis $\deg(d) \le 0$, azaz $\deg(d) = 0$, így d nemnulla konstans polinom. Ez azt jelenti, hogy $\tau^{(m)}$ és m^* relatív prím.

Most vizsgáljuk l_m-et. $\delta(\tau^{(m)}) < \deg(m) = \deg(x^{l_m} m_{(1)}) = \deg(x^{l_m}) + \deg(m_{(1)}) = l_m + \deg(m_{(1)})$, és ebből $l_m > \delta(\tau^{(m)}) - \deg(m_{(1)})$, azaz $l_m \ge \delta(\tau^{(m)}) - \deg(m_{(1)}) + 1$, hiszen l_m és $\deg(m_{(1)})$ egész szám, és $\delta(\tau^{(m)})$ is az, kivéve, ha $-\infty$, amikor viszont az 1 hozzáadása nem befolyásolja a jobb oldal értékét. Másrészt az is igaz, hogy $l_m \ge 0$, így az l_m-et korlátozó két egyenlőtlenséget összevonva azt kapjuk, hogy $l_m \ge \max\{0, \delta(\tau^{(m)}) - \deg(m_{(1)}) + 1\}$. Mivel m minimálpolinom, és m^* nem függ l_m-től, ezért l_m értéke a lehető legkisebb, így az előbbi kifejezésben egyenlőség áll, $l_m = \max\{0, \delta(\tau^{(m)}) - \deg(m_{(1)}) + 1\}$.

Ha $f = gm$ a $\mathcal{K}$ test fölötti g főpolinommal, akkor $S = \frac{\tau^{(m)}}{m^*} = \frac{g^*\tau^{(m)}}{g^*m^*} = \frac{g^*\tau^{(m)}}{(gm)^*} = \frac{g^*\tau^{(m)}}{f^*}$. Mivel $\delta(g^*\tau^{(m)}) = \deg(g^*) + \delta(\tau^{(m)}) < \deg(g^*) + \deg(m) \le \deg(g) + \deg(m) = \deg(gm) = \deg(f)$, ezért f karakterisztikus polinomja a sorozatnak, vagyis a minimálpolinom $\mathcal{K}$ fölötti minden főpolinom-szorosa karakterisztikus polinomja **s**-nek. Visszafelé, legyen a $\mathcal{K}$ feletti $h = x^{l_h} h_{(1)}$ főpolinom, ahol $l_h \in \mathbb{N}$ és $\hat{h}_{(1)}(0) \neq 0$ olyan, hogy $S \in \Omega(h)$. Ekkor $\frac{\tau^{(m)}}{m^*} = S = \frac{\tau^{(h)}}{h^*}$ és $\delta(\tau^{(h)}) < \deg(h)$. Innen $\tau^{(m)} h^* = \tau^{(h)} m^*$ és $m^*|h^*$, mert a korábbiak szerint $\tau^{(m)}$ és m^* relatív prím. Ha $m^*|h^*$, akkor $m_{(1)} = (m^*)^*\big|(h^*)^* = h_{(1)}$, továbbá

$$\begin{aligned} l_h + \deg(h_{(1)}) &= \deg(x^{l_h} h_{(1)}) = \deg(h) > \delta(\tau^{(h)}) \\ &= \delta(\tau^{(m)}) - \deg(m^*) + \deg(h^*) = \delta(\tau^{(m)}) - \deg(m^*) + \deg(h_{(1)}), \end{aligned}$$

tehát $l_h > \delta(\tau^{(m)}) - \deg(m^*) = \delta(\tau^{(m)}) - \deg(m_{(1)})$, azaz $l_h \ge \delta(\tau^{(m)}) - \deg(m_{(1)}) + 1$. Mivel $l_h \ge 0$, ezért $l_h \ge \max\{0, \delta(\tau^{(m)}) - \deg(m_{(1)}) + 1\} = l_m$, így $x^{l_m}\big|x^{l_h}$, és a fentebbi eredménnyel $m = x^{l_m} m_{(1)}\big|x^{l_h} h_{(1)} = h$, vagyis m osztja a sorozat minden karakterisztikus polinomját.

Korábban már beláttuk, hogy a minimálpolinom többszörösei karakterisztikus polinomjai a sorozatnak, most azt láttuk be, hogy csak ilyen polinomok lehetnek az **s** sorozat karakterisztikus polinomjai, vagyis egy f főpolinom akkor és csak akkor karakterisztikus polinomja az adott sorozatnak, ha osztható a sorozat minimál-polinomjával, amiből, mint láttuk, már következik a minimálpolinom egyértelműsége is.

□

10.28. Következmény

a) A nullsorozatnak és csak a nullsorozatnak e a minimál-polinomja;
b) nemnulla sorozat irreducibilis karakterisztikus polinomja minimálpolinom;
c) bármely f főpolinomhoz van olyan sorozat, amelynek f a minimál-polinomja.

Δ

Bizonyítás:

a) Ha $S = \frac{\tau}{e^*}$, akkor $\delta(\tau) < \deg(e) = 0$, így $\tau = 0$ és $S = 0$. Fordítva, bármely f főpolinommal $0 = \frac{0}{f^*}$, és $\delta(0) = -\infty < 0 \leq \deg(f)$, így $0 \in \Omega(f)$. Ekkor e is karakterisztikus polinomja a nullsorozatnak. Mivel e foka 0, és minden főpolinom foka legalább 0, ezért e a nullsorozat minimál-polinomja.

b) Ha a karakterisztikus polinom f és a minimálpolinom m, akkor m osztója f-nek. De f irreducibilis és m legalább elsőfokú, így ez csak úgy lehet, ha asszociáltak, és mivel a főegyütthatójuk azonos, ezért meg kell, hogy egyezzenek.

c) A konstans e polinom minimál-polinomja a nullsorozatnak. Most legyen $\deg(f) = n \geq 1$, $f = x^{l_f} f_{(1)}$, $\hat{f}_{(1)}(0) \neq 0$ és $\tau = x^{n-1}$, ekkor $\deg(\tau) < \deg(f)$ és $\frac{\tau}{f^*} \in \Omega(f)$. Maradékos osztással $\tau = uf^* + \sigma$, ahol $\deg(\sigma) < \deg(f^*)$, ha $\sigma \neq 0$. $(\sigma, f^*) = (uf^* + \sigma, f^*) = (\tau, f^*) = e$, így már csak azt kell belátni, hogy ha $l_f > 0$ (azaz $l_f \geq 1$, hiszen l_f egész szám), akkor $u \neq 0$, és az u polinom foka éppen $l_f - 1$. De ha $l_f \geq 1$, akkor $\deg(f^*) = \deg\left(f_{(1)}\right) = \deg(f) - l_f \leq n - 1 = \deg(\tau)$, tehát $u \neq 0$, és $\deg(u) = \deg(\tau) - \deg(f^*) = n - 1 - \deg(f^*) = \deg(f) - \deg(f^*) - 1 = l_f - 1$.

□

10.29. Tétel

Test feletti **s** sorozat pontosan akkor periodikus k-tól a p periódussal, ha $S \in \Omega\left(x^k(x^p - e)\right)$.

Δ

Bizonyítás:

a) Legyen a sorozat generátorfüggvénye S, továbbá $k' = kp$. $p \in \mathbb{N}^+$, ezért $kp \geq k$, **s** biztosan periodikus k'-től. Ha $\sigma = \sum_{i=0}^{p-1} s_{k'+i} x^i$, akkor σ legfeljebb $p - 1$-edfokú, így $T = \frac{\sigma}{e - x^p}$-ben bármely nemnegatív egész i-re $t_i = \sigma_{i \bmod p} = s_{k'+(i \bmod p)} = s_{k'+i}$, $\mathbf{t} = \mathbf{s}^{(k')}$. Ebből, és abból, hogy S k-tól periodikus a p periódussal következik, hogy **t** tisztán periodikus a p periódussal, és k-tól **s** és **t** azonos, hiszen $t_{k+i} = s_{k+i+k'} = s_{k+i+kp} = s_{k+i}$. Legyen $u = S - T$, ekkor az előbbiek szerint **u**-ban minden, a k-nál nem kisebb i indexre $u_i = s_i - t_i = 0$, ezért u legfeljebb $k - 1$-edfokú polinom, így

$$S = u + T = u + \frac{\sigma}{e - x^p} = \frac{u(e - x^p) + \sigma}{e - x^p} = \frac{\tau}{e - x^p} = \frac{\tau}{\left(x^k(e - x^p)\right)^*} = \frac{\tau}{f^*},$$

ahol $f = x^k(e - x^p)$ és $\tau = u(e - x^p) + \sigma$. Ha $\tau \neq 0$, akkor $\deg(\tau) < k + p = \deg(f)$, mert ha $u = 0$, akkor $\tau = \sigma \neq 0$, és $\deg(\sigma) < p \leq k + p$, míg $\deg(\tau) = \deg(u) + p \leq k - 1 + p < k + p$, ha $u \neq 0$.

b) Most legyen $g = x^k(e - x^p)$ és $S \in \Omega(g)$. Ekkor, maradékosan osztva τ-t a g duálisával, $S = \frac{\tau}{e - x^p} = u + \frac{\sigma}{e - x^p}$, ahol $\tau = ug^* + \sigma$, és $\sigma = 0$, vagy $\deg(\sigma) < p$. Ha $u = 0$, akkor $S = \frac{\sigma}{e - x^p}$, és ez a sorozat tisztán periodikus, tehát k-tól is periodikus a p periódussal. Amennyiben viszont u nem a nullpolinom, akkor $k + p = \deg(g) > \deg(\tau) = \deg(u) + \deg(g^*) = \deg(u) + p$, ezért $\deg(u) < k$, tehát k-tól S és $\frac{\sigma}{e - x^p}$ megegyezik, ami azt jelenti, hogy S k-tól periodikus a p periódussal.

□

10.30. Következmény

Legyen **s** a $\mathcal{K}$ test feletti homogén lineáris rekurzív sorozat.

a) Ha **s** periodikus a k küszöbtől a p minimális periódussal, és $\sigma = \sum_{i=0}^{p-1} s_{kp+i}x^i$, akkor a sorozat minimál-polinomja $x^k m_{(1)}$, ahol $m_{(1)} = \frac{x^p - e}{(\sigma^*, x^p - e)}$;

b) ha **s** minimál-polinomja $x^k m_{(1)}$, $m_{(1)}$ osztója $x^p - e$-nek, ahol $p \in \mathbb{N}^+$, de $p > p' \in \mathbb{N}^+$ esetén nem osztója $x^{p'} - e$-nek, akkor **s** periodikus a k küszöbtől a p minimális periódussal;

c) ha K véges, akkor **s** minimális periódusa osztója a karakterisztikus polinom rendjének;

d) véges K esetén **s** minimális periódusa megegyezik minimál-polinomjának rendjével;

e) ha $\mathcal{K} = \mathbb{F}_q$, akkor a sorozat k küszöbindexére és p minimális periódusára $p \leq k + p \leq q^n - 1$, eltekintve attól az esettől, amikor $n = 0$, vagy $q = 2$ és $f = x$;

f) ha $\mathbf{s} \in \Omega(f)$, ahol $f \in \mathbb{F}_q[x]$, $\hat{f}(0) \neq 0$, $\deg(f) = n$, és f irreducibilis $\mathbb{F}_q$ fölött, akkor a sorozat tisztán periodikus, és minimális periódusa osztója $q^n - 1$-nek.

Δ

Bizonyítás:

Az alábbiakban feltesszük, hogy a $g = x^l g_{(1)}$ alakú felírásban $\hat{g}_{(1)}(0) \neq 0$.

a) Azt már beláttuk, hogy a minimálpolinom $x^{k'} m_{(1)}$, ahol $k' \leq k$, így még azt kell igazolni, hogy $k' \geq k$. Ez viszont annak következménye, hogy ha $x^{k'} m_{(1)}$ karakterisztikus polinom, akkor a sorozat k'-től periodikus, ahonnan $k' \geq k$, hiszen k a küszöbindex.

b) **s** k-tól periodikus a p periódussal. Ha k'-től is periodikus a p' periódussal, akkor karakterisztikus polinomja $f = x^{k'}(x^{p'} - e)$, és $m|f$ csak úgy lehet, ha $k' \geq k$ és $m_{(1)} \big| x^{p'} - e$, azaz ha $p' \geq p$.

c) Ha $f = x^l f_{(1)}$ a karakterisztikus polinom, és f rendje p, akkor $f_{(1)}$ osztója $x^p - e$-nek, tehát p periódusa **s**-nek, és a minimális periódus osztója a sorozat bármely periódusának.

d) c) alapján a p minimális periódus osztója a rendnek, míg ha $m = x^{k'} m_{(1)}$ a minimálpolinom, akkor a) szerint $m_{(1)}$ osztója $x^p - e$-nek, amiből következik, hogy a rend osztója p-nek.

e) $p \leq k + p$ nyilván igaz. Legyen $f = x^u f_{(1)}$ az **s** karakterisztikus polinomja és $n = \deg(f)$. **s** u-tól biztosan periodikus, így $k \leq u$. $v \leq q^v - 1$ bármely $v \in \mathbb{N}$ és $1 < q \in \mathbb{N}$ esetén érvényes, és $v = q^v - 1$ csak $v = 0$, illetve $v = 1$ és $q = 2$ esetén áll. Ha $u = n$, akkor $p = 1$, és ebből $n = 0$, illetve $n = 1$ és $q = 2$ esetén $n + 1 > n = q^n - 1$, vagyis ilyenkor $k + p \leq q^n - 1$ nem feltétlenül áll. Ha viszont $n \geq 1$, és vagy $f \neq x$ vagy $q > 2$, akkor már $n < q^n - 1$, tehát $k + p \leq n + 1 \leq q^n - 1$.

