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.

Tartalomjegyzék

1. BEVEZETÉS **1**

2. CSOPORTOK **7**

2.1. A csoport fogalma; ekvivalens definíciók 7
2.2. Csoportok részcsoportjai 10
2.3. Ciklikus csoportok 12
2.4. Mellékosztályok. Lagrange tétele 14
2.5. Normális részcsoportok 17
2.6. Faktorcsoport, Homomorfizmus-tétel 19
2.7. Izomorfizmus-tételek 21
2.8. Centrum, centralizátor, normalizátor, a Cauchy-tétel bizonyítása 22
2.9. Normállánc, a Jordan–Hölder-tétel 28
2.10. Kommutátor részcsoport 32
2.11. Feloldható csoportok 34
2.12. Permutációcsoportok 37
2.13. Csoportok direkt szorzata 44
2.14. Véges Abel-csoportok 47
2.15. Sylow-tételek 54
2.16. Szabad csoportok, csoportok megadása definiáló relációkkal . . 58
2.17. Kis elemszámú csoportok 63

3. GYŰRŰK **65**

3.1. A gyűrű fogalma 65
3.2. Gyűrűk kitüntetett elemei 66
3.3. Gyűrűk ideáljai 68
3.4. Faktorgyűrűk 69
3.5. Gyűrűk homomorfizmusa, izomorfizmusa 70
3.6. Gyűrűk beágyzási tételei 71

3.7. Gyűrűk karakterisztikája 75
3.8. Egységelemes integritási tartományok 76
3.9. Gauss-gyűrűk 79
3.10. Főideálgyűrűk, euklideszi gyűrűk 83
3.11. Noether-féle gyűrűk 85
3.12. Dedekind-gyűrűk 88
3.13. Teljes mátrixgyűrűk 90
3.14. Féligegyszerű gyűrűk 93

4. MODULUSOK, VEKTORTEREK 101
4.1. A modulus fogalma 101
4.2. Modulusok homomorfizmusa 103
4.3. Szabad és projektív R-modulusok 105

5. FERDETESTEK, TESTEK 109
5.1. Véges testek 109
5.2. Ferdetestek, mint speciális gyűrűk 112
5.3. Testbővítések (általában) 113
5.4. Algebrai bővítések 119
5.5. Felbontási test 119
5.6. Normális testbővítés 121
5.7. Véges testek 121

6. FÜGGELÉK 127
6.1. Körosztási polinomok 127
6.2. Csoportok szemidirekt szorzata 129

1. fejezet

BEVEZETÉS

1.0.1 Definíció *(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.

1.0.2 Definíció *(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.*

1.0.3 Definíció *(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.

1.0.4 Megjegyzés (Cayley-féle művelettáblázat) 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.

1.0.5 Definíció *(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.

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

1.0.7 Definíció *(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.*

1.0.8 Tétel *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

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

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

1.0.10 Definíció *(Idempotes elem) Egy S félcsoport f elemét idempotens elemnek nevezzük, ha $f^2 = f$.*

1.0.11 Definíció *(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.*

Világos, hogy egy S félcsoport minden bal oldali, illetve jobb oldali nulleleme az S egy idempotens eleme.

1.0.12 Tétel *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. □

1.0.13 Definíció *(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.*

Világos, hogy egy S félcsoport minden bal oldali, illetve jobb oldali neutrális eleme az S egy idempotens eleme.

1.0.14 Tétel *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.□

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

1.0.16 Definíció *(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.*

1.0.17 Tétel *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. □

2. fejezet

CSOPORTOK

2.1. A csoport fogalma; ekvivalens definíciók

2.1.1 Definíció *(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.*

2.1.2 Definíció *(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.*

2.1.3 Tétel *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. □

2.1.4 Tétel *Minden csoport pontosan egy idempotens elemet tartalmaz; ez a csoport egységeleme.*

Bizonyítás Egy G csoport e egységeleme idempotens elem. Ha f a G egy idempotene eleme, akkor $ff = f = fe$, amiből $f = e$ következik, mivel G (bal) egyszerűsítéses. □

2.1.5 Tétel *Legyen φ egy G csoportnak egy G' csoportba való homomorfizmusa. Akkor φ a G csoport egységeleméhez a G' csoport egységelemét rendeli. Továbbá, tetszőleges $a \in G$ ele esetén $\varphi(a^{-1}) = (\varphi(a))^{-1}$.*

Bizonyítás Jelölje e a G csoport, e' pedig a G' csoport egységelemét. Akkor $(\varphi(e))^2 = \varphi(e^2) = \varphi(e)$, azaz $\varphi(e)$ a G' csoport egy idempotens eleme. Az előző tétel miatt $\varphi(e) = e'$.

Legyen $a \in G$ tetszőleges. Akkor $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$, ami miatt írhatjuk, hogy $\varphi(a^{-1}) = (\varphi(a))^{-1}$. □

2.1.6 Tétel *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. □

2.1.7 Tétel *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. □

2.1.8 Példa *(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*

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

2.1.9 Példa (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

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

2.2.2 Megjegyzés 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.

2.2.3 Megjegyzés 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.

2.2.4 Tétel *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. □

2.2.5 Megjegyzés 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 $a^{-1} = a^{k-1} \in H$.

2.2.6 Megjegyzés 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.

2.2.7 Tétel *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. □

2.2.8 Definíció *(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.*

2.2.9 Tétel *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

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

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

2.3.3 Tétel *Egy $\varphi : G \mapsto G'$ csoporthomomorfizmus a G csoport egységeleméhez a G' csoport egységelemét rendeli.*

Bizonyítás Jelölje $e \in G$ és $e' \in G'$ az egységelemeket. Akkor $\varphi(e)\varphi(e) = \varphi(ee) = \varphi(e)$, azaz $\varphi(e)$ a G' csoport idempotens eleme. Mivel egy csoportnak az egységeleme az egyetlen idempotens eleme, ezért $\varphi(e) = e'$. □

2.3.4 Tétel *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 $a^m = (a^n)^q a^r + a^r$, 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. □

2.3.5 Definíció *(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.*

2.3.6 Megjegyzés A 2.3.4 Tétel szerint egy csoport tetszőleges elemének rendje megegyezik az általa generált (ciklikus) részcsoport rendjével.

2.3.7 Tétel *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 $r \langle t$, ezért $r = 0$, és így $m = qt$, amiből $a^m = (a^t)^q \in \{a^t\}$ következik. □

2.3.8 Tétel *Egy n-edrendű ciklikus csoportban $\varphi(n)$ számú n-edrendű elem van, ahol φ az un. Euler-függvény ($\varphi(n)$ az n-nél nem nagyobb, 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

2.4.1 Definíció *(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.

2.4.2 Tétel *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) $\to$ (2): Ha $a \in bH$, akkor van olyan $h \in H$ elem, amelyre $a = bh$ teljesül. Ezért

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

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

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

□

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

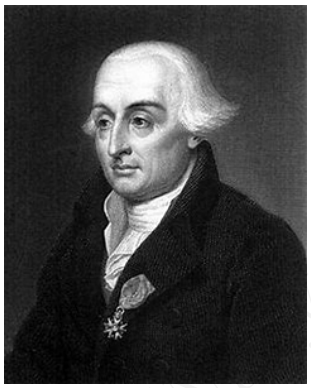
Bizonyítás. Tegyük fel, hogy G valamely x elemére $x \in aH \cap bH$ teljesül. Akkor $aH = xH = bH$ a 2.4.2 Tétel szerint. □

2.4.4 Tétel *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.

2.4.5 Definíció *(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.*



Joseph Louis Lagrange (1736 – 1813)

2.4.6 Tétel *(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 $|G| = |H||G : H|$. □

2.4.7 Következmény *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

2.5.1 Definíció *(Normális részcsoport) Egy G csoport N részcsoportját normális részcsoportnak nevezzük, ha minden $g \in G$ elem esetén $gN = Ng$.*

Ha N a G csoport normális részcsoportja, akkor ez $N \triangleleft G$ módon jelöljük.

2.5.2 Tétel *Egy G csoport valamely N részcsoportja akkor és csak akkor normális részcsoportja G-nek, ha $g^{-1}Ng \subseteq N$ teljesül a G csoport minden g elemére.*

Bizonyítás. Ha N normális részcsoportja egy G csoportnak, akkor $gN = Ng$ minden $g \in G$ elemre, azaz, $g^{-1}Ng = g^{-1}gN = N$. Fordítva, tegyük fel, hogy $g^{-1}Ng \subseteq N$ minden $g \in G$ elemre. Így $gNg^{-1} \subseteq N$ is teljesül minden $g \in G$-re. Ebből $N = g^{-1}gNg^{-1}g \subseteq g^{-1}Ng \subseteq N$ és így $N = g^{-1}Ng$, azaz $gN = Ng$ adódik minden $g \in G$ elemre. Tehát N normális részcsoportja G-nek. □

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

Bizonyítás. Legyen N_i $(i \in I)$ egy G csoport normális részcsoportjainak nem üres halmaza. A 2.2.7 Tétel szerint $N = \cap_{i\in I} N_i$ a G részcsoportja. Legyenek $a \in N$ és $g \in G$ tetszőleges elemek. Akkor $a \in N_i$ minden $i \in I$ indexre, és ezért $g^{-1}ag \in N_i$ minden $i \in I$ indexre, azaz $g^{-1}ag \in N$. Így $g^{-1}Ng \subseteq N$. Az előző tétel szerint N normális részcsoportja G-nek.

2.5.4 Tétel *Egy G csoport normális részcsoportja szerinti mellékosztályok a G egy kompatibilis osztályozását adják. Fordítva, G minden kompatibilis osztályozásának osztályai a G valamely normális részcsoportja szerinti mellékosztályok. Tehát kölcsönösen egyértelmű megfeleltetés áll fenn egy csoport kompatibilis osztályozásai és normális részcsoportjai között.*

Bizonyítás Ha N egy G csoport normális részcsoportja, akkor (a 2.4.3 Tétel szerint) a G csoport N szerinti mellékosztályai a G egy osztályozását alkotják. Mivel tetszőleges $a, b \in G$ esetén

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)N^2 = (ab)N$$

is teljesül, ezért G nek az N szerinti osztűlyai a G egy kompatibilis osztályozását alkotják.

