ALGEBRA

Nagy Attila

Egyetemi jegyzet

Budapesti Műszaki és Gazdaságtudományi Egyetem

Algebra Tanszék

2022

Ez a jegyzet a Budapesti Műszaki és Gazdaságtudományi Egyetem
Természettudományi Karának
matematikus hallgatói számára meghirdetett
Algebra 1
című tantárgy általam tartott előadásainak anyagát tartalmazza.

Chapter 1

BEVEZETÉS

Definíció 1.0.1 *(Halmazok Descartes szorzata) Az $A_1, \ldots, A_n$ nem üres halmazok (ebben a sorrendben képezett) Descartes szorzatán az*

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \ : \ a_1 \in A_1, \ldots, a_n \in A_n\}$$

halmazt értjük, azaz mindazon n-elemű sorozatok halmazát, amely sorozatok mindegyikében az i-dik elem az A_i halmaz valamely eleme.

Definíció 1.0.2 *(A művelet fogalma) Legyen A tetszőleges nem üres halmaz, és legyen n tetszőleges pozitív egész szám. Az n-szeres $A \times \cdots \times A$ Descartes szorzatnak az A halmazba való egyértelmű leképezését az A halmazon értelmezett n-változós műveletnek nevezzük. Az A halmaz egy elemének kijelölését az A halmazon értelmezett 0-változós műveletnek nevezzük.*

Definíció 1.0.3 *(Az algebrai struktúra fogalma) Egy olyan (nem üres) A halmazt, amelyen értelmezve van legalább egy művelet, algebrai struktúrának nevezünk. Ennek jelölése: $(A; \Omega)$, ahol Ω jelöli az A halmazon értelmezett műveletek halmazát. Az A halmazt az algebrai struktúra alaphalmazának is szokták nevezni.*

Ebben a jegyzetben műveleten mindig kétváltozós műveletet fogunk érteni. Ha $*$ jelöl egy A halmazon értelmezett (kétváltozós) műveletet, akkor az

$(a, b) \in A \times A$ elempár $*$ szerinti képét $*(a, b)$ helyett $a * b$ módon jelöljük. Az $a * a$ elemet jelölhetjük $2a$-val, de jelölhetjük a^2-tel is, annak mintájára, hogy a számoknál $a + a$ helyett $2a$-t, illetve $a \cdot a$ helyett a^2-t írunk. Az első esetben azt mondjuk, hogy additív írásmódot, a második esetben multiplikatív írásmódot használunk. Additív írásmód esetén a művelet jeleként a $+$ jelet, multiplikatív írásmód esetén a művelet jeleként a $\cdot$ jelet használjuk. Multiplikatív irásmód esetén (ha nem okoz félreértést) a művelet jelét elhagyjuk, és az $a \cdot b$ kifejezés helyett egyszerűen ab-t írunk. Ebben a jegyzetben főleg multiplikatív írásmódot használunk.

Megjegyzés 1.0.4 (Cayley-féle műveletáblázat) Egy kétváltozós műveletet táblázatos formában is megadhatunk. Például, ha az alaphalmaz $A = \{a, b\}$, akkor az alábbi táblázatban az a-sor és b-oszlop metszetében levő elem az ab műveleti eredmény; jelen példánkban ez egyenlő b-vel.

*	a	b
a	b	b
b	b	a

Egy, a fentieknek megfelelően konstruált táblázatot *Cayley-féle művelettáblázatnak* nevezünk.

Definíció 1.0.5 *(Műveleti tulajdonságok) Azt mondjuk, hogy egy A halmazon értelmezett művelet asszociatív, ha tetszőleges $a, b, c \in A$ elemek esetén fennáll az alábbi egyenlőség*

$$a(bc) = (ab)c.$$

A műveletről azt mondjuk, hogy kommutatív, ha tetszőleges $a, b \in A$ elemekre teljesül az alábbi egyenlőség

$$ab = ba.$$

Azt mondjuk, hogy a művelet invertálható (az A halmazon), ha tetszőleges $(a, b) \in A \times A$ elempárhoz megadhatók A-nak olyan x és y elemei, amelyekre teljesülnek az alábbi egyenlőségek

$$ax = b \quad \text{és} \quad ya = b.$$

Példák Az egész számok halmazán az összeadás asszociatív, kommutatív és invertálható. A szorzás is asszociatív és kommutatív, viszont nem invertálható. A racionális számok $\mathbb{Q}$ halmazán a szorzás asszociatív és kommutatív, valamint a $\mathbb{Q} \setminus \{0\}$ halmazon invertálható.

Ha egy legalább kételemű A halmazon azt a műveletet tekintjük, amelynél tetszőleges $(a, b) \in A \times A$ elempár esetén $a * b = b$ teljesül, akkor világos, hogy a művelet nem kommutatív. Az is világos, hogy a szóban forgó művelet nem invertálható, mert ugyan tetszőleges $(a, b) \in A \times A$ elempár esetén az $a * x = b$ egyenlőség az A halmaz $x = b$ elemére teljesül, de $a \neq b$ esetén A-nak nincs olyan y eleme, amelyre $y * a = b$ teljesülne.

Definíció 1.0.6 *(Gruppoid) Egy egyműveletes algebrai struktúrát gruppoidnak nevezünk.*

Definíció 1.0.7 *(Félcsoport) Egy S gruppoidról azt mondjuk, hogy félcsoport, ha az S-en értelmezett művelet asszociatív. Ha a művelet még kommutatív is, akkor az S félcsoportot kommutatív félcsoportnak nevezzük.*

Tétel 1.0.8 *Legyen S egy félcsoport. Akkor tetszőleges $n \geq 3$ egész szám és S elemeiből képezett tetszőleges n elemű sorozat esetén az elemek adott sorrendben képezett szorzata nem függ attól, hogy a szorzatot milyen zárójelezés mellett számítjuk ki.*

Egy multiplikatív S félcsoport tetszőleges a eleme és tetszőleges n pozitív egész szám esetén értelmezve van az a^n hatvány, amely olyan n-tényezős szorzat, melynek minden tényezője a. Így

$$a^1 = a, \quad a^2 = aa, \quad a^3 = aa^2 = a^2a, \ldots .$$

Additív írásmód esetén értelemszerűen az na alakú n-tagú összegről beszélhetünk; ekkor

$$1a = a, \quad 2a = a + a, \quad 3a = a + 2a = 2a + a, \ldots .$$

Tétel 1.0.9 *Kommutatív félcsoport tetszőleges $n \geq 2$ számú eleme esetén az elemek szorzata nem függ az elemek sorrendjétől.*

Definíció 1.0.10 *(Bal oldali, illetve jobb oldali nullelem) Egy S félcsoport valamely f elemét az S bal oldali [jobb oldali] nullelemének nevezzük, ha minden S-beli a elem esetén $fa = f$ $[af = f]$ teljesül. Egy S félcsoport valamely elemét az S nullelemének nevezzük, ha az illető elem az S-nek bal oldali és jobb oldali nulleleme.*

Tétel 1.0.11 *Minden félcsoportnak legfeljebb egy nulleleme lehet. Ha egy félcsoportnak van jobb oldali és bal oldali nulleleme, akkor mindegyikből csak egy van, amelyek egybeesnek, s a félcsoport egyetlen nullelemét adják.*

Bizonyítás Ha e, illetve f egy félcsoport bal oldali, illetve jobb oldali nullelemei, akkor $e = ef = f$. Ez bizonyítja a tétel minden állítását. □

Definíció 1.0.12 *(Bal oldali, illetve jobb oldali neutrális elem) Egy S félcsoport valamely e elemét a félcsoport bal oldali neutrális elemének nevezzük, ha S minden s eleme esetén fennáll az $es = s$ egyenlőség. Félcsoport jobb oldali neutrális elemének fogalma a bal oldali neutrális elem fogalmának duálisa. Egy félcsoport valamely elemét a félcsoport neutrális elemének nevezünk, ha az bal oldali és egyben jobb oldali neutrális eleme a félcsoportnak.*

Tétel 1.0.13 *Minden félcsoportnak legfeljebb egy neutrális eleme van. Továbbá, ha egy félcsoportnak van jobb oldali és bal oldali neutrális eleme is, akkor azok egyenlőek, s az S félcsoport egyetlen neutrális elemét adják.*

Bizonyítás. Jelölje e, illetve f egy S félcsoport bal oldali, illetve jobb oldali neutrális elemét. Akkor $e = ef = f$. Ez bizonyítja a tétel mindkét állítását. □

Definíció 1.0.14 *(Monoid) Egy neutrális elemes félcsoportot monoidnak is nevezünk.*

Definíció 1.0.15 *(Jobb oldali, illetve bal oldali inverz) Egy e neutrális elemes S félcsoport valamely b elemét [c elemét] egy $a \in S$ elem bal oldali [jobb oldali] inverzének nevezzük, ha $ba = e$ [$ac = e$] teljesül. Egy $a^{-1} \in S$ elemről azt mondjuk, hogy az $a \in S$ elem inverze, ha a^{-1} az a elem bal oldali és jobb oldali inverze is.*

Tétel 1.0.16 *Monoidban minden elemnek legfeljebb egy inverze van. Továbbá, ha egy a elemnek van jobb oldali és bal oldali inverze is, akkor azok egyenlők, és az a elem egyetlen inverzét adják.*

Bizonyítás. Jelölje a', illetve a'' egy S monoid valamely a elemének bal oldali, illetve jobb oldali inverzét. Akkor, e-vel jelölve az S neutrális elemét,

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$$

adódik. Ez bizonyítja a tétel mindkét állítását. □

Chapter 2

CSOPORTOK

2.1 A csoport fogalma; ekvivalens definíciók

Definíció 2.1.1 *(Csoport) Egy S félcsoportot csoportnak nevezünk, ha van neutrális eleme, és minden elemének van inverze. Egy kommutatív csoportot (azaz, amikor a művelet kommutatív is) Abel-csoportnak nevezünk.*

Definíció 2.1.2 *(Egyszerűsítéses félcsoport) Egy S félcsoportot bal egyszerűsítésesnek mondunk (vagy azt mondjuk, hogy S-ben teljesül a bal egyszerűsíthetőség), ha tetszőleges $a, b, x \in S$ elemek esetén az $xa = xb$ egyenlőségből $a = b$ következik. A jobb egyszerűsítéses félcsoport fogalma a bal egyszerűsítéses félcsoport fogalmának duálisa. Egy félcsoportot egyszerűsítésesnek nevezünk, ha bal egyszrűsítéses és jobb egyszerűsítéses.*

Tétel 2.1.3 *Minden csoport egyszerűsítéses.*

Bizonyítás. Ha $xa = xb$ teljesül valamely G csoport a, b, x elemeire, akkor x inverzével, x^{-1}-gyel balról szorozva az egyenlőséget, $a = b$ adódik. Hasonlóan igazolható a jobb egyszerűsíthetőség is. □

Tétel 2.1.4 *Tetszőleges S félcsoporton a következő feltételek egymással ekvivalensek:*

(1) *S csoport;*

(2) *S-nek van olyan e jobb oldali neutrális eleme, hogy minden $a \in S$ elemhez megadható olyan $a^{-1} \in S$ elem, melyre $aa^{-1} = e$ teljesül;*

(3) *S-nek van olyan f bal oldali neutrális eleme, hogy minden $a \in S$ elemhez megadható olyan $a^{-1} \in S$ elem, melyre $a^{-1}a = f$ teljesül;*

(4) *Az S-en értelmezett művelet invertálható, azaz, az $ax = b$ és $ya = b$ egyenletrendszer minden $a, b \in S$ elem esetén megoldható S-ben;*

(5) *Az $ax = b$ és $ya = b$ egyenletrendszer minden $a, b \in S$ elem esetén egyértelműen megoldható S-ben.*

Bizonyítás. Az nyilvánvaló, hogy az (1) feltételből következik a (2) és a (3) feltétel. Mivel tetszőleges $a, b \in S$ elemek esetén az $x = a^{-1}b$ és $y = ba^{-1}$ elemekre teljesülnek az $ax = b$ és $ya = b$ egyenlőségek, ezért az (1) feltételből következik a (4) feltétel. Mivel minden csoport egyszerűsítéses, ezért az (1) feltételből következik az (5) feltétel.

Megmutatjuk, hogy (2) maga után vonja (1)-et. Tegyük fel, hogy az S félcsoportban van olyan e jobb oldali neutrális elem, hogy S minden elemének van jobb oldali inverze erre a jobb oldali neutrális elemre nézve. Legyen a tetszőleges S-beli elem. Jelölje a_0 az a-nak, a_1 az a_0-nak egy-egy jobb oldali inverzét az e jobb oldali neutrális elemer nézve, azaz

$$aa_0 = e = a_0a_1.$$

Akkor

$$a_0a = (a_0a)e = (a_0a)(a_0a_1) = a_0(aa_0)a_1 = a_0ea_1 = a_0a_1 = e,$$

tehát a_0 bal oldali inverze a-nak e-re nézve. Ezért

$$ea = (aa_0)a = a(a_0a) = ae = a,$$

tehát e neutrális elem S-nek. Igy (1) teljesül.

Az előzőekhez hasonlóan igazolható, hogy a (3) feltételből következik az (1) feltétel. Az eddigi eredményekből már az is következik, hogy az (1), a (2) és a (3) feltételek egymással ekvivalensek.

Megmutatjuk, hogy a (4) feltételből következik a (2) feltétel. Ehhez tegyük fel, hogy tetszőleges $a, b \in S$ elemekhez vannak olyan $x, y \in S$ elemek, amelyekre $ax = b$ és $ya = b$ teljesül. Legyen $a \in S$ tetszőleges rögzített elem. Akkor megadható olyan e elem, amelyre $ae = a$ teljesül. Legyen $b \in S$ tetszőleges elem. Akkor van olyan $y \in S$ elem, hogy $ya = b$. Ezért $be = (ya)e = y(ae) = ya = b$, azaz e az S félcsoport jobb oldali neutrális eleme. Mivel a művelet invertálható, tetszőleges $a \in S$ elemhez megadható olyan $a^{-1} \in S$ elem, hogy $aa^{-1} = e$. Tehát (2) teljesül.

Mivel az (5) feltételből következik a (4) feltétel, ezért a tételt bebizonyítottuk. □

Tétel 2.1.5 *Egy véges félcsoport akkor és csak akkor csoport, ha egyszerűsítéses.*

Bizonyítás. Véges egyszerűsítéses S félcsoport tetszőleges a elemére $Sa = S$ és $aS = S$ teljesül. Ennek, valamint korábban bizonyított tételeknek felhasználásával már egyszerűen bizonyítható a tétel állítása. □

Példa 2.1.6 *(Kvaterniócsoport) A Q kvaterniócsoport elemei: $\pm 1, \pm i, \pm j, \pm k$. A közöttük levő műveletek a következőek: ± 1-gyel a szokott módon szorzunk, és*

$$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Példa 2.1.7 (Szimmetriacsoport, diédercsoport) Egy tetszőleges geometriai alakzatot önmagára vivő egybevágósági transzformációk csoportot alkotnak a leképezések szorzására nézve. Ezt a csoportot az illető alakzat szimmetriacsoportjának nevezzük.

A sík egy szabályos m-oldalú sokszögének szimmetriacsoportját m-edfokú D_m diédercsoportnak nevezzük. Ha f a $\frac{2\pi}{m}$-mel való forgatást, t pedig egy szimmetriatengelyre való tükrözést jelöl, akkor D_m elemei:

$$e, f, f^2, \ldots, f^{m-1}, t, tf, \ldots tf^{m-1}.$$

A számolás szabályai:

$$f^m = e, t^2 = e, ft = tf^{m-1}.$$

Az $m = 2$ esetben kapjuk a Klein-féle csoportot. Ez kommutatív és elemei: e, f, t, tf.

2.2 Csoportok részcsoportjai

Definíció 2.2.1 *(Részcsoport) Egy G csoport nem üres H részhalmazát a G egy részcsoportjának nevezzük, ha a G-beli műveletre nézve H egy csoport.*

Megjegyzés 2.2.2 Ha H a G csoport részcsoportja, akkor H neutrális eleme megegyezik G neutrális elemével. Ugyanis, ha e' jelöli H neutrális elemét, e pedig a G neutrális elemét, akkor $ee' = e' = e'e'$, amiből $e = e'$ következik a G csoport egyszerűsíthetősége miatt.

Megjegyzés 2.2.3 Ha H a G csoport részcsoportja, akkor tetszőleges $a \in H$ elem esetén az a H-beli inverze megegyezik G-beli inverzével. Ugyanis, ha x jelöli az $a \in H$ elem H-beli inverzét, akkor az egyben az a elem G-beli inverze is. Azt pedig már igazoltuk, hogy monoidban minden elemnek legfeljebb egy inverze van.

Tétel 2.2.4 *Egy G csoport tetszőleges nem üres részhalmaza esetén az alábbi feltételek egymással ekvivalensek.*

(1) H a G egy részcsoportja;

(2) $HH \subseteq H$ és $H^{-1} \subseteq H$;

(3) $HH^{-1} \subseteq H$.

Bizonyítás Az előző két megjegyzés alapján csak a (2) és (3) feltételek ekvivalenciáját kell bizonyítani. Ha (2) teljesül, akkor $HH^{-1} \subseteq HH \subseteq H$, azaz (2) is teljesül. Ha (3) teljesül, akkor

$$H^{-1} = eH^{-1} \subseteq HH^{-1} \subseteq H$$

és

$$HH = H(H^{-1})^{-1} \subseteq HH^{-1} \subseteq H,$$

azaz (2) is teljesül. □

Megjegyzés 2.2.5 Véges G csoport esetén (2)-ből a $H^{-1} \subseteq H$ feltétel elhagyható. Ugyanis tetszőleges $a \in H$ esetén $a, a^2, a^3, \cdots \in H$. Így G végessége miatt $a^m = a^{m+k}$ teljesül valamely pozitív egész m-re és k-ra. Az a^m inverzével balról szorozva az egyenlőséget, $e = a^k$ adódik. Ha $k = 1$, akkor $a^{-1} = a = e \in H$. Ha $k > 1$, akkor $a^{-1} = a^{k-1} \in H$.

Megjegyzés 2.2.6 Ha H egy G csoport részcsoportja (azaz $HH \subseteq H$ és $H^{-1} \subseteq H$), akkor $HH = H$ és $H^{-1} = H$. Ugyanis ekkor $H = He \subseteq HH$, amely a $HH \subseteq H$ feltétellel együtt a $HH = H$ egyenlőség teljesülését eredményezi. Továbbá, mivel tetszőleges $a \in H$ elem inverzének az a elem inverze, így $H \subseteq H^{-1}$, amiből $H^{-1} = H$ adódik a $H^{-1} \subseteq H$ tartalmazást is használva.

Tétel 2.2.7 *Ha H_i $(i \in I)$ egy G csoport részcsoportjainak tetszőleges nem üres halmaza, akkor $H = \cap_{i \in I} H_i$ is részcsoportja G-nek.*

Bizonyítás. Világos, hogy H nem üres, mert tartalmazza a G csoport neutrális elemét. Mivel tetszőleges $i \in I$ index esetén $HH \subseteq H_iH_i \subseteq H_i$ és $H^{-1} \subseteq H_i^{-1} \subseteq H_i$, ezért $HH \subseteq H$ és $H^{-1} \subseteq H$. Tehát H a G csoport részcsoportja. □

Definíció 2.2.8 *(Generált részcsoport) Legyen K egy G csoport nem üres részhalmaza. A G csoport K-t tartalmazó összes részcsoportjának metszetét a K által generált részcsoportnak nevezzük és $\{K\}$-val jelöljük. K-t a $\{K\}$ csoport generátorrendszerének nevezzük.*

Tétel 2.2.9 *Egy G csoport tetszőleges nem üres K részhalmaza esetén a $\{K\}$ csoport a G mindazon elemeinek összessége, amelyek K-beli elemek egész kitevőjű hatványainak véges szorzataként írhatók fel.*

Bizonyítás. Könnyen ellenőrízhető, hogy G mindazon elemeineke halmaza, amely elemek véges sok K-beli elem egész kitevőjű hatványainak szorzataként állnak elő, G-nek egy olyan részcsoportját alkotja, amely benne van G összes olyan részcsoportjába, amely K-t tartalmazza.

2.3 Ciklikus csoportok

Definíció 2.3.1 *(Ciklikus részcsoport) Egy csoportot ciklikus csoportnak nevezünk, ha egyetlen elemmel generálható.*

Definíció 2.3.2 *(Csoportok homomorfizmusa) Egy $(G_1;\star)$ csoportnak egy $(G_2;\circ)$ csoportba való φ leképezését homomorfizmusnak nevezzük, ha művelettartó, azaz tetszőleges $a,b\in G_1$ elemekre $\varphi(a\star b)=\varphi(a)\circ\varphi(b)$ teljesül. Egy bijektív (szürjektív és injektív) homomorfizmust izomorfizmusnak nevezünk.*

Tétel 2.3.3 *Egy ciklikus csoport izomorf vagy az egész számok additív csoportjával vagy az egész számok mod m maradékosztályainak additív csoportjával.*

Bizonyítás. Legyen G az a eleme által generált (ciklikus) csoport. Két eset lehetséges. Először vizsgáljuk azt az esetet, amikor nincs olyan n pozitív egész szám, amelyre $a^n=e$ teljesülne. Ekkor minden $m\neq n$ egész szám esetén $a^n\neq a^m$. Így $G=\{\dots,a^{-2},a^{-1},e,a,a^2,\dots\}$. Az $a^n\to n$ leképezés G-nek az egész számok additív csoportjára való injektív homomorfizmusa, azaz izomorfizmusa.

A második esetben van olyan (legkisebb) n pozitív egész szám, amelyre $a^n=e$ teljesül. Mivel tetszőleges pozitív egész m esetén megadhatók olyan q és r pozitív egész számok, amelyekre teljesül az $m=qn+r$ egyenlőség, ahol $r\in\{0,1,\dots,n-1\}$, ezért $a^m=(a^n)^qa^r+a^r$, amiből következik, hogy $G=\{e,a,\dots,a^{n-1}\}$. Az előzőekből az is következik, hogy az $a^m\mapsto m$ leképezés $(m\in\{0,1,\dots,a^{n-1}\})$ a G csoportnak az egész számok mod m maradékosztályainak additív csoportjára való izomorfizmusa. □

Definíció 2.3.4 *(Csoport elemének rendje) Ha egy G csoport a eleméhez megadható olyan pozitív gész szám, amelyre $a^m=e$, ahol e a G egységeleme, akkor azt a legkisebb n pozitív egész számot, amely ezzel a tulajdonsággal rendelkezik, az a elem rendjének nevezzük. Ha $a^m\neq e$ teljesül minden m pozitív egész számra, akkor azt mondjuk, hogy az a elem végtelen rendű. Az a elem rendjét $o(a)$-val jelöljük.*

Megjegyzés 2.3.5 A Tétel 2.3.3 szerint egy csoport tetszőleges elemének rendje megegyezik az általa generált (ciklikus) részcsoport rendjével.