$u < n$-nél $q^{n-u} - 1 \geq 1$, $\deg(f_{(1)}) = n - u$ és $p \leq o(f_{(1)}) \leq \max\{1, q^{n-u} - 1\} = q^{n-u} - 1$, és ekkor

$$k + p \leq u + (q^{n-u} - 1) \leq (q^u - 1) + (q^{n-u} - 1) \leq (q^u - 1)q^{n-u} + (q^{n-u} - 1) = q^n - 1.$$

f) Mivel $\hat{f}(0) \neq 0$, ezért az $f = x^k f_{(1)}$, $\hat{f}_{(1)}(0) \neq 0$ alakú felírásban $k = 0$, ami mutatja, hogy a sorozat 0-tól periodikus, és így tisztán periodikus. Ami a második állítást illeti, az abból következik, hogy $\mathbb{F}_q$ fölött irreducibilis n-edfokú polinom rendje osztója $q^n - 1$-nek.

□

Korábban láttuk, hogy q-elemű halmaz fölötti n-edrendű rekurzív sorozat periodikus, és a k küszöbindexre és p minimális periódusra teljesül a $p \leq k + p \leq q^n$ reláció, most ezt élesítettük homogén lineáris rekurzív sorozatokra. Ha csak azt akarjuk belátni, hogy a legalább elsőrendű homogén lineáris sorozatra $p < q^n$, akkor ez lényegesen egyszerűbben is megtehető. Ha a sorozatban előfordul a nullállapot, akkor a homogén lineáris rekurzió következtében minden további állapot a nullállapot, innen kezdve a sorozat minden eleme 0, a periódus 1, és $n \geq 1$, $q \geq 2$, tehát $q^n - 1 \geq 2^1 - 1 = 1 \geq 1$. Ha viszont a nullállapot nem fordul elő, akkor az állapotok száma legfeljebb $q^n - 1$, és az első q^n állapot között egyikük biztosan előfordul legalább kétszer, és a kettő közötti távolság legfeljebb $q^n - 1$.

10.31. Tétel

Legyen $\mathcal{K}$ test, f, g és h $K[x]$-beli főpolinom, $d = (f, g)$ és $t = [f, g]$, végezetül legyen $\Omega(f) + \Omega(g) = \{S^{(f)} + S^{g} | S^{(f)} \in \Omega(f) \wedge S^{(g)} \in \Omega(g)\}$. Ekkor

a) $\Omega(f) \subseteq \Omega(h)$ akkor és csak akkor, ha $f|h$;
b) $\Omega(f) \cap \Omega(g) = \Omega(d)$ és
c) $\Omega(f) \cup \Omega(g) \subseteq \Omega(f) + \Omega(g) = \Omega(t)$.

Δ

Bizonyítás:

a) Ha m az S minimál-polinomja, és $f|h$, akkor $m|h$, így h karakterisztikus polinomja S-nek, tehát $S \in \Omega(h)$, és így $\Omega(f) \subseteq \Omega(h)$. Fordítva, tegyük fel, hogy $\Omega(f) \subseteq \Omega(h)$. 10.28. c) pontja szerint van olyan $S \in \Omega(h)$, hogy **s** minimál-polinomja f, és ekkor $S \in \Omega(h)$-ból következik, hogy $f|h$.

b) Az előző pont alapján $\Omega(d) \subseteq \Omega(f) \cap \Omega(g)$. Most legyen $S \in \Omega(f) \cap \Omega(g)$, és m az S minimál-polinomja. $S \in \Omega(f) \cap \Omega(g)$-ből $S \in \Omega(f)$ és $S \in \Omega(g)$, így $m|f$ és $m|g$, tehát $m|(f, g) = d$, $S \in \Omega(d)$, azaz $\Omega(f) \cap \Omega(g) \subseteq \Omega(d)$. Ekkor a korábbi tartalmazással együtt $\Omega(f) \cap \Omega(g) = \Omega(d)$.

c) A nullsorozat eleme $\Omega(f)$-nek és $\Omega(g)$-nek, ezért a) alapján igaz a bal oldali tartalmazás.

Ha $S^{(f)} \in \Omega(f)$ és $S^{(g)} \in \Omega(g)$, akkor $S^{(f)} \in \Omega(t)$ és $S^{(g)} \in \Omega(t)$. $\Omega(t)$ lineáris tér, ezért az előbbiek alapján $\mathbf{s}^{(f)} + \mathbf{s}^{(g)} \in \Omega(t)$, így $\Omega(f) + \Omega(g) \subseteq \Omega(t)$. Visszafelé, legyen $S \in \Omega(t)$, ekkor $S = \frac{\tau}{t^*}$, ahol $\delta(\tau) < \deg(t)$. Ha $d = (f, g)$, akkor $t = \frac{fg}{d}$ és $t^* = \frac{f^* g^*}{d^*}$. Az $\frac{f^*}{d^*} = f_{(1)}$ és $\frac{g^*}{d^*} = g_{(1)}$ jelöléssel $(f_{(1)}, g_{(1)}) = e$, ezért létezik olyan u és v polinom, amellyel $f_{(1)}u + g_{(1)}v = \tau$, és van olyan is, ahol $\delta(u) < \deg(g_{(1)}) \leq \deg(g)$ és $\delta(v) < \deg(f_{(1)}) \leq \deg(f)$. Ha $u = \tau^{(f)}$ és $v = \tau^{(g)}$ egy ilyen megoldás, akkor $S = \frac{\tau}{t^*} = \frac{g_{(1)}\tau^{(f)} + f_{(1)}\tau^{(g)}}{f_{(1)}g_{(1)}d^*} = \frac{\tau^{(f)}}{f^*} + \frac{\tau^{(g)}}{g^*} \in \Omega(f) + \Omega(g)$, ugyanis most $\frac{\tau^{(f)}}{f^*} \in \Omega(f)$ valamint $\frac{\tau^{(g)}}{g^*} \in \Omega(g)$. Ebből következik, hogy $\Omega(t) \subseteq \Omega(f) + \Omega(g)$, vagyis $\Omega(t) = \Omega(f) + \Omega(g)$.

□

q-elemű test fölötti n-edrendű homogén lineáris rekurzív sorozat minimális periódusa legfeljebb $q^n - 1$. Kérdés, hogy elérhető-e ez a maximális érték.

10.32. Definíció

A q-elemű $\mathcal{K}$ test fölötti **s** n-edrendű homogén lineáris rekurzív sorozat **maximális periódusú**, ha nem az 1 küszöbindextől nulla bináris sorozat, és minimális periódusa $q^n - 1$.

Δ

10.33. Tétel

A q-elemű $\mathcal{K}$ test fölötti **s** n-edrendű homogén lineáris rekurzív sorozat akkor és csak akkor maximális periódusú, ha minimál-polinomja n-edfokú primitív polinom $\mathcal{K}$ fölött. Maximális periódusú sorozat tisztán periodikus.

Δ

Bizonyítás:

$\mathbb{F}_q$ feletti homogén lineáris rekurzív sorozat periodikus, minimális periódusa a minimálpolinom rendje, amely legfeljebb $\max\{1, q^n - 1\}$, és pontosan akkor $q^n - 1$, ha $q = 2$ és $m = x$, vagy ha m primitív polinom. Ám az első eset azt a bináris sorozatot generálja, amelynek első eleme e, a többi 0.

Maximális periódusú sorozatra $k + p \leq q^n - 1 = p$, és $k \geq 0$, így k valóban nulla.

□

10.34. Tétel

Ha $\hat{f}_{(1)}(0) \neq 0$, az **s** homogén lineáris rekurzív sorozat karakterisztikus polinomja $f = x^u f_{(1)}$, b nemnegatív egész, és $v = \max\{0, u-b\}$, akkor **s** b-eltoltjának karakterisztikus polinomja $x^v f_{(1)}$. Fordítva, ha **s** b-eltoltjának karakterisztikus polinomja $x^w f_{(1)}$, akkor $f = x^{w+b} f_{(1)}$ karakterisztikus polinomja **s**-nek.

Δ

Bizonyítás:

Legyen $\mathbf{s}^{(b)} = \mathbf{t}$, $\deg(f) = n$, $f = x^u f_{(1)} = x^u \sum_{i=0}^{n-u} c_i x^i = \sum_{i=u}^{n} c_{i-u} x^i$, ahol $c_{n-u} = e$, és legyen $r = \min\{u, b\}$. Ekkor $r \leq u \leq n$, így

$$t_{i+(n-r)} = s_{i+n-r+b} = s_{i-r+b+n} = \sum_{j=u}^{n-1} (-c_{j-u}) s_{i-r+b+j}$$
$$= \sum_{j=u}^{n-1} (-c_{j-u}) s_{i-r+j+b} = \sum_{j=u}^{n-1} (-c_{j-u}) t_{i-r+j} = \sum_{j=u-r}^{n-r-1} (-c_{j-u+r}) t_{i+j},$$

tehát $\sum_{i=u-r}^{n-r} c_{i-u+r} x^i = x^{u-r} \sum_{i=0}^{n-u} c_i x^i = x^{u-r} f_{(1)}$ karakterisztikus polinomja **t**-nek. u és b nemnegatív, így r is az, és $-r = \max\{-u, -b\}$, innen $u - r = \max\{u-u, u-b\} = \max\{0, u-b\} = v$.

Most tegyük fel, hogy **t** karakterisztikus polinomja $f = \sum_{i=w}^{n} c_{i-w} x^i$. Ekkor

$$s_{i+(n+b)} = t_{i+n} = \sum_{j=w}^{n-1} (-c_{j-w}) t_{i+j} = \sum_{j=w+b}^{n+b-1} (-c_{j-w-b}) s_{i+j},$$

ami mutatja, hogy **s**-nek karakterisztikus polinomja $\sum_{i=w+b}^{n+b} c_{i-(w+b)} x^i = x^b \sum_{i=w}^{n} c_{i-w} x^i = x^b f$.

□

10.35. Kiegészítés

Ha **s** minimál-polinomja $m = x^k m_{(1)}$, ahol $\widehat{m}_{(1)}(0) \neq 0$ és $k' = \max\{0, k-b\}$, akkor $\mathbf{s}^{(b)}$ minimál-polinomja $m^{(b)} = x^{k'} m_{(1)}$, és $m^{(b)} \big| m$. Ha **s** tisztán periodikus, akkor $m = m^{(b)}$.

Δ

Bizonyítás:

$m^{(b)}$ karakterisztikus polinomja $\mathbf{s}^{(b)}$-nek, így $\mathbf{s}^{(b)}$ minimál-polinomja osztja $m^{(b)}$-t. Ha a minimálpolinom $x^u m'$, akkor egyrészt $0 \leq u \leq k'$ és m' osztója $m_{(1)}$-nek, másrészt **s**-nek karakterisztikus polinomja $x^{u+b} m'$, ahonnan $u + b \geq k$ és $m_{(1)} \big| m'$. A két oszthatóságból $m' = m_{(1)}$ (mert mindkettő főpolinom), és $k' = \max\{0, k-b\} \leq u \leq k'$, tehát $u = k'$, $m^{(b)}$ az $\mathbf{s}^{(b)}$ minimál-polinomja.

Ha **s** tisztán periodikus, akkor $k = 0$, és ekkor k' is 0, tehát $s_{i+b} = s_{i+b'}$.

□

10.36. Tétel

Ha az $\mathbb{F}_q$ fölötti n-edrendű maximális periódusú **s** sorozat minimál-polinomja m, és **0** a nullsorozat, akkor $\Omega(m) = \{\mathbf{0}\} \cup \left\{\mathbf{s}^{(b)} \middle| q^n - 1 > b \in \mathbb{N}\right\}$, és $\mathbf{s}^{(b)}$ is n-edrendű maximális periódusú sorozat.

Δ

Bizonyítás:

Maximális periódusú sorozat tisztán periodikus, így $\mathbf{s}^{(b)} \in \Omega(m)$, másrészt $s_{i+b} = s_{i+b'}$ akkor és csak akkor teljesül, ha $b \equiv b' \ (p)$, ahol p a sorozat minimális periódusa, azaz ha $b \equiv b' \ (q^n - 1)$, ezért a $0 \leq b < q^n - 1$ eltoláshoz tartozó $\mathbf{s}^{(b)}$ sorozatok páronként különbözőek, és minden eltolt sorozat ezek valamelyikével azonos. Az eltolt sorozatok száma $q^n - 1$, és éppen ennyi $\Omega(m)$-ben a nullától különböző sorozatok száma, ezért a megadott két halmaz azonos.

Homogén lineáris rekurzív sorozat minimális periódusát a minimálpolinom egyértelműen meghatározza, így igaz a másik állítás is.

□

Az előbb kapott eredmények felhasználásával megvizsgáljuk a maximális periódusú sorozatok bizonyos statisztikus tulajdonságait.