Fordítva, tegyük fel, hogy σ a G csoport egy kompatibilis osztályozása. Jelölje e a G csoport egységelemét, N pedig az e-t tartalmazó σ-osztályt. Ha $a, b \in N$ tetszőleges elemek, akkor $(a, b) \in \sigma$ és $(b, e) \in \sigma$, amiből $(ab, e) \in \sigma$ következik σ kompatibilitása miatt. Tehát $N^2 \subseteq N$. Mivel tetszőleges $a \in N$ elem esetén $(a, e) \in \sigma$, ezért $(e, a^{-1}) = (aa^{-1}, a^{-1} \in \sigma$, ami $a^{-1} \in N$ teljesülését jelenti. Tehát $N^{-1} \subseteq N$. Mivel $N^2 \subseteq N$ és $N^{-1} \subseteq N$, ezért (a 2.2.4 Tétel (2) feltétele miatt) N a G egy részcsoportja. Ha $a \in N$ és $g \in G$ tetszőleges elemek, akkor az $(a, e) \in \sigma$ teljesüléséből $(g^{-1}ag, g^{-1}eg) \in \sigma$ következik, azaz $(g^{-1}ag, e) \in \sigma$. Így $g^{-1}ag \in N$. Tehát $g^{-1}Ng \subseteq N$ teljesül tetszőleges $g \in G$ elemre. A Tétel szerint ez azt jelenti, hogy N a G csoport egy normális részcsoportja. Jelölje Σ_a a G csoport a elemét tartalmazó σ-osztályt. Tetszőleges $b \in N$ elem esetén $(b, e) \in \sigma$ teljesül, és ezért $(ab, a) = (ab, ae) \in \sigma$. Így $aN \subseteq \Sigma_a$. Mivel $a^{-1}a = e$, ezért $\Sigma_{a^{-1}}\Sigma_a \subseteq N$, amiből $a^{-1}\Sigma_a \subseteq N$ adódik. Ez utóbbiból az $\Sigma_a \subseteq aN$ is következik. Ez a tartalmazás a fentebb már bizonyított $aN \subseteq \Sigma_a$ tartalmazással együtt a $\Sigma_a = aN$ egyenlőséget eredményezi. Ez pedig azt bizonyítja, hogy a G csoport σ szerinti osztályai az N normális részcsopprt szerinti mellékosztályok. □

2.5.5 Definíció *Egy G csoporton értelmezett σ ekvivalenciarelációt a G csoport egy kongruenciájának nevezzük, ha a G csoport σ szerinti osztályai a G csoport egy kompatibilis osztályozását adják. Más szavakkal: egy G csoporton értelmezett σ ekvivalenciarelációt a G csoport egy kongruenciájának nevezzük, ha tetszőleges $a, b, c, d \in G$ elemek esetén az $(a, b) \in \sigma$ és $(c, d) \in \sigma$ feltételekből $(ac, bd) \in \sigma$ következik.*

A 2.5.4 Tétel azt is állítja, hogy kölcsönösen egyértelmű megfeleltetés áll fenn egy csoport kongruenciái és normális részcsoportjai között.

2.6. Faktorcsoport, Homomorfizmus-tétel

2.6.1 Tétel *Egy G csoport tetszőleges N normális részcsoportja szerinti mellékosztályai csoportot alkotnak az $(aN)(bN) = (ab)N$ komplexusszorzásra nézve.*

Bizonyítás Legyen N egy G csoport normális részcsoportja. Azt már korábban láttuk, hogy tetszőleges $a, b \in G$ elemekre $(aN)(bN) = (ab)N$ teljesül. Mivel tetszőleges $a, b, c \in G$ elemekre

$$(aN)[(bN)(cN)] = (aN)[(bc)N] = [a(bc)]N = [(ab)c]N =$$

$$= (ab)N](cN) = [(aN)(bN)](cN)$$

teljesül, ezért az N szerinti mellékosztályok halmazán a komplexusszorzás asszociatív. Tehát a G csoport N normális részcsoportja szerinti mellékosztályai félcsoportot alkotnak a komplexusszorzásra nézve. Világos, hogy ennek a félcsoportnak az egységeleme az $N = eN$ osztály, ahol e jelöli a G egységelemét. Mivel tetszőleges aN mellékosztály esetén $(aN)(a^{-1}N = eN = N$, ezért az aN mellékosztálynak az $a^{-1}N$ mellékosztály az inverze (ahol a^{-1} jelöli az a elem G-beli inverzét). □

2.6.2 Definíció *(Faktorcsoport) Egy G csoportot N normális részcsoportja szerinti faktorcsoportján azt a csoportot értjük, amelynek alaphalmaza a G csoport N szerinti mellékosztályainak G/N módon jelölt halmaza, a művelet pedig a komplexusok szorzása (lásd az előző tételt).*

2.6.3 Tétel *Egy G csoport tetszőleges N részcsoportja esetén az $a \mapsto aN$ $(a \in G)$ leképezés a G csoportnak a G/N faktorcsoportra való homomorfizmusa.*

Bizonyítás Jelölje φ a tételben szereplő leképezést. Tetszőleges $a, b \in G$ esetén $\varphi(ab) = (ab)N = (aN)(bN) = \varphi(a)\varphi(b)$. Tehát φ a G csoportnak a G/N faktorcsoportra való homomorfizmusa. □

2.6.4 Definíció *(Természetes homomorfizmus) Egy G csoportnak a G egy N normális részcsoportja szerinti faktorcsoportjára való $a \mapsto aN$ homomorfizmusát a G csoport G/N faktorcsoportra való természetes homomorfizmusának is nevezzük.*

2.6.5 Definíció *(Homomorfizmus magja) Egy G csoportnak egy G' csoportba való φ homomorfizmusának magján G mindazon a elemeinek Ker_φ-vel jelölt halmazát értjük, amelyek esetén $\varphi(a)$ a G' csoport egységeleme.*

2.6.6 Tétel *Egy G csoport tetszőleges φ homomorfizmusának magja a G csoport normális részcsoportja. Fordítva, egy G csoport tetszőleges normális részcsoportja a G egy alkalmas homomorfizmusának magja.*

Bizonyítás Legyenek G és G' tetszőleges csopportok, *varphi* pedig G-nek G'-be való tetszőleges homomorfizmusa. Jelölje e a G csoport egységelemét, e' pedig a G' csoport egységelemét. Ha $a, b \in Ker_\varphi$, akkor

$$\varphi(ab) = \varphi(a)\varphi(b) = e'e' = e'.$$

Így $ab \in Ker_\varphi$. Tehát Ker_φ zárt a szorzásra nézve. Mivel G elemei között érvényes az asszociativitás, ezért Ker_φ a G csoport egy részfélcsoportja. A 2.1.5 Tétel miatt $\varphi(e) = e'$, így Ker_φ a G egy részmonoidja. Tetszőleges $a \in Ker_\varphi$ elem esetén $\varphi(a^{-1}) = (\varphi(a))^{-1} = (e')^{-1} = e'$ (lásd a 2.1.5 Tételt). Így $a^{-1} \in Ker_\varphi$. Következésképpen Ker_φ a G részcsoportja. Legyenek $a \in Ker_\varphi, g \in G$ tetszőleges elemek. Akkor

$$\varphi(g^{-1}ag) = \varphi(g^{-1})\varphi(a)\varphi(g) = \varphi(g^{-1})e'\varphi(g) =$$
$$= \varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e) = e',$$

azaz $g^{-1}ag \in Ker_\varphi$. Tehát Ker_φ a G csoport normális részcsoportja.

Fordítva, ha N egy G csoport normális részcsoportja, akkor N a G csoport G/N faktorcsoportra való természetes homomorfizmusának a magja. □

Megjegyezzük, hogy ha φ egy G csoport homomorfizmusa, akkor tetszőleges $a, b \in G$ elemekre $\varphi(a) = \varphi(b)$ akkor és csak akkor teljesül, ha $aKer_\varphi = bKer_\varphi$. Ugyanis, $\varphi(a) = \varphi(b)$ akkor és csak akkor igaz, ha $ab^{-1} \in Ker_\varphi$, azaz, ha $aKer_\varphi = bKer_\varphi$.

2.6.7 Tétel *(Homomorfizmus-tétel) Ha φ egy G csoportnak egy G' csoportra való (szürjektív) homomorfizmusa, akkor $G' \cong G/Ker_\varphi$.*

Bizonyítás Az előző tétel szerint Ker_φ a G egy normális részcsoportja. Legyen $a' \in G'$ tetszőleges. Mivel φ szürjektív, ezért van olyan $a \in G$ elem, melyre $\varphi(a) = a'$ teljesül. Az előző tételt követő megjegyzés szerint az a' elem φ szerinti teljes inverz képe megegyezik az $aKer_\varphi$ mellékosztállyal. A $\Phi : aKer_\varphi \mapsto \varphi(a) = a'$ megfeleltetés kölcsönösen egyértelmű. Legyenek $aKer_\varphi, bKer_\varphi \in G/Ker_\varphi$ tetszőleges elemek. Akkor

$$\Phi(aKer_\varphi)\Phi(bKer_\varphi) = \varphi(a)\varphi(b) = \varphi(ab) = \Phi((ab)Ker_\varphi) =$$

$$= \Phi(aKer_\varphi bKer_\varphi).$$

Tehát Φ (kölcsönösen egyértelmű) homomorfizmus. Így Φ a G/Ker_φ faktorcsoportnak a G' csoportra való izomorfizmusa. □

2.7. Izomorfizmus-tételek

2.7.1 Tétel *Legyen N egy G csoport normális részcsoportja. Kölcsönösen egyértelmű megfeleltetés áll fenn a G/N faktorcsoport részcsoportjai és a G csoport N-et tartalmazó részcsoportjai között. Ennél a megfeleltetésnél normális részcsoportnak normális részcsoport felel meg.*