Tétel 2.3.6 *Ciklikus csoport minden részcsoportja ciklikus.*

Bizonyítás. Legyen H a $G = \{a\}$ ciklikus csoport tetszőleges részcsoportja. Mivel a $\{e\}$ részcsoport ciklikus, ezért feltehetjük, hogy $H \neq \{e\}$. Ekkor van olyan legkisebb pozitív t egész szám, amelyre $a^t \in H$ teljesül. Megmutatjuk, hogy $H = \{a^t\}$. Mivel $\{a^t\} \subseteq H$, azért elegendő csak azt megmutatni, hogy $H \subseteq \{a^t\}$. Legyen $a^m \in H$ tetszőleges elem. Akkor $m = qt + r$ teljsül valamely q pozitív egész számra, ahol $r \in \{0, 1, \ldots, t-1\}$. Ekkor $a^r = a^{m-qt} = a^m(a^t)^q \in H$. Mivel $r < t$, ezért $r = 0$, és így $m = qt$, amiből $a^m = (a^t)^q \in \{a^t\}$ következik. □

Tétel 2.3.7 *Egy n-edrendű ciklikus csoportban $\varphi(n)$ számú n-edrendű elem van, ahol φ az un. Euler-függvény ($\varphi(n)$ az n-nél nem nagyob, az n-hez relatív prím pozitív egészek száma).*

Bizonyítás Mivel minden n-edrendű ciklikus csoport izomorf egymással, ezért elegendő a tételt a komplex n-dik egységgyökök C_n csoportjára bizonyítani. Ismert, hogy egy n-dik komplex egységgyök akkor és csak akkor generálja C_n-et, ha ez az elem primitív n-dik egységgyök. Legyen ϵ egy primitív n-dik egységgyök, akkor $C_n = \{\epsilon\}$, azaz C_n minden eleme ϵ valamelyik hatványa. Az is ismert, hogy ϵ^k akkor és csak akkor primitív komplex egységgyök, ha $(k, n) = 1$. Így a C_n ciklikus csoport n-edrendű elemeinek száma $\varphi(n)$. □

2.4 Mellékosztályok. Lagrange tétele

Definíció 2.4.1 *(Részcsoport szerinti mellékosztályok) Legyen H a G csoport részcsoportja és $a \in G$. Az*

$$aH = \{ah | h \in H\}$$

szorzatot a G csoport H részcsoport szerinti bal oldali mellékosztályának, a

$$Ha = \{ha | h \in H\}$$

szorzatot pedig a G csoport H részcsoport szerinti jobb oldali mellékosztályának nevezzük.

Tétel 2.4.2 *Egy G csoport tetszőleges H részcsoportja és tetszőleges $a, b \in G$ elemeire a következő feltételek egymással ekvivalensek.*

(1) $a \in bH$;

(2) $aH = bH$;

(3) $b^{-1}a \in H$.

Bizonyítás. (1) $\rightarrow$ (2): Ha $a \in bH$, akkor van olyan $h \in H$ elem, amelyre $a = bh$ teljesül. Ezért

$$aH = (bh)H = b(hH) = bH.$$

(2) $\rightarrow$ (3): Tegyük fel, hogy $aH = bH$. Mivel $a \in aH$, ezért $a \in bH$ és így van olyan $h \in H$ elem, hogy $a = bh$. Ekkor

$$b^{-1}a = b^{-1}bh = eh = h \in H.$$

(3) $\rightarrow$ (1): Ha $b^{-1}a \in H$, akkor $b^{-1}a = h$ valamely $h \in H$ elemmel. Ekkor

$$a = bb^{-1}a = bh \in bH.$$

□

Tétel 2.4.3 *Tetszőleges G csoport tetszőleges H részcsoportja szerinti aH és bH bal oldali mellékosztályaira vagy $aH = bH$ vagy $aH \cap bH = \emptyset$.*

Bizonyítás. Tegyük fel, hogy G valamely x elemére $x \in aH \cap bH$ teljesül. Akkor $aH = xH = bH$ a 2.4.2 Tétel szerint. □

Tétel 2.4.4 *Tetszőleges G csoport tetszőleges H részcsoportja esetén az $aH \mapsto Ha^{-1}$ leképezés a G csoport H szerini bal oldali mellékosztályainak halmazáról a H szerinti jobb oldali mellékosztályok halmazára való kölcsönösen egyértelmű leképezés.*

Bizonyítás Mivel $(a^{-1}H)^{-1} = H^{-1}((a^{-1})^{-1} = Ha$, ezért a leképezés szürjektív. A $(aH)^{-1} = (bH)^{-1}$ akkor és csak akkor teljesül, ha $aH = (Ha^{-1})^{-1} = (Hb^{-1})^{-1} = bH$ teljesül, ezért a leképzés injektív. □

Az előző tétel alapján, egy részcsoport szerinti jobb- és bal oldali mellékosztályok halmazának számossága azonos.

Definíció 2.4.5 *(Részcsoport indexe) Legyen H egy G csoport részcsoportja. Ha a H szerinti bal oldali mellékosztályok száma (ami ugyanaz, mint a jobb oldali mellékosztályok száma) véges, akkor ezt a számot a H részcsoport G-beli indexének nevezzük, és $|G : H|$ módon jelöljük.*

Tétel 2.4.6 *(Lagrange-tétel) Véges G csoport tetszőleges H részcsoportjára érvényes:*

$$|G| = |H||G : H|,$$

tehát a H részcsoport rendje és indexe osztója a csoport rendjének.

Bizonyítás. Mivel a G csoport tetszőleges a eleme esetén a $h \mapsto ah$ leképezés a H-nak az aH mellékosztályra való kölcsönösen egyértelmű leképezése, ezért $|H| = |aH|$. Így minden mellékosztályban annyi elem van, mint a H részcsoportban. Ebből következően a G csoportban levő elemek számára, azaz $|G|$-ra igaz, hogy $|G| = |H||G : H|$. □

Következmény 2.4.7 *Véges csoport minden elemének rendje osztója a csoport rendjének.*

Bizonyítás. Mivel elem rendje megegyezik az elem által generált ciklikus részcsoport rendjével, azért az állítás a 2.4.6 Tétel következménye. □

2.5 Normális részcsoportok

2.6 Faktorcsoport, Homomorfizmus-tétel

2.7 Izomorfizmus-tételek

2.8 Normállánc, a Jordan–Hölder-tétel

2.9 Kommutátor részcsoport, kommutátorlánc

Egy G csoport részcsoportjainak

$$G = G^{(0)} \rhd G^{(1)} \rhd \dots G^{(i-1)} \rhd G^{(i)} \rhd \dots$$

sorozatát a G csoport kommutátorláncának nevezzük, ha $G^{(i)}$ a $G^{(i-1)}$ kommutátor részcsoportja minden $i = 1, \dots$ indexre.

2.10 Feloldható csoportok

Tétel 2.10.1 *(Burnside-tétel) Ha* $\mid G \mid = p^n q^m$*, ahol* p *és* q *prímek, akkor* G *nem nemkommutatív egyszerű csoport.*

Következmény 2.10.2 *Ha* $\mid G \mid = p^n q^m$*, ahol* p *és* q *prímek, akkor* G *feloldható.*

Bizonyítás Mivel G véges, ezért van kompozíciólánca. Ebben az egyszerű kompozíciófaktorok elemszáma $p^x q^y$, ami Burnside tétele miatt csak kommutatív lehet. □

Tétel 2.10.3 *(Feit-Thompson-tétel) Ha* G *nemkommutatív véges egyszerű csoport, akkor* $\mid G \mid$ *páros.*

Következmény 2.10.4 *Minden véges páratlan rendű csoport feloldható.*

Bizonyítás Mivel G véges, ezért van kompozíciólánca. Ebben az egyszerű kompozíciófaktorok elemszáma páratlan, ami a Feit-Thompson tétel miatt csak kommutatív lehet. □

Tétel 2.10.5 *Egy G csoport akkor és csak akkor feloldható, ha kommutátorlánca leér a G egységeleméig.*

2.11 Permutációcsoportok

Tétel 2.11.1 *Ha $n \geq 3$, akkor az S_n szimmetrikus csoportban minden páros permutáció előállítható 3 hosszúságú ciklusok szorzataként, azaz az A_n ($n \geq 3$) alternáló csoportot generálják a 3 hosszúságú ciklusok.*

Bizonyítás. Legyen $n \geq 3$. Tudjuk, hogy S_n-ben minden permutáció előáll transzpozíciók szorzataként. Azt is tudjuk, hogy egy permutáció akkor és csak akkor páros, ha páros sok transzpozíció szorzataként állítható elő. Ezért, ha egy permutáció páros, akkor az előállításában szereplő transzpozíciókat párba állíthatjuk úgy, hogy az elsőt a másodikkal, a harmadikat a negyedikkel, stb . A transzpozíciópárok szorzata vagy $(a\ b)(a\ c)$ alakú, vagy (a b)(c d) alakú (itt a, b, c, d páronként különbözőek). Belátható, hogy

$$(a\ b)(a\ c) = (a\ b\ c)$$

és

$$(a\ b)(c\ d) = (a\ b\ c)(a\ d\ c), \quad \text{ha} \quad n \geq 4,$$

amiből már következik a tétel állítása. □

Tétel 2.11.2 *$n \geq 5$ esetén az A_n alternáló csoport egyszerű.*

Bizonyítás Legyen N az A_n ($n \geq 5$) alternáló csoport olyan normális részcsoportja, amely tartalmaz legalább két elemet. Megmutatjuk, hogy $N = A_n$. Ekkor van N-nek olyan $\sigma \neq e$ eleme, amely az $\{1, 2, \ldots, n\}$ elemek közül a legkevesebb elemet mozgatja. Mivel egy permutáció hatványai

csak azokat az elemeket mozgathatják, amelyeket σ, ezért σ^t ugyanannyi elemet mozgat mint σ, feltéve, hogy $\sigma^t \neq e$. Korábbi tétel szerint σ diszjunkt ciklusok szorzatára bontható. Ha ebben a felbontásban van m és n hoszúságú ciklus és $m < n$, akkor a $\sigma^m \neq e$ permutációban az m hosszúságú ciklus eltünne (de az n hosszúságú nem), és ezért σ^m kevesebb elemet mozgatna, mint σ, ami lehetetlen az előbbiek figyelembevételével. Tehát σ azonos hosszúságú diszjunkt ciklusok szorzata. Ha ez a hossz k, és ha $k = pj$ (itt p egy prímszám), akkor a $\sigma^j \neq e$ permutáció p hosszúságú diszjunkt ciklusok szorzata. Tehát van A_n-ben olyan permutáció, amely a lehető legkevesebb elemet mozgatja és prím hosszúságú diszjunkt ciklusok szorzata. Tegyük fel, hogy σ-t már úgy választottuk, hogy eleget tesz ezeknek a feltételeknek. A következő lehetőségek vannak:

(I) $\sigma = (12)(34)\ldots$, azaz σ transzpozíciók szorzata. (σ nem lehet transzpozíció, mert minden transzpozíció páratlan, s ezért nem eleme A_n-nek.)

(II) $\sigma = (123)$, azaz σ egy három hosszúságú ciklus.

(III) $\sigma = (123)(456)\ldots$, azaz σ két vagy több három hosszúságú diszjunkt ciklus szorzata.

(IV) $\sigma = (12345\ldots)$ vagy $\sigma = (12345\ldots)\ldots$, azaz σ olyan egy vagy több tényezős szorzat, amelynek tényezői legalább 5 hosszúságú diszjunkt ciklusok.

Megjegyezzük, hogy σ-ról feltehetjük, hogy a fenti alakúak, mert ha σ (például az (I) esetben) $(ab)(cd)$ alakú, akkor az n elem sorrendjének megváltoztatásával elérhetjük, hogy a legyen az 1. elem, b a 2. elem, c a 3. elem, d pedig a 4. elem. Mivel $n \geq 5$, ezért $\tau = (345) \in A_n$, és N normalitása miatt

$$\varrho = \sigma\tau\sigma^{-1}\tau^{-1} \in N.$$

Világos, hogy ϱ az 1-et fixen hagyja. A (III) és (IV) esetekben ϱ a 4-et a 2-be viszi, ezért ezekben az esetekben $\varrho \neq e$. A τ csak a 3-as, a 4-es és az 5-ös elemeket mozgatja. A (III) és (IV) esetekben σ mozgatja ezeket az elemeket, így ϱ csak azokat az elemeket mozgathatja, amelyeket a σ mozgat. Mivel $1\sigma = 2$ és $1\varrho = 1$, ezért ϱ kevesebb elemet mozgat, mint σ. Ez ellentmond σ választásának. Tehát a (III) és (IV) esetek nem lehetségesek. A továbbiakban csak a (I) és (II) eseteket vizsgáljuk. Az világos, hogy

$\alpha = (123) \in A_n$ és $\beta = (345) \in A_n$. Mivel N normális részcsoport, ezért az (I) esetben

$$\sigma\alpha\sigma^{-1}\alpha^{-1} = (14)(23) \in N,$$

a (II) esetben pedig

$$\beta^{-1}\sigma\beta\sigma = (13)(24) \in N.$$

Tehát az (I) és (II) esetek mindegyikében N tartalmazza valamely két diszjunkt transzpozíció szorzatát. Megmutatjuk, hogy mindkét esetben N tartalmazza bármely két diszjunkt transzpozíció szorzatát. Legyenek a, b, c, d az $\{1, 2, \ldots, n\}$ halmaz páronként különböző elemei. Mivel A_n a páros permutációk halmaza, ezért az alábbi két permutáció valamelyike eleme A_n-nek:

$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ a & b & c & d & \ldots \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ b & a & c & d & \ldots \end{pmatrix}.$$

Mivel

$$\gamma_1^{-1}(14)(23)\gamma_1 = (ad)(bc),$$
$$\gamma_2^{-1}(14)(23)\gamma_2 = (ac)(bd),$$

ezért az (I) esetben N tartalmazza bármely két diszjunkt transzpozíció szorzatát. Mivel

$$\gamma_1^{-1}(13)(24)\gamma_1 = (ac)(bd),$$
$$\gamma_2^{-1}(13)(24)\gamma_2 = (ad)(bc),$$

ezért a (II) esetben is N tartalmazza bármely két diszjunkt transzpozíció szorzatát. Tudjuk, hogy A_n minden eleme páros sok transzpozíció szorzata. Ha ebben a szorzatban a tényezők párba állíthatók úgy, hogy a párban lévő transzpozíciók diszjunktak, akkor a párban lévők szorzata, és így az egész szorzat benne van N-ben. Ha ilyen párosítás nincs, akkor minden párosításnál a párba állított szorzatok között van kettő, amelyik közül az egyik (ab), a másik (ac) vagy (cb) alakú. Legyenek d és e olyan $\{1, \ldots, n\}$-beli elemek, amelyek különböznek a-tól, b-től és c-től. Ekkor

$$(ab)(ac) = [(ab)(de)][(de)(ac)] \in N$$

és

$$(ab)(cb) = [(ab)(de)][(de)(cb)] \in N.$$

Tehát ebben az esetben is az egész szorzat eleme N-nek. Ezzel megmutattuk, hogy A_n minden eleme benne van N-ben, és így $N = A_n$. □

2.12 Csoportok direkt- és szemidirekt szorzata

Definíció 2.12.1 *(Csoportok belső direkt szorzata) Akkor mondjuk, hogy egy G csoport előáll A és B részcsoportjainak (belső) direkt szorzataként, ha*

- *A és B a G normális részcsoportjai,*
- *$A \cap B$ csak a G egységelemét tartalmazza,*
- *A és B együtt generálják G-t.*

A fentivel ekvivalens definíció:

Tétel 2.12.2 *Egy G csoport akkor és csak akkor áll elő A és B részcsoportjainak belső direkt szorzataként, ha*

- *G minden eleme előáll egyértelműen egy A-beli és egy B-beli elem szorzataként,*
- *$ab = ba$ teljesül minden $a \in A$ és $b \in B$ elemre.*

Definíció 2.12.3 *(Csoportok külső direkt szorzata) Legyenek A és B csoportok. Az $A \times B$ Descartes-szorzaton definiáljunk műveletet úgy, hogy tetszőleges $a_1, a_2 \in A$ és $b_1, b_2 \in B$ esetén legyen $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$. $A \times B$ erre a műveletre nézve csoport, amelyben (e_A, e_B) az egységelem (itt e_A az A csoport, e_B a B csoport egységeleme), és egy (a, b) elem inverze (a^{-1}, b^{-1}). Ezt a csoportot az A és B csoportok külső direkt szorzatának nevezzük.*

Megjegyzés 2.12.4 (Csoportok belső és külső direkt szorzata közötti kapcsolat) Az A és B csoportok külső direkt szorzatában az (a, e_B) alakú elemek egy olyan A' részcsoportot alkotnak, amely izomorf A-val, az (e_A, b) alakú elemek pedig egy olyan B' részcsoportot, amely izomorf B-vel. Egyszerűen belátható, hogy az $A \times B$ csoport az A' és B' részcsoportok belső direkt szorzata. Ha az egymással izomorf csoportokat azonosítjuk egymással, akkor azt is lehet mondani, hogy az A és B csoportok $A \times B$ külső direkt szorzata megegyezik a belső direkt szorzatukkal.

Az is megmutatható, hogy ha egy G csoport előáll A és B részcsoportjainak belső direkt szorzataként, akkor G izomorf az A és B csoportok külső direkt szorzatával. Itt G egy g elemének azt az $(a, b) \in A \times B$ elempárt feleltetjük meg, amelyekkel g előállítható egyértelműen $g = ab$ alakban.

Definíció 2.12.5 *(Csoportok belső szemidirekt szorzata). Akkor mondjuk, hogy egy G csoport előáll A és B részcsoportjainak (ebben a sorrendben vett) belső szemidirekt szorzataként, ha*

- *B a G normális részcsoportja,*
- *A és B metszete csak a G egységelemét tartalmazza,*
- *A és B együtt generálják G-t.*

Tétel 2.12.6 *Egy G csoport tetszőleges A részcsoportja és tetszőleges B normális részcsoportja esetén az alábbi feltételek egymással ekvivalensek.*

- *G az A és B (ebben a sorrendben vett) belső szemidirekt szorzata.*
- *G minden eleme egyértelműen előáll ab alakban egy A-beli a és egy B beli b elemmel.*
- *G minden eleme egyértelműen előáll ba alakban egy B-beli b és egy A beli a elemmel.*

Definíció 2.12.7 *(Csoportok külső szemidirekt szorzata) Legyenek A és B csoportok, és legyen φ az A csoportnak a B csoport $AutB$ automorfizmuscsoportjába való homomorfizmusa; a B csoport $\varphi(a)$ automorfizmusának B valamely b elemére való hatásásaként adódó elemet jelölje b^a. Az A és B csoportok $A \times B$ Descartes szorzatán definiáljunk egy műveletet a következőképpen: tetszőleges $(a_1, b_1), (a_2, b_2) \in A \times B$ párokra legyen*

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1^{a_2} b_2).$$

Az így keletkezett algebrai struktúra csoport, amelyet az A és B csoportok külső szemidirekt szorzatának nevezünk.

Tétel 2.12.8 *Ha egy G csoport előáll egy A részcsoportjának és egy B normális részcsoportjának belső szemidirekt szorzataként, akkor A-nak B automorfizmuscsoportjába való azon φ leképezés, amely A tetszőleges a eleméhez B elemeinek a-val való konjugáltjait rendeli, homomorfizmus. Továbbá G előáll az A-nak és B-nek ezen $\varphi : A \mapsto Aut(B)$ homomorfizmussal definiált külső szemidirekt szorzataként.*

2.13 Véges Abel-csoportok

2.14 Centrum, centralizátor, normalizátor

2.15 Sylow tételei

Definíció 2.15.1 *(p-Sylow részcsoport) Egy adott p prím szám esetén, egy véges G csoport p^k-adrendű részcsoportját p-Sylow részcsoportnak nevezzük, ha G rendjének prímtényezős felbontásában a p prím p^k alakban szerepel.*

Tétel 2.15.2 *(Sylow 1. tétele) Minden véges G csoportnak minden p prímre létezik p-Sylow részcsoportja.*

Tétel 2.15.3 *(Sylow 2. tétele) Véges G csoport p-Sylow részcsoportjainak száma kongruens 1-gyel modulo p.*

Tétel 2.15.4 *(Sylow 3. tétele) Véges G csoport p-Sylow részcsoportjai egymás konjugáltjai.*

Tétel 2.15.5 *(Cauchy-tétel) Ha egy p prímszám osztója a véges G csoport rendjének, akkor G-nek van p-edrendű eleme.*

Tétel 2.15.6 *Véges G csoport adott p prímhez tartozó p-Sylow részcsoportjainak metszete a G csoport normális részcsoportja.*

Bizonyítás. Sylow 3. tétele szerint, ha egy véges G csoport összes különböző p-Sylow részcsoportjai $H_1, \ldots, H_k$, akkor bármely H_i $(i = 1, \ldots, k)$ p-Sylow részcsoportnak G tetszőleges g elemével való $g^{-1}H_ig$ konjugáltja is p-Sylow részcsoport. Nyílvánvaló, hogy $g^{-1}H_ig = g^{-1}H_jg$ akkor és csak akkor teljesül, ha $i = j$. Ezért van olyan k-adfokú σ permutáció, melyre $g^{-1}H_ig = H_{\sigma(i)}$ teljesül $(i = 1, \ldots, k)$. Így $\cap_{i=1}^k H_i = \cap_{i=1}^k H_{\sigma(i)}$. Legyenek $g \in G$ és $a \in \cap_{i=1}^k H_i$ tetszőleges elemek. Mivel $a \in H_i$ minden i indexre, ezért $g^{-1}ag \in \cap_{i=1}^k H_{\sigma(i)} = \cap_{i=1}^k H_i$. Tehát a $\cap_{i=1}^k H_i$ metszet minden elemének G tetszőleges elemével való konjugáltja is eleme a $\cap_{i=1}^k H_i$ metszetnek, amiből következik, hogy G összes p-Sylow részcsoportjainak $\cap_{i=1}^k H_i$ metszete normális részcsoportja G-nek. □

2.16 Szabad csoportok, csoportok megadása definiáló relációkkal

2.17 Kis elemszámú csoportok

Használni fogjuk a következő tételt.