10.37. Tétel

Legyen $\mathbf{s}$ $\mathbb{F}_q$ fölötti n-edrendű maximális periódusú sorozat, $r \in \mathbb{N}^+$, $c^{(r)} = (c_0, \dots, c_{r-1}) \in \mathbb{F}_q^r$. Ekkor a sorozat egy periódusában $c^{(r)}$ előfordulási gyakorisága q^{n-r}, ha $r \leq n$ és legalább egy indexre $c_i \neq 0$, $q^{n-r} - 1$, ha $r \leq n$ és valamennyi i-re $c_i = 0$, míg $r > n$ esetén vagy 0, vagy 1.

Δ

Bizonyítás:

Legyen először $r \leq n$. Mivel egy maximális periódusú sorozatban a nullától különböző minden állapot pontosan egyszer fordul elő, ezért könnyen látható, hogy kölcsönösen egyértelmű megfeleltetés létesíthető az egy periódusban található $c^{(r)}$-sorozatok, valamint a sorozat azon állapotai között, amelyekben az első r elem éppen $c^{(r)}$, így annyi ilyen sorozat van egy periódusban, ahányféleképpen az állapot utolsó $n - r$ eleme választható. Az ilyen választások száma q^{n-r}, kivéve azt az esetet, amikor az állapot valamennyi eleme 0, azaz amikor mind $c^{(r)}$ minden eleme, mind a további elemek mindegyike nulla, ez indokolja ebben az esetben a -1-es korrekciót.

Mint korábban bizonyítottuk, n-edrendű rekurzív sorozatban bármely n egymás utáni elem meghatározza az összes utána következőt, így ha $r > n$, és $c^{(r)}$ első n eleme $c^{(r)}$-et generálja, akkor $c^{(r)}$ egyszer szerepel a sorozatban egy adott periódusba eső kezdőponttal, míg ha az utolsó $r - n$ elem nem felel meg az elől álló n elemnek, akkor egyszer sem, ide sorolva a csupa 0-ból álló $c^{(r)}$-et is, mert bár ez generálódna az első n elemből, de a sorozatban nem szerepel.

□

10.38. Tétel

Legyen $\mathbf{s}$ az $\mathbb{F}_q$ fölötti n-edrendű maximális periódusú sorozat, és $r \in \mathbb{N}^+$. Ekkor bármely t nemnegatív egészre $k(r) = \frac{1}{q^n-1} \sum_{i=0}^{q^n-2} \kappa(s_{t+i}) \bar{\kappa}(s_{t+i+r}) = -\frac{1}{q^n-1}$, ha r nem osztható a periódussal, egyébként 1 (κ a test kanonikus additív karaktere, és $\bar{c}$ a c komplex szám konjugáltja).

Δ

Bizonyítás:

$\kappa(s_{t+i})\bar{\kappa}(s_{t+i+r}) = \kappa(s_{t+i} - s_{t+i+r}) = \kappa(s_{t+i+b})$, ahol $q^n - 1 > b \in \mathbb{N}$, ha r nem többszöröse a periódusnak. Ha most egy teljes periódusra összegzünk, és a sorozathoz hozzáadunk $\kappa(0)$-t, akkor ez egy olyan összeg, ahol κ argumentumaként a test valamennyi eleme ugyanannyiszor fordul elő, ezért az összeg 0 (mert kanonikus karakter nem főkarakter), így ismét levonva $\kappa(0) = 1$-et, kapjuk az első eredményt. A második eset abból adódik, hogy ekkor $s_{t+i} = s_{t+i+r}$, tehát $\kappa(s_{t+i})\bar{\kappa}(s_{t+i+r}) = 1$, így ekkor csupa 1-et adunk össze.

□

10.39. Megjegyzés

Az előbbi két tétel közül az első alapján véges test feletti n-edrendű maximális periódusú sorozatban minden nem nulla elem azonos gyakorisággal fordul elő, míg a nulla eggyel kevesebbszer, továbbá tetszőleges, n-nél rövidebb sorozat után bármely elem ugyanazon valószínűséggel következik, kivéve a csupa 0-t követő 0, és ez is csak eggyel kisebb gyakorisággal található a sorozatban. A másik tétel szerint a sorozat lényegében véve korrelálatlan, ha a távolság nem a periódus többszöröse.

Δ

Megadva egy n-edrendű homogén lineáris rekurzív sorozat első n elemét és a rekurziós összefüggés n együtthatóját, a sorozat minden eleme kiszámolható, vagyis ez a $2n$ adat egyértelműen meghatározza a teljes sorozatot. Ebből arra gondolhatunk, hogy egy ilyen sorozat $2n$ egymás utáni elemének ismerete elegendő információt tartalmaz a teljes további sorozatról, így nem meglepő az alábbi eredmény.

10.40. Tétel

Test fölötti n-edrendű homogén lineáris rekurzív sorozat $2n$ egymás utáni elemének ismeretében a sorozat tetszőleges további eleme egyértelműen meghatározható. Ha n a minimális rend, akkor ennél kevesebb elemmel az egyértelműség nem teljesül.

Δ

Bizonyítás:

Mivel a sorozat n-edrendű homogén lineáris rekurzív sorozat, ezért egy $s_{i+n} = \sum_{j=0}^{n-1} c_j s_{i+j}$ alakú rekurziós összefüggéssel generálható, ahol i tetszőleges nemnegatív egész, és az n darab c_j együttható egyelőre ismeretlen. Tegyük fel, hogy az $r \in \mathbb{N}$ indextől kezdve ismerjük a sorozat $2n$ számú egymás után következő $s_r, \dots, s_{r+2n-1}$ elemét. Most $n > t \in \mathbb{N}$-re $\sum_{j=0}^{n-1} s_{r+t+j} x_j = s_{r+t+n}$ egy n egyenletből álló, n ismeretlent tartalmazó lineáris egyenletrendszer, amely megoldható, hiszen egy megoldása például $c_0, \dots, c_{n-1}$. Legyen egy megoldás $b_0, \dots, b_{n-1}$. Ekkor egyrészt minden $n > t \in \mathbb{N}$ esetén $\sum_{j=0}^{n-1} b_j s_{r+t+j} = s_{r+t+n}$, hiszen éppen így határoztuk meg a b_i együtthatókat, másrészt

$$\sum_{j=0}^{n-1} b_j s_{r+n+j} = \sum_{j=0}^{n-1} \left(b_j \sum_{t=0}^{n-1} c_t s_{r+j+t} \right) = \sum_{t=0}^{n-1} \left(c_t \sum_{j=0}^{n-1} b_j s_{r+t+j} \right) = \sum_{t=0}^{n-1} (c_t s_{r+n+t}) = s_{r+2n},$$

ezért a $\sum_{j=0}^{n-1} b_j s_{r+t+j} = s_{r+t+n}$ rekurziós összefüggés $t = n$-re és innen indukcióval bármely $t \in \mathbb{N}$-re is érvényes.

$2n$-nél kevesebb tagot ismerve $n > 0$, és n-nél kevesebb egyenlet írható fel, viszont ha a rekurzió minimális rendje n, úgy a minimál-polinomban n ismeretlen van, és minden, a sorozatot generáló karakterisztikus polinom megadásához legalább ennyi együttható meghatározása szükséges. Ekkor tehát a rekurziós összefüggésben legalább egy együtthatót szabadon választunk. Ha két azonos fokszámú főpolinom egyikében egyetlen együtthatót szabadon választunk, akkor van olyan választás is, ahol a két polinom nem azonos és így nem is asszociált (hiszen a főegyütthatók azonosak). Ebben az esetben viszont a két polinom különböző sorozatot generál, mert ellenkező esetben nem lenne egyértelmű a sorozat minimál-polinomja.

□

Bizonyos esetekben az előbb bemutatott tulajdonság nem kívánatos. A rejtjelezésben inkább olyan sorozatra van szükségünk, amely rendelkezik az álvéletlen sorozatok tulajdonságaival, de az előrejelzés minél bonyolultabb. Ezen bonyolultság egy lehetséges mértéke az, hogy mekkora n-nel tudjuk az adott sorozatot homogén lineáris rekurzióval generálni. Ez persze véges test és nem periodikus sorozat esetén nem lehetséges, de bármely k nemnegatív egészre a sorozat első k elemből álló szegmensére

már igen (másrészt véges test feletti rekurzív sorozat biztosan periodikus). Ez indokolja az alábbi definíciót.

10.41. Definíció

Legyen e_b bal oldali egységelem az $\mathcal{R}$ gyűrűben, $k \in \mathbb{N}$, $\mathbf{s}: \mathbb{N} \to R$ és $S = \sum_{i=0}^{\infty} s_i x^i$. Ekkor

1. $s^{[k]} = S \bmod x^k$ az $\mathbf{s}$ k-**hosszúságú kezdőszelete**;
2. ha $A^{(k)}(\mathbf{s}) = \{f \in R[x] | \hat{f}^*(0) = e_b \wedge (\exists(\mathbf{t} \in \Omega(f)): t^{[k]} = s^{[k]})\}$, akkor $\mathbf{s}$ k-**hosszúságú kezdőszeletének lineáris komplexitása** $L_k(\mathbf{s}) = \min_{f \in A^{(k)}(\mathbf{s})} \{\deg(f)\}$;
3. $\mathbf{s}$ **lineáris komplexitása** $L(\mathbf{s}) = \sup_{k \in \mathbb{N}} \{L_k(\mathbf{s})\} \in \mathbb{N} \cup \{\infty\}$.

Δ

$A^{(k)}(\mathbf{s})$ az $\mathcal{R}$ feletti azon polinomok halmaza, amelyek által generált homogén lineáris rekurzív sorozatok között van olyan, amelynek a k hosszúságú kezdőszelete azonos a szintén $\mathcal{R}$ feletti $\mathbf{s}$ sorozat k hosszúságú kezdőszeletével, $s^{[k]}$-val, vagyis amely karakterisztikus polinomja egy olyan homogén lineáris rekurzív sorozatnak, amelynek első k eleme azonos $\mathbf{s}$ első k elemével. $L_k(\mathbf{s})$ az ilyen karakterisztikus polinomok fokszámainak a minimuma.

$L_k(\mathbf{s})$ – ha létezik – nemnegatív egész szám, ezért ha az $L_k(\mathbf{s})$-ek halmaza korlátos, akkor van benne maximális elem, és ekkor $L(\mathbf{s}) \in \mathbb{N}$, míg ha nem korlátos, akkor $L(\mathbf{s}) = +\infty$ (ha $L_k(\mathbf{s})$ egyetlen nemnegatív egész k-ra sem létezik, akkor $L(\mathbf{s})$ az üres halmaz felső határa, és ez szintén $+\infty$).

A következőkben többek között igazoljuk, hogy $L_k(\mathbf{s})$ minden nemnegatív egész k-ra létezik.

A sorozat elemeit 0-tól kezdve indexeljük, így az első k elem a $k > i \in \mathbb{N}$ indexekhez tartozik, azaz $s^{[k]} = s_0, \dots, s_{k-1}$.

Célunk a továbbiakban, hogy becslést adjunk a lineáris komplexitásra. A $\mathcal{K}$ test feletti sorozatokat vizsgáljuk, egy $A^{(k)}(\mathbf{s})$-beli, $L_k(\mathbf{s})$-fokú polinomot $m_{\mathbf{s}}^{\langle k \rangle}$-val jelölünk, és $\mathbf{s}^{\langle k \rangle}$ egy $\Omega(m^{\langle k \rangle})$-beli sorozat, amelynek k hosszúságú kezdőszelete $s^{[k]}$. Amennyiben nyilvánvaló, hogy melyik sorozatról van szó, akkor $L_k(\mathbf{s})$ helyett egyszerűen L_k-t írunk.

10.42. Tétel

Legyen $\mathbf{s}: \mathbb{N} \to K$ egy $\mathcal{K}$ feletti sorozat, és $k \in \mathbb{N}$. Ekkor

1. $L_k(\mathbf{s})$ létezik és egyértelmű;
2. bármely $\mathbf{s}^{\langle k \rangle}$-ra $m_{\mathbf{s}}^{\langle k \rangle}$ az $\mathbf{s}^{\langle k \rangle}$ minimál-polinomja;
3. $k \geq L_k(\mathbf{s}) \in \mathbb{N}$;
4. minden $k \geq j \in \mathbb{N}$-hez van olyan $\mathbf{s}$, hogy $L_k(\mathbf{s}) = j$;
5. ha $\mathbf{s}$ és $\mathbf{s}'$ k-hosszúságú kezdőszelete azonos, akkor $A^{(k)}(\mathbf{s}) = A^{(k)}(\mathbf{s}')$ és $L_k(\mathbf{s}) = L_k(\mathbf{s}')$;
6. $L_k(\mathbf{s}) \leq L_{k+1}(\mathbf{s})$;
7. $A^{(k)}(\mathbf{s}^{\langle k \rangle}) = A^{(k)}(\mathbf{s})$, és így $L_k(\mathbf{s}^{\langle k \rangle}) = L_k(\mathbf{s})$;
8. ha $s_k = s_k^{\langle k \rangle}$, akkor $L_{k+1}(\mathbf{s}) = L_k(\mathbf{s})$;
9. $L_{k+1}(\mathbf{s}^{\langle k \rangle}) = L_k(\mathbf{s}^{\langle k \rangle})$.