Bizonyítás

2.7.2 Tétel *(I. izomorfizmus-tétel) Ha a G csoportnak H tetszőleges részcsoportja, N pedig normális részcsoportja, akkor $N \cap H$ normális részcsoportja H-nak és*

$$NH/N \cong H/(N \cap H).$$

Bizonyítás Mivel N és H részcsoportjai G-nek, ezért metszetük is részcsoportja G-nek, így H-nak is. Legyenek $g \in H$ és $a \in N \cap H$ tetszőleges elemek. Mivel $a \in N$ és N normális részcsoportja G-nek, ezért $g^{-1}ag \in N$. Mivel $g, h \in H$, ezért $g^{-1}ag \in H$. Tehát $g^{-1}ag \in N \cap H$. A normális részcsoportok jellemzésére vonatkozó tétel szerint ez azt jelenti, hogy $N \cap H$ normális részcsoportja H-nak. Mivel N normális részcsoportja G-nek, ezért az N és a H

részcsoport által generált részcsoport egyenlő az $NH = HN$ szorzattal. Jelölje φ az NH szorzatnak az NH/N faktorcsoportra való természetes homomorfizmusát. Tetszőleges $nh \in NH$ elemre $\varphi(nh) = \varphi(n)\varphi(h) = \varphi(h)$, mert $\varphi(n)$ az NH/N faktorcsoport egységeleme. Így $\varphi(NH) = \varphi(H) = NH/N$, és ezért a φ homomorfizmusnak a H részcsoportra való φ^* leszűkítése a H részcsoportnak az NH/N csoportra való (szürjektív) homomorfizmusa. Ennek a homomorfizmusnak a magja egyenlő az $N \cap H$ metszettel. A homomorfizmus-tétel szerint ebből $H/(N \cap H) \cong NH/N$ következik. □

2.7.3 Tétel *(II. izomorfizmus-tétel) Ha N és M egy G csoport olyan normális részcsoportjai melyekre teljesül az $N \subseteq M$ tartalmazás, akkor M/N a G/N-nek normális részcsoportja és*

$$(G/N)/(M/N) \cong G/M.$$

Bizonyítás A 2.7.1 Tétel szerint M/N a G/N faktorcsoport egy normális részcsoportja. Jelölje $\varphi_1()$ a G csoportnak a G/N faktorcsoportra, $\varphi_2()$ pedig a G/N faktorcsoportnak a $(G/N)/(M/N)$ faktorcsoportra való természetes homomorfizmusát. Akkor a ezen homomorfizmusok egymás után való végrehajtásával definiált $\varphi_2 \circ \varphi_1()$ leképezés a G csoportnak a $(G/N)/(M/N)$ faktorcsoportra val (szürjektív) homomorfizmusa, melynek magja M. A homomorfizmus-tétel miatt ebből $G/M \cong (G/N)/M/N)$ következik. □

2.8. Centrum, centralizátor, normalizátor, a Cauchy-tétel bizonyítása

2.8.1 Definíció *(Centrum) Egy G csoportnak $Z(G)$-vel jelölt centrumán értjük mindazon c elemeinek összességét, amelyekre $ac = ca$ teljesül a G minden a eleme esetén. Más szavakkal, $c \in Z(G)$ akkor és csak akkor, ha c felcserélhető a G minden a elemével.*

2.8.2 Definíció *(Konjugálás) Egy G csoport a elemének G egy g elemével való konjugáltján a G csoport $g^{-1}ag$ elemet értjük.*

Legyen G egy csoport. Definiáljunk egy σ binér relációt G-n a következőképpen. A G valamely a és b elemei esetén $(a, b) \in \sigma$ akkor és csak akkor, ha van olyan G-beli g elem, amelyre $g^{-1}ag = b$ teljesül. Megmutatható, hogy σ ekvivalenciareláció, melynek osztályait a G konjugáltsági osztályainak nevezzük. Egy elemet tartalmazó konjugáltsági osztály az illető elem összes lehetséges különböző konjugáltjait tartalmazza.

2.8.3 Tétel *Egy G csoport valamely a eleme akkor és csak akkor eleme a G centrumának, ha megegyezik G tetszőleges elemével képezet konjugáltjával (azaz, ha az a elem minden konjugáltja önmaga).*

Bizonyítás A G csoport valamely a elemére $a \in Z(G)$ akkor és csak akkor teljesül, ha minden $g \in G$ elemre $ag = ga$ teljesül, ami azzal akvivalens (g inverzével balról való szorzás révén), hogy $g^{-1}ag = a$. □

2.8.4 Definíció *(normalizátor, centralizátor) Egy G csoport valamely A részhalmazának normalizátorán értjük G mindazon x elemeinek $N(A)$ összességét, amelyekre $xA = Ax$ teljesül. Az egyelmű $\{a\}$ halmazok normalizátorát az a elem centralizátorának is nevezzük és $C(a)$-val jelöljük. Tehát $C(a) = \{x \in G : \ xa = ax\}$.*

2.8.5 Tétel *Egy G csoport minden A részhalmazának normalizátora (és így minden a elemének centralizátora) a G csoportnak részcsoportja.*

Bizonyítás Legyen $A \subseteq G$ tetszőleges részhalmaz. Mivel $e \in N(A)$, ezért $N(A) \neq$. Ha $x, y \in N(A)$, akkor $(xy)A = x(yA) = x(Ay) = (xA)y = (Ax)y = A(xy)$, és ezért $xy \in N(A)$. Ha $x \in N(A)$, akkor $xA = Ax$. Ha ezt az egyenlőséget megszorozzuk mindkét oldalról az x^{-1} elemmel, akkor az $x^{-1}A = Ax^{-1}$ egyenlőséget kapjuk, azaz $x^{-1} \in N(A)$. Tehát $N(A)$ a G csoport olyan nem üres részhalmaza, amelyre $N(A)N(A) \subseteq N(A)$ és $N^{-1}(A) \subseteq N(A)$ teljesül. A 2.2.4 Tétel szerint ebből az következik, hogy $N(A)$ a G csoport egy részcsoportja. □

2.8.6 Tétel *Egy G csoport valamely A részhalmazának (a elemének) annyi különböző konjugáltja van, amennyi az A részhalmaz normalizátorának (az a elem centralizátorának) G-beli indexe.*

Bizonyítás Legyen $A \subseteq G$ és $g, h \in G$ tetszőlegesek. $g^{-1}Ag = h^{-1}Ah$ akkor és csak akkor teljesül, ha $A(gh^{-1}) = (gh^{-1})A$ (itt g-vel szoroztunk balról és h^{-1}-gyel jobbról, de használtuk azt a tényt is, hogy minden csoport egyszerűsitéses). Ezen utóbbi egyenlőség azzal ekvivalens a 2.4.2 Tétel duálisa szerint, hogy a és b az $N(A)$ részcsoportnak ugyanabban a jobb oldali mellékosztályában vannak. Ebből már következik, hogy az A részhalmaznak annyi különböző konjugáltja van, ahány jobb oldali mellékosztálya van az $N(A)$ részcsoportnak, azaz amennyi az $N(A)$ normalizátor G-beli indexe. □

A centrum definíciója alapján, egy csoport akkor és csak akkor kommutatív, ha megegyezik centrumával. Véges G csoport esetén ez a $\mid G \mid = \mid Z(G) \mid$ egyenlőség teljesülését jelenti

2.8.7 Tétel *(Osztályegyenlet) Legyen G egy véges nem kommutatív csoport. Akkor megadható olyen r pozitív egész szám és megadhatók olyan egynél nagyobb $k_1, \ldots, k_r$ egészek, hogy*

$$\mid G \mid = \mid Z(G) \mid + k_1 + \cdots + k_r$$

teljesül. Ebben a képletben r egyenlő a G csoport $Z(G)$ komplementere által tartalmazott konjugáltsági osztályok számával, $k_1, \ldots, k_r$ pedig rendre az ezen konjugáltsági osztályokban levő elemek számát jelöli, és így a G csoport rendjének osztói.

Bizonyítás Jelölje σ a fentiekben definiált relációt: $(a, b) \in \sigma$ akkor és csak akkor teljesül valamely $a, b \in G$ elemekre, ha ezen elemek egymás konjugáltjai. Mint ahogy azt már említettük, a σ reláció ekvivalencia-reláció. A $Z(G)$-beli elemek σ-osztályai egyeleműek, a $G \setminus Z(G)$ halmazban lévő elemek σ-osztályai legalább kételeműek. Jelöljük r-rel a $G \setminus Z(G)$ halmazban lévő σ-osztályok számát, továbbá jelölje rendre $k_1, \ldots, k_r$ az ezen σ-osztályokban lévő elemek számát. Mivel k_i $(i = 1, \ldots, r)$ a hozzá tartozó K_i σ-osztályban lévő elemek számét jelöli, ezért tetszőleges $a \in K_i$ elemre az teljesül, hogy k_i megegyezik a $C(a)$ centralizátor indexével, amely (a Lagranre-tétel szerint) osztója a G csoport rendjének; tehát k_i a G csoport rendjének osztója. □

2.8.8 Tétel *Ha egy G véges csoport rendje p^n, ahol p egy prím és $n \geq 1$ egész szám, akkor $\mid Z(G) \mid > 1$.*

Bizonyítás Kommutatív G csoport esetén az állítás nyilvánvaló. Ha G nem kommutatív, akkor a 2.8.7 Tétel szerint

$$\mid G \mid = \mid Z(G) \mid + k_1 + \cdots + k_r$$

teljesül, ahol $k_1, \ldots, k_r$ jelöli a $Z(G)$ komplementere által tartalmazott konjugáltsági osztályokban levő elemek számát, és így ezek olyan 2-nél nem kisebb egész számok, amelyek a G csoport rendjének osztói. Mivel G rendje p-hatvány, ezért a k_i számok mindegyike p-hatvány, és így oszthatók p-vel. Mivel p osztója a G csoport rendjének, ezért az osztályegyenlet $\mid Z(G) \mid$ tagja is osztható p-vel, és ezért $\mid Z(G) \mid \geq 2$. □