Tétel 2.17.1 *Ha G egy $2p$-rendű csoport, ahol $p > 2$ prím, akkor G izomorf a $C(2p)$ ciklikus csoport és a D_p diédercsoport közül az egyikkel.*

Bizonyítás. Legyen G egy $2p$-rendű csoport, ahol p egy 2-nél nagyobb prínszám. A Cauchy-tétel alapján tudjuk, hogy G-nek van olyan f és t eleme, melyre $o(f) = p$ és $o(t) = 2$. Az f elem által gerált F részcsoport izomorf a $C(p)$ ciklikus csoporttal. Mivel F indexe 2, ezért F normális részcsoportja G-nek. A t elem által generált T részcsoport izomorf a $C(2)$ csoporttal. Továbbá, $F \cap T = \{e\}$, ahol e jelöli a g egységelemét. Így $|G| = |FT|$. Ha t felcserélhető f-fel, akkor G kommutatív, és ekkor $G = F \times T \cong C(p) \times C(p)$.

Mivel $(2, p) = 1$, ezért G ciklikus csoport. Vizsgáljuk azt az esetet, amikor $ft \neq tf$. Ekkor G elemei $e, t, f f^2, \ldots, f^{n-1}, tf, tf^2, \ldots, tf^{n-1}$, azaz $G \cong D_p$.□

Izomorfiától eltekintve, az alábbi (legalább két, de legfeljebb tíz elemet tartalmazó) kis elemszámú csoportok léteznek:

- Egyetlen kételemű csoport van: ez a $C(2)$ ciklikus csoport.
- Egyetlen háromelemű csoport van: ez a $C(3)$ ciklikus csoport.
- Mivel a négyelemű csoportok mindegyike kommutatív (mert minden p^2 rendű (p prím) csoport kommutatív), ezért két négyelemű csoport létezik a véges kommutatív csoportok alaptétele szerint: az egyik a $C(4)$ ciklikus csoport, a másik a $C(2) \times C(2)$ csoport.
- Egyetlen ötelemű csoport van: ez a $C(5)$ ciklikus csoport.
- Két hatelemű csoport van a 2.17.1 Tétel szerint: az egyik a $C(6)$ ciklikus csoport, a másik a D_3 diédercsoport.
- Egyetlen hételemű csoport van: ez a $C(7)$ ciklikus csoport.
- Öt nyolcelemű csoport van. A kommutatív nyolcadrendűek: a $C(8)$, a $C(4) \times C(2)$ és a $C(2) \times C(2) \times C(2)$ csoportok. A nem kommutatív nyolcadrendűek: a D_4 diédercsoport és a Q kvaterniócsoport. A 8 elemű csoportról először is kimutatjuk, hogy – ha nem kommutatív – van negyedrendű eleme. Általában igaz ugyanis az, hogy ha egy csoport minden eleme másodrendű, akkor a csoport kommutatív. Valóban, ha $a^2 = b^2 = (ab)^2 = 1$, akkor ba = 1ba1 = aababb = a(ab)2b = a1b = ab. Így a kérdéses csoportban van egy negyedrendű a elem. Ha $b \notin < a >$, akkor $< a, b >$ rendje nagyobb, mint négy, tehát ez az egész csoport. Mivel a centrum szerinti faktorcsoport nem lehet ciklikus, ezért $< a >$ képe ebben a faktorcsoportban nem lehet az egész csoport. Ez azt jelenti, hogy $< a >$-ban van az e egységelemtől különböző centrumelem, ami csak a^2 lehet, mert a centrumnak nem lehet négy eleme. Mivel a csoport nem kommutatív, ezért generátorelemeik nem felcserélhetőek. Így az $[a; b] = aba^{-1}b^{-1}$ nem az egységelem. A centrum szerinti faktor azonban kommutatív, így a fenti kommutátor benne van a centrumban, azaz $aba^{-1}b^{-1} = a^2$. Ebből azonnal adódik a $ba = a^3b$ összefüggés. Ha $b^2 = e$, akkor a kapott csoport nyilván D4 lesz. A másik lehetséges eset az, hogy $b^2 = a^2$ amikor az úgynevezett kvaterniócsoportot nyerjük.

- Két kilencelemű csoport van (mivel a p^2 (p prímszám) rendű csoportok kummutatívak): a $C(9)$ ciklikus csoport és a $C(3) \times C(3)$ csoport.
- Két tízelemű csoport van a 2.17.1 Tétel szerint: a $C(10)$ ciklikus csoport és a D_5 diédercsoport.

Chapter 3

GYŰRŰK

3.1 A gyűrű fogalma

Definíció 3.1.1 *(A gyűrű fogalma) Egy összeadással és szorzással ellátott kétműveletes algebrai struktúrát gyűrűnek nevezünk, ha a következő három feltételnek eleget tesz:*

(1) R az összeadásra nézve kommutatív csoport (más néven: Abel-csoport);

(2) R a szorzásra nézve félcsoport;

(3) Az összeadás mindkét oldalról disztributív az összeadásra nézve, azaz $a(b+c) = ab + ac$ és $(b+c)a = ba + ca$ teljesül R tetszőleges a, b, c elemeire.

Ha egy R gyűrűben a szorzás kommutatív, akkor a gyűrűt kommutatív gyűrűnek nevezzük.

Az (1) feltétel miatt minden R gyűrűben az összeadásra nézve van neutrális elem, amelyet a gyűrű nullelemének nevezzük, és 0-val jelöljük. Egy R gyűrű minden a elemének van az összeadásra nézve $-a$ inverze, amelyet az a elem ellentettjének nevezzük. A disztributivitás alapján tetszőleges $a, b \in R$ elemekre $ab = a(b+0) = ab + a0$ és $ba = (b+0)a = ba + 0a$, ahonnan

$$(\forall a \in R)\ a0 = 0 \quad \text{és} \quad 0a = 0$$

adódik. Mivel egy R gyűrű tetszőleges a és b elemeire $0 = a0 = a(b+(-b)) = ab + a(-b)$, $0 = 0b = (a + (-a))b = ab + (-a)b$, teljesül, ezért

$$(\forall a, b \in R)\ a(-b) = (-a)b = -(ab) \text{ és } (-a)(-b) = ab.$$

Ezért a disztributivitás a különbségre is teljesül:

$$a(b - c) = ab - ac \quad \text{és} \quad (b - c)a = ba - ca.$$

Egy R gyűrű tetszőleges a eleme és tetszőleges n egész szám esetén az na szorzat értelmezve van. Ha n pozitív, akkor na az az n-tagú összeg, amelyben minden tag egyenlő a-val. Ha $n = -m$ negatív, akkor na azt az m-tagú összeget jelöli, amelyben minden tag $-a$. Az a elemnek a 0 számmal való szorzatán a gyűrű nullelemét értjük (azaz $0a = 0$). Tetszőleges gyűrűben érvényesek a következő azonosságok:

$na+ma = (n+m)a$, $n(ma) = (nm)a$, $n(a+b) = na+nb$, $n(ab) = (na)b = a(nb)$.

3.2 Gyűrűk kitüntetett elemei

Definíció 3.2.1 *(Nullosztó) Egy R gyűrű a elemét bal oldali nullosztónak nevezzük, ha van a gyűrűnek olyan $b \neq 0$ eleme, amelyre $ab = 0$ teljesül. A jobb oldali nullosztó fogalma a bal oldali nullosztó fogalmának duálisa.*

Az egész számok modulo 6 maradékosztály gyűrűjében pl. 2 maradékosztály bal oldali nullosztó (a szorzás kommutativitása miatt jobb oldali is), mivel a 2 és 3 maradékosztályok szorzata a 0 maradékosztály (ami a $\mathbb{Z}_m$ maradékosztálygyűrű nulleleme).

Ha egy gyűrűben nincs a nullelemtől különböző bal oldali nullosztó, akkor nincs a nullelemtől különböző jobb oldali nullosztó sem.

Definíció 3.2.2 *(Nullosztómentes gyűrű) Egy olyan gyűrűt, amelyben nincs a nullelemtől különböző nullosztó, nullosztómentes gyűrűnek nevezünk. Egy kommutatív nullosztómentes gyűrűt integritási tartománynak nevezünk.*

Tétel 3.2.3 *Tetszőleges R gyűrűben az $ab = ac$ egyenlőségből akkor és csak akkor következik a $b = c$ egyenlőség, ha a nem bal oldali nullosztója az R-nek.*

Bizonyítás. Legyen a nem bal oldali nullosztója egy R gyűrűnek. Tegyük fel, hogy $ab = ac$ valamely $b, c \in R$ elemekre. Akkor $a(b - c) = 0$. Mivel a nem bal oldali nullosztó, ezért ez az egyenlőség csak akkor állhat fenn, ha $b - c = 0$, azaz $b = c$. Fordítva, tegyük fel, hogy a az R gyűrű olyan eleme, amelyre a következő feltétel teljesül: minden $b, c \in R$ elemekre az $ab = ac$ feltételből $b = c$ következik. Ha ennek ellenére a bal oldali nullosztó lenne, akkor létezne olyan $0 = b \in R$ elem, hogy $ab = 0$ teljesülne. Ekkor $ab = 0 = a0$ miatt $b = 0$ következne az a elemre vonatkozó feltétel miatt. Ez viszont ellentmond a $b \neq 0$ feltételnek. □

Definíció 3.2.4 *(Gyűrű egységeleme) Ha egy R gyűrű a szorzásra nézve monoid, azaz van a szorzásra nézve neutrális eleme, akkor ezt a gyűrű egységelemének nevezzük. Ekkor a gyűrűt egységelemes gyűrűnek nevezzük.*

Definíció 3.2.5 *(Inverz) Egységelemes R gyűrű x elemét az $a \in R$ elem bal oldali inverzének nevezzük, ha $xa = e$, ahol e a gyűrű egységeleme. Elem jobb oldali inverzének fogalma a bal oldali inverz fogalmának duálisa. Egy gyűrű valamel a elemének inverzén azt az a^{-1}-gyel jelölt elemét értjük (ha létezik, akkor egyértelműen meghatározott), amelyre $aa^{-1} = a^{-1}a = e$ teljesül.*

Tétel 3.2.6 *Ha egy R gyűrű valamely a elemének van bal oldali inverze, akkor az a elem az R-nek nem bal oldali nullosztója.*

Bizonyítás Ha egy $a \in R$ elemnek $x \in R$ bal oldali inverze, akkor R tetszőleges b eleme esetén az $ab = 0$ feltételből $b = eb = (xa)b = x(ab) = x0 = 0$ következik. □

3.3 Gyűrűk ideáljai

Definíció 3.3.1 *(Részgyűrű) Egy R gyűrű részgyűrűjén értjük R olyan nem üres részhalmazát, amely maga is gyűrű az R-en értelmezett eredeti összeadásra és szorzásra nézve.*

Egy R gyűrű valamely nem üres S részhalmaza akkor és csak akkor részgyűrű, ha tetszőleges $a, b \in R$ elemek esetén $a - b \in S$ és $ab \in S$.

Definíció 3.3.2 *(Gyűrű ideáljai) Egy R gyűrű nem üres I részhalmazát az R gyűrű egy bal oldali ideáljának nevezzük, ha tetszőleges $a, b \in R$ elemek esetén $a - b \in I$ és minden $a \in I$ és $r \in R$ elemre $ra \in I$ teljesül. A jobb oldali ideál fogalma a bal oldali ideál fogalmának duálisa. Egy R gyűrű nem üres I részhalmazát az R egy ideáljának nevezzük, ha I az R-nek bal oldali és egyben jobb oldali ideálja is.*

Tetszőleges R gyűrű esetén R és 0 mindig bal oldali, jobb oldali, illetve kétoldali ideálok; ezeket triviális bal oldali, jobb oldali, illetve kétoldali ideáloknak nevezzük.

Definíció 3.3.3 *(Egyszerű gyűrű) Egy R gyűrűt egyszerű gyűrűnek nevezünk, ha a triviális ideálokon kívül nincs R-nek más ideálja.*

Egy R gyűrű tetszőleges sok ideáljának metszete is ideálja R-nek, így beszélhetünk egy gyűrű nem üres részhalmaza által generált ideálról, azaz a részhalmazt tartalmazó összes ideál metszetéről. Az $a_1, \ldots, a_n \in R$ elemek által generált ideált $(a_1, \ldots, a_n)$ módon jelöljük. Hasonló állítás érvényes az egyoldali ideálokra is. Az $a_1, \ldots, a_n \in R$ elemek által generált bal oldali ideált $(a_1, \ldots, a_n)_b$ módon, a jobb oldali ideált $(a_1, \ldots, a_n)_j$ módon jelöljük.

Az egy elem által generált ideálokat főideáloknak nevezzük. Könnyen ellenőrízhető, hogy tetszőleges R gyűrű tetszőleges a eleme setén

$$(a)_b = \{na + ra : \ n \in \mathbb{Z}, \ r \in R\},$$

$$(a)_j = \{na + ar : \ n \in \mathbb{Z}, \ r \in R\},$$

$$(a) = \{na + ra + ar' + \sum_{\text{véges összeg}} r_i a r_i' : \ n \in \mathbb{Z}, \ r, r', r_i, r_i' \in R\}.$$

Ha az R gyűrű egységelemes, akkor

$$(a) = \sum_{\text{véges összeg}} r_i a r_i' : \ r_i, r_i' \in R\}.$$

Kommutatív egységelemes R gyűrű esetén

$$(a) = (a)_b = (a)_j = \{ra : \ r \in R\}.$$

3.4 Maradékosztálygyűrű (faktorgyűrű)

Legyen I egy R gyűrű ideálja. Akkor I az $(R;+)$ kommutatív csoport normális részcsoportja. Tekintsük az $(R;+)$ csoport I szerinti mellékosztályait (maradékosztályait): az $a+I$ alakú részhalmazokat.

Tétel 3.4.1 *Egy R gyűrű tetszőleges ideálja szerinti maradékosztályai a gyűrű kompatibilis osztűályozását adják. Megfordítva, gyűrű tetszőleges kompatibilis osztályozásának osztályai valamely ideál szerinti maradékosztályok.*

Bizonyítás. Legyen I egy R gyűrű ideálja. Az R gyűrű I szerinti $a+I$ maradékosztályai kompatibilisek az összeadásra nézve. Mivel tetszőleges $a+I$ és $b+I$ mellékosztályra $(a+I)(b+I) = ab + aI + Ib + II \subseteq ab + I$, ezért a maradékosztályok szerinti osztályozás kompatibilis a gyűrűbeli szorzásra nézve is. Tehát a gyűrű egy kompatibilis osztályozása.

Fordítva, tegyük fel, hogy adott az R gyűrűnek egy kompatibilis osztályozása. Csoportelméleti eredmények miatt a gyűrű 0-elemét tartalmazó I osztály részcsoportja az $(R;+)$ kommutatív csoportnak, és az osztályok az I szerinti $a+I$ alakú maradékosztályok. Mivel ez az osztályozás a szorzásra nézve is kompatibilis, ezért tetszőleges $a \in I$ és tetszőleges $r \in R$ elemek esetén az ra és ar szorzat abban a mellékosztályban van, amelyben az $r0 = 0$ és a $0r = 0$ szorzat van, azaz, $ra, ar \in I$. Tehát I az R gyűrű ideálja. □

Nem bizonyítjuk, de egyszerűen igazolható a következő tétel.

Tétel 3.4.2 *Egy R gyűrű tetszőleges I ideálja szerinti mellékosztályok halmaza az osztályok $(a+I)+(b+I) = (a+b)+I$ összeadására és $(a+I)(b+I) = ab + I$ szorzására nézve gyűrűt alkot (ennek neve: R-nek I szerinti faktorgyűrűje).*

3.5 Gyűrűk homomorfizmusa, izomorfizmusa

Definíció 3.5.1 *(Gyűrűk homomorfizmusa) Egy $(R;+,\cdot)$ gyűrűnek egy $(R';\oplus,\circ)$ gyűrűbe való φ leképezését homomorfizmusnak nevezzük, ha tetszőleges $a,b\in R$ elemekre*

$$\varphi(a+b)=\varphi(a)\oplus\varphi(b) \quad \text{és} \quad \varphi(ab)=\varphi(a)\circ\varphi(b)$$

teljesül. Ha φ szürjektív, akkor azt mondjuk, hogy φ epimorfizmus, és R' az R epimorf képe. Ha φ szürjektív és injektív, akkor φ-t izomorfizmusnak nevezzük; ekkor azt mondjuk, hogy R és R' izomorfak.

Definíció 3.5.2 *(Homomorfizmus magja) Ha φ egy R gyűrűnek egy R' gyűrűbe való homomorfizmusa, akkor φ magján az R gyűrű mindazon elemeinek összességét értjük, melyeknek a φ szerinti képe az R' gyűrű nulleleme.*

Tétel 3.5.3 *Egy R gyűrű tetszőlege homomorfizmusának magja R-nek ideálja. Fordítva, R minden ideáljához van R-nek olyan homomorfizmusa, melynek magja I.*

Bizonyítás. Legyen φ egy R gyűrűnek egy R' gyűrűbe való homomorfizmusa. Ha R valamely a és b elemei φ magjának elemei, akkor $\varphi(a-b)=\varphi(a)-\varphi(b)=0'$ és tetszőlegse $r\in R$ elemre $\varphi(ra)=\varphi(r)\varphi(a)=\varphi(a)0'=0'$ és , hasonlóan, $\varphi(ar)=0'$, ahol $0'$ jelöli az R' gyűrű nullelemét. Tehát φ magja az R egy ideálja. Mivel minden R gyűrűnek tetszőleges I ideálja szerinti R/I faktorgyűrűre való természetes homomorfizmusának magja I, ezért a tételt bebizonyítottuk. □

Tétel 3.5.4 *(Gyűrűk homomorfizmustétele) Ha az R' gyűrű az R gyűrű epimorf képe, és I ennek az epimorfizmusnak a magja, akkor $R'\cong R/I$.*

Tétel 3.5.5 *(Gyűrűk I. izomorfizmustétele) Ha I az R gyűrű ideálja, A pedig egy részgyűrűje, akkor $A\cap I$ az A ideálja, és $A+I/I\cong A/A\cap I$.*

Tétel 3.5.6 *(Gyűrűk II. izomorfizmustétele) Ha I és J az R gyűrű olyan ideáljai, amelyekre $I \subseteq J$ teljesül, akkor J/I az R_I ideálja, és $(R/I)/(J/I) \cong R/J$.*

3.6 Gyűrűk beágyzási tételei

Tétel 3.6.1 *Minden gyűrű beágyazható ideálként egy egységelemes gyűrűbe.*

Bizonyítás Képezzük az adott R gyűrű alaphalmazának és az egész számok $\mathbb{Z}$ halmazának $R^* = R \times \mathbb{Z}$ Descartes szorzatát! Az R^* halmazon értelmezzük az egyenlőséget a szokásos módon, azaz $(a, n) = (b, m)$ akkor és csak akkor, ha $a = b$ és $n = m$. Az R^* halmazon értelmezünk egy összeadást és egy szorzást a következőképpen: tetszőleges R^*-beli (a, n) és (b, m) elemek esetén

$$(a, n) + (b, m) = (a + b, n + m)$$

és

$$(a, n)(b, m) = (ab + nb + ma, nm).$$

Az világos, hogy $(R^*; +)$ az R gyűrű additív csoportjának és az egész számok additív csoportjainak direkt összege, így $(R^*; +)$ kommutatív csoport. R^* a szorzásra nézve félcsoport, mert a szorzás asszociatív:

$$[(a, n)(b, m)](c, k) = (ab + nb + ma, nm)(c, k) =$$

$$= (abc + nbc + mac + nmc + kab + knb + kma, nmk) =$$

$$= (a, n)(bc + mc + kb, mk) = (a, n)[(b, m)(c, k)].$$

A szorzás mindkét oldalról disztributív az összeadásra nézve (csak a balról való disztributivitást részletezzük, a másik oldali hasonlóan igazolható):

$$(a, n)[(b, m) + (c, k)] = (a, n)(b + c, m + k) =$$

$$= (a(b + c) + n(b + c) + (m + k)a, n(m + k)) =$$

$$= (ab + nb + ma + ac + nc + ka, nm + nk) = (a, n)(b, m) + (a, n)(c, k).$$

Tehát R^* gyűrű. Mivel R^* minden (a, n) elemére

$$(0, 1)(a, n) = (a, n) \quad \text{és} \quad (a, n)(0, 1) = (a, n),$$

ezért $(0, 1)$ az R^* egységeleme. Az R gyűrű tetszőleges a és b elemei, valamint tetszőleges m egész szám esetén

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

és

$$(a, 0)(b, m) = (ab + 0b + ma, 0), (b, m)(a, 0) = (ba + ma + 0b, 0)$$

ezért az R^* gyűrű $(a, 0)$ alakú elemei az R^* egy I_R ideálját alkotják. A $\varphi : a \mapsto (a, 0)$ leképezés az R gyűrűnek az I_R ideálra való injektív leképezése. Tetszőleges $a, b \in R$ elemekre

$$\varphi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \varphi(a) + \varphi(b)$$

és

$$\varphi(ab) = (ab, 0) = (a, 0)(b, 0) = \varphi(a)\varphi(b).$$

Tehát φ az R gyűrűnek az I_R ideálra való injektív homomorfizmusa, azaz az R gyűrűnek az R^* egységelemes gyűrűbe ideálként való beágyazása. □

Tétel 3.6.2 *Legyen R olyan kommutatív gyűrű, amelyben a nem 0-osztók M halmaza nem üres. Akkor R beágyazható részgyűrűként olyan $\overline{R}$ egységelemes kommutatív gyűrűbe, amelyben M minden elemének van inverze. Az $\overline{R}$ gyűrű úgy is megválasztható, hogy annak minden eleme ra^{-1} alakban írható ($r \in R$, $a \in M$). Az ilyen tulajdonságú $\overline{R}$ gyűrű izomorfizmus erejéig egyértelműen van meghatározva.*

Bizonyítás. Az $R \times M$ Descartes szorzaton definiálunk egy összeadást és egy szorzást a következőképpen: tetszőleges $R \times M$-beli (r, a) és (s, b) elemek esetén

$$(r, a) + (s, b) = (rb + sa, ab)$$

és

$$(r, a)(s, b) = (rs, ab).$$

Definiálunk az $R \times M$ halmazon egy $=$ egyenlőség relációt is:

$$(r, a) = (s, b) \quad \text{akkor és csak akkor, ha} \quad rb = sa.$$

Nem részletezzük, de könnyen igazolható, hogy ez a reláció ekvivalencia-reláció, amely meghatározza az $R \times M$ halmaz egy osztályozását. Megmutatjuk, hogy ez az osztályozás kompatibilis az előzőekben definiált két műveletre nézve. Ugyanis, ha $(r, a) = (r', a')$ és $(s, b) = (s', b')$, azaz, $ra' = r'a$ és $sb' = s'b$, akkor

$$(rb + sa, ab) = (r'b' + s'a', a'b'),$$

mert

$$(rb + sa)a'b' = rba'b' + saa'b' = r'abb' + s'baa' = (r'b' + s'a')ab.$$

Ugyancsak igaz, hogy

$$(rs, ab) = (r's', a'b'),$$

mert $(rsa'b' = r'as'b$. Ezért

$$(r, a) + (s, b) = (rb + sa, ab) = (r'b' + s'a', a'b') = (r', a') + (s', b')$$

és

$$(r, a)(s, b) = (rs, ab) = (r's', a'b') = (r', a')(s', b').$$

Tehát a szóban forgó osztályozás valóban kompatibilis mindkét műveletre nézve. Jelölje $\overline{R}$ az $(R \times M)/=$ faktorhalmazt. Jelölje $[r, a]$ az $(r, a) \in R \times M$ elemet tartalmazó $=$-osztályt. Két osztály között definiáljunk egy összeadást és egy szorzást a következőképpen: tetszőleges $[r, a]$ és $[s, b]$ osztályok esetén legyen

$$[r, a] + [s, b] = [rb + sa, ab]$$

és

$$[r, a][s, b] = [rs, ab].$$

Nem részletezzük, de egyszerűen igazolható, hogy $\overline{R}$ kommutatív gyűrű erre a két műveletre nézve. A $(0, a)$ $(a \in M)$ alakú elemekről meg lehet mutatni, hogy egy osztályt alkotnak, és $[0, a]$ az $\overline{R}$ nulleleme. Az $[r, a]$ osztály ellentettje (negatívja) a $[-r, a]$ osztály. Az (a, a) alakú elemek (itt $a \in M$) is egy osztályt alkotnak. Az $[a, a]$ osztály az $\overline{R}$ gyűrű egységeleme. Adott $r \in R$ elem esetén az összes (ra, a) alakú elemek is egy osztályt alkotnak.