Δ

Bizonyítás:

1. A $\mathcal{K}$ feletti valamennyi legalább k-adfokú f főpolinom eleme $A^{(k)}(\mathbf{s})$-nek, mert egy n-edrendű rekurzió első n eleme szabadon választható. Ekkor $A^{(k)}(\mathbf{s})$ nem üres, és a nullpolinom nem főpolinom, tehát biztosan nem eleme a halmaznak, így az $A^{(k)}(\mathbf{s})$-hez tartozó polinomok fokainak halmaza a

nemnegatív egész számok halmazának nem üres részhalmaza. $\mathbb{N}$ jólrendezett, így bármely nem üres részhalmazának van legkisebb eleme, amely egyértelmű, ezért $L_k(\mathbf{s})$ létezik és egyértelmű;

2. ha $\mathbf{t} \in \Omega(f)$ olyan, hogy $t^{\langle k \rangle} = s^{\langle k \rangle}$, és m a $\mathbf{t}$ minimál-polinomja, akkor $m \in A^{(k)}(\mathbf{s})$, és m foka legfeljebb akkora, mint f foka;
3. 1.-ből következik, hogy $L_k(\mathbf{s}) \in \mathbb{N}$, valamint az is, hogy $L_k(\mathbf{s}) \leq k$;
4. a nullsorozat minden f főpolinomra, tehát e-re is eleme $\Omega(f)$-nek, így $e \in A^{(k)}(\mathbf{0})$, tehát $0 \leq L_k(\mathbf{0}) \leq \deg(e) = 0$, azaz $L_k(\mathbf{0}) = 0$. Most legyen $k \geq j \in \mathbb{N}$, és legyen $s_i = \delta_{i,j}e$, vagyis $\mathbf{s}$ olyan sorozat, amelyben a j indexhez tartozó, azaz a $j+1$-edik, és csak ez az elem nem 0. Ha $f = x^{j+1}$, akkor $\mathbf{s} \in \Omega(f)$, és ekkor $f \in A^{(k)}(\mathbf{s})$. Valóban, az f-hez tartozó homogén lineáris rekurzióban az első $j+1$ elem szabadon választható, tehát lehet például $s^{[j+1]} = s_0 \dots s_{j-1}s_j = 0 \dots 0e$, míg a sorozat további elemei $s_{j+1+l} = \sum_{i=0}^{j}(-f_i)s_{i+l} = 0$, ahol $f = \sum_{i=0}^{j+1} f_i x^i$, hiszen $f = x^{j+1}$-ből a j-nél nem nagyobb i indexekre $f_i = 0$, míg $f_{j+1} = e$. Ugyanakkor, ha a $g = \sum_{i=0}^{j'+1} g_i x^i$ főpolinomban j' kisebb j-nél, akkor bármely olyan $\mathbf{t} \in \Omega(g)$-re, amelyre $t^{[j]} = 0 \cdots 0$, $t_j = \sum_{i=0}^{j'} g_i t_{j-j'+i} = 0$, tehát az ilyen g-hez tartozó valamennyi $\mathbf{t}$ sorozat esetén $t_j \neq s_j$, és így $t^{[k]} \neq s^{[k]}$, hiszen $j < k$, ezért $g \notin A^{(k)}(\mathbf{s})$, amiből következik, hogy erre az $\mathbf{s}$ sorozatra $L_k(\mathbf{s}) = j+1$;
5. $f \in A^{(k)}(\mathbf{s})$ akkor és csak akkor, ha van olyan $\mathbf{t} \in \Omega(f)$, hogy $t^{[k]} = s^{[k]}$. A feltétel szerint viszont $s^{[k]} = s'^{[k]}$, vagyis $t^{[k]} = s'^{[k]}$ és így $f \in A^{(k)}(\mathbf{s}')$, tehát $A^{(k)}(\mathbf{s}) \subseteq A^{(k)}(\mathbf{s}')$. Mivel ez akkor is igaz, ha felcseréljük $\mathbf{s}$-t és $\mathbf{s}'$-t, ezért $A^{(k)}(\mathbf{s}) = A^{(k)}(\mathbf{s}')$, ebből viszont következik, hogy $L_k(\mathbf{s}) = L_k(\mathbf{s}')$;
6. Ha $t^{[k+1]} = s^{[k+1]}$, akkor $t^{[k]} = s^{[k]}$, és ezért $A^{(k+1)}(\mathbf{s}) \subseteq A^{(k)}(\mathbf{s})$. De szűkebb halmaz minimuma nagyobb, vagy egyenlő, mint az őt tartalmazó halmaz minimuma, így $L_k(\mathbf{s}) \leq L_{k+1}(\mathbf{s})$;
7. $s^{\langle k \rangle^{[k]}} = s^{[k]}$, így az állítás következik 5.-ből;
8. $s^{\langle k \rangle^{[k]}} = s^{[k]}$, és ha még $s_k = s_k^{\langle k \rangle}$, akkor $s^{\langle k \rangle^{[k+1]}} = s^{[k+1]}$, tehát 7.-ből $L_{k+1}(\mathbf{s}) = L_k(\mathbf{s})$;
9. $s^{\langle k \rangle^{[k]}} = s^{[k]}$, és ezért ez az állítás következik 8.-ból.

□

10.43. Tétel

Ha $\mathbf{s}$ és $\mathbf{t}$ test fölötti sorozatok, és a, b a test eleme, akkor $L_k(a\mathbf{s} + b\mathbf{t}) \leq L_k(\mathbf{s}) + L_k(\mathbf{t})$.

Δ

Bizonyítás:

Ha az $\mathbf{s}$ sorozat kezdő k-hosszúságú szeletének lineáris komplexitása $L_k(\mathbf{s})$, akkor van olyan $L_k(\mathbf{s})$-rendű $\mathbf{s}^{\langle k \rangle}$ homogén lineáris rekurzív sorozat, amelynek első k eleme megegyezik $\mathbf{s}$ első k elemével, és ugyanez igaz az $\mathbf{s}$ és $\mathbf{t}$ felcserélésével a másik sorozatra is. Az előbbi két sorozattal az is teljesül, hogy a $k > i \in \mathbb{N}$ indexekre $a\mathbf{s} + b\mathbf{t}$ és $a\mathbf{s}^{\langle k \rangle} + b\mathbf{t}^{\langle k \rangle}$ megegyezik, vagyis ha f karakterisztikus polinomja $a\mathbf{s}^{\langle k \rangle} + b\mathbf{t}^{\langle k \rangle}$-nak, akkor $L_k(a\mathbf{s} + b\mathbf{t}) \leq \deg(f)$. Legyen a két homogén lineáris rekurzív sorozat minimál-polinomja $m_{\mathbf{s}}^{\langle k \rangle}$ és $m_{\mathbf{t}}^{\langle k \rangle}$. Ekkor $m_{\mathbf{s}}^{\langle k \rangle}$, $m_{\mathbf{t}}^{\langle k \rangle}$ és $m_{\mathbf{s}}^{\langle k \rangle} m_{\mathbf{t}}^{\langle k \rangle}$ foka az előbbi sorrendben $L_k(\mathbf{s})$, $L_k(\mathbf{t})$ és $L_k(\mathbf{s}) + L_k(\mathbf{t})$. $m_{\mathbf{s}}^{\langle k \rangle} m_{\mathbf{t}}^{\langle k \rangle}$ karakterisztikus polinomja mind $\mathbf{s}^{\langle k \rangle}$-nak, mind $\mathbf{t}^{\langle k \rangle}$-nak, de akkor ezen két sorozat bármely lineáris kombinációjának, így $a\mathbf{s}^{\langle k \rangle} + b\mathbf{t}^{\langle k \rangle}$-nak is, amiből az előzőek alapján következik a tételben megadott egyenlőtlenség.

□

10.44. Tétel

Ha $m^{\langle k \rangle}$ helytelenül generálja $\mathbf{s}$ $k+1$-edik elemét, akkor $L_{k+1} = \max\{L_k, k + 1 - L_k\}$.

Δ

Bizonyítás:

Legyen $\delta_k = s_k - s_k^{\langle k \rangle}$. A feltétel szerint az $\mathbf{u} = \mathbf{s} - \mathbf{s}^{\langle k \rangle}$ sorozat első k eleme 0, míg a $k+1$-edik éppen $u_k = \delta_k \neq 0$. Ekkor

$$\begin{aligned} k+1 = L_{k+1}(\mathbf{u}) &= L_{k+1}\left(\mathbf{s} - \mathbf{s}^{\langle k \rangle}\right) \leq L_{k+1}(\mathbf{s}) + L_{k+1}\left(\mathbf{s}^{\langle k \rangle}\right) \\ &= L_{k+1}(\mathbf{s}) + L_k\left(\mathbf{s}^{\langle k \rangle}\right) = L_{k+1}(\mathbf{s}) + L_k(\mathbf{s}) = L_{k+1} + L_k, \end{aligned}$$

vagyis $L_{k+1} \geq k + 1 - L_k$, és korábban már beláttuk, hogy $L_{k+1} \geq L_k$.

Most megmutatjuk az ellenkező irányú egyenlőtlenséget azáltal, hogy megadunk egy olyan $L = \max\{L_k, k+1-L_k\}$-fokú polinomot, amely helyesen generálja **s**-nek valamennyi elemét a k indexűig, beleértve még ezt a tagot is.

A bizonyítás indukcióval történik. A nullahosszúságú kezdőszeletre nyilván vehető $L_0 = 0$ és $m^{\langle 0 \rangle} = e$, ahol e a test egységeleme. Ez a polinom mindaddig helyesen generálja a sorozatot, amíg a sorozat tagjai 0-k. Legyen a sorozat első nem nulla eleme az u indexnél (ez tehát az $u+1$-edik elem!). Ekkor L_u még 0, $m^{\langle u \rangle} = e$, míg $L_{u+1} = u + 1 = \max\{0, u+1\} = \max\{L_u, u+1-L_u\}$, és $m^{\langle u+1 \rangle} = x^{u+1}$ egy alkalmas minimálpolinom (de tetszőleges $u+1$-edfokú főpolinom megfelel, így látható, hogy míg a lineáris komplexitás egyértelmű, tehát a polinom foka is, addig maga a polinom nem). Tegyük fel, hogy az $u+1 \leq k$ esetekben $m^{\langle k \rangle}$ helyesen állítja elő az **s** sorozat első k elemét, de a $k+1$-ediket, azaz s_k-t egy $\delta_k \neq 0$ hibával. Mivel $L_0 = 0$, de a feltétel szerint $L_k \geq L_{u+1} > 0 = L_0$, ezért kell lennie olyan $u \leq t < k$ indexnek, hogy $L_{t+1} = \max\{L_t, t+1-L_t\} \neq L_t$, vagyis amelyre $L_{t+1} = t + 1 - L_t$, és ha az ilyen indexek maximuma r, akkor tehát $L_k = L_{r+1} = r + 1 - L_r$. Ebből az is következik, hogy $m^{\langle r \rangle}$ az s_r-et a megelőző elemekből egy $\delta_r \neq 0$ eltéréssel generálta. Nézzük az

$$x^{L-L_k} m^{\langle k \rangle} - \delta_k \delta_r^{-1} x^{L-(k+1-L_k)} m^{\langle r \rangle} = \sum_{i=0}^{L_k} c_i^{\langle k \rangle} x^{i+(L-L_k)} - \delta_k \delta_r^{-1} \sum_{i=0}^{L_r} c_i^{\langle r \rangle} x^{i+\left(L-(k+1-L_k)\right)}$$

polinomot. A jobb oldali első polinom egy L-edfokú, míg a második $L-(k-r) < L$-edfokú főpolinom, hiszen $\delta_k \delta_r^{-1} \neq 0$, és $L_k = L_{r+1} = r + 1 - L_r$-ből $L_r + \left(L-(k+1-L_k)\right) = L-(k-r)$, ahol $r < k$. Ez azt jelenti, hogy m egy L-edrendű homogén lineáris rekurzív sorozat karakterisztikus polinomja, és pontosan akkor generálja **s** első $k+1$ elemét, ha bármely $k - L \geq i \in \mathbb{N}$-re

$$\begin{aligned} &\sum_{j=0}^{L_k} c_j^{\langle k \rangle} s_{i+j+(L-L_k)} - \delta_k \delta_r^{-1} \sum_{j=0}^{L_r} c_j^{\langle r \rangle} s_{i+j+\left(L-(k+1-L_k)\right)} \\ &\qquad = \sum_{j=0}^{L_k} c_j^{\langle k \rangle} s_{i+j+(L-L_k)} - \delta_k \delta_r^{-1} \sum_{j=0}^{L_r} c_j^{\langle r \rangle} s_{i+j+\left((L-L_r)-(k-r)\right)} = 0. \end{aligned}$$

Adott i-re **s** legnagyobb indexe az első összegben $u = i + L_k + L - L_k = i + L$, míg a másodikban hasonló számítással $v = i + L - k + r$. Ha $i < k - L$, akkor tehát $u < k, v < r$, így mindkét összeg nullát ad. Maradt az $i = k - L$ eset, vagyis amikor $u = k$ és $v = r$. Ekkor az első összeg az s_k-nak és az $m^{\langle k \rangle}$ által generált $\mathbf{s}^{\langle k \rangle}$ sorozat k indexű tagjának, $s_k^{\langle k \rangle}$-nak a különbsége, vagyis δ_k, míg a szumma előtt álló tényező nélkül a második összeg hasonló módon δ_r-et ad, így a teljes összeg értéke ismét 0. Ez azt bizonyítja, hogy m egy olyan karakterisztikus polinom, amely helyesen generálja az **s** sorozatot a $k \geq i \in \mathbb{N}$ indexekre. Ebből következik, hogy $L_{k+1} \leq L$, és mivel korábban beláttuk az ellenkező irányú egyenlőtlenséget, ezért $L_{k+1} = L$.