2.8.9 Tétel *Minden p^2-rendű csoport kommutatív.*

Bizonyítás Ha G tartalmaz p^2-rendű a elemet, akkor $G = \langle a \rangle$, azaz G ciklikus, és így kommutatív. Vizsgáljuk azt az esetet, amikor G minden e-től különböző eleme p-edrendű. Mivel $\mid Z(G) \mid \leq 2$ a 2.8.8 Tétel szerint, ezért $Z(G)$ tartalmaz egy p-edrendű c elemet. Ha $b \in G$ és $b \notin \langle c \rangle$, akkor $G = \langle b, c \rangle$ és $bc = cb$. Mivel a két generáló elem egymással felcserélhető, ezért az általuk generált G csoport kommutatív. □

Augustin Cauchy (1789 – 1857)

2.8.10 Tétel *(Cauchy-tétel) Ha egy p prímszám osztója egy véges G csoport rendjének, akkor a G csoport tartalmaz p-edrendű elemet.*

Bizonyítás. A bizonyítást a csoportok n rendjére vonatkozó teljes indukcióval végezzük. Ha $n = 2$, akkor az állítás nyilvánvalóan teljesül. Legyen

$n > 2$ tetszőleges pozitív egész szám, és tegyük fel, hogy az állítás minden n-nél kisebb rendszámú csoportra érvényes, azaz minden m-edrendű ($m < n$) H csoport esetén igaz, hogy ha valamelyik prím osztója m-nek, akkor H tartalmaz p-edrendű elemet. Megmutatjuk, hogy minden n-edrendű G csoportra és n minden p prím osztójára igaz, hogy G tartalmaz p-ederndű elemet. A bizonyítást indirekt módon végezzük el. Tegyük fel (indirekt módon), hogy van olyan n-edrendű G csoport és olyan p prím, amely osztója n-nek, de G-nek nincs p-edrendű eleme. Természetesen, ekkor G egyetlen részcsoportja sem tartalmaz p-edrendű elemet. Két esetet vizsgálunk.

Az első esetben feltesszük, hogy G nem kommutatív. Ekkor $G \neq Z(G)$, ahol $Z(G)$ jelöli a G centrumát. Mivel $Z(G)$ rendje kisebb n-nél (és mert $Z(G)$ nem tartalmaz p-edrendű elemet, ezért (az indukciós feltételt is használva) $Z(G)$ rendje nem osztható p-vel. Használjuk az osztályegyenlőséget:

$$\mid G \mid = \mid Z(G) \mid + k_1 + \cdots + k_m,$$

ahol $k_1, \ldots, k_m$ jelöli rendre $Z(G)$ komplementerében levő $K_1, \ldots, K_m$ konjugált osztályokban lévő elemek számát. Ezen számok mindegyike legalább 2. Ismert, hogy k_j megegyezik a K_j konjugáltsági osztály tetszőleges a_j eleméhez tartozó $C(a_j)$ centralizátor $\mid G : C(a_j) \mid$ indexével. Az világos, hogy $C(a_j) \neq G$; ellenkező esetben azt kapnánk, hogy a_j centrumbeli elem, s ekkor $k_j = 1$ teljsülne. Így (az indukciós feltételt is használva) $C(a_j)$ rendje nem osztható p-vel. Mivel p osztja a G csoport rendjét és

$$\mid G \mid = \mid C(a_j) \mid\mid G : C(a_j) \mid,$$

ezért p osztja a $k_j = \mid G : C(a_j) \mid$ számok mindegyikét. Az osztályegyenlőség alapján ebből arra következtethetünk, hogy p osztja a $Z(G)$ centralizátor rendjét (használva azt is, hogy p osztja a G csoport rendjét). Ez ellentmond annak a már korábban kapott eredménynek, hogy p nem osztója a $Z(G)$ centralizátor rendjének.

A második esetében feltesszük, hogy a vizsgált G csoport kommutatív. Legyen $G = \{g_1, g_2, \ldots, g_n\}$. Tetszőleges $j \in \{1, 2, \ldots, n\}$ index esetén jelölje m_j a g_j elem rendjét. Az világos, hogy p nem osztja az m_j számok egyikét sem. Ugyanis, ha valamelyik j indexre teljesülne, hogy p osztja az m_j számot, akkor a $g_j^{\frac{m_j}{p}}$ elem rendje p lenne, ami az indirekt feltétel miatt nem lehet. Jelölje m az $m_1, m_2, \ldots m_n$ számok legkisebb közös többszörösét. Akkor $g_j^m = e$ teljesül minden $j = 1, 2, \ldots, n$ indexre, ahol e jelöli G egységelemét. Mivel p

nem osztója az m_j számnak minden $j = 1, 2, \ldots, n$ index esetén, ezért p nem osztója m-nek. Jelölje f a $(Z/(m))^n$ additív csoportnak G-be való következő leképezését: a $(Z/(m))^n$ csoport tetszőleges $([a_1], [a_2], \ldots, [a_n])$ eleme esetén

$$f : ([a_1], [a_2], \ldots, [a_n]) \mapsto g_1^{a_1} g_2^{a_2} \cdots g_n^{a_n}.$$

Megjegyezzük, hogy f jól definiált, ugyanis, ha $[a_j] = [b_j]$, akkor a_j-nek és b_j-nek az m-mel való maradékos osztásánál ugyanaz a maradék, azaz $a_j = mt_j + r$, $b_j = ms_j + r$, és ezért

$$g_j^{a_j} = g_j^{mt_j+r} = (g_j^m)^{t_j} g_j^r = g_j^r = (g_j^m)^{s_j} g_j^r = g_j^{ms_j+r} = g_j^{b_j}.$$

Ha $[a_j]$ az 1-et tartalmazó osztály, a többi osztály mindegyike pedig a 0-t tartalmazza, akkor

$$f : ([a_1], [a_2], \ldots, [a_n]) \mapsto g_j.$$

Így f szürjektív. G kommutativitása miatt f homomorfizmus. A homomorfizmustétel szerint

$$(Z/(m))^n / ker f \cong G,$$

amiből

$$| (Z/(m))^n | = | G | \, | ker f |$$

adódik, és így $m^n = n \mid ker f \mid$. Mivel a p prím osztja n-et, azért ebből az egyenlőségből az adódik, hogy a p prím osztja az m^n hatványt. Ez csak úgy lehetséges, hogy p osztja m-et. Korábban már megállapítottuk, hogy p nem osztja m-et. Így ellentmondásra jutottunk.

Mivel mind a két esetben ellentmondásra jutottunk, ezért az indirekt feltétel nem igaz. Ezzel bebizonyítottuk, hogy a tétel állítása igaz. □

2.8.11 Definíció *(p-csoport) Adott p prímszám esetén, egy csoportot p-csoportnak nevezünk, ha minden elemének rendje a p prímszám valamely (nemnegatív egész kitevőjű) hatványa.*

2.8.12 Következmény *Minden véges p-csoport rendje p-hatvány.*

Bizonyítás Egyelemű csoportra az állítás nyilvánvaló. Legyen G egy olyan véges p-csoport, amely legalább két elemet tartalmaz. A Lagrange-tétel szerint G rendje osztható p-vel. Ha G rendje osztható lenne egy olyan q prímmel is, amely különbözik p-től, akkor a Cauchy-tétel miatt G-nek lenne q-adrendű eleme, ami nem lehetséges, hiszen G minden elemének rendje p-hatvány. □

2.9. Normállánc, a Jordan–Hölder-tétel

2.9.1 Definíció *(Normállánc) Egy G csoportot részcsoportjainak olyan véges sorozatát, amely G-vel kezdődik, G egységelemével, e-vel végződik, és mindegyik közbülső részcsoport normális részcsoportja a megelőzőnek, a G csoport normálláncának nevezzük:*

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = e.$$

A

$$G_0/G_1, G_1/G_2, \ldots G_{r-1}/G_r$$

faktorcsoportokat a normállánc faktorainak nevezzük. Ezek száma r, azaz megegyezik a lánc hosszával. Ha egy normálláncban szereplő részcsoportok mind különbözőek, akkor a normálláncot ismétlődés nélkülinek mondjuk.

2.9.2 Definíció *(Normálláncok izomorfiája) Egy G csoport*

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = e$$

és

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd_{s-1} \rhd H_s = e$$

normálláncáról azt mondjuk, hogy izomorfak, ha az egyes normálláncok faktoraiból álló $\{G_0/G_1, G_1/G_2, \ldots G_{r-1}/G_r\}$ és $\{H_0/H_1, H_1/H_2, \ldots H_{s-1}/H_s\}$ halmazok között megadható olyan kölcsönösen egyértelmű megfeleltetés, hogy az egymásnak megfeleltetett faktorcsoportok izomorfak.

Egymással izomorf normálláncok hossza szükségképpen megegyezik. Normálláncok izomorfizmusa reflexiv, szimmetrikus és tranzitív reláció egy G csoport összes normálláncának halmazán.

2.9.3 Definíció *(Normálláncok finomítása) A*

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_{s-1} \rhd H_s = e$$

normálláncot a

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = e$$

normállánc finomításának nevezzük, ha a G_i $(i = 0, \dots r)$ részcsoportok mindegyike megegyezik valamely H_j $(j = 0, \dots, s)$ részcsoporttal. Ekkor természetesen $r \leq s$.