A $\varphi : r \mapsto [ra, a]$ hozzárendelés az R gyűrűnek az $\overline{R}$ gyűrűbe való injective leképezése. Könnyen igazolható, hogy ez a leképezés homomorfizmus, és így az R gyűrűnek az $\overline{R}$ gyűrűbe való beágyazása. Mivel gyűrű homomorf képe is gyűrű, ezért részgyűrűként való beágyazása. Azonosítsuk az $\overline{R}$ gyűrű r elemét a neki megfeleltetett $[ra, a]$ osztállyal. Tetszőleges $a, b \in M$ elemekre igaz, hogy

$$a[b, ab] = [ab, b][b, ab] = [ab^2, ab^2].$$

Mivel az $[ab^2, ab^2]$ osztály az $\overline{R}$ gyűrű egységeleme, ezért a $[b, ab]$ osztály az $a = [ab, b]$ elem inverze. Tehát M minden elemének van inverze az $\overline{R}$ gyűrűben. Az $\overline{R}$ gyűrű tetszőleges $[r, a]$ elemére

$$[r, a] = [rb^2, ab^2] = [rb, b][b, ab] = ra^{-1}.$$

Tehát $\overline{R}$ minden eleme a tételben említett módon írható fel.

Tegyük fel, hogy R' is olyan gyűrű, amelybe az R gyűrű beágyazható olymódon részgyűrűként, hogy M minden elemének van inverze R'-ben és R' minden eleme ra^{-1} alakban írgató fel valamely $r \in R$ és $a \in M$ elem segtségével. Feltehetjük, hogy R mindkét gyűrűben benne van részgyűrűként. Ha R elemeit önmaguknak feleltetjük meg, akkor ezzel az $\overline{R}$ és R' gyűrűk egy-egy részgyűrűje között létesítünk izomorfizmust. Ha minden $a \in M$ elem $\overline{R}$-beli a^{-1} és R'-beli a'^{-1} inverzét egymásnak feletetjük meg, akkor a $\varphi : ra^{-1} \mapsto ra^{-1}$ megfeleltetés az az $\overline{R}$ gyűrűnek az R' gyűrűre való izomorfizmusa. □

Az előző tételben szereplő $\overline{R}$ gyűrűt az R gyűrű hányadosgyűrűjének (vagy kvóciensgyűrűjének) nevezzük. Ha ez a gyűrű test, akkor hányadostestnek nevezzük.

Tétel 3.6.3 *Minden integritási tatománynak van hányadosteste, amely izomorfizmus erejéig egyértelmű.*

Bizonyítás. Ha R integritási tartomány, akkor R nem 0-osztóinak M halmaza az R nem 0 elemeiből áll. Ez esetben a hányadosgyűrű már test, mert a 0-tól különböző elemei ab^{-1} alakúak ($a, b \in M$), és az ab^{-1} elemnek a ba^{-1} elem inverze. □

3.7 Gyűrűk karakterisztikája

Definíció 3.7.1 *(Gyűrű karakterisztikája) Azt mondjuk, hogy az R gyűrű karakterisztikája az n pozitív egész szám, ha R minden r elemére $nr = 0$ teljesül, és n a legkisebb ilyen tulajdonságú pozitív egész. Azt mondjuk, hogy az R gyűrű karakterisztikája 0, ha R minden a eleme és minden n pozitív egész szám esetén az $na = 0$ feltételből $a = 0$ következik.*

Ha egy gyűrűnek van karakterisztikája, akkor az egyértelműen meghatározott. Például, a $\mathbb{Z}_m$ maradékosztálygyűrű karakterisztikája m. A racionális számok, a valós számok, a komplex számok testének karakterisztikája 0. Az egyetlen elemből álló 0-gyűrű karakterisztikája 1.

Tétel 3.7.2 *Nullosztómentes gyűrű karakterisztikája 0, 1, vagy prímszám.*

Bizonyítás. Legyen R nullosztómentes gyűrű. Ha $R = \{0\}$, akkor R karakterisztikája 1. Tegyük fel, hogy R karakterisztikája nem 1 és nem 0. Akkor van olyan $0 \neq a \in R$ elem és olyan n pozitív egész szám, amelyekre $na = 0$ teljesül. n legyen a legkisebb ilyen tulajdonságú pozitív egész. Ha p egy prímosztója n-nek, akkor $n = pn'$, és ezért $0 = 0a = (na)a = pn'aa = (pa)(n'a)$, amiből $pa = 0$ vagy $n'a = 0$ következik. Az $n'a = 0$ nem teljesülhet, mert $p \geq 2$ miatt $n' < n$, ami ellentmond annak, hogy n a legkisebb olyan pozitív egész, amelyre $na = 0$. Tehát $pa = 0$. Mivel p sem lehet kisebb n-nél, ezért $n = p$. Legyen $b \in R$ tetszőleges. Akkor $0 = 0b = (pa)b = a(pb)$, amiből R nullosztómentessége miatt, $pb = 0$ következik, mivel $a \neq 0$. Tehát a p prímszám az R nullosztómentes gyűrű karakterisztikája. □

Tétel 3.7.3 *Ferdetest (és így test) karakterisztikája 0 vagy prímszám.*

Bizonyítás. Mivel minden ferdetest legalább két elemet tartalmaz és nullosztómentes, azért a Tétel 3.7.2 miatt ferdetest karakterisztikája 0 vagy prímszám. □

Példa 0-karakterisztikájú testre a racionális számok teste. Példa p-karakterisztikájú (p prímszám) testre a $\mathbb{Z}_p$ test.

Definíció 3.7.4 *(Prímtest) Prímtesteknek nevezzük azokat a testeket, amelyek a racionális számok teste és a $\mathbb{Z}_p$ testek (p prímszám) valamelyikével izomorfak.*

Tétel 3.7.5 *Tetszőleges ferdetest összes részferdetestének metszete prímtest. Ez a racionális számok testével vagy a $\mathbb{Z}_p$ testtel izomorf aszerint, hogy T karakterisztikája 0 vagy a p prímszám.*

Bizonyítás.

3.8 Egységelemes integritási tartományok

Definíció 3.8.1 *(Elem osztója) Egy R egységelemes integritási tartomány a és b elemeiről akkor mondjuk, hogy b osztója a-nak (jelben: $b|a$), ha megadható R-nek olyan c eleme, amelyre $a = bc$ teljesül. Ez azzal ekvivalens, hogy $(a) \subseteq (b)$.*

Az oszthatóság reflexív és tranzitív, de nem feltétlenül szimmetrikus.

Definíció 3.8.2 *(Asszociált elemek) Egységelemes R intgitási tartomány két eleméről, a-ról és b-ről azt mondjuk, hogy aszszociáltak, ha $a|b$ és $b|a$ (jelben: $a \sim b$).*

Tétel 3.8.3 *Egységelemes integritási tartomány elemei akkor és csak akkor asszociáltak, ha az általuk generált főideálok megegyeznek.*

Bizonyítás. Egy R egységelemes integritási tartomány a és b elemei asszociáltak akkor és csak akkor ha $a|b$ és $b|a$, azaz $(b) \subseteq (a)$ and $(a) \subseteq (b)$, ami azzal ekvivalens, hogy $(a) = (b)$. □

Definíció 3.8.4 *(Az egység fogalma) Egységelemes interitási tartomány egységelemének osztóit egységeknek nevezzük. Tehát egy R egységelemes integritási tartomány ϵ eleme akkor és csak akkor egysége R-nek, ha van inverze R-ben.*

Az egész számok gyűrűjében (amely egységelemes integritási tartomány) egységek az 1 és a -1.

Tétel 3.8.5 *Egy egységelemes integritási tartomány két eleme akkor és csak akkor asszociált, ha egység faktorban különböznek.*

Bizonyítás. Legyenek a és b egy R egységelemes integritási tartomány asszociált elemei. Feltehetjük, hogy $a \neq 0$ és $b \neq 0$. Mivel $a|b$ és $b|a$, azért megadhatók R-nek olyan x és y elemei, hogy $ax = b$ és $by = a$. Ebből $axy = a$, azaz, $a(xy - 1) = 0$ adódik. Mivel R integritási tartomány és $a \neq 0$, ezért $xy = 1$, azaz x és y egységek. Tehát a és b egység faktorban különböznel.

Fordítva, tegyük fel, hogy a és b egy R egységelemes integritási tartomány olyan elemei, amelyekre $a = \epsilon_1 b$ és $b = \epsilon_2 a$ teljesül valamely R-beli ϵ_1 és ϵ_2 egységekkel. Ekkor $a|b$ és $b|a$, azaz a és b asszociáltak. □

Definíció 3.8.6 *(legnagyobb közös osztó) Egy egységelemes integritási tartomány valamely d elemét az R-beli a és b elemek legnagyobb közös osztójának nevezzük, ha d osztója a-nak is és b-nek is, és az a és b elemek bármely c közös osztójára $c|d$ teljesül.*

Megjegyzés 3.8.7 Ha d legnagyobb közös osztója a-nak és b-nek, akkor tetszőleges ϵ egység esetén $d\epsilon$ is legnagyobb közös osztója a-nak és b-nek. Továbbá, ha d és d' az a és b elemek legnagyobb közös osztói, akkor $d \sim d'$, és így van olyan ϵ egység, hogy pl. $d' = d\epsilon$.

Definíció 3.8.8 *(Irreducibilis elem) Egy egységelemes integritási tartomány valamely nem nulla, nem egység d elemét irreducibilis elemnek nevezzük, ha tetszőleges $a, b \in R$ elemek esetén a $d = ab$ feltételből $d \sim a$ vagy $d \sim b$ következik. Megjegyezzük, hogy $d \sim a$ esetén b egység, a $d \sim b$ esetén pedig a egység.*

Az egész számok gyűrűjében a prímszámok az irreducibilis elemek. Test feletti polinomok gyűrűjében az irreducibilis polinomok az irreducibilis elemek.

Tétel 3.8.9 *Ha d irreducibilis eleme egy egységelemes integritási tartománynak, akkor tetszőleges ϵ egységgel képezett szorzata is irreducibilis elem.*

Bizonyítás. Legyen d egy R egységelemes integritási tartomány irreducibilis eleme, ϵ pedig az R egy egysége. Az világos, hogy $d\epsilon$ nem nulla és nem egység. Tegyük fel, hogy $d\epsilon = ab$ valamely $a, b \in R$ elemekre. Akkor $d = a(b\epsilon^{-1})$, és ezért $d \sim a$ vagy $d \sim b\epsilon^{-1}$. A $d \sim a$ esetben $d = ax$ és $a = dy$ $(x, y \in R)$. A $d = ax$ egyenlőségből $d\epsilon = ax\epsilon$ következik, így $a|d\epsilon$. Az $a = dy$ egyenlőség $a = d\epsilon\epsilon^{-1}y$ alakban is írható, ezért $d\epsilon|a$. Tehát $d\epsilon \sim a$. Ha $d \sim b\epsilon^{-1}$, akkor $d|b\epsilon^{-1}$ és $b\epsilon^{-1}|d$. A $d|b\epsilon^{-1}$ feltételből $b\epsilon^{-1} = dx$, $(x \in R)$ következik, és ezért $b = d\epsilon x$, ami miatt $d\epsilon|b$. A $b\epsilon^{-1}|d$ feltételből $d = yb\epsilon^{-1}$ $(y \in R)$ következik, amiből pedig $d\epsilon = yb$ adódik; tehát $b|d\epsilon$. Így $d\epsilon \sim b$. Tehát a $d\epsilon = ab$ feltételből $d\epsilon \sim a$ vagy $d\epsilon \sim b$ következik, ami bizonyítja, hogy $d\epsilon$ irreducibilis. □

Definíció 3.8.10 *(Prímelem) Egy egységelemes integritási tartomány valamely nem nulla, nem egység p elemét prímelemnek nevezzük, ha tetszőleges $a, b \in R$ elemek esetén a $p|ab$ feltételből $p|a$ vagy $p|b$ következik.*

Az egész számok gyűrűjében a prímszámok a prímelemek.

Tétel 3.8.11 *Ha p prímeleme egy egységelemes integritási tartománynak, akkor tetszőleges egységgel képezett szorzata is prímelem.*

Bizonyítás. Legyen p egy R egységelemes integritási tartomány prímeleme, ϵ pedig az R egy egysége. Tegyük fel, hogy $p\epsilon|ab$ valamely $a, b \in R$ elemekre. Akkor $xp\epsilon = ab$ valamely $x \in R$ elemmel, és így $p|a(b\epsilon^{-1})$. Mivel p prímelem, ezért $p|a$ vagy $p|b\epsilon^{-1}$. Ha $p|a$, akkor $py = a$ valamely $y \in R$ elemmel. Ez így is írható: $p\epsilon\epsilon^{-1}y = a$, ami miatt $p\epsilon|a$. Ha $p|b\epsilon^{-1}$, akkor $pz = b\epsilon^{-1}$ valamely $z \in R$ elemmel. Ebből $p\epsilon z = b$, azaz $p\epsilon|b$ következik. Tehát a $p\epsilon|ab$ feltételből $p\epsilon|a$ vagy $p\epsilon|b$ következik. Így $p\epsilon$ prímelem. □

Tétel 3.8.12 *Egységelemes integritási tartomány minden prímeleme irreducibilis elem.*

Bizonyítás. Legyen p egy R integritási tartomány prímeleme. Tegyük fel, hogy $p = ab$ valamely R-beli a és b elemekkel. Ekkor $a|p$ és $b|p$. Mivel p prímelem, ezért $p|a$ vagy $p|b$. Az első esetben $p \sim a$, a második esetben $p \sim b$. Tehát p irreducibilis elem. □

Megjegyezzük, hogy hogy az előző tétel állításának megfordítása általában nem igaz. Az $R = \{x + yi\sqrt{5} : \ a, b \in F\}$ egységelemes integritási tartományban $3|9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$, de $3 \not| (2 + i\sqrt{5})$ és $3 \not| (2 - i\sqrt{5})$, tehát 3 nem prímelem. Viszont 3 irreducibilis elem. Tegyük fel, hogy $3 = ab$ teljesül R valamely a és b elemeire. Tetszőleges R-beli $x+yi\sqrt{5}$ elemre legyen $N(x + yi\sqrt{5}) = x^2 + 5y^2$. Akkor $9 = N(3) = N(ab) = N(a)N(b)$, amiből $N(a) = 1$ és $N(b) = 9$ vagy $N(a) = 9$ és $N(b) = 1$ vagy $N(a) = N(b) = 3$ adódik. Megmutatható, hogy $N(A) = 1$ akkor és csak akkor, ha a egység. Ha $a = x+yi\sqrt{5}$, akkor $N(a) = x^2+5y^2$. Így az $N(a) = N(b) = 3$ egyenlőség nem lehetséges. Ugyanis, ha $x^2 + 5y^2 = 3$, akkor $y \neq 0$ nem lehet (ekkor már a második tag legalább 5), tehát $y = 0$, viszont $x^2 = 3$ sem teljesülhet, hiszen x egész szám. Tehát csak $N(a) = 1$ és $N(b) = 9$ vagy $N(a) = 9$ és $N(b) = 1$ teljesülhet. Ekkor a egység és így $p \sim b$, vagy b egység, és így $p \sim a$. Tehát 3 irreducibilis elem, de nem prímelem.

3.9 Gauss-gyűrűk

Definíció 3.9.1 *(Gauss-gyűrű) Egy egységelemes integritási tartományt Gauss-gyűrűnek nevezünk, ha minden 0-tól és egységtől különböző eleme felbontható - a sorrendtől és asszociálttól eltekintve - egyértelműen véges sok irreducibilis elem szorzatára.*

Az egész számok gyűrűje Gauss-gyűrű. Például -30 előáll $3 \cdot (-2) \cdot 5 = (-2) \cdot 3 \cdot 5 = 2 \cdot (-3) \cdot 5 = (-2) \cdot (-3) \cdot (-5)$ szorzatok formájában. Az egyes szorzatok a tényezők sorrendjében különböznek, vagy abban, hogy az egyik szorzatban szereplő prímszám helyett a másik szorzatban a prímszám (-1)-szerese (azaz egy asszociáltja) szerepel.

Lemma 3.9.2 *Gauss-gyűrű minden irreducibilis eleme prímelem.*

Bizonyítás. Legyen d az R Gauss-gyűrű egy irreducibilis eleme. Legyenek $a, b \in R$ tetszőleges elemek. Tegyük fel, hogy $d|ab$, azaz $ab = dc$ teljesül valamely $c \in R$ elemre. Ha $a = 0$ vagy $b = 0$, akkor $d|a$ és $d|b$. Ha a és b valamelyike egység, akkor ab is egység, amiből adódik, hogy d is egység, ami nem lehetséges, mert d irreducibilis elem. Vizsgálhatjuk tehát azt az esetet,

amikor a és b egyike sem nulla és egyike sem egység. Ekkor $c \neq 0$ is teljesül. Ha c nem egység, akkor előáll

$$c = c_1 \cdots c_k$$

alakban irreducibilis tényezőkkel. Tekintsük az a és b elemeknek irreducibilis tényezőkre való bontását:

$$a = a_1 \cdots a_m,$$
$$b = b_1 \cdots b_n.$$

Akkor

$$a_1 \cdots a_m b_1 \cdots b_n = dc$$

vagy

$$a_1 \cdots a_m b_1 \cdots b_n = dc_1 \cdots c_k,$$

attól függően, hogy c egység vagy nem egység. Mivel d irreducibilis elem, ezért az R Gauss-gyűrűben egy elemnek két irreducibilis tényezőkre való felbontását kaptuk. A két oldalon lényegében véve ugyanazon irreducibilis elemeknek kell állni, legfeljebb más sorrendben és asszociáltan. A jobb oldalon az egyik irreducibilis tényező d. Ezért d valamely asszociáltjának a bal oldalon szerepelnie kell. Mivel két elem akkor és csak akkor asszociált, ha egységfaktorban különböznek, ezért d-nek is szerepelni kell a bal oldalon. Mivel a bal oldalon csak a és b irreducibilis tényezői szerepelnek, így valamelyikük felbontásában elő kell fordulni d egy asszociáltja, és ezért d az a és b elemek valamelyikének osztója. Tehát d prímeleme az R Gauss-gyűrűnek. □

Megjegyzés. Tudjuk, hogy minden egységelemes integritási tartományban minden prímelem irreucibilis elem. Ebből a tényből és az előző lemmából következik, hogy a Gauss-gyűrű definíciójában az irreducibilis elem kifejezés helyettesíthető a prímelem kifejezéssel. A következő tétel bizonyításában ez meg is történik.

Tétel 3.9.3 *Egy R egységelemes integritási tartomány akkor és csak akkor Gauss-gyűrű, ha R nem tartalmazza főideálok szigorúan növekvő láncát, és R-nek minden irreducibilis eleme prímelem.*

Bizonyítás. Legyen R egy Gauss-gyűrű. Akkor benne minden irreducibilis elem prímelem a Lemma 3.9.2 alapján. Tegyük fel, indirekt módon, hogy R főideáljainak van egy szigorúan növekvő lánca:

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \ldots$$

Jelölne n_1 az a_1 elem irreducibilis tényzőkre való felbontásában szereplő irreducibilis elemek számát. Mivel $(a_1) \subset (a_2)$, ezért $a_2|a_1$, amiből következik, hogy az a_1 elem irreducibilis tényezőkre való felbontásában szereplő irreducibilis elemek között ott szerepelnek az a_2 irreducibilis tényezőkre való felbontásában szereplő irreducibilis elemek, de nem mindegyik. Ellenkező esetben a_1 és a_2 asszociáltak lennének, és ekkor $(a_1) = (a_2)$ teljesülne. Tehát a_2 irreducibilis tényezőkre való felbontásában n_1-nél kevesebb irreducibilis elem szerepel. Folytatva ezt az eljárást, kell lenni olyan i indexnek, hogy $(a_i) = (a_{i+1}) = \dots$. Ez ellentmondás. Tehát R nem tartalmaz főideálok szigorúan növekvő láncát.