□

Ismét hangsúlyozzuk, hogy míg a lineáris komplexitás értéke, tehát L_k egyértelműen meghatározott, addig egy alkalmas $m^{\langle k \rangle}$ polinomra ez általában nem igaz, hiszen nyilvánvalóan több olyan L_k-rendű homogén lineáris rekurzív sorozat létezik, amelynek az első k tagja azonos. Ha egy adott k-nál

$\delta_k \neq 0$, akkor $m^{\langle k+1 \rangle}$ biztosan nem egyenlő $m^{\langle k \rangle}$-val. Ugyanakkor $L_{k+1} = \max\{L_k, k+1-L_k\}$ alapján előfordul, hogy $L_{k+1} = L_k$. Ekkor $m^{\langle k+1 \rangle} \neq m^{\langle k \rangle}$, de $\deg\left(m^{\langle k+1 \rangle}\right) = L_{k+1} = L_k = \deg\left(m^{\langle k \rangle}\right)$, ami azt jelenti, hogy $m^{\langle k \rangle}$ mellett $m^{\langle k+1 \rangle}$ is olyan homogén lineáris rekurzív sorozatot generál, amelynek k hosszúságú kezdőszelete megegyezik a vizsgált sorozat hasonló szakaszával, vagyis $\mathbf{s}^{\langle k \rangle}$-hoz $m^{\langle k+1 \rangle} = m^{\langle k \rangle'}$ is alkalmas generáló polinom, ami mutatja azt, hogy ez a polinom nem mindig egyértelműen meghatározott. Érdemes még a következőt észrevenni. $L_{k+1} = \max\{L_k, k+1-L_k\} > L_k$ pontosan akkor, amikor $k+1-L_k > L_k$, azaz akkor, amikor $L_k < \frac{k+1}{2}$, vagyis $L_k \leq \frac{k}{2}$. De a legutóbbi reláció éppen azt jelenti, hogy $\mathbf{s}$ első k eleme egyértelműen meghatározza azt az egyetlen legfeljebb $\frac{k}{2}$-edrendű homogén lineáris rekurziót, amelynek ugyanez az első k eleme, hiszen egy n-edrendű homogén lineáris rekurzív sorozatot egy adott ponttól kezdve egyértelműen meghatározza az adott ponttól kezdődő $2n$ egymás utáni eleme, vagyis ha $L_k \leq \frac{k}{2}$ és $\delta_k \neq 0$, akkor L_{k+1} nem lehet egyenlő L_k-val. Ha viszont még $k < 2L_k$, akkor az aktuális $\mathbf{s}^{\langle k \rangle}$ első k eleme nem határozza meg egyértelműen a sorozat további részét, több különböző L_k-rendű homogén lineáris rekurzió is ugyanezt a kezdő sorozatot generálja, amelyek azonban más és más soron következő elemet generálnak, vagyis ekkor még egy ugyanolyan rendű, de másik rekurzióval elő tudjuk állítani $\mathbf{s}^{\langle k+1 \rangle}$-et.

Függelék: Ábel-csoportok karakterei

Véges Abel-csoportok alaptétele

F.1. Definíció

Legyen $\mathcal{G}$ Abel-csoport, $\emptyset \neq B \subseteq G$. B **a** $\mathcal{G}$ **Abel-csoport bázisa**, ha B generálja $\mathcal{G}$-t, és a B bármely nem üres B' részhalmazára $\prod_{b \in B' \subseteq B} b^{t_b} = e \Rightarrow (\forall (b \in B'): b^{t_b} = e)$, ahol e a csoport egységeleme, és t_b minden b-re racionális egész szám.

Δ

F.2. Tétel

Ha B a $\mathcal{G}$ Abel-csoport bázisa, e az egységelem, és G legalább kételemű, akkor $B \setminus \{e\}$ is bázis.

Δ

Bizonyítás:

Ha $e \notin B$, akkor nincs mit bizonyítani, legyen ezért $e \in B$. $|G| > 1$ következtében létezik $g \in G \setminus \{e\}$, ezért $[e] = \{e\} \neq G$ ($[A]$ az A generátuma), $\emptyset \neq B \neq \{e\}$, $B \setminus \{e\} \neq \emptyset$. e előáll bármely $B \setminus \{e\}$-beli elem nulladik hatványaként. B generátorrendszer, így az előző g előállítható B-beli elemek hatványának szorzataként. Mivel $g \neq e$, ezért ez a szorzat biztosan tartalmaz legalább egy e-től különböző elemet, és ha e egy hatványa is tényező, akkor ezt az e-vel egyenlő tényezőt elhagyva ismét g-t kapjuk, $B \setminus \{e\}$ is generátorrendszer. Ha egy szorzat csak úgy lehetett e, hogy a szorzatban szereplő valamennyi különböző B-beli b-hez tartozó hatvány külön-külön e, akkor ez a tulajdonság megmarad akkor is, ha csupán azokat a szorzatokat nézzük, amelyek nem tartalmazzák e valamely hatványát, tehát $B \setminus \{e\}$ is bázis.

□

A továbbiakban $|G| > 1$ esetén bázis olyan halmaz, amely nem tartalmazza a csoport egységelemét.

F.3. Tétel

Ha B a legalább kételemű $\mathcal{G}$ Abel-csoport bázisa, akkor B a $\mathcal{G}$ minimális generátorrendszere.

Δ

Bizonyítás:

Tegyük fel, hogy $b \in B$-re $B' = B \setminus \{b\}$ is generálja $\mathcal{G}$-t. Mivel $|G| > 1$, ezért $e \notin B$, $b \neq e$, és $e \notin B'$. Ha B' generátorrendszer, akkor az elemeiből vett hatványok szorzataként felírható b is. Legyen b egy ilyen felírása $b = \prod_{c \in C \subseteq B'} c^{t_c}$, ahol C nem üres (mert $b \neq e$). Ezek szerint a csupa báziselem-hatványokból álló $b^{-1} \prod_{c \in C \subseteq B'} c^{t_c}$ szorzat a csoport egységelemét, vagyis e-t adja úgy, hogy van a szorzatban olyan báziselem-hatvány, amely maga nem az egységelem (mert $b \neq e \Rightarrow b^{-1} \neq e$), ami ellentmond a bázis definíciójának. Az ellentmondás úgy oldható fel, hogy B' nem generátorrendszer, tehát B egyetlen valódi részhalmaza sem generálja $\mathcal{G}$-t, B minimális generátorrendszer.

□

Három fontos megjegyzést fűzünk az előző tételhez.

a) Ugyanazon csoportnak több különböző elemszámú bázisa lehet. Ha például $\mathcal{G}$ egy n-edrendű ciklikus csoport, és g egy generátoreleme, akkor g a $\mathcal{G}$ csoport egyelemű bázisa. Legyen n összetett,

$n = uv$, ahol $1 < u \in \mathbb{N}$, $1 < v \in \mathbb{N}$ és $(u, v) = 1$. Mind g^u, mind g^v $\mathcal{G}$-nek valódi részcsoportját generálják, ugyanakkor alkalmas r és s egészekkel $1 = ru + sv$, így g előállítható g^u r-edik és g^v s-edik hatványának szorzataként, de akkor $\mathcal{G}$ minden elemét is felírhatjuk g^u és g^v alkalmas hatványának szorzataként, így g^u és g^v a $\mathcal{G}$ minimális generátorrendszerét adja. Végül, ha $e = (g^u)^k (g^v)^j$, akkor $e = e^w = g^{v^2 j}$, ami csak akkor lehet u és v relatív prímsége miatt, ha $u|j$, de akkor $(g^v)^j = e$, és hasonlóan adódik a $(g^u)^k = e$ egyenlőség is, $\{g^u, g^v\}$ a $\mathcal{G}$-nek kételemű bázisa.

b) Minimális generátorrendszer nem feltétlenül bázis. Legyen $\mathcal{G}$ ismét ciklikus csoport a g generátorelemmel, a rendje n, u és v 1-nél nagyobb relatív prím természetes számok úgy, hogy szorzatuk az n egy valódi osztója. Ekkor az előző ponthoz hasonlóan g^u és g^v (együtt) minimális generátorrendszer. Ugyanakkor ha $n = quv$ (a feltétel alapján $q > 1$), és $q = r + s$ pozitív egész r-rel és s-sel, akkor sem g^{ruv}, sem g^{suv} nem az egységelem, a szorzatuk viszont az.

c) A tétel megfordításaként kapjuk, hogy ha egy kommutatív csoportnak nincs minimális generátorrendszere, akkor bázisa sem lehet. Kérdés, hogy van-e minimális generátorrendszerrel nem rendelkező Abel-csoport. Ha igen, akkor ez végtelen elemszámú, hiszen véges csoportnak van véges generátorrendszere (például önmaga), és véges generátorrendszerből biztosan kiválasztható minimális generátorrendszer. Az előző kérdésre a válasz pozitív, amint az alábbi példa mutatja.

A racionális számok halmazának az összeadással mint Abel-csoportnak nincs minimális generátorrendszere, bármely generátorrendszer tartalmaz nála szűkebb generátorrendszert. Ezt a következőképpen láthatjuk be. Legyen az A nem üres halmaz egy generátorrendszer. Ha A tartalmazza a 0-t, az nyilván elhagyható, feltehetjük ezért, hogy egyetlen A-ba tartozó α sem egyenlő nullával. Ekkor egy tetszőleges A-beli α és $1 < s \in \mathbb{N}$ kiválasztásával $\frac{1}{s}\alpha$ is (nullától különböző) racionális szám, így A-val generálható, $\frac{1}{s}\alpha \in [A]$. Az $[A]$-t A-beli elemek egész-számszorosainak összege alkotja (hiszen a művelet az összeadás), ezért minden elem és így $\frac{1}{s}\alpha$ is ilyen formájú, azaz $\frac{1}{s}\alpha = u\alpha + \beta$, ahol u egész szám, és β az A α-tól különböző elemei által az összeadással generált halmaz egy eleme, vagyis $\beta \in [A \setminus \{\alpha\}]$. $\beta \neq 0$ biztosan teljesül, mivel ellenkező esetben $us = 1$ lenne, ami $s > 1$-gyel lehetetlen (hiszen u egész szám), ezért semmilyen u egésszel nem lehet $\frac{1}{s}\alpha$-t α többszöröseként, tehát csupán α generátumaként kifejezni. Amennyiben $u = 0$, akkor máris $\alpha = s\beta \in [A \setminus \{\alpha\}]$. Ellenkező esetben a korábbi egyenlőségből azt kapjuk, hogy $(1 - us)\alpha = s\beta$. $\frac{1}{1-us}\alpha$ is racionális szám ($1 - us$ nem lehet nulla, hiszen akkor β is nulla lenne, amiről előbb láttuk, hogy lehetetlen), ennélfogva $\frac{1}{1-us}\alpha = v\alpha + \gamma$ megfelelő v egész és $\gamma \in [A \setminus \{\alpha\}]$ számmal. Most írhatjuk, hogy

$$\begin{aligned}\alpha &= (1 - us)(v\alpha + \gamma) = (1 - us)v\alpha + (1 - us)\gamma \\ &= v\big((1 - us)\alpha\big) + (1 - us)\gamma = vs\beta + (1 - us)\gamma.\end{aligned}$$

$vs\beta + (1 - us)\gamma \in [A \setminus \{\alpha\}]$, ennélfogva α előállítható a generátorrendszer többi elemével, ezért elhagyható A-ból, így A-ból bármelyik elemet elhagyva ismét generátorrendszert kapunk, továbbá ez bármely generátorrendszerre igaz, így nem létezhet minimális generátorrendszer.

Az előző három pont alapján látjuk, hogy ez a bázis nem mindenben rendelkezik a lineáris algebrában látott bázis ismérveivel (például, hogy egy lineáris tér minden bázisának számossága azonos, bár láttunk már más ilyen struktúrát is, nevezetesen a modulusokat). Ennek ellenére van közös tulajdonságuk.

F.4. Tétel

Ha B a $\mathcal{G}$ Abel-csoport bázisa, akkor G minden eleme lényegében véve egyértelműen írható B-beli elemek hatványának szorzataként, vagyis $\prod_{b \in B' \subseteq B} b^{t_b^{(1)}} = \prod_{b \in B' \subseteq B} b^{t_b^{(2)}}$ esetén minden $b \in B'$-re $b^{t_b^{(1)}} = b^{t_b^{(2)}}$. Fordítva, ha B a G nem üres részhalmaza, és a csoport minden eleme lényegében véve egyértelműen írható fel B-beli véges sok elem hatványának szorzataként, akkor B a csoport bázisa.

Δ

Bizonyítás:

Ha a $\mathcal{G}$ csoport g elemére $\prod_{b\in B'\subseteq B} b^{t_b^{(1)}} = g = \prod_{b\in B'\subseteq B} b^{t_b^{(2)}}$, akkor $e = \prod_{b\in B'\subseteq B} b^{t_b^{(1)}-t_b^{(2)}}$, ami báziselemekkel csak úgy teljesülhet, ha a B' valamennyi elemére $e = b^{t_b^{(1)}-t_b^{(2)}}$, azaz $b^{t_b^{(1)}} = b^{t_b^{(2)}}$. Viszszafelé láthatóan B generátorrendszer, és ha minden elem alapvetően egyértelműen írható B-beli elemek hatványának szorzataként, akkor ez igaz a csoport egységelemére is, márpedig ez mindig írható úgy, hogy a báziselem-hatványok maguk az egységelemmel azonosak.