2.9.4 Definíció *(Kompozíciólánc) Egy normálláncot kompozícióláncnak nevezünk, ha ismétlődés nélküli és tovább már csak úgy finomítható, hogy a benne szereplő részcsoportokat ismételten kiírjuk.*

2.9.5 Tétel *Egy normállánc akkor és csak akkor kompozíciólánc, ha faktorai egyszerű csoportok.*

Bizonyítás Ha egy $G = G_0 \rhd G_1 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_{r-1} \rhd G_r = e$ normálláncban $G_i \neq G_{i+1}$, akkor a 2.7.1 Tétel szerint kölcsönösen egyértelmű megfeleltetés van a G_i/G_{i+1} faktorcsoport részcsoportjai és G_i-nek a G_{i+1}-et tartalmazó részcsoportjai között; ennél a megfeleltetésnél normális részcsoportnak normális részcsoport felel meg. Így a G_i és G_{i+1} közzé akkor és csak akkor nem iktatható be egy olyan G' részcsoport, hogy $G_i \rhd G' \rhd G_{i+1}$ teljesüljön, ha a G_i/G_{i+1} faktorcsoport egyszerű. □

Camille Jordan (1838 – 1922)

Otto Hölder (1859 – 1937)

2.9.6 Tétel *(Jordan-Hölder tétele) Ha egy G csoportnak van kompozíciólánca, akkor G bármely két kompozíciólánca egymással izomorf.*

Bizonyítás (Véges G csoportra) A tételt a lánc r hosszára vonatkozó teljes indukcióval igazoljuk. Ha egy G csoportnak van $r = 1$ hosszúságú kompozíciólánca, akkor ez a $G \rhd e$ lánc, amiből következik, hogy a G csoport egyszerű, és így G-nek nincs is több kompozíciólánca. Legyen $r \geq 2$, és tegyük fel, hogy a tétel állítása igaz minden olyan véges csoportra, amelynek van r-nél kisebb hosszúságú kompozíciólánca. Legyen G olyan csoport, amelynek van r hosszúságú

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = e \tag{2.1}$$

kompozíciólánca. Megmutatjuk, hogy ez a kompozíciólánc izomorf a G csoport bármely másik

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_{s-1} \rhd H_s = e \tag{2.2}$$

kompozícióláncával.

Ha $G_1 = H_1$, akkor

$$G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = e$$

a $G_1 = H_1$ csoport egy $r - 1$ hosszúságú kompozíciólánca. Mivel

$$H_1 \rhd H_2 \rhd \cdots \rhd H_{s-1} \rhd H_s = e$$

ugyancsak kompozíciólánca a $G_1 = H_1$ csoportnak, ezért (az indukciós feltétel miatt) $r = s$ és ezen két, $G_1 = H_1$-ből induló kompozíciólánc egymással izomorf. Mivel $G/G_1 = G/H_1$, ezért az eredeti (2.1) és (2.2) kompozíciólláncok is izomorf egymással.

A továbbiakban vizsgáljuk azt az esetet, amikor $G_1 \neq H_1$. Mivel sem G és G_1, sem G és H_1 közzé nem iktatható be tőlük különböző normális részcsoport, ezért G_1 is és H_1 is a G csoport maximális részcsoportjai. Mivel a G_1 és H_1 által generált G_1H_1 részcsoport a G csoport G_1-et és H_1-et valódi módon tartalmazó normális részcsoportja, ezért $G_1H_1 = G$. Mivel a

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = e$$

lánc a G egy kompozíciólánca, ezért

$$G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = e$$

a G_1 egy kompozíciólánca. Mivel ennek hossza $r - 1$, ezért G_1-re alkalmazhatjuk az indukciós feltételt, ami miatt G_1 bármely két kompozíciólánca

egymással izomorf, és így bármely kompozícióláncának hossza $r-1$. Az I. izomorfizmus-tétel szerint $G_1/(G_1 \cap H_1) \cong G/H_1$. Mivel G/H_1 egyszerű csoport, ezért $G_1 \cap H_1$ a G_1 csoport maximális normális részcsoportja. Mivel $G_1 \cap H_1$ véges csoport, ezért van kompozíciólánca:

$$(G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_u = e.$$

Így

$$G_1 \rhd (G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_u = e \tag{2.3}$$

a G_1 csoport egy kompozíciólánca. Mivel G_1 minden kompozícióláncának hossza $r-1$, ezért ennek a kompozícióláncnak a hossza is $r-1$, és így $u+1 = r-1$, azaz $u = r-2$. Tehát a $G_1 \cap H_1$ csoport

$$(G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_{r-2} = e.$$

kompozíciólánc hossza $r-2$. Az világos, hogy a

$$G \rhd G_1 \rhd (G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_{r-2} = e$$

és

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = e$$

kompozícióláncok egymással izomorfak, mert

$$G_1 \rhd (G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_{r-2} = e$$

és

$$G_1 \rhd G_2 \rhd \cdots \rhd G_r = e$$

a G_1 csoport ($r-1$ hosszúságú) kompozícióláncai, és így ezek egymással izomorfak az indukciós feltétel miatt.

Az előzőekhez hasonló gondolatmenet alkalmazásával kapjuk, hogy

$$G \rhd H_1 \rhd (G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_{r-2} = e$$

és

$$G \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_s = e$$

kompozícióláncok egymással izomorfak, és $s = r$. Az I. izomorfizmus-tétel szerint nem csak $G_1/(G_1 \cap H_1) \cong G/H_1$, hanem $H_1/(G_1 \cap H_1) \cong G/G_1$ is teljesül, így a

$$G \rhd G_1 \rhd (G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_{r-2} = e$$

és

$$G \rhd H_1 \rhd (G_1 \cap H_1) \rhd T_2 \rhd \cdots \rhd T_{r-2} = e$$

kompozícióláncok izomorfak. A normálláncok izomorfiájának tranzitivitása miatt a

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = e$$

és

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_{s-1} \rhd H_s = e$$

kompozícióláncok izomorfak. □

2.10. Kommutátor részcsoport

2.10.1 Definíció *(Két elem kommutátora) Egy G csoport a és b elemeiből képezett (a, b) elempár kommutátorán a G csoport $[a, b] = a^{-1}b^{-1}ab$ elemét értjük.*

Világos, hogy egy G csoport tetszőleges a és b elemei esetén $[a, b]^{-1} = [b, a]$. Így $[a, b] = e$ (e a G csoport egységeleme) akkor és csak akkor teljesül, ha $[b, a] = e$. Továbbá, egy G csoport a és b elemei akkor és csak akkor felcserélhetőek (azaz, $ab = ba$), ha $[a, b] = e$ és $[b, a] = e$.

2.10.2 Definíció *(Kommutátor részcsoport) Egy G csoport azon részcsoportját, amelyet a G elemeiből képezhető összes elempár kommutátorainak halmaza generál, a G csoport kommutátor részcsoportjának nevezzük és G'-vel jelöljük.*

2.10.3 Tétel *Egy G csoport G' kommutátor részcsoportja a G-nek normális részcsoportja és a G/G' faktorcsoport kommutatív.*

Bizonyítás A G csoport tetszőleges a, b és g elemei esetén

$$g^{-1}[a, b]g = g^{-1}a^{-1}b^{-1}abg = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = [g^{-1}ag, g^{-1}bg].$$

Igy tetszőleges $[a_1, b_1][a_2, b_2] \cdots [a_r, b_r] \in G'$ és $g \in G$ elemek esetén

$$g^{-1}([a_1, b_1][a_2, b_2] \cdots [a_r, b_r])g = g^{-1}[a_1, b_1]gg^{-1}[a_2, b_2]g \cdots gg^{-1}[a_r, b_r]g \in G'$$

, amiből következik, hogy a G' karakterisztikus részcsoport a G csoport normális részcsoportja.

A G csoport tetszőleges a és b elemeire

$$(ba)^{-1}(ab) = a^{-1}b^{-1}ab = [a, b] \in G',$$

amiből $abG' = baG'$ azaz $(aG')(bG') = (bG')(aG')$ következik. Ez pedig azt jelenti, hogy a G/G' faktorcsoport elemei egymással felcserélhetőek, azaz a G/G' faktorcsoport kommutatív. □

2.10.4 Tétel *Egy G csoport valamely N normális részcsoportja esetén a G/N faktorcsoport akkor és csak akkor kommutatív, ha $G' \subseteq N$.*

Bizonyítás Tegyük fel, hogy $G' \subseteq N$. Akkor (a második izomorfizmustétel szerint) N/G' a G/G' normális részcsoportja és a $(G/G')/(N/G')$ faktorcsoport izomorf a G/K faktorcsoporttal. Mivel a G/G' csoport kommutatív (az előző tétel szerint), ezért annak bármely faktorcsoportja is kommutatív. Így a G/N faktorcsoport kommutatív.

Fordítva, tegyük fel, hogy a G/N faktorcsoport kommutatív. Akkor tetszőleges $a, b \in G$ elemekre $(aN)(bN) = (bN)(aN)$, azaz $abN = baN$. Ez azzal ekvivalens, hogy

$$[a, b] = a^{-1}b^{-1}ab = (ba)^{-1}(ab) \in N.$$

Tehát $G' \subseteq N$. □

2.10.5 Definíció *(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.

2.11. Feloldható csoportok

2.11.1 Definíció *(Feloldható csoport) Egy csoportot feloldható csoportnak nevezünk, ha van olyan normállánca, melynek faktorai kommutatív csoportok.*

Megjegyezzük, hogy minden kommutatív csoport feloldható. A következő tétel a véges felodható csoportokat jellemzi.

2.11.2 Tétel *Egy véges csoport akkor és csak akkor feloldható, ha kompozícióláncának faktorai prímrendű ciklikus csoportok.*

Bizonyítás Mivel véges csoport minden normállánca kompozíciólánccá finomítható, ezért egy véges csoport akkor és csak akkor feloldható, ha kompozícióláncának faktorai kommutatívak. Mivel a kompozícióláncok faktorai egyszerű csoportok, ezért egy kompozíciólánc faktorai akkor és csak akkor kommutatívak, ha azok kommutatív egyszerű csoportok, amelyek pontosan a prímrendű ciklikus csoportok. □

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

Bizonyítás ... □

Bizonyítás nélkül ismertetjük a következő két tételt.