Fordítva, tegyük fel, hogy R olyan egységelemes integritástartomány, amely nem tartalmazza főideálok szigorúan növekvő láncát, és R-nek minden irreducibilis eleme prímelem. Elegendő azt megmutatni, hogy R minden 0-tól és egységtől különböző eleme előáll (a sorrendtől és asszociálttól eltekintve) egyértelműen irreducibilis elemek szorzataként. Legyen $r \in R$ nem nulla és nem egység. Ha r irreducibilis elem, akkor , mert r önmagának egytényezős szorzata. Tegyük fel, hogy r nem irreducibilis. Megmutatjuk, hogy r előáll ds szorzat alakban, ahol d irreducibilis elem ($s \in R$). Mivel r nem irreducibilis, ezért vannak olyan $a_1, b_1 \in R$ elemek, hogy $r = a_1 b_1$ és sem a_1 sem b_1 nem asszociált r-rel (ekkor $(r) \subset (a_1)$ és $(r) \subset (b_1)$). Ha a_1 és a_2 egyike irreducibilis elem, akkor készen vagyunk. Ha nem, akkor pl. a_1 előáll $a_1 = a_2 b_2$ alakban, ahol a_2 és b_2 egyike sem asszociált a_1-gyel (és ezért $(a_1) \subset (a_2)$ és $(a_1) \subset (b_2)$). Ha a_2 és b_2 valamelyike irreducibilis, akkor készen vagyunk, mert $r = a_2 b_2 b_1$. Ha egyike sem az, akkor - folytatva az eljárást - kell, hogy legyen r-nek olyan $r = a_n b_n \cdots b_1$ előállítása, amelyben szereplő a_n és b_n valamelyike irreducibilis elem. Ellenkező esetben az

$$(r) \subset (a_1) \subset \cdots (a_n) \subset \cdots$$

végtelen lánchoz jutnánk, ami a feltétel miatt ellentmondáshoz vezetne. Tehát van R-nek olan d irreducibilis eleme, amelyre $r = ds$ teljesül ($s \in R$). Ha s egység, akkor készen vagyunk. Ha nem, akkor az előző gondolatmenetet s-re alkalmazva, s vagy irreducibilis (ekkor készen vagyunk), vagy előáll $s = d_1 s_1$ alakban, ahol d_1 irreducibilis ($s_1 \in R$). Világos, hogy $(r) \subset (d) \subset (d_1) \subset \cdots$. Mivel nem kaphatunk végtelen láncot, ezért kell, hogy legyen olyan n pozitív egész szám, hogy $r = d_1 d_2 \cdots d_n s$, ahol s egység. Tehát r előáll irreducibilis elemek szorzatatként.

Megmutatjuk, hogy az előállítás egyértelmű. Tegyük fel, hogy

$$p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_s$$

teljesül az R valamely primelemeire. Tegyük fel, hogy $s \geq t$. Mivel p_1 prímelem és p_1 osztja a jobb oldali szorzatot, ezért valamelyik tényezőnek (mondjuk q_1-nek) osztója. Mivel q_1 irreducibilis, ezért ebből $p_1 \sim q_1$ következik. A p_1 tényzővel osztva mindkét oldalt,

$$p_2 \cdots p_t = \epsilon_1 q_2 \cdots q_s$$

adódik, ahol ϵ_1 az R egy egysége. Folytatva az eljárást,

$$e = \epsilon_1 \epsilon_2 \cdots \epsilon_t q_{t+1} \cdots q_s$$

adódik. Ebből már következik, hogy $s = t$ (és a p_i és q_i tényezők csak egység faktorban különböznek, azaz asszociáltak). □

3.10 Főideálgyűrűk, euklideszi gyűrűk

Definíció 3.10.1 *(Főideálgyűrű) Egy egységelemes integritási tartományt főideálgyűrűnek nevezünk, ha minden ideálja főideál.*

Definíció 3.10.2 *(Maximális ideál) Egy R gyűrű M ideálját maximális ideálnak nevezünk, ha $M \neq R$ és R minden J ideáljára az $M \subseteq J \subseteq R$ feltételből $M = J$ vagy $J = R$ következik.*

Tétel 3.10.3 *Egy R főideálgyűrű valamely (d) ideálja akkor és csak akkor maximális ideál, ha d az R irreducibilis eleme.*

Bizonyítás. Egy R főideálgyűrű (d) ideálja akkor és csak akkor maximális ideál, ha $(0) \neq (d) \neq R$ (azaz d nem nulla és nem egységminden) és minden $a \in R$ elemre a $(d) \subseteq (a)$ feltételből (azaz abból a feltételből, hogy $a|b$) $(d) = (a)$ vagy $(a) = R$ (azaz $d \sim a$ vagy a egység) következik. Tehát (d) akkoe és csak akkor maximális ideál, ha d irreducibilis elem. □

Tétel 3.10.4 *Minden főideálgyűrű Gauss-gyűrű.*

Bizonyítás. Legyen R egy főideálgyűrű. Megmutatjuk, hogy R nem tartalmazza főideálok szigorúan növekvő láncát, és R-nek minden irreducibilis eleme prímelem. Tegyük fel, indirekt módon, hogy R főideáljainak van egy

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \ldots$$

szigorúan növekvő lánca. Legyen $I = \cup_{i=1}^{\infty}(a_i)$. Ha $a, b \in I$, akkor $a, b \in (a_j)$ valamely j indexre, és ezérz $a - b \in (a_j)$, amiből $a - b \in I$ következik. Ha $a \in I$, akkor $a \in (a_j)$ valamely j indexre, és ezért tetszőleges $r \in R$ elemre $ar \in (a_j) \subseteq I$ teljesül. Tehát I ideálja R-nek. Legyen $I = (c)$. akkor $c \in (a_k)$ valamely k indexre, és ezért $I \subseteq (a_t)$ minden $t \geq k$ indexre. Ez ellentmondás.

Annak bizonyítását, hogy R minden irreducibilis eleme prímelem, azzal kezdjük, hogy megmutatjuk: R bármely két elemének van legnagyobb közös osztója. Legyenek $a, b \in R$ tetszőleges elemek. Akkor van olyan $d \in R$ elem, hogy $(a, b) = (d)$. Mivel $(a) \subseteq (d)$ és $(b) \subseteq (d)$, ezért $d|a$ és $d|b$. Tegyük fel, hogy valamely $c \in R$ elemere $c|a$ és $c|b$ teljesül. Akkor $a = xc$ és $b = yc$, azaz $(a) \subseteq (c)$ és $(b) \subseteq (c)$ és ezért $(d) = (a, b) \subseteq (c)$. Ez azt jelenti, hogy $c|d$. Tehát d az a és b elemek legnagyobb közös osztója. A következőkben megmutatjuk, hogy tetszőleges $a, b, c \in R$ elemekre $c(a, b) = (ca, cb)$. Az (a, b) elemei az $ra + sb$ $(r, s \in R)$ alakú elemek. Így $c(a, b)$ elemei $rca + scb$ alakúak. Ezért $c(a, b) \subseteq (ca, cb)$. Fordítva, (ca, cb) elemei $rca + scb$ alakúak, amelyek a disztributivitás miatt $c(ra + sb)$ alakban írhatók. Ezért $(ca, cb) \subseteq c(a, b)$. Most pedig megmutatjuk, hogy minden ireducibilis elem prímelem. Legyen p irreducibilis elem. Tegyük fel, hogy $p|ab$ $(a, b \in R)$. Tegyük fel, hogy $p \not| a$. Megmutatjuk, hogy $p|b$. Mivel $p \not| a$, ezért $(a) \not\subseteq (p)$, és ezért $a \notin (p)$. Így $(p) \subset (p, a)$. Mivel p irreducibilis elem, ezért (p) maximális ideál a Tétel 3.10.3 miatt. Ezért $(p, a) = R$. Az világos, hogy $pb \in (p)$ és $ab \in (p)$. Így

$$(p) \supseteq (pb, ab) = (p, a)b = Rb = (b),$$

amiből már adodik, hogy $p|b$. □

Definíció 3.10.5 *(Euklideszi gyűrű) Egy egységelemes integritási tartományt euklideszi gyűrűnek nevezünk, ha minden nem nulla a eleméhez hozzá van rendelve egy $\varphi(a)$-val jelölt nemnegatív egész szám úgy, hogy minden $a \in R$ és $0 \neq b \in R$ eleméhez megadhatók olyan $q, r \in R$ elemek, hogy $a = bq + r$, ahol $r = 0$ vagy $\varphi(r) < \varphi(b)$.*

Tétel 3.10.6 *Minden euklideszi gyűrű főideálgyűrű.*

Bizonyítás. Legyen R egy euklideszi gyűrű. Legyen I az R egy ideálja. Feltehetjük, hogy $I \neq \{0\}$. Legyen b az I-nek olyan nem nulla eleme, amelyre teljesül, hogy minden $0 \neq a \in I$ elemre $\varphi(a) \geq \varphi(b)$ teljesül. Megmutatjuk, hogy $I = (b)$. Legyen $a \in I$ tetszőleges elem. Akkor megadhatók olyan $q, r \in R$ elemek, amelyekre $a = bq + r$ teljesül, valamint igaz az is, hogy $r = 0$ vagy $\varphi(r) < \varphi(b)$. Ha $r \neq 0$, akkor $r = a - bq \in I$ és $\varphi(r) < \varphi(b)$. Ez azonban ellentmond a b elem választásának. Így $r = 0$ lehet csak, azaz $a = bg \in (b)$. Így $I \subseteq (b)$, amiből $I = (b)$ következik. □

3.11 Noether-féle gyűrűk

Definíció 3.11.1 *(Maximum feltétel) Azt mondjuk, hogy az R gyűrűben a bal oldali ideálokra teljesül a maximum feltétel, ha R bali oldali ideáljainak tetszőleges nem üres halmazában van legalább egy maximális elem, azaz olyan, melyet valódi módon a tekintetbe vett halmazhoz tartozó egyetlen bal oldali ideál sem tartalmaz.*

Megjegyzés 3.11.2 Egy R gyűrűben a bal oldali ideálokra akkor és csak akkor teljesül a maximum feltétel, ha az R gyűrű bal oldali ideáljainak bármely

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n \subseteq \ldots$$

növekvő lánca esetén megadható olyan m index, hogy $L_m = L_{m+1} = \cdots$ Ezzel ekvivalens, hogy R bal oldali ideáljainak egyetlen szigorúan növekvő lánca sem lehet végtelen.

Tétel 3.11.3 *(E. Noether) Egy R gyűrűben akkor és csak akkor teljesül a bal oldali ideálokra a maximum feltétel, ha R bármely bal oldali ideálja végesen generált.*

Bizonyítás. Tegyük fel, hogy az R gyűrűben a bal oldali ideálokra teljesül a maximum feltétel. Legyen L az R egy bal oldali ideálja. Tekintsük R azon végesen generált bal oldali ideáljainak halmazát, amelyek benne vannak L-ben. A maximum feltétel miatt ezek között van egy maximális. Jelöljük ezt L^*-gal. Ha L^* nem egyezne meg L-lel, akkor lenne olyan a eleme R-nek, amely $L \setminus L^*$-ban helyezkedne el. Ekkor viszont az $L^* \cup a$ által (végesen) generált bal oldali ideál benne lenne L-ben és bővebb lenne L^*-nál. Ez ellentmondás. Tehát L megegyezik a végesen generált L^* bal oldali ideállal.

Fordítva, tegyük fel, hogy R minden bal oldali ideálja végesen generált. Legyen

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n \subseteq \ldots$$

az R bal oldali ideáljainak egy monoton növekvő lánca. Egyszerűen igazolható, hogy ezek L-lel jelölt uniója is bal oldali ideálja R-nek, és ezért ez végesen generálható, azaz $L = (a_1, a_2, \ldots, a_n)_b$. Ekkor megadható olyan m index, hogy a generáló elemek mindegyikét tartalmazza az L_m bal oldali ideál. Ekkor viszont $L \subseteq L_m \subseteq L_{m+1} \subseteq \ldots$. Innen már egyszerűen adódik, hogy $L_m = L_{m+1} = \cdots$ □

Definíció 3.11.4 *(Noether-gyűrű) Egy kommutatív R gyűrűt Noether-féle gyűrűnek nevezünk, ha R-ben teljesül az ideálokra a maximum feltétel, azaz R bármely ideálja végesen generált.*

Tétel 3.11.5 *(Hilbert bázis tétele) Ha R egységelemes Noether-gyűrű, akkor az $R[x]$ polinomgyűrű is Noether-féle.*

Bizonyítás. Legyen R egységelemes Noether-féle gyűrű. Legyen A az $R[x]$ polinomgyűrű tetszőleges ideálja. Megmutatjuk, hogy A végesen generálható. Jelölje C_n az A-hoz tartozó legfeljebb n-edfokú polinomok x^n-et tartalmazó tagjának együtthatóiból álló halmazt. Megmutatható, hogy C_n ideálja R-nek, és

$$C_0 \subseteq C_1 \subseteq \cdots \subseteq C_n \subseteq \ldots$$

Mivel R Noether-féle, ezért van olyan m index, hogy $C_m = C_{m+1} \ldots$ Legyenek a C_i $(i = 1, 2, \ldots, m)$ ideál generátorai $a_{i1}, \ldots, a_{ik_i}$. Jelöljön f_{ij} olyan A-beli i-edfokú polinomot, amelyben az x^i tag együtthatója a_{ij}. Megmutatható, hogy ezek a polinomok generálják az A ideált. Legyen f tetszőleges A-beli

polinom. Ha f foka 0, azaz $f \in R$, akkor $f \in C_0 = \{f_{01}, \ldots, f_{0k_0}\}$. Ha f foka $n > 1$ és az n-nél alacsonyabb fokúakról már tudjuk, hogy az f_{ij} polinomok által generált ideálhoz tartoznak, akkor az f polinom a kezdőegyütthatója

$$a = r_1 a_{n1} + \cdots + r_{k_n} a_{nk_n} \quad \text{vagy} \quad a = r_1 a_{m1} + \cdots + r_{k_m} a_{mk_m},$$

attól függően, hogy $n < m$ vagy $n \geq m$. De ekkor

$$f - r_1 f_{n1} + \cdots + r_{k_n} f_{nk_n} \quad \text{vagy} \quad f - x^{n-m}(r_1 f_{m1} + \cdots + r_{k_m} f_{mk_m})$$

n-nél kisebb fokszámú polinom, így eleme az f_{ij} polinomok által generált ideálnak, amiből már következik, hogy az f is eleme az f_{ij} polinomok által generált ideálnak. Mivel az f_{ij} polinomok mindegyike eleme A-nak, ebből már következik, hogy A megegyezik a véges sok f_{ij} polinom által generált ideállal. □

3.12 Dedekind-gyűrűk

Definíció 3.12.1 *(Balideálok szorzata) Legyenek A és B egy R gyűrű bal oldali ideáljai. Az AB szorzaton értjük az összes olyan $\sum_i a_i b_i$ véges összegek halmazát, amelyekben $a_i \in A$ és $b_i \in B$. Ez maga is bal oldali ideál, mert az ilyen összegek különbsége és R-beli elemmel balról vett szorzata is hasonló alakú.*

Hasonlóan értelmezhető jobb oldali ideálok, illetve egy A bal oldali és egy B jobb oldali ideál szorzata is. Megjegyezzük, hogy ha A bal oldali, B pedig jobb oldali ideálja egy R gyűrűnek, akkor AB ideálja R-nek.

Tétel 3.12.2 *Ha A és B egy R gyűrű kétoldali ideáljai, akkor $AB \subseteq A \cap B$. Ha az R kommutatív gyűrűben $A = (a_1, \ldots, a_n)$ és $B = (b_1, \ldots, b_m)$, akkor $AB = (a_1 b_1, \ldots a_1 b_m, a_2 b_1, \ldots a_n b_1, \ldots, a_n b_m)$, vagyis végesen generált ideálok szorzata is végesen generált.*

Definíció 3.12.3 *(Prímideál) Egy R kommutatív gyűrű valamely P ideálját prímideálnak nevezzük, ha R tetszőleges a és b elemei esetén az $ab \in P$ feltételből $a \in P$ vagy $b \in P$ következik.*

Tétel 3.12.4 *Egy R kommutatív gyűrű P ideálja akkor és csak akkor prímideál, ha az R/P faktorgyűrű nullosztómentes.*

Bizonyítás. Tetszőleges $a, b \in R$ elemek esetén $ab \in P$ akkor és csak akkor, ha az R/P faktorgyűrűben az $a+P$ és $b+P$ mellékosztályok sorzata 0. Így $ab \in P$-ből akkor és csak akkor következik $a \in P$ vagy $b \in P$, ha az R/P faktorgyűrűben az $(a+P)(b+P) = 0$ feltételből $a+P = 0$ vagy $b+P = 0$ következik, azaz, ha az R/P faktorgyűrű nullosztómenets. □

Tétel 3.12.5 *Egy R kommutatív gyűrű P ideálja akkor és csak akkor prímideál, ha az R gyűrű tetszőleges A és B ideáljaira $AB \subseteq P$-ből $A \subseteq P$ vagy $B \subseteq P$ következik.*

Bizonyítás. Tegyük fel, indirekt módon, hogy van olyan R kommutatív gyűrű és abban olyan P prímideál, valamint olyan A és B ideálok, amelyekre $AB \subseteq P$ teljesül, de $A \not\subseteq P$ és $B \not\subseteq P$. Legyenek $a \in A$ és $b \in B$ olyan elemek, amelyekre $a, b \notin P$ teljsül. Mivel P prímideál, ezért $ab \notin P$, és ezért $AB \not\subseteq P$, ami ellentmondás. Így egy kommutatív gyűrű minden P primideáljára teljesül, hogy az $AB \subseteq P$ feltételből $A \subseteq P$ vagy $B \subseteq P$ következik minden R-beli A és B ideálra.

Fordítva, tegyük fel, hogy P a kommutatív R gyűrű olyan ideálja, amelyre $AB \subseteq P$-ből $A \subseteq P$ vagy $B \subseteq P$ következik R minden A és B ideáljára. Tegyük fel, hogy $ab \in P$ az R valamely a és b elemeire. Az $ab \in P$ feltétel miatt $(ab) \in P$. Kommutatív gyűrűben $(ab) = (a)(b)$. Ezért $(a)(b) \in P$, amiből $(a) \subseteq P$, és így $a \in P$ vagy $(b) \subseteq P$, és így $b \in P$ következik. □

Tétel 3.12.6 *Egységelemes R kommutatív gyűrű M ideálja akkor és csak akkor maximális, ha az R/M faktorgyűrű test.*

Bizonyítás. Egységelemes R gyűrű M ideálja akkor és csak akkor maximális, ha az R/M faktorgyűrű egyszerű. Mivel R/M is kommutatív, ezért R/M vagy test vagy zérógyűrű. Ha R egységelemes, akkor R/M is, és ezért nem lehet zérógyűrű. Kaptuk tehát, hogy egységelemes kommutatív gyűrű M ideálja akkor és csak akkor maximális, ha az R/M faktorgyűrű test. □

Tétel 3.12.7 *Egységelemes kommutatív gyűrű minden maximális ideálja prímideál.*

Bizonyítás. Ha M egy egységelemes kommutatív gyűrű maximális ideálja, akkor az előző tétel miatt az R/M faktorgyűrű test. Mivel minden test nullosztómentes, ezért a 3.12.4 Tétel miatt M prímideál. □

Tétel 3.12.8 *Legyen K test. A $K[x]$ polinomgyűrűben egy M ideál akkor és csak akkor maximális ideál, ha M-et a $K[x]$ egy irreducibilis polinomja generálja.*

Bizonyítás. Mivel tetszőleges K test feletti $K[x]$ polinomgyűrű arkhimédeszi gyűrű, ezért főideálgyűrű is. Így a Tétel 3.10.3-ből már következik a jelen tétel állítása.

□

Definíció 3.12.9 *(Dedekind-gyűrű) Egy R egységelemes integritási tartományt Dedekind-gyűrűnek nevezünk, ha R minden nem zérus A ideálja (sorrendtől eltekintve) egyértelműen írható az*

$$A = P_1 P_2 \cdots P_k \quad (k \geq 1)$$

szorzat alakban, ahol a P_i-k R-től különböző prímideálok.

Tétel 3.12.10 *Egy R integritási tartomány akkor és csak akkor Dedekind-gyűrű, ha*

(1) R-ben teljesül az ideálokra a maximum-feltétel,

(2) R tetszőleges A ideáljához van olyan $B \neq \{0\}$ ideál, hogy $AB = (c)$ főideál.

3.13 Teljes mátrixgyűrűk

Közismert a következő tétel.