□

A következő tétel a **véges Abel-csoportok alaptétele**.

F.5. Tétel

Minden véges Abel-csoportnak van bázisa.

Δ

Bizonyítás:

Elsőként leszögezzük, hogy véges csoport minden olyan generátorrendszere, amelyben egy elem csak egyszer fordul elő véges (hiszen legfeljebb csak annyi elemből állhat, amennyi magában a csoportban van), ezért ha van bázis, az is csak véges lehet mint minimális generátorrendszer (minimális generátorrendszer nyilván nem tartalmaz többszörös elemet). Ha a $\mathcal{G}$ véges Abel-csoport ciklikus, akkor egyetlen elemmel generálható, és ha egy ilyen generátorelem g, akkor $g^k = e$ nyilván pontosan akkor teljesül, amikor $g^k = e$, $\{g\}$ tehát bázis (ha G legalább kételemű, akkor a generátorelem nem lehet az egységelem).

Nézzük ezek után azt az esetet, amikor $\mathcal{G}$ nem ciklikus. Ekkor van G-ben e-től különböző elem, így $n = \max_{g\in G}\{o(g)\} \in \mathbb{N}^+ \setminus \{1\}$, hisz véges csoport minden eleme véges rendű, és $g^{o(g)} = e$-ből $o(g) = 1$-re $g = e$. Legyen $g \in G$ olyan, hogy $o(g) = n$ (ilyen elem biztosan létezik), és legyen $\mathcal{G}_1$ a $\mathcal{G}$ g által generált ciklikus részcsoportja. A feltétel szerint $\mathcal{G} \neq \mathcal{G}_1$, ezért a $\mathcal{H} = \mathcal{G}/\mathcal{G}_1$ csoport is legalább kételemű, és $|G_1| = o(g) = n > 1$ következtében $|H| = |\mathcal{G}/\mathcal{G}_1| = \frac{|G|}{|G_1|} = \frac{|G|}{n} < |G|$. Mivel ciklikus csoportra beláttuk a tétel állításának helyességét, és az egy- és kételemű csoport ciklikus, ezért tegyük fel, hogy már minden $s > k \in \mathbb{N}^+ \setminus \{1\}$-re bizonyítottuk a tételt, és legyen $|G| = s$. $1 < |H| < s$ azt jelenti, hogy $\mathcal{H}$-nak van bázisa, mondjuk $B = \{\bar{h}_i | r \geq i \in \mathbb{N}\}$, és $o(\bar{h}_i) = d_i$. $\bar{h}_i$ a $\mathcal{G}$-nek egy $\mathcal{G}_1$ szerinti mellékosztálya, és ha g_1 és g_2 azonos mellékosztály elemei, akkor $\bar{g}_1 = \bar{g}_2$, $o(\bar{g}_1) = o(\bar{g}_2)$. $o(\bar{h}) = d$ azt jelenti, hogy $h^d\mathcal{G}_1 = (h\mathcal{G}_1)^d = \mathcal{G}_1$, ami másként írva azzal egyenértékű, hogy $h^d \in G_1$, és d a legkisebb ilyen tulajdonságú pozitív egész. Legyen $\bar{h}$ a B egyik eleme, h a $\bar{h} = h\mathcal{G}_1$ mellékosztálynak egy olyan eleme, amelynek $h^d = g^u$, $n \geq u \in \mathbb{N}^+$ alakú felírásában u a lehető legnagyobb, és legyen $o(h) = m$. Belátjuk, hogy $d = m$. Tegyük fel az ellenkezőjét. $h^m = e \in G_1$, így $d \leq m$. Ha $d < m$, akkor $h^d \neq e$ (mert $d > 0$), g^u sem az egységelem, $n > u \in \mathbb{N}^+$. $h^d\mathcal{G}_1 = (h\mathcal{G}_1)^d = \mathcal{G}_1$, ezért $d|m$, másrészt véges kommutatív csoportban minden elem rendje osztója a maximális rendnek (lásd a 3.52. Tétel bizonyításának b) és c) pontját a 64. oldalon) így $m|n$ (és ebből következik, hogy $m \leq n$ is teljesül). $e = h^m = \left(h^d\right)^{\frac{m}{d}} = (g^u)^{\frac{m}{d}} = g^{u\frac{m}{d}}$, ennélfogva $u\frac{m}{d} \equiv 0\ (n)$, tehát $u \equiv 0\ \left(\frac{n}{\left(n,\frac{m}{d}\right)}\right)$. $d|m|n$-ből $\frac{m}{d}\Big| n$, innen $\frac{n}{\left(n,\frac{m}{d}\right)} = \frac{n}{m}d$ és $u \equiv 0\ \left(\frac{n}{m}d\right)$, azaz $u = q\frac{n}{m}d$, és az u korlátai alapján $\frac{m}{d} > q \in \mathbb{N}^+$. h-val együtt gh is eleme $h\mathcal{G}_1$-nek, ezért hg d-edik hatványa is benne van G_1-ben, hg is g-nek egy hatványa, méghozzá a legkisebb pozitív egész kitevővel írva hg a g-nek legfeljebb u-kitevős hatványa. $(hg)^d = h^d g^d = g^u g^d = g^{u+d}$, és így $u + d > u$, tehát $u + d > n$, mivel d pozitív egész. Ekkor $n < u + d = q\frac{n}{m}d + d$-ből $\frac{m}{d} > q > \frac{m}{d} - \frac{m}{n} \geq \frac{m}{d} - 1$ (a legelső egyenlőtlenség a korábbi feltétel q-ra), ami egész q-val lehetetlen, mert $\frac{m}{d}$ egész. Az ellentmondás a $q < \frac{m}{d}$, azaz az $u < n$ feltételből ered, amit azért kellett feltennünk, mert $d < m$ csak így teljesülhet, tehát az ellentmondás oka a $d < m$ megkötés, és így $d = m$.

A $B_1 = \{g\} \cup \{h_i | r \geq i \in \mathbb{N}^+\}$ halmaz generálja $\mathcal{G}$-t. Legyen ugyanis a a G egy eleme. G minden eleme, így a is benne van egy $\mathcal{G}_1$ szerinti mellékosztályban, mondjuk $a \in hG_1$. hG_1 megadható a h_iG_1 hatványainak szorzataként, azaz a h_i hatványainak és G_1-nek a szorzataként, $a \in \left(\prod_{i=1}^{r} h_i^{t_i}\right)G_1$, így $a = \left(\prod_{i=1}^{r} h_i^{t_i}\right)g^t$, azaz $a \in [B_1]$.

Végül belátjuk, hogy B_1 bázis. A h_i-k egyike sem e, ugyanis $h_i = e$-ből $\bar{h}_i = \bar{e}$, ami nem lehet, hiszen B a legalább kételemű $\mathcal{H}$ bázisa, g sem az egységelem, így B_1-nek nem eleme e. Tegyük fel, hogy $g^t \prod_{i=1}^{r} h_i^{t_i} = e$. Innen $\bar{e} = \overline{g^t \prod_{i=1}^{r} h_i^{t_i}} = \overline{g^t} \prod_{i=1}^{r} \bar{h}_i^{t_i} = \prod_{i=1}^{r} \bar{h}_i^{t_i}$, ami akkor és csak akkor lehetséges, ha minden i-re $\bar{h}_i^{t_i} = \bar{e}$, tehát $m_i = d_i | t_i$. Ekkor viszont $h_i^{t_i} = e$, emiatt $g^t = e$, és B_1 bázis.

□

Csoportkarakterek

Az alábbiakban $\varepsilon_k^{(n)} = \left(\varepsilon_1^{(n)}\right)^k = \left(1, k\frac{2\pi}{n}\right)$ a $k\frac{2\pi}{n}$ szöghöz tartozó n-edik komplex egységgyök.

F.6. Definíció

Legyen $\mathcal{G}$ kommutatív csoport, χ a $\mathcal{G}$-nek a komplex számok multiplikatív félcsoportjába való nem azonosan nulla félcsoport-homomorfizmusa. Ekkor χ **a** $\mathcal{G}$ **karaktere**.

Δ

F.7. Megjegyzés

Karaktertől általában megkívánják, hogy abszolút értéke 1 legyen a csoport minden elemén. Mi ezt nem kötjük ki, de látni fogjuk, hogy véges esetben a szűkebb és tágabb értelmezés megegyezik.

Δ

F.8. Tétel

Legyen χ a $\mathcal{G}$ kommutatív csoport karaktere, ekkor

1. $\forall(g \in G): \chi(g) \neq 0$;
2. $\chi(e) = 1$, ahol e a $\mathcal{G}$ egységeleme;
3. $\forall(g \in G): \chi(g^{-1}) = \left(\chi(g)\right)^{-1}$;
4. ha $g \in G$ -re $o(g) = n \in \mathbb{N}^+$, akkor $\chi(g) = \varepsilon_k^{(n)} = \left(\varepsilon_1^{(n)}\right)^k$ ($\Rightarrow |\chi(g)| = 1$) egy $n > k \in \mathbb{N}$ egésszel; véges G esetén $|\chi|$ az azonosan 1 függvény, így χ korlátos;
5. ha χ korlátos, akkor $\forall(g \in G): |\chi(g)| = 1$;
6. ha $|\chi(g)| = 1$, akkor $\chi(g^{-1}) = \overline{\chi(g)}$.

Δ

Bizonyítás:

1. Tetszőleges G-beli g-hez adott h esetén van olyan g', hogy $hg' = g$. Ha $\chi(h) = 0$, akkor

$$\chi(g) = \chi(hg') = \chi(h)\chi(g') = 0 \cdot \chi(g') = 0,$$

tehát χ azonosan nulla, ami ellene mond a definíciónak.

2. Az előző pont alapján $\chi(e) \neq 0$, ezért $1 \cdot \chi(e) = \chi(e) = \chi(e^2) = \chi(e \cdot e) = \chi(e) \cdot \chi(e)$. $\chi(e)$-vel egyszerűsíthetünk, és ekkor $\chi(e) = 1$.

3. $\chi(g^{-1})\chi(g) = \chi(g^{-1}g) = \chi(e) = 1$, ahonnan adódik az állítás.

4. A feltétel szerint $g^n = e$, ezért $\big(\chi(g)\big)^n = \chi(g^n) = \chi(e) = 1$, $\chi(g)$ egy n-edik komplex egységgyök, ennek abszolút értéke viszont 1. Véges csoport minden eleme végesrendű, tehát minden csoportbeli elemen a karakter értékének abszolút értéke 1, ami egyben korlátosságot is jelent.

5. Legyen g a G-nek olyan eleme, amelyre $|\chi(g)| \neq 1$. Láttuk, hogy ekkor g rendje végtelen. Ha $|\chi(g)| < 1$, akkor a 3. pont alapján $|\chi(g^{-1})| > 1$, ezért feltehetjük, hogy $|\chi(g)| > 1$. Innen bármely $n \in \mathbb{N}$-re $|\chi(g^n)| = \left|\big(\chi(g)\big)^n\right| = |\chi(g)|^n$, és ez tart a végtelenhez, a karakter nem korlátos.

6. $\chi(g^{-1}) = \big(\chi(g)\big)^{-1}$, és egységnyi hosszúságú komplex szám inverze a szám konjugálja.

□

F.9. Tétel

Legyen $\mathcal{G}$ egy kommutatív csoport. Ha χ_1, χ_2, χ a $\mathcal{G}$ karaktere, akkor a $g \mapsto \chi_1(g)\chi_2(g)$, $g \mapsto \chi(g^{-1})$, $g \mapsto \overline{\chi(g)}$ szabályok karaktert definiálnak. Amennyiben χ korlátos, akkor a két utóbbi karakter egybeesik.

Δ

Bizonyítás:

a) Mind $\chi_1(g)$, mind $\chi_2(g)$ minden g-re értelmezett és nem nulla komplex szám, ezért nullától különböző komplex szám a szorzatuk is, továbbá egy g-hez χ_1 és χ_2 egyértelműen rendel egyetlen komplex számot, ezek szorzata is egyértelműen meghatározott, így az első szabály egy leképezést definiál G-ről $\mathbb{C}^\times$-be. Komplex számok szorzása kommutatív és asszociatív,

$$\begin{aligned}\chi_1(g_1g_2)\chi_2(g_1g_2) &= \big(\chi_1(g_1)\chi_1(g_2)\big)\big(\chi_2(g_1)\chi_2(g_2)\big)\\ &= \big(\chi_1(g_1)\chi_2(g_1)\big)\big(\chi_1(g_2)\chi_2(g_2)\big),\end{aligned}$$

így g_1g_2 képe a g_1 és g_2 képének szorzata, a leképezés művelettartó.

b) g egyértelműen meghatározza az inverzét, ehhez egyértelműen rendel χ egy nem nulla komplex számot; ez minden g-re érvényes, így $g \mapsto \chi(g^{-1})$ a G-nek $\mathbb{C}^\times$-be való leképezése.

$$\chi((g_1g_2)^{-1}) = \chi(g_2^{-1}g_1^{-1}) = \chi(g_2^{-1})\chi(g_1^{-1}) = \chi(g_1^{-1})\chi(g_2^{-1}),$$

így a leképezés homomorfizmus.

c) Minden $g \in G$-re $\chi(g)$ létezik és egyértelmű nem nulla komplex szám, de akkor ez igaz a konjugáltjára is, hiszen a konjugálás automorfizmus $\mathbb{C}$-n. Mivel szorzat konjugáltja a konjugáltak szorzata, ezért ez ismét homomorfizmus.

d) Ha a feltétel teljesülés, akkor az előző tétel 5. és 6. pontja alapján a G minden g elemére teljesül, hogy $\chi(g^{-1}) = \overline{\chi(g)}$, de ekkor a két függvény megegyezik.