William Burnside (1852 – 1927)

2.11.4 Tétel *(Burnside-tétel) Ha a G csoport rendje $p^n q^m$, ahol p és q prímek, n és m pedig nemnegatív egészek, akkor a G csoport feloldható.*

Walter Feit (1930 – 2004)

John G. Thompson (1736 – 1813)

2.11.5 Tétel *(Feit-Thompson-tétel) Minden véges páratlan rendű csoport feloldható.*

A következő tétel ugyan a 2.11.4 Tétel egy következménye, de részletezzük a bizonyítását is.

2.11.6 Tétel *Minden prímhatványrendű csoport feloldható.*

Bizonyítás Legyen a G csoport rendje p^n. Ha $n = 0$, akkor G egyelemű, és ezért feloldható. Tegyük fel, hogy $n > 1$. Akkor a 2.8.8 Tétel szerint G centruma nem triviális (azaz nem csak az egységelemet tartalmazza). Jelöljük ezt a centrumot C_1-gyel. Ha $C_1 = G$, akkor G kommutatív, és ezért feloldható. Tegyük fel, hogy $C_1 \neq G$. A G/C_1 faktorcsoport alacsonyabb rendű, mint G, a rendje pedig ismét 1-nél nagyobb p-hatvány. A 2.7.1 Tétel szerint G-nek van olyan C_1-et tartalmazó C_2 normális részcsoportja, hogy a $C_2/C1$ faktorcsoport izomorf a G/C_1 faktorcsoport centrumával. Folytatva a gondolatmenetet, kapjuk az

$$e \lhd C_1 \lhd C_2 \lhd \dots$$

szigorúan növekvő láncot, amely G végessége miatt egyszer csak eléri G-t:

$$e \lhd C_1 \lhd C_2 \lhd \cdots \lhd C_r \lhd G.$$

Ez a G-nek olyan normállánca, melynek faktorai kommutatívak. Így G feloldható csoport. □

2.11.7 Definíció *(Nilpotens csoport) Egy G csoportot nilpotens csoportnak nevezünk, ha van centrális lánca, azaz olyan*

$$\{e\} = G^{(0)} \lhd G^{(1)} \lhd \cdots \lhd G^{(k)} = G$$

normállánca, amelyben szereplő részcsoportok G-nek normális részcsoportjai, és minden $0 \leq i < leqk - 1$ indexre $G^{(i+1)}/G^{(i)} \subseteq Z(G/G^{(i)})$.

2.11.8 Tétel *Minden nilpotens csoport feloldható.*

Bizonyítás Mivel a centrális lánc olyan normállánc melynek minden $G^{(i+1)}/G^{(i)}$ faktora kommutatív (ugyanis része a $G/G^{(i)}$ faktorcsoport centrumának), ezért a tétel állítása nyilvánvaló. □

2.12. Permutációcsoportok

2.12.1 Definíció *(n-edfokú permutáció) Az $\{1, 2, \ldots, n\}$ halmaz önmagára való kölcsönösen egyértelmű leképezéseit n-edfokú permutációknak nevezzük és a következőképpen jelöljük:*

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ (1)\sigma & (2)\sigma & \ldots & (n)\sigma \end{pmatrix}.$$

Mint ahogy az a jelölésből is látható, a permutációknál a jobbról való hatásnak megfelelő írásmódot használjuk. Ennek megfelelően, ha σ és τ n-edfokú permutációk, akkor $\sigma\tau$ szorzatukra

$$\sigma\tau : k \mapsto ((k)\sigma)\tau \tag{2.4}$$

teljesül.

2.12.2 Definíció *Az n-edfokú permutációk S_n halmaza $n!$ rendű csoportot alkot a permutációk (2.4) szorzására nézve.*

Bizonyítás Közismert, hogy $| S_n | = n!$. Egy halmaz önmagába való leképezései (transzformációi) félcsoportot alkotnak a leképezések szorzására (mint a leképezések egymás után való végrehajtására) nézve, így S_n is félcsoportot alkot a (2.4) szorzásra nézve. Az identikus reláció az S_n félcsoport egységeleme. Egy n-edfokú σ permutáció inverz leképezése a σ permutáció S_n-beli inverze. Tehát azt kaptuk, hogy S_n egy $n!$ rendű csoportot alkot a permutációk (2.4) szorzására nézve. □

2.12.3 Definíció *(n-edfokú szimmetrikus csoport) Az $\{1, 2, \ldots, n\}$ halmaz önmagára való kölcsönösen egyértelmű leképezéseinek S_n csoportját n-edfokú szimmetrikus csoportnak, az S_n csoport részcsoportjait n-edfokú permutációcsoportoknak nevezzük.*

2.12.4 Definíció *Legyen (i, j) olyan számpár, amelyben i és j is az $1, 2, \ldots, n$ számok valamelyike úgy, hogy $i < j$. Egy ilyen számpárról azt mondjuk, hogy az n-edfokú σ permutáció egy inverziója, ha $(i)\sigma > (j)\sigma$. Egy σ permutációt páros permutációnak vagy páratlan permutációnak nevezünk attól függően, hogy σ inverzióinak száma páros vagy páratlan.*

2.12.5 Tétel *Az n-edfokú páros permutációk A_n-nel jelölt halmaza az S_n csoport normális részcsoportja.*

Bizonyítás Az $x_1, x_2, \ldots, x_n$ határozatlanokkal készítsük el azt az $\mathcal{A}$ szorzatot, amelynek tényezői az olyan $x_i - x_k$ különbségek, amelyekre $1 \leq k < i \leq n$ teljesül. Adott n-edfokú σ permutáció esetén jelölje $\mathcal{A}_\sigma$ az összes olyan $x_{(i)\sigma} - x_{(k)\sigma}$ különbség szorzatát, amelyekre $1 \leq (k)\sigma < (i)\sigma \leq n$ teljesül. Könnyen belátható, hogy minden n-edfokú σ permutációra $\mathcal{A}_\sigma = \pm\mathcal{A}$; az $\mathcal{A}_\sigma = \mathcal{A}$ egyenlőség akkor és csak akkor teljesül, ha σ páros permutáció. Ebből már adódik, hogy páros permutációk szorzata páros, így A_n az S_n csoport egy részfélcsoportja. Mivel az identikus permutáció páros, és páros permutáció inverze is páros, ezért A_n az S_n csoport egy részcsoportja. Mivel $\mid S_n \mid = n!$ és $\mid A_n \mid = \frac{n!}{2}$, ezért az A_n részcsoport S_n-beli indexe 2, és így A_n az S_n csoport normális részcsoportja. □

2.12.6 Definíció *Az S_n csoport A_n részcsoportját n-edfokú alternáló csoportnak nevezzük.*

2.12.7 Megjegyzés Mivel S_n-ben a páros permutációk A_n részcsoportja egy 2 indexű normális részcsoport, ezért azonos paritású permutációk szorzata páros, ellentétes paritású permutációk szorzata pedig páratlan.

2.12.8 Definíció *Legyen $i_1, i_2, \ldots, i_{k-1}, i_k$ páronként különböző $\{1, 2, \ldots, n\}$ halmazbeli elemek egy sorozata. Ha egy n-edfokú σ permutációra*

$$\sigma : i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_{k-1} \mapsto i_k, i_k \mapsto i_1$$

teljesül, viszont az $i_1, i_2, \ldots, i_{k-1}, i_k$ elemek között nem szereplőket fixen hagyja, akkor a σ permutációt k hosszúságú ciklusnak nevezzük és $(i_1\ i_2\ \ldots\ i_k)$ módon jelöljük. A 2 hosszúságú ciklusokat transzpozícióknak nevezzük.

2.12.9 Definíció *Akkor mondjuk, hogy az* $(i_1\ i_2\ \dots\ i_k)$ *és* $(j_1, j_2, \dots j_r)$ *ciklusok diszjunktak, ha az* $\{i_1, i_2, \dots, i_k\}$ *és* $\{j_1, j_2, \dots, j_r\}$ *halmazok diszjunktak.*

2.12.10 Tétel *Minden* S_n*-beli permutáció előáll (a tényezők sorrendjétől eltekintve) egyértelműen* S_n*-beli diszjunk ciklusok szorzataként.*

Bizonyítás (Csak az egzisztenciát igazoljuk, azt is vázlatosan) Az nyilvánvaló, hogy diszjunkt ciklusok szorzata kommutatív. Legyen

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

tetszőleges n-edfokú permutáció. Akkor

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} = (1\ i_1\ \dots)(k\ i_k\ \dots)(t\ i_t\ \dots)\cdots,$$

ahol, a második ciklustól kezdve, az egyes ciklusok kezdő eleme az előző ciklusban nem szereplő elemek között a legkisebb. Például:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} = (1\ 2)(3\ 5\ 4).$$

□

2.12.11 Megjegyzés Világos, hogy egy k hosszúságú ciklus rendje k. Mivel tetszőleges csoportban az egymással felcserélhető elemek szorzatának rendje megegyezik a tényezők rendjének legkisebb közös többszörösével, ezért egy permutáció rendje megegyezik az előállításában szereplő diszjunkt ciklusok hosszának legkisebb közös többszörösével.

2.12.12 Tétel *Minden* S_n*-beli permutáció előáll* S_n*-beli transzpozíciók szorzataként.*

Bizonyítás Mivel minden legalább kettő hosszúságú $(i_1\ i_2\ \dots\ i_k)$ ciklusra

$$(i_1\ i_2\ \dots\ i_k) = (i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_k) \tag{2.5}$$

teljesül, ezért a tétel állítása a 2.12.10 Tétel következménye. □

Megjegyezzük, hogy permutációk transzpozíciók szorzataként való előállítása nem egyértelmű. Például:

$$(1\ 2)(2\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix} = (1\ 5)(1\ 2).$$

Az világos, hogy a transzpozíciók páratlan permutációk. Így a 2.12.7 Megjegyzés szerint bárhogyan is bontunk fel egy σ permutációt transzpozíciók szorzatára, a felbontásban szereplő tényezők számának paritása megegyezik σ paritásával. Tehát egy páros permutációt csak páros sok transzpozícióra lehet felbontani, egy páratlan permutációt pedig csak páratlan sokra. A (2.5) felbontás szerint az is igaz, hogy egy ciklus paritása mindig ellentétes a hosszának paritásával: a páros hosszúságú ciklusok páratlan permutációk, a páratlan hosszúságú ciklusok páros permutációk.