Tétel 3.13.1 *Tetszőleges R gyűrű elemeiből képezett $n \times n$-típusú mátrixok $M_n(R)$ halmaza a mátrixok összeadására és szorzására nézve gyűrűt alkot (ezt az R gyűrű feletti teljes mátrixgyűrűnek nevezzük). Ha R egységelemes, akkor az $M_n(R)$ teljes mátrixgyűrű is egységelemes. $n \geq 2$ esetén az $M_n(R)$ teljes mátrixgyűrű általában nem kommutatív, még akkor sem, ha az R gyűrű kommutatív. Ha R egységelemes kommutatív gyűrű, akkor az $M_n(R)$ teljes mátrixgyűrű valamely A mátrixának akkor és csak akkor van inverze, ha A determinánsa az R gyűrű egysége, azaz (R-ben) van inverze.*

Tétel 3.13.2 *F ferdetes feletti $M_n(F)$ teljes mátrixgyűrű egyszerű.*

Bizonyítás. Legyen I az $M_n(F)$ gyűrű nullától különböző ideálja. Legyen A az I-hez tartozó tetszőleges nem nulla mátrix. Legyen a_{ik} az A egy nem nulla eleme. Jelölje E_{ij} azt az $M_n(F)$-beli mátrixot, melynek az i-dik sorában álló j-dik elem a test egységeleme, az összes többi eleme pedig a test nulleleme. Felhasználva azt, hogy I ideál és $A \in I$, kapjuk, hogy

$$(E_{ji}a_{ik}^{-1})AE_{kt} \in I$$

tetszőleges $j, t \in \{1, , 2, \ldots, n\}$ indexre. Mivel $M_n(F)$ az F test feletti vektortér, ezért $M_n(F)$ tetszőleges C mátrixához megadhatók olyan $c_{ij} \in F$ elemek, hogy

$$C = \sum_{i,j=1}^{n} c_{ij}E_{ij} = c_{ij}E_{ii}E_{ij} \in I.$$

Ezért $M_n(F) \subseteq I$, és így $I = M_n(F)$. Így az F test feletti $M_n(F)$ teljes mátrixgyűrű egyszerű. □

Tétel 3.13.3 *Egy F ferdetest feletti $M_n(F)$ teljes mátrixgyűrű L bal oldali ideáljához tartozó mátrixok sorvektorai az F test feletti F^n vektrotérnek egy $F^n(L)$ alterét alkotják. Az $L \mapsto F^n(L)$ megfeleltetés bijektív az $M_n(F)$ gyűrű összes bal oldali ideála és az F^n vektortér alterei között. Ennél a megfeleltetésnél az F^n vektortér egy W alterének az az L bal olali ideál felel meg, mely az összes olyan mátrixokból áll, melyeknek sorvektorai W-ből valók.*

3.14 Féligegyszerű gyűrűk

Definíció 3.14.1 *(Minimum feltétel) Azt mondjuk, hogy az R gyűrűben a bal oldali ideálokra teljesül a minimum feltétel, ha R bali oldali ideáljainak tetszőleges nem üres halmazában van legalább egy minimális elem, azaz olyan, mely valódi módon a tekintetbe vett halmazhoz tartozó bal oldali ideálok egyikét sem tartalmazza.*

Megjegyzés 3.14.2 Egy R gyűrűben a bal oldali ideálokra akkor és csak akkor teljesül a minimum feltétel, ha az R gyűrű bal oldali ideáljainak bármely

$$L_1 \supseteq L_2 \supseteq \cdots \supseteq L_n \supseteq \dots$$

csökkenő lánca esetén megadható olyan m index, hogy $L_m = L_{m+1} = \cdots$ Ezzel ekvivalens, hogy R bal oldali ideáljainak egyetlen szigorúan csökkenő lánca sem lehet végtelen.

Definíció 3.14.3 *(Nilpotens elem, nilpotens balideál) Egy R gyűrű a elemét nilpotens elemnek nevezzük, ha megadható olyan n pozitív egész szám, amelyre $a^n = 0$ teljesül. Az R gyűrű egy L bal oldali ideálját nilpotensnek nevezzük, ha $L^n = \{0\}$ teljesül valamely n pozitív egész számra, azaz az L elemeiből képezett n-tényezős szorzatok mindegyike 0.*

Egy nilpotens bal oldali ideál minden eleme nilpotens. Az viszont általában nem igaz, hogy ha egy L bal oldali ideál minden eleme nilpotens, akkor L nilpotens.

Definíció 3.14.4 *(Féligegyszerű gyűrű) Egy R gyűrűt féligegyszerűnek nevezünk, ha*

(1) R bal oldali ideáljaira teljesül a minimum feltétel, és

(2) R nem tartalmaz a 0-tól különböző nilpotens bal oldali ideált.

Lemma 3.14.5 *Egy R féligegyszerű gyűrű tetszőleges L bal oldali ideáljához megadható R-nek olyan e idempotens eleme, hogy $L = Re$.*

Definíció 3.14.6 *(Direkt összeg) Azt mondjuk, hogy egy R gyűrű az $L_1, \ldots, L_k$ bal oldali ideálok direkt összege, ha R additív csoportja az $L_1, \ldots . L_k$ részcsoportok direkt összege.*

Definíció 3.14.7 *(Minimális balideál) Egy R gyűrű valamely M bal oldali ideálját minimális bal oldali ideálnak nevezzük, ha $M \neq \{0\}$ és az R minden A bal oldali ideáljára a $\{0\} \subseteq A \subseteq M$ feltételből $\{0\} = A$ vagy $A = M$ következik.*

A minimális jobb oldali ideál fogalma a minimális bal oldali ideál fogalmának duálisa.

Tétel 3.14.8 *(Noether) Minden féligegyszerű gyűrű véges sok minimális bal oldali ideáljának direkt összege; ezen bal oldali ideálok mindegyike idempotenssel generálható.*

Bizonyítás. Legyen R tetszőleges féligegyszerű gyűrű. Akkor R-nek van egy L_1 minimális bal oldali ideálja, amelyet idempotens generál az előző lemma szerint, azaz van R-nek olyan e_1 idempotens eleme, hogy $L_1 = Re_1$. Legyen $L' = \{(x - xe_1 : \ x \in R\}$. Megmutatható, hogy L' az R egy olyan bal oldali ideálja, melyre $L \cap L' = \{0\}$ teljesül. (Ugyanis, ha $re_1 = x - xe_1$, akkor $re_1 = (re_1)e_1 = (x - xe_1)e_1 = xe_1 - xe_1 = 0$.) Az R tetszőleges r eleme előáll $r = re_1 + r - re_1$ alakban, ezért $L_1 = Re_1$ és L' generálják R additív csoportját. Tehát $(R; +)$ előáll az L_1 és L' részcsoportok direkt összegeként. Így az R gyűrű az L_1 és L' bal oldali ideálok direkt összege: $R = L_1 \oplus L'$. Ezek szerint R minden minimális bal oldali ideálja az R egy direkt összeadandója. Ha $L' = \{0\}$, akkor készen vagyunk a bizonyítással. Ha nem, akkor legyen L_2 az R gyűrű L' által tartalmazott egyik minimális bal oldali ideálja. Erre ugyancsak érvényes, hogy $R = L_2 \oplus L''$. Itt $L_2 = Re_2$ és $L'' = \{x - xe_2 : \ x \in R\}$. Ezt a felbontást alkalmazva az L' elemeire,

adódik, hogy $L' = L_2 \oplus (L' \cap L'')$, és így $R = L_1 \oplus L_2 \oplus (L' \cap L'')$. Folytatva ezt az eljárást, véges sok lépésben eljutunk az

$$R = L_1 \oplus L_2 \oplus \cdots \oplus L_k$$

direkt felbontáshoz, mivel $L' \supset L' \cap L'' \supset \cdots$. Az előző lemma szerint az L_i $(i = 1, \ldots, k)$ bal oldali ideálok idempotens elemmel generálhatók. □

Lemma 3.14.9 *Ha A egy féligegyszerű R gyűrű kétoldali ideálja, akkor A-nak mint gyűrűnek van egységeleme, és R-nek van olyan kétoldali B ideálja, hogy $R = A \oplus B$.*

A következő tétel bizonyítása előtt megjegyezzük, hogy ha A és B egy R gyűrű olyan ideáljai, amelyekre $R = A \oplus B$ teljesül, akkor A és B egyoldali, illetve kétoldali ideáljai az R-nek is egyoldali, illtve kétoldali ideáljai. Ugyanis, ha $a \in A$ és $b \in B$, akkor $ab \in A \cap B = \{0\}$, és ezért $ab = 0$. Tehát az $r = a + b$ és $r' = a' + b'$ $(a, a' \in A, b, b' \in B)$ elemek szorzatára $rr' = aa' + bb'$ adódik (mert $ab' = 0 = a'b$). Ha I az A egy bal oldali ideálja, akkor $I = I + \{0\}$ és ezért tetszőleges $r = a + b \in R$ $(a \in A, b \in B)$ elemre $rI = (a + b)(I + \{0\}) = aI + \{b0\} \subseteq I + \{0\} = I$. Tehát I az R-nek is bal oldali ideálja. Hasonlóan, A tetszőleges kétoldali ideálja ideálja R-nek is.

Tétel 3.14.10 *(Wedderburn-Artin 1. tétele) Minden féligegyszerű R gyűrű egységelemes, és felbontható véges sok olyan kétoldali ideáljának direkt összegére, melyek mindegyike olyan egyszerű gyűrű, amelyekben a bal oldali ideálokra teljesül a minimum-feltétel. R-nek ez a felbontása egyértelmű.*

Bizonyítás. Mivel minden kétoldali ideál bal oldali ideál is, ezért az előző tétel bizonyításánál választhattunk volna csak két oldali ideálokat. Így

$$R = A_1 \oplus A_2 \oplus \cdots \oplus A_k,$$

ahol az A_i-k az R gyűrű kétoldali ideáljai. Az A_i direkt összeadandók ideáljai R-nek is ideáljai. Mivel az ideálok minimális ideálok voltak, ezért az előzőekből következően egyszerűek is. Mivel R önmagának kétoldali ideálja, ezért van egységeleme az előző lemma miatt. Mivel az A_i-k bal oldali ideáljai bal oldali ideáljai R-nek is, ezért az A_i ideálok is eleget tesznek a minimum-feltételnek a bal oldali ideáljaikra nézve.

Már csak az egyértelműség bizonyítása van hátra. Elég ehhez megmutatni, hogy R minden minimális ideálja ott szerepel a felbontásban, azaz valamelyik A_i-vel megegyezik. Legyen tehát B az R tetszőleges minimális ideálja. Akkor $B \neq \{0\}$. Legyen b a B egy nem 0 eleme. Akkor $b = a_1 + \cdots + a_k$ ($a_i \in A_i$), amely tagok között van olyan (pl. a_1), amely nem nulla. Akkor az A_1 ideál e_1 egységelemére $a_1 = e_1 a_1 = e_1 b \in B$. B tehát tartalmazza az a_1 által generált ideált, ami nem lehet más, mint A_1, mert A_1 minimális ideál. Tehát $A_1 \subseteq B$. Mivel B minimális ideál, ezért $A_1 = B$. □

Mivel minden egységelemes kommutatív egyszerű gyűrű test, ezért a Wedderburn-Artin 1. tételének kapjuk egy következményét.

Tétel 3.14.11 *Minden kommutatív féligegyszerű R gyűrű egységelemes, és felbontható véges sok olyan kétoldali ideáljának direkt összegére, melyek mindegyike test.*

A Wedderburn-Artin 1. tételében szereplő direkt összeg tagjait jellemzi a következő tétel.

Tétel 3.14.12 *(Wedderburn-Artin 2. tétele) Egy $R \neq \{0\}$ gyűrű akkor és csak akkor olyan egyszerű gyűrű, amelyben a bal oldali ideálokra teljesül a minimum-feltétel, ha R vagy prímszámrendű zérógyűrű, vagy izomorf valamely F ferdetest feletti F^n teljes mátrixgyűrűvel.*

Chapter 4

MODULUSOK, VEKTORTEREK

4.1 A modulus fogalma

Definíció 4.1.1 *(A modulus fogalma) Legyen R egységelemes gyűrű, M pedig Abel-csoport. Azt mondjuk, hogy M bal oldali R-modulus, ha minden $r \in R$ és $a \in M$ elempárhoz hozzá van rendelve egy ra-val jelölt M-beli elem úgy, hogy minden $r, s \in R$ és $a, b \in M$ elemekre teljesülnek az alábbiak:*

- $r(a+b) = ra + rb$,
- $(r+s)a = ra + sa$.
- $r(sa) = (rs)a$,
- $1a = a$,

ahol 1 az R egységelemét jelöli.

Megjegyzés 4.1.2 Ha az R elemeivel való szorzást jobbról írjuk, akkor a jobb oldali R-modulus fogalmához jutunk. Ügyeljünk arra, hogy tetszőleges $r, s \in R$ elemek rs szorzatának az M egy a elemével való szorzásánál először s-sel, majd r-el szorzunk, ha M bal oldali R-modulus; ha M jobb oldali R-modulus, akkor először r-rel, majd s-sel szorzunk. Kommutatív R gyűrű

esetén a bal oldali és jobb oldali R-modulus között nem kell különbséget tenni. Tekintettel arra, hogy a bal oldali , illetve a jobb oldali modulusok elmélete analóg, ezért elegendő csak az egyik oldali modulusokkal foglalkozni. Mi itt a bal oldali modulusokat vizsgáljuk, és a bal oldali jelzőt elhagyjuk. Tehát moduluon mindig bal oldali modulust értünk.

Példák.

(1) Legyen M tetszőlegs Abel-csoport és $\mathbb{Z}$ az egész számok gyűrűje. Az M tetszőlegs a elemének és tetszőlegs m egész számnak értelmezve van az ma szorzata, és erre a szorzatra teljesülnek a fenti definícióban szereplő azonosságok. Tehát minden Abel-csoport $\mathbb{Z}$-modulus.

(2) Válaszuk M-et egy egységelemes gyűrű additív csoportjaként, és az R elemeinek az M elemeivel való szorzás legyen a gyűrűbeli szorzás. Megmutatható, hogy teljesülnek a modulus defuníciójában szereplő feltételek. Tehát minden R gyűrű R-modulus.

(3) Legyen M egy tetszőleges Abel-csoport és R egy egységelemes gyűrű. Minden $r \in R$ és $a \in M$ elemre legyen ra az M nulleleme. Ekkor M egy R-modulus (un. triviális R-modulus).

(4) Legyen M egy Abel-csoport és R az M endomorfizmusainak gyűrűje. Az M tetszőleges a elemének és M tetszőleges φ endomorfizmusának szorzata legyen egyenlő $\varphi(a)$-val. Könnyen belátható, hogy az M Abel-csoport erre az R gyűrűre nézve R-modulus.

(5) Ha R egy ferdetest, akkor az R-modulust vektortérnek (R-vektortérnek, vagy R feletti vektortérnek nevezzük.

Definíció 4.1.3 *(Részmodulus) Legyenek M és N mindketten R-modulusok. Azt mondjuk, hogy N az M részmodulusa, ha N az M részcsoportja, és minden $r \in R$ és $a \in N$ esetén $ra \in N$.*

Tétel 4.1.4 *Legyen M egy R-modulus. Ha N_i $(i \in I)$ az M modulus R-részmodulusainak tetszőleges nem üres halmaza, akkor $\cap_{i\in I} N_i$ is R-részmodulusa M-nek.*

Definíció 4.1.5 *(Generált részmodulus) Legyen M egy R-modulus, és legyen X az M egy nem üres részhalmaza. Az M mindazon R-részmodulusainak*

metszetét, amely részmodulusok tartalmazzák X-et, az X által generált R-részmodulusnak nevezzük.

Tétel 4.1.6 *Legyen M egy R-modulus és X az M-nek egy nem üres részhalmaza. Az M-nek az X által generált R-részmodulusa mindazon véges $r_1a_1 + \cdots r_na_n$ szorzatösszegek (lineáris kombinációk) halmaza, amelyekben n tetszőleges pozitív egész szám, $r_i \in R$ és $a_i \in M$ $(i = 1, \ldots, n)$.*

Definíció 4.1.7 *(Faktormodulus) Legyen M egy R-modulus, és legyen N az M-nek egy R-részmodulusa. Akkor az M tetszőleges $a + N$ mellékosztályára és tetszőleges $r \in R$ elemre $r(a + N) = ra + rN \subseteq ra + N$. Ha az M/N faktorcsoport $a + N$ elemének és az R gyűrű tetszőleges r elemének szorzatát $r(a_N) = ra = N$ módon értelmezzük, akkor M/N egy R-modulus lesz. Ezt az M modulus N szerinti faktormodulusának nevezzük.*

4.2 Modulusok homomorfizmusa

Definíció 4.2.1 *(Modulusok homomorfizmusa) Legyenek M_1 és M_2 R-modulusok. Az M_1-nek M_2-be való φ leképezését R-homomorfizmusnak nevezzük, ha*

- $\varphi(a + b) = \varphi(a) + \varphi(b)$,
- $\varphi(ra) = r\varphi(a)$

teljesül tetszőleges $a, b \in M$ és tetszőleges $r \in R$ elemekre. A φ R-homomorfizmus magján a

$$Ker\varphi = \{a \in M_1 : \ \varphi(a) = 0_2\}$$

halmazt értjük, ahol 0_2 jelöli az M_2 csoport nullelemét.

Tétel 4.2.2 *(Homomorfizmustétel) Tetszőleges $\varphi : M_1 \to M_2$ szürjektív R-homomorfizmus magja az M_1-nek egy R-részmodulusa, és az $M_1/Ker\varphi$ faktormodulus R-izomorf az M_2 modulussal.*

Tétel 4.2.3 *Legyenek M és N mindketten R-modulusok. Az M-nek N-be való R-homomorfizmusai a*

$$(\varphi_1 + \varphi_2) : a \mapsto \varphi_1(a) + \varphi_2(a) \quad (a \in M)$$

módon definiált összeadásra nézve Abel-csoportot alkotnak.

Az előző tételben szereplő Abel-csoport jele $Hom(M, N)$, neve pedig: homomorfizmuscsoport.

Legyen I tetszőleges halmaz és A_i $(i \in I)$ indexezett halmazrendszer. Azon f függvények halmazát, amelyek az I indexhalamazt az $\cup_{i\in I} A_i$ halmazba képezik le úgy, hogy minden i indexre $f(i) \in A_i$ teljesül, az A_i $(i \in I)$ halmazrendszer Descartes-szorzatának nevezzük és $\Pi_{i\in I} A_i$ módon jelöljük. A Descartes-szorzat elemeit kiválasztási függvényeknek nevezzük.

Ha $(G_i; \star_i)$ $(i \in I)$ csoportok tetszőleges rendszere, akkor annak Descartes-szorzatán értelmethezünk egy műveletet a következőképpen:

$$f_1 \star f_2 : i \mapsto f_1(i) \star_i f_2(i).$$

Könnyen igazolható, hogy a $\Pi_{i\in I} G_i$ Descartes-szorzat erre a műveletre nézve csoportot alkot, amelyet a G_i $(i \in I)$ csoportok (külső) direkt szorzatának nevezünk.

Definíció 4.2.4 *(Modulusok direkt szorzata) Legyenek M_i $(i \in I)$ tetszőleges R-modulusok. Legyen M az M_i csoportok külső direkt szorzata. Az M csoport tetszőleges f elemének az R gyűrű tetszőleges r elemével való szorzatát értelmezzük a következőképpen: $rf : i \mapsto rf(i)$. M egy R-modulussá válik, amelyet az M_i $(i \in I)$ modulusok direkt szorzatának nevezünk, és $\Pi_{i\in I} M_i$ módon jelölünk.*

Definíció 4.2.5 *(Modulusok direkt összege) Egy R gyűrű feletti M_i $(i \in I)$ modulusok direkt összegén (más néven a diszkrét direkt szorzatán) direkt szorzatuk azon $\sum_{i\in I} M_i$-mel jelölt részmodulusát értjük, amely azon f kiválasztási függvényekből áll, amelyeknél véges sok i indexre teljesül, hogy $f(i) \neq 0_i$, ahol 0_i az M_i modulus nullelemét jelöli.*

Megjegyzés 4.2.6 A $\sum_{i\in I} M_i$ direkt összeg a formálisan képezett összes lehetséges $a_{k_1} + \cdots + a_{k_n}$ véges összegek halmazaként is tekinthető, ahol mindegyik a_{k_j} az azonos indexű M_{k_j} eleme, és az indexek egy ilyen formális összegben páronként különböznek. Két ilyen formális összeg egymással egyenlő, ha ugyanazon tagokból áll, és a két összeg csak a tagok sorrendjében különbözik. Két ilyen formális összeg összegét úgy képezzük, hogy formálisan a + jellel kötjük össze őket és az azonos indexű modulusból származó tagokat összeadjuk. R-beli r elemmel pedig úgy szorozzuk őket, hogy a tagok mindegyikét szorozzuk r-rel (balról, ha bal oldali R-modulusokról van szó).

4.3 Szabad és projektív R-modulusok. Tenzori szorzat

Definíció 4.3.1 *(Szabad modulus) Az F R-modulust az $X \subseteq F$ szabad generátorrendszer által generált szabad R-modulusnak nevezzük, ha*

- *X az F generátorrendszere és*
- *bármely N R-modulus esetén bármely $f : X \to N$ leképezés kiterjeszthető F-nek N-be való R-homomorfizmusává.*

Tétel 4.3.2 *Minden szabad R-modulus az R-rel R-izomorf R-modulusok direkt összege.*

Bizonyítás. Legyen az F R-modulus az $X \subseteq F$ szabad generátorrendszer által generált szabad R-modulus. Akkor F minden x eleme előáll $x = r_1x_1 + \cdots + r_nx_n$ alakban, ahol az x_i-k az X-nek páronként különböző elemei, az r_i-k az X-nek elemei. Minden $x \in X$ elemhez rendeljünk hozzá egy, az R gyűrűvel R-izomorf R_x R-modulust. Jelöljük x-szel az R_x modulus azon elemét, amelyet az $R \cong R_x$ R-izomorfizmus az R gyűrű egységeleméhez rendel. Képezzük az R_x $(x \in X)$ R-modulusok direkt összegét. Jelölje ezt F'. A fenti utasítással X minden eleméhez hozzárendeltük az F' egy jól meghatározott elemét. Mivel X az F R-modulus szabad generátorrendszere, ezért ez a hozzárendelés kiegészíthető F-nek F'-re való φ homomorfizmusává. A φ homomorfizmus az F egy $x = r_1x_1 + \cdots + r_nx_n$ eleméhez az F' $\varphi(x) =$

$r_1\varphi(x_1) + \cdots + r_n\varphi(x_n) = r_1x_1 + \cdots + r_nx_n$ elemét rendeli. Ebből már következik, hogy φ R-izomorfizmus. □

Definíció 4.3.3 *(Modulusok egzakt sorozata) R-modulusok és R-homomorfizmusok egy*

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots \xrightarrow{f_k} M_k \quad (k \geq 2)$$

sorozatát egzakt sorozatnak nevezzük, ha minden $i = 1, 2, \ldots, k-1$ indexre

$$Im f_i = Ker f_{i+1},$$

azaz f_i az M_{i-1} modulust az M_i modulus azon részmodulusára képezi le, amely az f_{i+1} homomorfizmus magja.

Megjegyzés 4.3.4 A

$$\{0\} \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2$$

sorozat pontosan akkor egzakt, ha f_2 injektív, azaz az M_1 modulusnak az M_2 modulusba való beágyazása.

Megjegyzés 4.3.5 Az

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \{0\}$$

sorozat pontosan akkor egzakt, ha f_1 szürjektív, azaz M_1 az M_0 epimorf képe.

Megjegyzés 4.3.6 A

$$\{0\} \longrightarrow M_1 \xrightarrow{f_2} M_2 \xrightarrow{f_3} M_3 \longrightarrow \{0\}$$

sorozat pontosan akkor egzakt, ha f_2 injektív és f_3 szürjektív; ekkor M_1 úgy is tekinthető, mint M_2 azon részmodulusa, amely megegyezik az f_3 magjával, és ezért az M_2/M_1 faktormodulus izomorf az M_3 modulussal.