□

F.10. Definíció

Legyen χ_1, χ_2, χ a $\mathcal{G}$ kommutatív csoport karaktere. Ekkor **a $g \mapsto \chi_1(g)\chi_2(g)$ karakter a χ_1 és χ_2 karakter szorzata, a $g \mapsto \chi(g^{-1})$ karakter a χ karakter inverze, a $g \mapsto \overline{\chi(g)}$ karakter a χ karakter konjugáltja**, az első jele $\chi = \chi_1\chi_2$, a másodiké χ^{-1}, az utolsóé $\bar{\chi}$. $\mathcal{G}$ karaktereinek halmazát $\hat{G}$-vel jelöljük.

Δ

F.11. Tétel

Tetszőleges $\mathcal{G}$ kommutatív csoport esetén $\hat{G}$ kommutatív csoport a karakterszorzással.

Δ

Bizonyítás:

1. $\hat{G}$ nem üres: ha minden g-hez 1-et rendelünk, akkor ez egy leképezés G-ről $\mathbb{C}$-be, nem azonosan nulla, és nyilván szorzattartó, tehát karakter, jelöljük χ_0-val.

2. A karakterszorzás asszociatív: ha χ_1, χ_2 és χ három karakter, akkor tetszőleges g-re

$$\begin{aligned}\big((\chi_1\chi_2)\chi_3\big)(g) &= \big((\chi_1\chi_2)(g)\big)\chi_3(g) = \big(\chi_1(g)\chi_2(g)\big)\chi_3(g) = \chi_1(g)\big(\chi_2(g)\chi_3(g)\big)\\ &= \chi_1(g)\big((\chi_2\chi_3)(g)\big) = \big(\chi_1(\chi_2\chi_3)\big)(g)\end{aligned}$$

tehát $(\chi_1\chi_2)\chi_3 = \big(\chi_1(\chi_2\chi_3)\big)(g)$.

3. Bármely χ karakterrel a G minden g elemére $(\chi_0\chi)(g) = \chi_0(g)\chi(g) = 1\cdot\chi(g) = \chi(g)$, így $\chi_0\chi = \chi$, tehát χ_0 baloldali egységelem $\hat{G}$-ben.

4. Ismét tetszőleges $\hat{G}$-beli χ-vel és G-beli g-vel

$$(\chi^{-1}\chi)(g) = \chi^{-1}(g)\chi(g) = \chi(g^{-1})\chi(g) = \chi(g^{-1}g) = \chi(e) = 1 = \chi_0(g),$$

azaz a karakterekre átírva $\chi^{-1}\chi = \chi_0$.

1.-4. együtt biztosítja, hogy $\hat{G}$ csoport a χ_0 egységelemmel és χ^{-1}-gyel mint inverzzel. Ezt a csoportot $\hat{\mathcal{G}}$-vel fogjuk jelölni.

5. $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = \chi_2(g)\chi_1(g) = (\chi_2\chi_1)(g)$, mivel $\mathbb{C}$-ben a szorzása kommutatív, így $\chi_1\chi_2 = \chi_2\chi_1$, a karakterszorzás kommutatív.

□

F.12. Definíció

Ha $\mathcal{G}$ Abel-csoport, és $\chi_0\colon G \to \mathbb{C}^\times$-gal minden G-beli g-re $\chi_0(g) = 1$, akkor χ_0 a **főkarakter**.

Δ

F.13. Tétel

Ha $\mathcal{G}$ véges Abel-csoport, akkor $\hat{\mathcal{G}} \cong \mathcal{G}$.

Δ

Bizonyítás:

A véges $\mathcal{G}$ Abel-csoportnak van bázisa, legyen ez $B = \{b_i | r \geq i \in \mathbb{N}^+\}$, és $o(b_i) = n_i \in \mathbb{N}^+$. Az, hogy $\hat{G}$ véges, nyilvánvaló: G minden eleméhez csak véges sok érték rendelhető, hiszen $g \in G$-re tetszőleges χ karakterrel $\chi(g)$ egy véges fokú komplex egységgyök valamilyen hatványa, és ilyen csak véges számú van, a kommutativitást pedig már beláttuk. $\hat{\mathcal{G}}$ így véges kommutatív csoport, ezért van bázisa. Legyen $r \geq i \in \mathbb{N}^+$-ra $\chi_i\colon G \to \mathbb{C}$ olyan, hogy $b_j \in B$-re $\chi_i(b_j) = \varepsilon_1^{(n_i)}$, ha $i = j$, egyébként $\chi_i(b_j) = 1$, továbbá $\chi_i(g) = \chi_i\big(\prod_{t=1}^r b_t^{k_t}\big) = \prod_{t=1}^r\big(\chi_i(b_t)\big)^{k_t} = \left(\varepsilon_1^{(n_i)}\right)^{k_i}$, ha $g = \prod_{t=1}^r b_t^{k_t}$. Belátjuk, hogy ekkor $\hat{B} = \{\chi_i | r \geq i \in \mathbb{N}^+\}$ egy bázis $\hat{\mathcal{G}}$-ben.

a) $\left(1, k\frac{2\pi}{n}\right) = \left(1, \frac{2\pi}{n}\right)^k = 1 = (1,0)$ akkor és csak akkor teljesül, ha $k\frac{2\pi}{n} = t\cdot 2\pi$, ami azzal ekvivalens, hogy $n|k$, és így $\varepsilon_1^{(n_i)}$ rendje n_i.

b) χ_i karakter. A definícióból látszik, hogy értéke minden csoportelemre egy nullától különböző komplex szám. g felírása a bázis elemeivel egyértelmű, ezért a g-hez rendelt komplex szám egyértelmű. Legyen $g_1 = \prod_{t=1}^r b_t^{k_t^{(1)}}$ és $g_2 = \prod_{t=1}^r b_t^{k_t^{(2)}}$ két elem a csoportból. Ekkor $g_1 g_2 = \prod_{t=1}^r b_t^{k_t}$, ahol $r \geq t \in \mathbb{N}^+$ mellett $n_t > k_t \in \mathbb{N}$ és $k_t \equiv k_t^{(1)} + k_t^{(2)}\ (n_t)$. A definícióból

$$\chi_i(g_1 g_2) = \left(\varepsilon_1^{(n_i)}\right)^{k_i}$$
$$\chi_i(g_1)\chi_i(g_2) = \left(\varepsilon_1^{(n_i)}\right)^{k_i^{(1)}} \left(\varepsilon_1^{(n_i)}\right)^{k_i^{(2)}} = \left(\varepsilon_1^{(n_i)}\right)^{k_i^{(1)}+k_i^{(2)}}$$

és a két komplex szám azonos a k-kra vonatkozó kongruencia következtében.

c) Legyen χ a $\mathcal{G}$ egy karaktere. b_i rendje n_i, ezért $\chi(b_i) = \left(\varepsilon_1^{(n_i)}\right)^{m_i}$ egy $n_i > m_i \in \mathbb{N}$ egésszel. Terkintsük a $\chi' = \prod_{t=1}^{r} \chi_t^{m_t}$ karaktert, ekkor $\chi'(b_i) = \prod_{t=1}^{r} \chi_t^{m_t}(b_i) = \left(\varepsilon_1^{(n_i)}\right)^{m_i}$. Amennyiben $g = \prod_{t=1}^{r} b_t^{k_t}$, akkor

$$\chi(g) = \chi\left(\prod_{t=1}^{r} b_t^{k_t}\right) = \prod_{t=1}^{r}\left(\chi(b_t)\right)^{k_t} = \prod_{t=1}^{r}\left(\left(\varepsilon_1^{(n_t)}\right)^{m_t}\right)^{k_t}$$
$$= \prod_{t=1}^{r}\left(\chi'(b_t)\right)^{k_t} = \chi'\left(\prod_{t=1}^{r} b_t^{k_t}\right) = \chi'(g)$$

így a χ_i-k generálják $\hat{\mathcal{G}}$-ot. Ha $\prod_{t=1}^{r} \chi_t^{s_t} = \chi_0$, akkor $1 = \chi_0(b_i) = \prod_{t=1}^{r} \chi_t^{s_t}(b_i) = \left(\varepsilon_1^{(n_i)}\right)^{s_i}$, ami csak úgy lehet, ha $n_i | s_i$. Ekkor viszont χ_i a B minden elemén 1, de akkor G valamennyi elemén is 1, $\chi_i \equiv 1$, vagyis $\chi_i = \chi_0$. Mivel ez minden $r \geq i \in \mathbb{N}^+$-re igaz, ezért $\hat{B}$ valóban bázis.

Végül B és $\hat{B}$ elemeinek száma és minden i-re b_i és χ_i rendje azonos, ezért $\mathcal{G}$ és $\hat{\mathcal{G}}$ izomorf.

□

F.14. Tétel

Ha a $\mathcal{G}$ kommutatív csoportnak van bázisa, akkor tetszőleges $g \in G \setminus \{e\}$-hez van olyan χ karakter, hogy $\chi(g) \neq 1$ (e a $\mathcal{G}$ egységeleme).

Δ

Bizonyítás:

Jelöljük $\mathcal{G}$ bázisát B-vel. g báziselemek hatványainak szorzataként való felírásában van legalább egy olyan tényező, amely nem az egységelem, vagyis ha ez $b \in B$ a k kitevővel, akkor $b^k \neq e$. Ha b n-edrendű, akkor legyen $\alpha = \varepsilon_1^{(n)}$, különben $\alpha = e^{i2\pi c}$, ahol $k^{-1} \neq c \in \mathbb{R}$ (itt most e a természetes logaritmus alapja, és $k \neq 0$ a feltétel értelmében). Definiáljuk χ-t úgy, hogy $\chi(b) = \alpha$, $b' \in B \setminus \{b\}$-re $\chi(b') = 1$, és ha a G g' eleme $g' = b^{k_b} \prod_{b' \in B' \subseteq B\setminus\{b\}} (b')^{k_b'}$ alakú, akkor $\chi(g') = \alpha^{k_b}$. Ez G minden eleméhez hozzárendel egy és csak egy nem nulla komplex számot, hiszen a bázisban való felírás egyértelmű. Ha $g_1 = b^{k_1} h_1$, $g_2 = b^{k_2} h_2$, ahol h_1 és h_2 felírásában már nem szerepel b, akkor $\chi(g_1 g_2) = \alpha^{k_1+k_2} = \alpha^{k_1}\alpha^{k_2} = \chi(g_1)\chi(g_2)$, így χ karakter $\mathcal{G}$-n. α választása folytán $\alpha^k \neq 1$, ezért $\alpha^k = \chi(g) \neq 1$.

□

F.15. Következmény

Véges kommutatív csoport $g \neq e$ eleméhez van $\mathcal{G}$-nek olyan χ karaktere, amelyre $\chi(g) \neq 1$.

Δ

Bizonyítás:

Véges Abel-csoportnak van bázisa, így alkalmazható az előző tétel.

□

F.16. Tétel

Legyen χ a $\mathcal{G}$ véges Abel-csoport karaktere. Ekkor $\sum_{g\in G}\chi(g)=\begin{cases}|G|, \text{ha } \chi=\chi_0\\ 0, \text{ ha } \chi\neq\chi_0.\end{cases}$

Δ

Bizonyítás:

Ha $\chi=\chi_0$, akkor az összeg minden tagja 1, így az összeg megegyezik G elemeinek számával. Ellenkező esetben van G-nek olyan g_0 eleme, amelyre $\chi(g_0)\neq 1$, vagyis $1-\chi(g_0)\neq 0$. $\mathcal{G}$ csoport, ezért bármely G-beli g-hez van pontosan egy olyan g', hogy $g=g_0g'$, így, miközben g' végigfut G elemein, azalatt g is egyszer és csakis egyszer egybeesik G valamennyi elemével, következésképpen

$$1\cdot\sum_{g\in G}\chi(g)=\sum_{g'\in G}\chi(g_0g')=\chi(g_0)\sum_{g'\in G}\chi(g')=\chi(g_0)\sum_{g\in G}\chi(g).$$

Innen $\big(1-\chi(g_0)\big)\sum_{g\in G}\chi(g)=0$, és mivel az első tényező különbözik nullától, így $\sum_{g\in G}\chi(g)=0$.