2.12.13 Tétel *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. □

2.12.14 Tétel *$n \geq 5$ 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 $N = A_n$. □

2.12.15 Tétel *Az S_2, S_3, S_4 szimmetrikus csoportok mindegyike feloldható, viszont $n \geq 5$ esetén az S_n szimmetrikus csoport nem feloldható.*

Bizonyítás Mivel S_2 kommutatív, ezért feloldható.

S_3 elemei $(1), (123), (132), (12), (13), (23)$. Az első három alkotja A_3-at. S_3 kompozíciólánca $e \lhd A_3 \lhd S_3$. Ennek faktorai $C(3)$ és $C(2)$. Mivel ezek a faktorok prímrendű ciklikus csoportok, a 2.11.2 Tétel szerint az S_3 csoport feloldható.

S_4-nek 24 eleme van. Mivel A_n indexe 2, ezért normális részcsoport S_4-ben. Az A_4-nek normális részcsoportja az $(1), (12)(34), (13)(24), (14)(23)$ elemekből álló Klein-féle csoport. Jelöljük ezt K-val. A K-nak három nem triviális részcsoportja van:

$$B_1 = \{(1), (12)(34)\},$$

$$B_2 = \{(1), (13)(24)\}$$

és

$$B_3 = \{(1), (14)(23)\}.$$

Ezek mindegyike másodrendű (így kommutatívak) és mindegyiknek a K-beli indexe (így normális részcsoportjai K-nak). Az S_4 csoport kompozícióláncai:

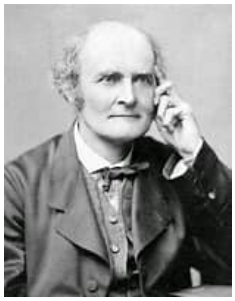
$$e \lhd B_i \lhd K \lhd A_4 \lhd G.$$

Ezek mindegyikének faktorai $C(2), C(2), C(3), C(2)$, melyek mindegyike prímrendű ciklikus csoport. Így a 2.11.2 Tétel szerint az S_4 csoport feloldható.

$n \geq 5$ esetén az S_n csoport kompozíciólánca

$$e \lhd A_n \lhd S_n.$$

Ennek faktorai A_n és $C(2)$; közülük A_n nem prímrendű ciklikus csoport. Így S_n nem feloldható $n \geq 5$ esetén. □



Arthur Cayley (1821 – 1895)

2.12.16 Tétel *(Cayley tétele) Tetszőleges n-edrendű csoport izomorf egy n-edfoku permutációcsoporttal.*

Bizonyítás Legyen G n-edrendű csoport, és legyenek elemei valamilyen sorrendben

$$a_1, a_2, \ldots, a_n.$$

Legyen φ a G csoportnak az S_n csoportba való alábbi leképezése. Ha $a \in G$, akkor legyen $\varphi(a)$ a következő n-edfoku permutáció:

$$\varphi(a) = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

ahol i_k jelöli azt az indexet, amelyre $a_i a = a_{i_k}$ teljesül. Mivel $a_i a = a_j a$ akkor és csak akkor teljesül, ha $A_i = A_j$, ezért $\varphi(a) \in S_n$. Mivel az $xa = b$ egyenlet G-ben megoldható egyértelműen minden $a, b \in G$ esetén, ezért φ szürjektív. Ha $\varphi(a) = \varphi(b)$, akkor $a = ea = eb = b$, és ezért φ injektív. Tetszőleges $a, b \in G$ elemek esetén $\varphi(ab) = \varphi(a)\varphi(b)$, mert tetszőleges $a_i \in G$ elem esetén $a_i(ab) = (a_i a)b$. Kaptuk theát, hogy φ a G csoportnak az S_n csoportra való izomorfizmusa. □

2.13. Csoportok direkt szorzata

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

- $\langle A, B\rangle = G$,
- $A \cap B = e$, *ahol* e *a* G *egységeleme,*
- A *és* B *a* G *normális részcsoportjai.*

A fentivel ekvivalens definíció:

2.13.2 Tétel *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.*

2.13.3 Definíció *(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.*

2.13.4 Megjegyzés (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.

2.13.5 Tétel *Ha a egy n-edrendű eleme egy A csoportnak, b pedig egy m-edrendű eleme egy B csoportnak, akkor az $(a, b) \in A \times B$ elem rendje az n és m legkisebb közös többszöröse.*

Bizonyítás Ha k jelöli n és m legkisebb közös többszörösét, akkor $k = nk_1$ és $k = mk_2$ valamely pozitív egész k_1 és k_2 egészekre. Így $(a, b)^k = (a^k, b^k) = (a^{nk_1}, b^{nk_2}) = (e_A, e_B)$, ahol e_A és e_B jelöli az A, illetve a B csoport egységelemét. Ha $(a, b)^t = (e_A, e_B)$, akkor $a^t = e_A$ és $b^t = e_B$, ezért t többszöröse n-nek és m-nek. Tehát t az n és m közös többszöröse. Ezért az (a, b) elem rendje az n és m legkisebb közös többszöröse. □

Több részcsoport direkt szorzatát két részcsoport direkt szorzatának mintájára értelmezhetjűk.

2.13.6 Definíció *(Több részcsoport (belső) direkt szorzata) Akkor mondjuk, hogy egy G csoport előáll A_i $(i = 1, \ldots, n)$ részcsoportjainak (belső) direkt szorzataként, ha*

- $\langle A_1, \ldots, A_n \rangle = G$,
- $A_i \cap \langle A_1, \ldots, A_{i-1}, A_{i+1}, \ldots A_n \rangle = e$ *minden* $i = 1, \ldots, n$ *indexre, , ahol* e *a* G *egységeleme,*
- A_i *a* G *csoport normális részcsoportja minden* $i = 1, \ldots, n$ *indexre.*

2.13.7 Tétel *Egy G csoport akkor és csak akkor áll elő A_i $(i = 1, \ldots, n)$ részcsoportjainak (belső) direkt szorzataként, ha*

- *G minden a eleme egyértelműen előáll $a = a_1 \cdots a_n$ alakban $(a_i \in A_i)$,*
- *$a_i a_j = a_j a_i$ teljesül minden $a_i \in A_i$ és $a_j \in A_j$ elemre, ha $i \neq j$.*

2.14. Véges Abel-csoportok

2.14.1 Definíció *Egy kommutatív csoportot Abel-csoportnak (vagy Abel-féle csoportnak) is nevezünk.*

Niels Henrik Abel (1802 – 1829)

A fejezet első tétele arra a kérdésre ad választ, hogy két véges ciklikus csoport direkt szorzata mikor ciklikus.

2.14.2 Tétel *Egy n-edrendű $\langle a\rangle$ és egy m-edrendű $\langle b\rangle$ ciklikus csoport direkt szorzata akkor és csak akkor ciklikus, ha n és m relatív prímek.*

Bizonyítás. Először megmutatjuk, hogy ha n és m relatív prímek, akkor az $\langle a\rangle \times \langle b\rangle$ direkt szorzat ciklikus. Mivel két relatív prím legkisebb közös többszöröse megegyezik a két szám szorzatával, ezért ha n és m relatív prímek, akkor az előző tétel szerint az $(a,b) \in \langle a\rangle \times \langle b\rangle$ elem rendje nm, ami megegyezik az $\langle a\rangle \times \langle b\rangle$ ciklikus csoportban lévő elemek számával. Tehát az (a,b) elem generálja a két ciklikus csoport direkt szorzatát. Fordítva, tegyük fel, hogy az $\langle a\rangle \times \langle b\rangle$ direkt szorzat ciklikus. Jelölje (x,y) a direkt szorzat egy generáló elemét. Akkor az (x,y) elem rendje nm. Az előző tételt is használva, azt kapjuk, hogy az $x \in \langle a\rangle$ elem rendjének és az $y \in \langle b\rangle$ elem rendjének legkisebb közös többszöröse nm. Megmutatjuk, hogy x generálja $\langle a\rangle$-t és y generálja $\langle b\rangle$-t. Legyen $x' \in \langle a\rangle$ tetszőleges elem. Mivel (x,y) generálja az $\langle a\rangle \times \langle b\rangle$ direkt szorzatot, ezért van olyan k pozitív egész szám, hogy $(x', e_B) = (x,y)^k = (x^k, y^k)$, amiből $x' = x^k$ adódik. Tehát x generálja $\langle a\rangle$-t. Hasonlóan igazolható, hogy y generálja $\langle b\rangle$-t. Így x rendje n és y rendje m.

Az előző tételt is használva, azt kapjuk, hogy nm (azaz az (x, y) elem rendje) megegyezik az n és m legkisebb közös többszörösével. Mivel

$$lkkt\{n, m\} = \frac{nm}{lnko\{n, m\}},$$

ezért $lnko\{n, m\} = 1$, azaz n és m relatív prímek. □

A következő tétel véges ciklikus csoportok prímhatványrendű ciklikus csoportok direkt szorzatára való felbontással kapcsolatos.