Megjegyzés 4.3.7 A

$$\{0\} \longrightarrow M \xrightarrow{f} M \longrightarrow \{0\}$$

sorozat pontosan akkor egzakt, ha f az M-nek automorfizmusa.

Tétel 4.3.8 *Tetszőleges M R-modulus alkalmas F szabad R-modulusnak homomorf képe. Másképpen fogalmazva: minden M R-modulushoz létezik olyan F szabd R-modulus és olyan φ R-homomorfizmus, hogy*

$$F \xrightarrow{\varphi} M \longrightarrow \{0\}$$

egzakt sorozat.

Definíció 4.3.9 *(Projektív modulus) Legyen P egy R-modulus. Azt mondjuk, hogy P egy projektív R-modulus, ha tetszőleges olyan*

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow{\scriptstyle \varphi} & & \\ B & \xrightarrow[\alpha]{} & C & \longrightarrow & 0, \end{array}$$

diagramm, amelyben a

$$B \xrightarrow{\alpha} C \longrightarrow 0$$

sor egzakt, kiegészíthető olyan

$$\begin{array}{ccccc} & & F & & \\ & {\scriptstyle \psi}\swarrow & \downarrow{\scriptstyle \varphi} & & \\ B & \xrightarrow[\alpha]{} & C & \longrightarrow & 0 \end{array}$$

diagrammá, amely kommutatív, azaz, amelyben szereplő ψ, α, φ R-homomorfizmusokra $\psi\alpha = \varphi$ teljesül.

Tétel 4.3.10 *Minden szabad R-modulus projektív.*

Tétel 4.3.11 *Egy P R-modulus akkor és csak akkor projektív, ha valamely F szabad R-modulus direkt összeadandójával R-izomorf.*

Definíció 4.3.12 *(Vektorterek tenzori szorzata) Legyenek U és V ugyanazon R gyűrű feletti modulusok. A $\sum_{(u,v)\in U\bigoplus V} R$ szabad modulus*

$$(u_1+u_2,v)-(u_1,v)-(u_2,v),$$

$$(u,v_1+v_2)-(u,v_1)-(u,v_2),$$

$$(\alpha u,v)-\alpha(u,v),$$

$$(u,\beta v)-\beta(u,v)$$

alakú elemei által generált W részmodulus szerinti faktorteret, az U és V vektorterek tenzori szorzatának nevezzük és $U\bigotimes V$ módon jelöljük. Az $(u,v)\in U\times V$ elempárt tartalmazó W-osztályt (mint $U\bigotimes V$-beli elemet) az u és v elemek tenzori szorzatának nevezzük és $u\otimes v$ módon jelöljük.

Tétel 4.3.13 *Ugyanazon $\mathbb{F}$ test feletti tetszőleges U és V vektorterek esetén*

$$dim(U\bigotimes V)=(dimU)(dimV).$$

Tétel 4.3.14 *Ugyanazon $\mathbb{F}$ test feletti tetszőleges U és V vektorterek esetén*

$$\mathcal{F}:(u,v)\mapsto u\otimes v$$

az $U\bigoplus V$ direkt összegnek az $U\bigotimes V$ tenzori szorzatba való bilineáris leképezése.

Tétel 4.3.15 *Ha U, V és W ugyanazon $\mathbb{F}$ test feletti vektorterek és f az $U\bigoplus V$ direkt összegnek a W-be való tetszőleges bilineáris leképezése, akkor megadható az $U\bigotimes V$ tenzori szorzatnak a W vektortérbe olyan φ lineáris leképezése, hogy*

$$f((u,v))=\varphi(\mathcal{F}((u,v)))$$

teljesül tetszőleges $(u,v)\in U\bigoplus V$ vektorra.

Chapter 5

FERDETESTEK, TESTEK

Mint ahogy arról már volt szó, egy olyan gyűrűt, amelyben a nullelemtől különböző elemek a szorzásra nézve csoportot alkotnak, ferdetestnek nevezünk. Egy olyan ferdetestet pedig, amelynek multiplikatív csoportja kommutatív, testnek nevezünk.

5.1 Véges testek

Tétel 5.1.1 *Ha a K test az L véges ferdetest részteste, akkor van olyan pozitív egész n, hogy $\mid L \mid = \mid K \mid^n$.*

Bizonyítás. Bebizonyítható, hogy L vektorteret alkot a K test felett. Mivel F véges sok elemet tartalmaz, ezért L dimenziója véges. Legyen ez a dimenzió n. Ha $b_1, \ldots, b_n$ egy bázis elemei, akkor L minden eleme egy és csak egyféleképpen írható fel K-beli $k_1, \ldots, k_n$ együtthatókkal

$$k_1 b_1 + \cdots + k_n b_n$$

alakban, amiből már adódik (az n elem k-adosztályú ismétléses variációinak számára vonatkozó képletből), hogy $\mid L \mid = \mid K \mid^n$. □

Tétel 5.1.2 *Véges test elemeinek száma prímhatvány.*

Bizonyítás. Legyen L véges test. L katakterisztikája p prímszám. Az L-ban lévő prímtest izomorf a p elemet tartalmazó $\mathbb{Z}_p$ résztesttel. A Tétel 5.1.1 felhasználásával kapjuk az $\mid L \mid = p^n$ eredményt valamely n pozitív egész számmal. □

Tétel 5.1.3 *(Wedderburn) Minden véges ferdetest kommutatív.*

Bizonyítás Legyen F egy véges ferdetest, melynek karakterisztikája a p prím. Az F ferdetest $Z(F)$ centruma F-nek p karakterisztikájú részteste. A Tétel 5.1.2 szerint $Z(F)$ elemszáma p-nek valamely hatványa. Jelölje ezt a hatványt q. Az F tetszőleges nem nulla f elemének F-beli $C(f)$ centralizátora F-nek részferdeteste, amely résztestként tartalmazza F centrumát. Így $C(f)$ elemszáma $Z(F)$ elemszámának, q-nak egy q^{n_f} hatványa. Mivel $Z(F)$ az F részteste, ezért a Tétel 5.1.1 szerint $\mid F \mid = q^n$ valamely n pozitív egész számra. Mivel $C(f)$ részferdetest F-ben, ezért $q^n = \mid F \mid = \mid C(f) \mid^k = q^{n_f k}$, amiből $n_f | n$ adódik. Ha meg tudjuk mutatni, hogy a fenti $\mid F \mid = q^n$ képletben szereplő n kitevő egyenlő 1-gyel, akkor abból $F = K$ következne, ami bizonyítaná a tétel állítását. Tegyük fel, indirekt módon, hogy $n \geq 2$. Használni fogjuk a körosztási polinomokat. Tudjuk, hogy az n-dik körosztási polinomok azok a komplex változós polinomok, melynek gyökei az n-dik primitív egységgyökök. Mivel $n \geq 2$, ezért minden egyes ξ_j primitív n-dik egységgyök valós része kisebb 1-nél (mivel ezek a komplex számsíkon az origó középpontú 1 sugarú körön helyezkednek el), és emiatt a ξ_j, 1, q pontok által meghatározott komplex síkbeli háromszögből $\mid q - \xi_j \mid > \mid g - 1 \mid = q - 1$ adódik. Az előzőek alapján a n-dik körosztási $\Phi_n(x)$ polinomra $\mid \Phi_n(q) \mid > (q-1)^{\varphi(n)} > q - 1$ teljesül, és ezért $\Phi_n(q)$ nem osztja $q - 1$-t. Ellentmondásra úgy fogunk jutni, hogy megmutatjuk azt is, hogy $\Phi_n(q)$ osztja a $q - 1$ különbséget. Jelölje G az F ferdetest multiplikatív csoportját, azaz $G = F \setminus \{0\}$. Az osztályegyenlet alkalmazásával:

$$\mid G \mid = \mid Z(G) \mid + \mid K_1 \mid + \cdots + \mid K_m \mid,$$

ahol $K_1, \ldots, K_m$ a G csoportnak a nem egyelemű konjugáltsági osztályai (azaz, amelyek a G centrumának komplementerében helyezkednek el). Világos, hogy a G csoport $Z(G)$ centruma egyenlő a $(Z(F) \setminus \{0\}$ multiplikatív csoporttal, így $\mid Z(G) \mid = q - 1$. Legyen $k_j \in K_j$ tetszőleges elem. Jelölje $C(k_j)$ a k_j elem F ferdetestbeli centralizátorát. A fent már bizonyítottak alapján

$| C(k_j) | = q^{n_j}$ alkalmas n_j pozitív egész számmal (megjegyezzük, hogy a fentiek alapján $n_j|n$ is teljesül). Ezek szerint a fenti osztályegyenlet a következő alakú:

$$q^n - 1 = q - 1 + \frac{q^n - 1}{q^{n_1} - 1} + \cdots \frac{q^n - 1}{q^{n_m} - 1}. \tag{5.1}$$

Tudjuk, hogy

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

minden pozitív egész n-re és minden valós x-re. Mivel n_j osztója n-nek minden j index esetén, ezért $\Phi_n(x)$ osztója minden egyes $\frac{x^n-1}{x^{n_j}-1}$ tagnak. Világos, hogy $\Phi_n(x)$ osztója $x^n - 1$-nek is. Az x helyébe q-t írva, adódik, hogy az (5.1) egyenlet bal oldalát és a jobb oldalán szereplő tagokat, a második tagtól kezdve, osztja $\Phi_n(q)$, így a bal oldal első tagját, azaz $q - 1$-et is osztja. Ez ellentmodt a bizonyítás első részében kapott eredménynek, ezért az $n > 1$ feltétel nem teljesülhet. Így $n = 1$, azaz $F = Z(F)$. Tehát F-ben a szorzás kommutatív, azaz F egy test. □

Tétel 5.1.4 *Minden véges test multiplikatív csoportja ciklikus.*

Bizonyítás. Legyen T $k + 1$ elemet tartalmazó test. Jelölje G a T multiplikatív csoportját. Akkor $| G | = k$. Ha g a G csoport d-edrendű eleme, akkor $d|k$ a Lagrange tétel szerint, és a T test feletti $x^d - 1$ polinomnak a gyökei éppen a g különböző hatványai, azaz a g által generált d-edrendű ciklikus részcsoport elemei. Ezért ha G-ben van d-edrendű elem, akkor azok száma száma $\varphi(d)$, mert egy d-edrendű ciklikus részcsoportban $\varphi(d)$ számú olyan elem van, amelyek rendje d. Mivel az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben, ezért gyökeinek száma 0 vagy d. Így G-ben vagy nincs d-edrendű elem (ilyen eset például az, amikor d nem osztója k-nak) vagy van, és ekkor azok száma $\varphi(d)$ (a fentiek alapján). A körosztási polinomokról tudjuk, hogy $x^k - 1 = \prod_{d|k} \Phi_d(x)$, ahol $\Phi_d(x)$ jelöli a d-dik körosztási polinomot. Az egyenlőségben szereplő polinomok fokszámát tekintve, $k = \sum_{d|k} \varphi(d)$. Ennek az egyenlőségnek tehát teljesülni kell, amely (a fentieket is figyelembe véve) azt eredményezi, hogy k minden d osztójára kell, hogy legyen G-ben d-edrendű elem. Így viszont van G-ben k-adrendű a elem. Tehát G az a elem által generált ciklikus csoport. □

Tétel 5.1.5 *Minden olyan véges nullosztómentes gyűrű, amelynek legalább két eleme van, test.*

Bizonyítás. Mivel R nullosztómentes, ezért a nem nulla elemeinek halmaza zárt a szorzásra nézve, és ezért félcsoport. Legyenek $a_1, \ldots, a_n$ az R gyűrű összes nem nulla elemei. Tetszőleges $0 \neq a \in R$ elemre az $aa_1, \ldots, aa_n$ szorzatok egyike sem nulla, mivel a nem bal oldali nullosztó. Ezért az $ax = b$ egyenletnek van megoldása R nullától különböző elemeinek félcsoportjában minden nem nulla b elemre. Hasonlóan igazolható, hogy az $ya = b$ egyenletnek is van megoldása R nem nulla elemeinek félcsoportjában tetszőleges $0 \neq b \in R$ elem esetén. Ebből már következik, hogy az $R \setminus \{0\}$ halmaz csoport a szorzásra nézve. Tehát R ferdetest. Mivel R véges, ezért Wedderburn tétele miatt R kommutatív, és ezért R test. □

5.2 Ferdetestek, mint speciális gyűrűk

Tétel 5.2.1 *Ferdetestnek nincs nem-triviális egyoldali ideálja. Fordítva, ha R olyan gyűrű, amelyben nincs nem-triviális bal oldali ideál (vagy nincs benne nem-triviális jobb oldali ideál) és $R^2 \neq \{0\}$, azaz R nem zérógyűrű, akkor R szükségképpen ferdetest.*

Bizonyítás. Tegyük fel, hogy L egy F ferdetest 0-tól különböző bal oldali ideálja. Legyen $0 \neq a \in L$ tetszőleges elem. Mivel F ferdetest, a-nak létezik a^{-1} inverze, és ezért minden $x \in F$ elemre $x = xe = xa^{-1}a \in L$, azaz, $L = F$. Hasonlóan igazolható, hogy F minden 0-tól különböző J jobboldali ideálra $F = J$ adódik. Ezzel e tétel első állítását bebizonyítottuk.

Forditva, tegyük fel, hogy R olyan gyűrű, amelyben nincs nem-triviális bal oldali ideál és R nem zérógyűrű. Először bebizonyítjuk, hogy R nullosztómentes. Tegyük fel, indirekt módon, hogy R-nek vannak olyan $a \neq 0$ és $b \neq 0$ elemei, amelyekre $ab = 0$ teljesül. Legyen

$$A = \{x \in R |\ xb = 0\}$$

és

$$B = \{y \in R |\ Ry = \{0\}\}.$$

Mivel $a \in A$ és A bal oldali ideálja R-nek, ezért $A = R$. Így $Rb = \{0\}$, és ezért $b \in B$. Mivel B is bal oldali ideélja R-nek, ezért $B = R$, amiből

$R^2 = \{0\}$ következik. Ez viszont ellentmond az $R^2 \neq \{0\}$ feltételnek. Tehát R nullosztómentes. Így R nem nulla elemeinek halmaza félcsoportot alkot a szorzásra nézve. Ebből következően, R tetszőleges nem nulla a eleme esetén Ra az R nem nulla bal oldali ieálja, és ezért $Ra = R$. Tehát van olyan $0 \neq e \in R$ elem, melyre $ea = a$. Ekkor $e^2a = ea = a$, amiből $(e^2 - e)a$ következik. Ebből viszont a nullosztómentesség miatt $e^2 - e = 0$, azaz $e^2 = e$ adódik. Innen $e^2b = eb$ következik tetszőleges $b \in R$ elemre, azaz $e(eb - b) = 0$. Mivel $e \neq 0$ és R nullosztómenentes, ezért $eb - b = 0$, azaz $eb = b$. Tehát e az R bal oldali egységeleme. A fenti $Ra = R$ egyenlőségnek R tetszőleges $a \neq 0$ elemére való fennállásából következik, hogy minden $0 \neq a \in R$ elemhez van olyan $a^{-1} \neq 0$ eleme R-nek, amelyre $a^{-1}a = e$ teljesül. Tehát R nem nulla elemeinek halmaza csoportot alkot a szorzásra nézve. Így R egy ferdetest. □

Tétel 5.2.2 *Ha R olyan kommutatív egyszerű gyűrű, amely nem zérógyűrű, akkor R test.*

Bizonyítás. A tétel az előző tétel következménye. □

Tétel 5.2.3 *Ferdetest tetszőleges epimorfizmusa vagy izomorfizmus vagy a 0 gyűrűre való leképezés.*

Bizonyítás. Mivel F ferdetestnek nincs valódi ideálja, ezért tetszőleges epimorfizmusának magja vagy 0 vagy F; az első esetben az epimorf kép izomorf F-fel, a második esetben az epimorf kép egy elemet tartalmaz, azaz 0-gyűrű. □

5.3 Testbővítések (általában)

Definíció 5.3.1 *Ha a K test része az L testnek, akkor K-t az L résztestének, L-et pedig a K bővítésének nevezzük. Ennek jele: $L|K$. Legyen $\alpha, \beta, \ldots$ az L test véges vagy végtelen sok eleme. Az L test azon legszűkebb résztestét, amely K-t is és az $\alpha, \beta, \ldots$ elemek mindegyikét is tartalmazza (vagyis a K és az $\alpha, \beta, \ldots$ elemek által generált résztestet) a K test $\alpha, \beta, \ldots$ elemekkel való bővítésének nevezzük, és $K(\alpha, \beta, \ldots)$ módon jelöljük. Azt is mondjuk, hogy a $K(\alpha, \beta, \ldots)$ test a K testből az $\alpha, \beta, \ldots$ elemek adjunkciója révén áll elő.*

Definíció 5.3.2 *Ha az L test a K test egy bővítése, akkor L tekinthető úgy, mint egy K test feletti vektortér. Az L-nek, mint K feletti vektortérnek a dimenzióját az $L|K$ testbővítés fokának nevezzük. Ha ez a fok véges, akkor véges fokú bővítésről, ellenkező esetben végtelen bővítésről beszélünk.*

Tétel 5.3.3 *Ha K, L, M olyan testek, amelyekre a $K \subseteq L \subseteq M$ teljesül, akkor az $M|K$ bővítés foka egyenlő az $L|K$ és az $M|L$ bővítések fokának szorzatával. Ha az $L|K$ és $M|L$ bővítések valamelyikének foka végtelen, akkor az $M|K$ bővítés foka is végtelen.*

Bizonyítás. Csak azt az esetet bizonyítjuk, amikor az $L|K$ és az $M|L$ bővítések foka véges. Legyen $\alpha_1, \ldots, \alpha_n$ az L-nek K-ra vonatkozó, $\beta_1, \ldots, \beta_m$ pedig M-nek L-re vonatkozó bázisa. Megmutatjuk, hogy az $\alpha_i\beta_j$ szorzatok ($i = 1, \ldots, n$; j=1, …, m;) M-nek K-ra vonatkozó bázisát alkotják. Ehhez először megmutatjuk, hogy ezek a szorzatok generálják M-et. Legyen $x \in M$ tetszőleges elem. Akkor megadhatók olyan $b_j \in L$ elemek ($j = 1, \ldots, m$), hogy

$$x = b_1\beta_1 + \cdots + b_m\beta_m.$$

Minden $b_j \in L$ elemhez megadhatók olyan K-beli a_{ij} elemek ($i = 1, \ldots, n$), amelyekre

$$b_j = a_{1j}\alpha_1 + \cdots + a_{nj}\alpha_n.$$

Így

$$x = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}\alpha_i\beta_j.$$

Tehát az $\alpha_i\beta_j$ szorzatok M-nek K-ra vonatkozó generátorrendszerét alkotják. Már csak azt kell megmutatni, hogy ezek a szorzatok lineárisan függetlenek. Tegyük fel, hogy

$$a_{11}(\alpha_1\beta_1) + \cdots + a_{ij}(\alpha_i\beta_j) + \cdots + a_{nm}(\alpha_n\beta_m) = 0,$$

ahol $a_{ij} \in K$. Rendezzük az egyenlőséget a β_j-k szerint, akkor azt kapjuk, hogy

$$(a_{11}\alpha_1 + \cdots + a_{n1}\alpha_n)\beta_1 + \cdots + (a_{1m}\alpha_1 + \cdots + a_{nm}\alpha_n)\beta_m = 0.$$

A β_j-k együtthatói L elemei. Mivel $\beta_1, \ldots, \beta_m$ az M-nek, mint L feletti vektortérnek a bázisa, ezért

$$a_{1j}\alpha_1 + \cdots + a_{nj}\alpha_n = 0 \quad (j = 1, \ldots, m).$$

Kihasználva, hogy az α_i-k az L nek, mint K feletti vektortérnek a bázisa, azt kapjuk, hogy

$$a_{ij} = 0 \quad (i = 1, \ldots, n; j = 1, \ldots, m).$$

Tehát az $\alpha_i\beta_j$ szorzatok lineárisan független generátorrendszertét, és így bázisát alkotják M-nek, mint K feletti vektortérnek. □

Definíció 5.3.4 *Legyen α egy L test tetszőleges eleme, K pedig az L egy részteste. Azt mondjuk, hogy α a K felett algebrai elem, ha van olyan legalább elsőfokú K-beli együtthatós $f(x)$ polinom, melynek az α elem gyöke, azaz, amelyre $f(\alpha) = 0$ teljesül. Ellenkező esetben azt mondjuk, hogy az α elem transzcendens a K felett.*

Ha K a racionális számtest és α egy komplex szám, akkor α aszerint algebrai vagy transzcendens szám, hogy α gyöke-e egy racionális együtthatójú legalább elsőfokú polinomnak, vagy nem. Például $\sqrt{2}$ és $1+i$ algebrai számok, mert $\sqrt{2}$ gyöke az $x^2 - 2$ polinomnak, $i + 1$ pedig gyöke az $\frac{1}{2}x^2 - x + 1$ polinomnak. Megmutatható, hogy e és π transzcendens számok.

Legyen L a K test bővítése és $\alpha \in L$. Tekintsük a $K[x]$ polinomgyűrű mindazon polinomjait, amelyeknek az α elem gyöke. Világos, hogy ezek a polinomok a $K[x]$ egy I ideálját alkotják. Mivel a K test feletti polinomgyűrű euklideszi gyűrű, ezért főideálgyűrű is, így megadható olyan $p(x) \in K[x]$ polinom, amely generálja az I ideált, azaz $I = (p(x))$. Világos, hogy ez a polinom aszerint 0 vagy nem nulla, hogy az α elem tarnszcendens (ekkor α csak a 0 polinomnak gyöke) vagy algebrai (ekkor α gyöke egy legalább elsőfokú polinomnak). Vizsgáljuk azt az esetet, amikor az α elem algebrai K felett. Ekkor a $p(x)$ polinom legalább elsőfokú. Mivel a $(p(x))$ ideál minden polinomja a $p(x)$ polinomnak $K[x]$-beli polinommal képezett szorzata, ezért $p(x)$ a legkisebb olyan fokszámú polinom, amelynek az α elem gyöke. $p(x)$ választható úgy is, hogy főegyütthatója 1 legyen. Megmutatható, hogy $p(x)$ irreducibilis polinom. Ellenkező esetben lenne két olyan, a $p(x)$ polinom fokszámánál kisebb fokszámú $h(x), g(x) \in K[x]$ nem nulla polinom, melyekre

$p(x) = h(x)g(x)$ teljesülne. Ekkor a $0 = p(\alpha) = g(\alpha)h(\alpha)$ egyenlőségből $g(\alpha) = 0$ vagy $h(\alpha) = 0$ következne, mert minden test nullosztómentes. Tehát az α elem gyöke lenne a $g(x)$ és a $h(x)$ polinomok egyikének, ami viszont nem lehet, mert mindkettő fokszáma kisebb a $p(x)$ polinom fokszámánál, és $p(x)$ a legkisebb fokszámú olyan polinom, melynek az α elem gyöke. Tehát a $p(x)$ polinom irreducibilis. Ezt a $p(x)$ polinomot az α algebrai elem definiáló polinomjának (vagy minimálpolinomjának) nevezzük.