□

F.17. Tétel

Legyen g a $\mathcal{G}$ véges Abel-csoport rögzített eleme. Ekkor $\sum_{\chi\in\hat{G}}\chi(g)=\begin{cases}|G|, \text{ha } g=e\\ 0, \text{ ha } g\neq e.\end{cases}$

Δ

Bizonyítás:

Ha g a csoport egységeleme, akkor minden karakter értéke g-n 1, az összeg megegyezik a karakterek számával, ami viszont azonos G elemszámával, hiszen $\mathcal{G}$ és $\hat{\mathcal{G}}$ izomorf csoportok. Ha viszont $g\neq e$, akkor az F.15. Következmény szerint van olyan χ_1 karakter $\mathcal{G}$-n, amelyre $\chi_1(g)\neq 1$. $\hat{\mathcal{G}}$ csoport, így valamennyi $\hat{G}$-beli χ-hez egyértelműen megadható egy olyan χ', amellyel $\chi=\chi_1\chi'$, ezért

$$1\cdot\sum_{\chi\in\hat{G}}\chi(g)=\sum_{\chi'\in\hat{G}}(\chi_1\chi')(g)=\chi_1(g)\sum_{\chi'\in\hat{G}}\chi'(g)=\chi_1(g)\sum_{g\in\hat{G}}\chi(g),$$

tehát $\big(1-\chi_1(g)\big)\sum_{\chi\in\hat{G}}\chi(g)=0$, ami csak úgy lehet, ha az összeg nulla.

□

F.18. Tétel (ortogonalitási tételek)

Legyen $\mathcal{G}$ véges Abel-csoport, χ_1 és χ_2 illetve g_1 és g_2 a $\mathcal{G}$ két karaktere és két eleme. Ekkor

a) $\sum_{g\in G}\chi_1(g)\bar{\chi}_2(g)=\begin{cases}|G|, \text{ha } \chi_1=\chi_2\\ 0, \text{ ha } \chi_1\neq\chi_2;\end{cases}$

b) $\sum_{\chi\in\hat{G}}\chi(g_1)\bar{\chi}(g_2)=\begin{cases}|G|, \text{ha } g_1=g_2\\ 0, \text{ ha } g_1\neq g_2;\end{cases}$

Δ

Bizonyítás:

a) $\chi_1(g)\bar{\chi}_2(g)=(\chi_1\chi_2^{-1})(g)=\chi(g)$, és χ akkor és csak akkor a főkarakter, ha $\chi_1=\chi_2$;

b) $\chi(g_1)\bar{\chi}(g_2)=\chi(g_1g_2^{-1})=\chi(g)$, és g pontosan akkor lesz $\mathcal{G}$ egységeleme, ha $g_1=g_2$.

Most mindkét esetben alkalmazhatjuk az előző tételek eredményeit.

□

Véges test karakterei

Amennyiben a csoport művelete additív, akkor a művelettartás követelménye azt jelenti, hogy $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$. Ezt figyelembe véve testnek mind az additív, mind a multiplikatív csoportján definiálhatjuk a karaktereket, és értelemszerűen beszélünk a test additív illetve multiplikatív karakteréről, ahol ez utóbbit kiegészítjük azzal, hogy a nullelemen legyen az értéke 0. Véges test multiplikatív csoportja ciklikus, így ciklikus a multiplikatív karakterek csoportja is ugyanazon renddel. Könnyen meg tudjuk adni a generátorelemét: ha a test q-elemű, és egy primitív eleme g, akkor legyen $\chi_g(g) = \varepsilon_1^{(q-1)}$, a test többi nem nulla elemére pedig a szorzattartás definiálja χ_g és vele együtt tetszőleges karakter értékét.

Most megvizsgáljuk a véges test additív karaktereit.

F.19. Tétel

Legyen $\mathbb{F}_q$ egy q-elemű véges test, $\mathbb{F}_p$ a prímteste, a bővítés foka n, $\alpha \in \mathbb{F}_q$-ra $\mathrm{S}(\alpha)$ az α $\mathbb{F}_p$ fölötti nyoma, továbbá $\varphi\colon \mathbb{F}_p \to \mathbb{Z}$ olyan, hogy $p > k \in \mathbb{N}$-re $\varphi(ke) = k$, ahol e az $\mathbb{F}_p$ egységeleme. Ekkor a $\kappa(\alpha) = \left(\varepsilon_1^{(p)}\right)^{\varphi(\mathrm{S}(\alpha))}$ definícióval κ az $\mathbb{F}_q$ additív csoportjának karaktere, $\mathbb{F}_q$ minden más karaktere κ_β, ahol β az $\mathbb{F}_q$ tetszőleges eleme és $\kappa_\beta(\alpha) = \kappa(\beta\alpha)$, és különböző β_1, β_2-höz különböző karakter tartozik.

Δ

Bizonyítás:

$\mathbb{F}_q$ minden nem nulla elemének additív rendje p. Legyen γ a test primitív eleme, ekkor minden elem egyértelműen írható fel a γ legfeljebb $n-1$-edfokú nemnegatív egész kitevős hatványainak $\mathbb{F}_p$ elemeivel vett lineáris kombinációjaként. $\kappa(\gamma^j)$ a definícióból láthatóan egy nem nulla komplex szám, és az S-függvény tulajdonsága alapján ez igaz lesz $\mathbb{F}_q$ minden elemére. A bázisfelírás egyértelműsége miatt $\kappa(\alpha)$ egyértelmű, és ismét S valamint φ additivitása miatt κ művelettartó, tehát karakter. Mindez igaz $\kappa(\beta\alpha)$-ra is, így κ_β szintén karakter. Azt kell még megmutatni, hogy a κ_β-k halmaza ekvivalens $\mathbb{F}_q$-val. Tudjuk, hogy ha $\beta_1 \neq \beta_2$, akkor van olyan α, hogy $u' = \mathrm{S}(\beta_1\alpha) \neq \mathrm{S}(\beta_2\alpha) = v'$, de ekkor különböző lesz $u = \varphi(u')$ és $v = \varphi(v')$ is. Ugyanakkor $p > u \in \mathbb{N}$, $p > v \in \mathbb{N}$, és egy p-edik primitív komplex egységgyök két különböző, p-nél kisebb nemnegatív egész kitevős hatványa különböző, így a κ_β-k száma legalább q. De több karakter nem lehet, hiszen véges Abel-csoport esetén a karakterek száma azonos a csoport elemszámával, így valóban nincs más additív karaktere $\mathbb{F}_q$-nak.

□

F.20. Definíció

Legyen $\mathbb{F}_q$ a p-elemű test bővítése, $\mathbb{F}_q$-ra $\mathrm{S}(\alpha)$ az α $\mathbb{F}_p$ fölötti nyoma, $\varphi\colon \mathbb{F}_p \to \mathbb{Z}$ olyan, hogy $p > k \in \mathbb{N}$-re $\varphi(ke) = k$, ahol e az $\mathbb{F}_p$ egységeleme. A $\kappa\colon \mathbb{F}_q \to \mathbb{C}$, $\kappa\colon \alpha \mapsto \left(\varepsilon_1^{(p)}\right)^{\varphi(\mathrm{S}(\alpha))}$ függvény **az** $\mathbb{F}_q$ **(additív csoportjának) kanonikus karaktere**.

Δ

Ciklikus csoport karaktereinek csoportja is ciklikus, így a csoport egyetlen alkalmas karakterének ismeretében ismert a csoport bármely karaktere. Az előző tétel alapján a kanonikus karakter meghatározza a véges test additív csoportjának minden karakterét, a test összes additív karakterét, jóllehet nem pímszámelemű véges test additív csoportja nem ciklikus csoport. Mindez azt jelenti, hogy véges testben mind a multiplikatív, mind az additív csoport karaktereinek csoportja egyszerű szerkezetű.

Félcsoport-karakterek

Test multiplikatív struktúrája nem csoport, így a multiplikatív csoport karaktere nem a teljes testet képezi le a komplex számok halmazába. Hasonló a helyzet, ha egy összetett m egész számra tekintjük a modulo m maradékosztályok multiplikatív félcsoportját. Az alábbiakban kiterjesztjük a karakter fogalmát bizonyos feltételeket kielégítő félcsoportokra.

Tekintsük az S egységelemes kommutatív félcsoportot az $\mathcal{E}$ egységcsoporttal. Most ez a csoport is kommutatív. Ha $c = ab$ egység, akkor mind a, mind b egység. Ezt elegendő a-ról belátni, köszönhetően a kommutativitásnak. Ha ugyanis ab invertálható, akkor jobbról invertálható, tehát a jobbról invertálható, másrészt $ab = ba$-ból hasonlóan adódik, hogy a balról is invertálható, végeredményben tehát invertálható.

Legyen most κ az $\mathcal{E}$ egy karaktere, és legyen $\kappa' : S \to \mathbb{C}$ olyan, hogy $\kappa'(s) = \kappa(s)$, ha $s \in E$, míg az S minden más s elemén legyen $\kappa'(s) = 0$. Ezzel a szabállyal κ' valóban az S-t $\mathbb{C}$-be képező függvény, amelynek E-re való megszorítása κ. $\kappa'(ab) = \kappa'(a)\kappa'(b)$, mert $\kappa'(u) = 0$ akkor és csak akkor, ha u nem egység, és az előbb már beláttuk, hogy ab akkor és csak akkor egység, ha mindkét tényezője egység, ekkor viszont $\kappa'(ab) = \kappa(ab) = \kappa(a)\kappa(b) = \kappa'(a)\kappa'(b)$. A kiterjesztett függvény tehát szorzattartó, vagyis κ' S-nek $\mathbb{C}$-be való homomorfizmusa.

Ha κ_1 és κ_2 az egységcsoport két karaktere, akkor ezek $\kappa = \kappa_1\kappa_2$ szorzata is karaktere a csoportnak. Legyen κ', κ_1' és κ_2' rendre a κ, κ_1 és κ_2 kiterjesztése, ekkor E-beli a-ra $\kappa'(a) = \kappa(a) = \kappa_1(a)\kappa_2(a) = \kappa_1'(a)\kappa_2'(a)$, míg ha $a \in S \backslash E$, akkor $\kappa'(a) = 0 = 0 \cdot 0 = \kappa_1'(a)\kappa_2'(a)$, tehát $\kappa_1\kappa_2$ kiterjesztése a kiterjesztések szorzata. A $\mathbb{C}$-beli szorzás asszociatív és kommutatív, ezért a kiterjesztett függvények szorzása is ilyen tulajdonságú. A κ_0 főkarakter kiterjesztése neutrális eleme a szorzásnak, mert E-beli elemeken az értéke 1, míg a többi helyen bármely kiterjesztett karakter értéke 0, és $0 \cdot 0 = 0$, így a kiterjesztett függvények a szokásos függvényszorzással egységelemes kommutatív félcsoportot képeznek. Végül, ha egy κ-hoz tekintjük a κ^{-1} kiterjesztését, akkor könnyen igazolhatóan $(\kappa^{-1})'\,\kappa' = \kappa_0'$, vagyis κ'-nek van inverze, a kiterjesztett függvények a függvényszorzással csoportot alkotnak, és ez az $\hat{S}$ csoport lényegében véve megegyezik $\hat{\mathcal{E}}$-pal, az $\mathcal{E}$ karaktereinek csoportjával.

Az így kiterjesztett függvények a **félcsoport-karakter**ek.

A fentebbi kiterjesztéssel már egy test, valamint egy maradékosztály-gyűrű minden elemére létezik a struktúra multiplikatív műveletére vonatkozó karakter. A szummációs és az ortogonalitási tételek is lényegében véve, értelemszerű módosításokkal érvényesek:

$$\sum_{a \in S} \chi'(a) = \begin{cases} |E|, \text{ha } \chi' = \chi_0' \\ 0\,, \text{ha } \chi' \neq \chi_0' \end{cases}$$

$$\sum_{\chi' \in \hat{S}} \chi'(a) = \begin{cases} |E|, \text{ha } a = e \\ 0\,, \text{ha } a \neq e \end{cases}$$

$$\sum_{a \in S} \chi_1'(a)\overline{\chi_2'}(a) = \begin{cases} |E|, \text{ha } \chi_1' = \chi_2' \\ 0\,, \text{ha } \chi_1' \neq \chi_2' \end{cases}$$

$$\sum_{\chi' \in \hat{S}} \chi'(a_1)\overline{\chi'}(a_2) = \begin{cases} |E|, \text{ha } a_1 = a_2 \\ 0\,, \text{ha } a_1 \neq a_2 \end{cases}$$

Tárgymutató

F

G

Gy

H

I,Í

J

K

L

M

N

Ny

O,Ó

Ö,Ő

P

Q

R

S

Sz

T

V

Z

Zs

Irodalomjegyzék

Berlekamp, E. R.
Algebraic Coding Theory
Aegean Park Press, 1984.

Fried, E.
Algebra II.
Nemzeti Tankönyvkiadó, 2002.

Fuchs, L.
Bevezetés az algebrába és számelméletbe II
Tankönyvkiadó, 1972.

Fuchs, L.
Algebra
Tankönyvkiadó, 1971.

Gonda, J.
Bevezető fejezetek a matematikába III
ELTE, 1998.

Gonda, J.
Bevezető fejezetek a matematikába Kiegészítés
ELTE, 1998.

Hungerford, T. W.
Algebra
Springer, 1980.

Járai, A.
Bevezetés a matematikába
ELTE Eötvös Kiadó, 2009.

Láng, Cs-né.
Bevezető fejezetek a matematikába II.
ELTE, 1998.

Lidl, R., Pilz, G.
Applied Abstract Algebra
Springer-Verlag, New York, 1984.

Lidl, R., Niederreiter, H.
Finite Fields
Addison-Wesley, Reading, Mass., 1983.