Tétel 5.3.5 *Legyen L a K test bővítése és $\alpha \in L$ egy K feletti algebrai elem. Akkor a $K(\alpha)$ test izomorf a $K[x]/(p(x))$ maradékosztálygyűrűvel, ahol $p(x)$ az α elem definiáló polinomja. Ha a $p(x)$ polinom fokszáma n, akkor a $K(\alpha)|K$ bővítés foka n, és a $K(\alpha)$ test minden eleme egyértelműen felírható $c_0 + c_1\alpha_1 + \cdots + c_{n-1}\alpha^{n-1}$ alakban K-beli $c_0, c_1, \ldots, c_{n-1}$ elemekkel.*

Bizonyítás. Jelölje $K[\alpha]$ az α elem K-beli együtthatókkal képezett polinomjainak összességét, azaz az L test $c_m\alpha^m + \cdots + c_1\alpha + c_0$ formában felírható elemeinek halmazát, amelyben szereplő c_i elemek a K test elemei, m pedig tetszőleges nemnegatív egész szám. Ez a halmaz az L test egy részgyűrűje. Világos, hogy $K[\alpha] \subseteq K(\alpha)$. Legyen φ a $K[x]$ polinomgyűrűnek a $K[\alpha]$ gyűrűbe való azon leképezése, amely minden egyes $f(x) \in K[x]$ polinomhoz annak az α elemhez tartozó $f(\alpha) \in K$ helyettesítési értékét rendeli. Világos, hogy φ szürjektív homomorfizmus, melynek magja megegyezik az α elem $p(x)$ definiáló polinomja által generált $(p(x))$ ideállal. Mivel $p(x)$ irreducibilis polinom, ezért az $(p(x))$ ideál maximális ideálja $K[x]$-nek, és ezért a $K[x]/(p(x))$ faktorgyűrű test. A gyűrűkre vonatkozó homomorfizmustétel miatt $K[x]/(p(x)) \cong K[\alpha]$. Ezért $K[\alpha]$ test. Ebből már következik, hogy $K(\alpha) = K[\alpha] \cong K[x]/(p(x))$.

Tegyük fel, hogy az $p(x)$ definiáló polinom fokszáma n. Akkor a $K(\alpha)$-beli

$$1, \alpha, \ldots \alpha^{n-1}$$

elemek lineárisan függetlenek. Ugyanis, ha lineárisan függők lennének, akkor meg lehetne adni olyan $c_i \in K$ $(i = 0, \ldots, n-1)$ együtthatókat, amelyek nem mindegyike nulla, és amelyekkel

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0$$

teljesülne. Ez viszont azt jelentené, hogy α gyöke a definiáló polinomjánál kisebb fokszámú

$$f(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$$

polinomnak. Ez viszont ellentmondás. Megmutatható, hogy az $1, \ldots, \alpha^{n-1}$ elemek nem csak lineárisan függetlenek, hanem generálják is $K(\alpha)$-t. Ha

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

akkor

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0,$$

és így α n-dik és annál magasabb kitevőjű hatványai kifejezhetők az $1, \alpha, \ldots, \alpha^{n-1}$ elemek lineáris kombinációjaként. Tehát az $1, \alpha, \ldots, \alpha^{n-1}$ elemek a $K(\alpha)$-nak mint K feletti vektortérnek egy bázisát alkotják. Ezért a $K(\alpha)|K$ testbővítés foka megegyezik az α elem definiáló polinomjának fokszámával, és $K(\alpha)$ minden eleme egyértelműen felírható $c_0 + c_1\alpha_1 + \cdots + c_{n-1}\alpha^{n-1}$ alakban K-beli $c_0, c_1, \ldots, c_{n-1}$ elemekkel. □

Tétel 5.3.6 *Legyen L a K test bővítése és $\alpha \in L$ egy K feletti transzcendens elem. Akkor a $K(\alpha)$ test izomorf a $K(x)$ függvénytesttel. Ekkor a $K(\alpha)|K$ bővítés foka végtelen, és a $K(\alpha)$ test minden eleme felírható*

$$\frac{b_n\alpha^n + \cdots + b_1\alpha + b_0}{c_m\alpha^m + \cdots + c_1\alpha + c_0}$$

alakban. Két ilyen tört csak akkor reprezentálja $K(\alpha)$-nak ugyanazt az elemét, ha x megfelelő racionális törtjei egymással egyenlők.

Bizonyítás. A bizonyítás elején alkalmazzuk az előző tétel gondolatmenetét. Jelölje φ itt is a $K[x]$ polinomgyűrűnek a $K[\alpha]$ gyűrűre való azon szürjektív homomorfizmusát, amely minden $f(x) \in K[x]$ polinomhoz annak $f(\alpha)$ helyettesítési értékét rendeli. Mivel α transzcendens elem, ezért $ker\varphi = \{0\}$ és így (a homomorfizmustétel miatt) $K[x] \cong K[\alpha]$. A $K(\alpha)$ test izomorf a $K[\alpha]$ egységelemes integritási tartomány hányadostestével, és így $K(\alpha) \cong K(x)$. □

Definíció 5.3.7 *Legyen a K test az L_1 és L_2 testek részteste. Akkor mondjuk, hogy L_1 izomorf L_2-vel K felett, ha megadható L_1-nek L_2-re olyan izomorfizmusa, amely K elemeit fixen hagyja.*

Tétel 5.3.8 *Legyenek α és β egy K test L bővítésének olyan elemei, amelyek ugyanazon K feletti irreducibili polinom gyökei, akkor létezik olyan K feletti izomorfizmus $K(\alpha)$ és $K(\beta)$ között, amely az α-t a β-ba viszi át.*

Bizonyítás. Az 5.3.5 Tétel szerint $K(\alpha)$ elemei felírhatók $c_0 + c_1\alpha_1 + \cdots + c_{n-1}\alpha^{n-1}$ alakban. Nem nehéz belátni, hogy a

$$c_0 + c_1\alpha_1 + \cdots + c_{n-1}\alpha^{n-1} \mapsto c_0 + c_1\beta_1 + \cdots + c_{n-1}\beta^{n-1}$$

megfeleltetés a $K(\alpha)$ testnek a $K(\beta)$ testre való olyan izomorfizmusa, amely K elemeit fixen hagyja. □

Tétel 5.3.9 *Ha α és β mindketten transzcendes elemek a K test egy L bővítésében, akkor $K(\alpha)$ izomorf $K(\beta)$-val K felett.*

Bizonyítás. Mivel $K(\alpha) \cong K(x)$ és $K(\beta) \cong K(x)$, ezért $K(\alpha) \cong K(\beta)$. Ennél az izomorfizmusnál az $\frac{f(\alpha)}{g(\alpha)} \in K(\alpha)$ elemennek az $\frac{f(\beta)}{g(\beta)} \in K(\beta)$ elem felel meg. Ez a K elemeit fixen hagyja. □

Tétel 5.3.10 *Legyen K egy test. Létezik K -nak olyan $K(\alpha)$ bővítése, amelyben α transzcendens elem K felett.*

Tétel 5.3.11 *Legyen $p(x)$ a K test feletti irreducibilis polinom. Létezik K-nak olyan $K(\alpha)$ bővítése, amelyben α a $p(x)$ gyöke.*

Bizonyítás. A $K[x]/(p(x))$ faktorgyűrű test, mert $(p(x))$ maximális ideál. Ebben a testben K különböző elemei különböző mellékosztályokban vannak, így K részteste a $K[x]/(p(x))$ testnek. Jelölje α az x polinomot tartalmazó mellékosztályt. Ez gyöke a $p(x)$ polinomnak és $K(\alpha) \cong K[x]/(p(x))$. □

5.4 Algebrai bővítések

Definíció 5.4.1 *Egy $L|K$ testbővítést algebrainak nevezünk, ha L minden eleme algebrai K felett.*

Tétel 5.4.2 *Ha az L test a K testnek véges bővítése, úgy az az $L|K$ testbővítés algebrai, és L a K-ból véges sok algebrai elem adjunkciójával áll elő.*

Bizonyítás. Legyen az $L|K$ testbővítés foka n. Ha α az L tetszőleges eleme, akkor az

$$1, \alpha, \ldots, \alpha^n$$

elemek lineárisan függőek, így megadhatók olyan K-beli $c_0, \ldots, c_n$ elemek, amelyek nem mindegyike nulla, és $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$. Ez pedig azt jelenti, hogy α algebrai elem K felett. Ha K-hoz az L test egy bázisát adjungáljuk (amely n elemből áll), akkor bővítésként az L testet kapjuk. □

Tétel 5.4.3 *Ha $\alpha \in L$ algebrai K felett, akkor $K(\alpha)$ a K algebrai bővítése.*

Bizonyítás. Ha $\alpha \in L$ algebrai K felett akkor $K(\alpha)$ a K-nak véges bővítése, és ezért algebrai. □

Tétel 5.4.4 *Ha egy L test a K testből véges sok algebrai elem adjungálásával áll elő, akkor L algebrai bővítése K-nak.*

Bizonyítás. Mivel véges sok véges bővítés véges bővítés, ezért az állítás nyílvánvaló. □

Következmény 5.4.5 *Algebrai bővítés algebrai bővítése algebrai.*

5.5 Felbontási test

Az algebrai testbővítések között különösen fontosak azok, amelyek úgy állnak elő, hogy egy K testhez egy $K[x]$-beli polinom gyökeit adjungáljuk.

Definíció 5.5.1 *Legyen $f(x)$ egy K test feletti n-edfokú ($n \geq 1$) polinom. Tegyük fel, hogy K-nak van olyan M bővítése, amelyben $f(x)$ elsőfokú tényezők szorzatára bomlik*

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

Az M testnek azt az L résztestét, amely a K testből az $\alpha_1, \ldots, \alpha_n$ gyökök adjunkciójával áll elő, az $f(x)$ polinom felbontási testének nevezzük: $L = K(\alpha_1, \ldots, \alpha_n)$.

Az előző definícióban feltételeztük, hogy van olan M test, amely tartalmazza az $f(x) \in K[x]$ polinom összes gyökét. Így kérdéses, hogy egy polinomnak van-e felbontási teste, illetve, hogy egyértelműe-e? Erre a két kérdésre ad választ a következő két tétel.

Tétel 5.5.2 *(Egzisztencia-tétel) Egy K test feletti $K[x]$ polinomgyűrű tetszőleges $f(x)$ polinomjához létezik felbontási test.*

Bizonyítás. Feltehetjük, hogy a vizsgált polinom legalább elsőfokú. Akkor $f(x)$ felbontható K felett irreducibilis polinomok szorzatára:

$$f(x) = p_1(x)p_2(x)\cdots p_r(x).$$

Mivel $p_1(x)$ irreducibilis K felett, ezért létezik K-nak olyan $K(\alpha_1)$ algebrai bővítése, hogy $K \subseteq K(\alpha_1)$ és α_1 a $p_1(x)$ irreducibilis polinom gyöke. Ez az α_1 az $f(x)$-nek is gyöke. Így $f(x)$-ből az $x - \alpha_1$ gyöktényező leválasztható. Tegyük fel, hogy már megkonstruáltunk egy $K_i = K(\alpha_1, \ldots, \alpha_i)$ $(i < n)$ bővítést, amelyben $x - \alpha_1, \ldots, x - \alpha_i$ az $f(x)$ gyöktényezői. Ekkor $f(x)$, mint K_i feletti polinom a következő alakban írható:

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_i)q_{i+1}(x)\cdots q_t(x),$$

ahol a $q_j(x)$ polinomok a K_i test feletti irreducibilis polinomok, és legalább másodfokúak. Alkalmazva az előző gondolatmenetet, kapunk egy $K_{i+1} = K_i(\alpha_{i+1}) = K(\alpha_1, \ldots \alpha_i, \alpha_{i+1})$ bővítést a q_{i+1} valamely α_{i+1} gyöke segítségével. Tovább haladva, véges sok lépés után eljutunk egy kívánt $K(\alpha_1, \ldots, \alpha_n)$ bővítéshez, amely az $f(x)$ polinom felbontási teste.

Tétel 5.5.3 *(Unicitás-tétel) Ha L és L' egy K test feletti $f(x)$ polinom két felbontási teste K felett, akkor az $L|K$ és $L'|K$ testbővítések izomorfak, azaz megadható L-nek L'-re olyan izomorfizmusa, amely K elemeit fixen hagyja.*

5.6 Normális testbővítés

Definíció 5.6.1 *Egy $N|K$ testbővítést normálisnak nevezünk, ha*

(1) N a K-nak algebrai bővítése;

(2) ha egy K feletti $p(x)$ irreducibilis polinomnak van egy gyöke N-ben, akkor az összes gyöke N-ben van, azaz $p(x)$ az N test feletti lineáris tényzők szorzatára bomlik.

Tétel 5.6.2 *Ha N az $f(x) \in K[x]$ polinom felbontási teste, akkor az $N|K$ testbővítés normális. Megfordítva, ha az $N|K$ véges normális bővítés, akkor N valamely $f(x) \in K[x]$ polinom felbontási teste.*

Tétel 5.6.3 *Ha $L|K$ tetszőleges véges bővítés, akkor létezik egy olyan $N|K$ véges normális bővítés, hogy L benne van N-ben.*

5.7 Véges testek

A Tétel 5.1.2 szerint minden véges test elemszáma prímhatvány.

Tétel 5.7.1 *Azonos elemszámú véges testek egymással izomorfak.*

Bizonyítás. Legyen K egy véges test. Jelölje q a K elemeinek számát. A K test 0-tól különböző elemei csoportot alkotnak, melynek rendje $q-1$. Ezért K minden nem nulla α elemére teljesül az $\alpha^{q-1} = 1$ egyenlőség, és így K minden α elemére $\alpha^q - \alpha = 0$. A K test elemei tehát az $x^q - x \in \mathbb{Z}_p[x]$ polinom gyökei. A K test tehát az $x^q - x \in \mathbb{Z}_p[x]$ polinom felbontási teste. Mivel egy adott alaptest feletti polinom felbontási testei egymással izomorfak, abből következik, hogy bármely két q-elemű test egymással izomorf. □

Tétel 5.7.2 *Minden $q = p^n$ $(n \geq 1)$ prímhatványhoz létezik q elemű test.*

Bizonyítás. Tekintsük a $\mathbb{Z}_p$ test feletti $x^q - x$ polinomot. Mivel $p|q$, ezért $x^q - x$ deriváltja $q^{q-1} - 1 = -1$, és ezért az $x^q - x$ polinomnak minden gyöke egyszeres. Legyen K az $x^q - x$ polinom felbontási teste. Ebben a testben

$$x^q - x = (x - \alpha_1) \cdots (x - \alpha_q)$$

alakban írható, ahol az $\alpha_1, \ldots, \alpha_q$ elemek páronként különbözőek. Mivel tetszőleges α_i és α_j gyökre

$$(\alpha_i - \alpha_j)^q = \alpha_i^q - \alpha_j^q = \alpha_i - \alpha_j,$$

és $\alpha_j \neq 0$ esetén

$$(\frac{\alpha_1}{\alpha_j})^q = \frac{\alpha_i^q}{\alpha_j^q} = \frac{\alpha_i}{\alpha_j},$$

ezért az $\alpha_1, \ldots, \alpha_q$ gyökök test alkotnak. Emiatt $K = \{\alpha_1, \ldots, \alpha_q\}$, amely egy q elemű test. □

Tétel 5.7.3 *Ha a K véges test elemeinek száma $q = p^n$, akkor a következő leképezések K-nak automorfizmusai:*

$$a \mapsto a^p,\ a \mapsto a^{p^2},\ \ldots, a \mapsto a^{p^{n-1}},\ a \mapsto a^{p^n}.$$

Bizonyítás. Mivel tetszőleges $a, b \in K$ esetén $(a + b)^p = a^p + b^p$ és $(ab)^p = a^p b^p$, azért az $a \mapsto a^p$ művelettartó leképezés. Ha $a^p = b^p$, akkor $(a - b)^p = 0$, amiből a K nullosztómentessége miatt $a - b = 0$, azaz $a = b$ következik. Tehát a vizsgált leképezés injektív. K végessége miatt szürjektív is. Tehát az $a \mapsto a^p$ leképezés K-nak egy automorfizmusa. Ebből már következik, hogy a többi leképezés is K automorfizmusai. □

Példa 5.7.4 *Határozzuk meg a négyelemű testet!*
Megoldás.Ha K négyelemű test, akkor K úgy tekinthető, mint a kételemű $\mathbb{Z}_2 = \{0, 1\}$ test feletti $f(x) = x^4 - x$ polinom felbontási teste. Az $x^4 - x$ polinom $\mathbb{Z}_2$ feletti irreducibilis polinomok szorzatára való bontása: $x^4 - x = x(x^3 - 1) = x(x - 1)(x^2 + x + 1)$. Van a $\mathbb{Z}_p$ testnek olyan $\mathbb{Z}_2(\alpha)$ bővítése, ahol α az $x^4 - x$ polinom gyöke. Ezért ebben a bővebb testben az $x^4 - x$ polinom elsőfokú tényezők szorzatára bomlik. Ez a bővebb test a $\mathbb{Z}_2$ test feletti 2 dimenziós vektortér, ennek egy bázisa 1 és α. Így K elemei: $0, 1, \alpha, 1 + \alpha$. A K testben $\alpha^2 = 1 + \alpha$, $(1 + \alpha)^2 = \alpha$, $\alpha(1 + \alpha) = 1$ (ezért $\alpha^{-1} = 1 + \alpha$ és $(1 + \alpha)^{-1} = \alpha$), $-1 = 1$, $-\alpha = \alpha$, $-(1 + \alpha) = 1 + \alpha$.

Chapter 6

FÜGGELÉK

6.1 Körosztási polinomok

Definíció 6.1.1 *n-edik egységgyököknek nevezzük azokat a komplex számokat, amelyek n-dik hatványa egyenlő* 1*-gyel.*

Az n-edik egységgyökök a következő alakú komplex számok:

$$\epsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad (k = 0, 1, \ldots, n-1).$$

Ezt a jelölést használva, az n-dik egységgyökök:

$$\epsilon_0 = 1, \epsilon_1, \epsilon_1^2, \ldots \epsilon_1^{n-1}.$$

Definíció 6.1.2 *Egy ϵ komplex számot primitív n-dik egyéggyöknek nevezünk, ha n az a legkisebb pozitív egész szám, amelyre $\epsilon^n = 1$ teljesül. Más szavakkal, a primitív n-dik egységgyökök azok a komplex számok, amelyek rendje (a komplex számok multiplikatív csoportjában) egyenlő n-nel.*

Tétel 6.1.3 *Egy ϵ_1^k n-dik egységgyök akkor és csak akkor primitív n-dik egységgyök, ha $(k, n) = 1$, azaz k és n relatív prímek. Így a primitív n-dik egységgyökök száma egyenlő $\varphi(n)$-nel, ahol φ az un. Euler függvény.*

Definíció 6.1.4 *n-edik körosztási polinomon azt az* 1 *főegyütthatójú polinomot értjük, melynek gyökei a primitív n-dik egységgyökök, s ezek mindegyike egyszeres gyök. Ezt a polinomot $\Phi_n(x)$-szel jelöljük.*

Az n-dik körosztái polinom fokszáma egyenlő $\varphi(n)$-nel.

Példák körosztási polinomokra:

$$\Phi_1(x) = x - 1,$$

$$\Phi_2(x) = x + 1,$$
$$\Phi_3(x) = x^2 + x + 1,$$
$$\Phi_4(x) = x^2 + 1.$$

Tétel 6.1.5 *Tetszőleges n pozitív egész számra $\prod_{d|n} \Phi_d(x) = x^n - 1$.*

Bizonyítás Világos, hogy az $x^n - 1$ polinom gyökei az n-dik egységgyökök (minegyik egyszeres gyök), így

$$x^n - 1 = (x - 1)(x - \epsilon_1) \cdots (x - \epsilon_k) \cdots (x - \epsilon_{n-1}).$$

Az n-dik egységgyökök a nem nulla komplex számok multiplikatív csoportjának egy részcsoportját alkotják; ennek a részcsoportnak a rendje n. Így az n-dik egységgyökök rendje osztja n-et. A $\Phi_n(x)$ gyökei ezek közül pontosan azok, amelyek rendje kisebb n-nél. Amikor az $x^n - 1$ polinomot elosztjuk az összes d-adrendű ($d < n$ és $d \mid n$) egységgyökkel definiált $\Phi_d(x)$-szel, akkor az olyan tényezőkkel egyszerűsítünk, amelyek d-edrendű egységgyökökhöz tartoznak. Tehát

$$\frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)} = \Phi_n(x).$$

Innen már adódik a $\prod_{d|n} \Phi_d(x) = x^n - 1$ egyenlőség. □

A tétel alkalmazásával adódik. hogy

$$\Phi_5(x) = \frac{x^5 - 1}{\Phi_1(x)} = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1.$$

Hasonlóan, ha p tetszőleges prím szám, akkor

$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Tétel 6.1.6 *A Φ_n körosztási polinom együtthatói egész számok.*

Bizonyítás Φ_1 együtthatói egészek. Az előző tétel szerint $\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)}$, azaz $\Phi_2(x)$ egy egész együtthatós polinomnak egy 1 főegyütthatójú egész együtthatós polinommal való hányadosa, s ezért $\Phi_2(x)$ együtthatói egészek. Innen már a teljes indukció alkalmazásával adódik a tétel állítása.

Tétel 6.1.7 *Minden körosztási polinom irreducibilis a racionális számok teste felett.*

Bibliography

[1] Fuchs László, Algebra, Nemzeti Tankönyvkiadó, Budapest, 1997

Contents