2.14.3 Tétel *Ha az n pozitív egész szám kanonikus felbontása $n = p_1^{k_1} \cdots p_r^{k_r}$, akkor az a elem által generált n-edrendű ciklikus csoport felbontható a $p_i^{k_i}$-rendű $\langle a^{n_i} \rangle$ $(i = 1, \ldots, r)$ ciklikus részcsoportok direkt szorzatára, ahol $n_i = \frac{n}{p_i^{k_i}}$ $(i = 1, \ldots, r)$.*

Bizonyítás Legyen t tetszőleges egész szám. Mivel $lnko(n_1, \ldots, n_r) = 1$, ezért az $n_1u_1 + \cdots n_ru_r = t$ diphantosi egyenlet megoldható, és így

$$a^t = (a^{n_1})^{u_1} \cdots (a^{n_r})^{u_r} \in \langle a^{n_1} \rangle \cdots \langle a^{n_r} \rangle = \langle \langle a^{n_1} \rangle, \ldots, \langle a^{n_r} \rangle \rangle.$$

Tehát az $\langle a \rangle$ ciklikus csoportot generálják a $\langle a^{n_1} \rangle$ $(i = 1. \ldots, r)$ ciklikus csoportok. Így teljesül a 2.13.6 Definíció (1) feltétele. Ahhoz, hogy megmutassuk a (2) feltétel teljesülését, tegyük fel, hogy valamely s kitevőre

$$a^s \in \langle a^{n_i} \rangle \cap \langle \langle a^{n_1} \rangle, \ldots, \langle a^{n_{i-1}} \rangle, \langle a^{n_{i+1}} \rangle \ldots \rangle a^{n_r} \rangle \rangle$$

teljesül. Akkor megadhatók olyan $v_1, \ldots v_n$ egészek, hogy

$$a^s = an_iv_i = a^{n_1v_1} \cdots a^{n_{i-1}v_{i-1}} a^{n_{i+1}v_{i+1}} \cdots a^{n_rv_r},$$

és így

$$a^{n_1v_1 + \cdots + n_{i-1}v_{i-1} - n_iv_1 + n_{i+1}v_{i+1} + \cdots n_rv_r} = e,$$

amiből

$$n | n_1v_1 + \cdots + n_{i-1}v_{i-1} - n_iv_1 + n_{i+1}v_{i+1} + \cdots n_rv_r$$

következik. Minden $j \neq i$ indexre az n_jv_j tagok mindegyike osztható $p_i^{k_i}$-vel, így a $-n_iv_i$ tag is. Mivel $lnko(n_i, p_i^{k_i}) = 1$, ezért $p_i^{k_i}$ osztja v_i-t. Ekkor viszont az n_i-vel képezett $n_ip_i^{k_i}$ és n_iv_i szorzatokra is teljesül, hogy $n_ip_i^{k_i}$ osztja n_iv_i-t. Minen $n_ip_i^{k_i} = n$, ezért azt kapjuk, hogy $n | n_iv_i$. Ebből viszont $a^s = a^{n_iv_i} =$

e adódik. Tehát teljesül a 2.13.6 Definíció (2) feltétele. Mivel a ciklikus csoportok kommutatívak, ezért a 2.13.6 Definíció (3) feltétele nyilvánvalóan teljesül. Tehát az a elem által generált ciklikus csoport előáll az $\langle a^{n_i} \rangle$ $(i = 1, \ldots, r)$ ciklikus csoportok direkt szorzataként. □

A következő tételben a véges kommutatív p-csoportok játszanak szerepet. Mint ahogy azt már korábban definiáltuk, adott p prímszám esetén egy csoportot p-csoportnak nevezünk, ha minden elemének rendje a p valamely (nemnegatív egész kitevőjü) hatványa.

2.14.4 Tétel *Minden G véges Abel-csoport különböző primekhez tartozó p-csoportok direkt szorzata. A direkt szorzatban szereplő p-csoportok a G csoport által egyértelműen meg vannak határozva.*

Bizonyítás Legyen G véges Abel-csoport. A tétel állítása nyilvánvalóan teljesül az egyelemű csoportra, így feltehetjük, hogy G-nek legalább két eleme van. Adott p prím esetén jelölje G_p a G csoport mindazon elemeinek összességét, amelyek rendje a p prím valamely nemnegatív egész kitevőjű hatványa. G_p nem üres, mert a G csoport e egységelemére $e \in G_p$ teljesül. Ha $a, b \in G_p$ tetszőleges elemek, akkor megadhatók olyan m és n kitevők, hogy $a^{p^m} = e$ és $b^{p^n} = e$. A két kitevő közül válasszuk a nyagyobbikat. Tegyük fel, hogy ez m. Akkor

$$(ab^{-1})^{p^m} = a^{p^m}(b^{-1})^{p^m} = a^{p^m}(b^{p^m})^{-1} = e^2 = e,$$

azaz $ab^{-1} \in G_p$. Tehát $G_p(G_p)^{-1} \subseteq G_p$, és így G_p a G csoport részcsoportja. A G csoport végessége miatt csak véges sok olyan p prím van, amelyre $G_p \neq e$. Legyenek ezek $p_1, \ldots, p_k$. A G_{p_i} részcsoport egy p_i-csoport $(i = 1, \ldots, k)$. Megmutatjuk, hogy a G csoport előáll a $G_{p_1}, \ldots, G_{p_k}$ részcsoportok direkt szorzataként. Mivel G kommutatív csoport, ezért a $G_{p_1}, \ldots, G_{p_k}$ részcsoportok a G csoport normális részcsoportjai. Legyen $a \in G$ tetszőleges elem. Mivel G véges, ezért az a elem rendje is véges. Így (az előző tétel szerint) az a elem által generált ciklikus csoport előáll prímhatványrendű ciklikus csoportok direkt szorzataként, amiből

$$G = \langle G_{p_1}, \ldots, G_{p_k} \rangle$$

következik. Már csak azt kell megmutatni, hogy mindegyik G_{p_i} részcsoportnak a többi által generált részcsoporttal vett metszete csak G egységelemét

tartalmazza. Jelölje x a G egy olyan elemét, amelyre

$$x \in G_{p_i} \cap \langle G_{p_1}, \ldots, G_{p_{i-1}}, G_{p_{i+1}}, \cdots G_{p_k} \rangle$$

teljesül. Mivel $x \in G_{p_i}$, ezért $x^{p_i^{r_i}} = e$ valamely k_i kitevővel. Mivel $x \in \langle G_{p_1}, \ldots, G_{p_{i-1}}, G_{p_{i+1}}, \cdots g_{p_k} \rangle$, ezért vannak olyan $x_j \in G_{p_j}$ elemek $j \neq i$, hogy $x = x_1 \cdots x_{i-1} x_{i+1} \cdots x_k$, és emiatt megadható a p_j $(j \neq i)$ prímek elég magas hatványainak szorzataként előálló olyan t kitevő, amelyre $x^t = e$ teljesül. Az világos, hogy $lnko(t, p_i^{r_i}) = 1$. Ezért a $tu + p_i^{r_i} v = 1$ diophantosi egyenlet megoldható, és így

$$x = x^{tu + p_i^{r_i} v} = (x^t)^u (x p_i^{r_i})^v = e^2 = e.$$

Ezzel tehát bebizonyítottuk, hogy

$$G = G_{p_1} \times \cdots \times G_{p_k}. \tag{2.6}$$

Már csak a felbontás egyértelműségének bizonyítása van hátra. Itt is feltehetjük, hogy G-nek lagalább két eleme van. Tegyük fel, hogy a G csoportra az (2.6) felbontás mellett teljesül egy

$$G = H_{p_1} \times \cdots \times H_{p_k} \tag{2.7}$$

felbontás is, amelyben szereplő H_{p_i} $(i = 1, \ldots, k)$ részcsoport a G_{p_i} részcsoport egy részcsoportja (egyes tényezők esetleg G egységelemével egyenlőek). Megjegyezzük, hogy ha G egy direkt felbontásban olyan p-csoport is szerepel, ahol $p \notin \{p_1, \ldots, p_k\}$, akkor ez a p-csoport a G egységelemével egyezik, és ezért a felbontásból elhagyható. Meg fogjuk mutatni, hogy $H_{p_i} = G_{p_i}$ minden $i = 1, \ldots, k$ indexre. Legyen $i \in \{1, \ldots, k\}$ tetszőleges. Mivel $H_{p_i} \subseteq G_{p_i}$, ezért elegendő a $G_{p_i} \subseteq H_{p_i}$ tartalmazás igazolása. Legyen $g \in G_{p_i}$ tetszőleges elem. Akkor $g^{p_i^t} = e$ valamely t kitevőre. A (2.7) felbontás miatt megadhatók olyan $h_i \in H_{p_i}$ $(i = 1, \ldots, k)$ elemek, amelyekre $g = h_1 \cdots h_k$ teljesül. Így

$$e = g^{p_i^t} = (h_1 \cdots h_k)^{p_i^t} = h_1^{p_i^t} \cdots h_k^{p_i^t}.$$

Mivel a (2.7) direkt felbontás miatt a G minden eleme, így az e egységelem is (a sorrendtől eltekintve) egy és csak egyféleképpen állítható elő H_{p_i}-beli $(i = 1, \ldots, k)$ elemek szorzataként, ezért minden $j = 1, \ldots, k$ indexre $h_j^{p_i^t} = e$. Ebből viszont $h_j = e$ következik minden $j \neq i$ indexre. Tehát $g = h_i \in H_{p_i}$. Következésképpen $G_{p_i} \subseteq H_{p_i}$. □

2.14.5 Tétel *Minden véges Abel-féle p-csoport felbontható p-hatványrendű ciklikus csoportok direkt szorzatára. A felbontásban szereplő ciklikus csoportok rendjei (sorrendtől eltekintve) egyértelműen meg vannak határozva.*

Bizonyítás Legyen G egy véges Abel-féle p-csoport. Akkor G minden elemének rendje p-nek valamely hatványa. G végessége miatt ezen p-hatványrendek között van maximális: p^k. Legyen a a G egy olyan eleme, amelynek rendje ez a p^k hatvány. Megmutatjuk, hogy G-nek van olyan B részcsoportja, hogy G előáll az a elem által generált $\langle a\rangle$ ciklikus csoportnak és a B részcsoportnak a direkt szorzataként. Mivel B ismét p-csoport és a rendje kisebb G rendjénél, ezért indukcióval következik a tétel állítása. Tekintsük a G mindazon részcsoportjainak halmazát, amely részcsoportoknak az $\langle a\rangle$ ciklikus részcsoporttal vett metszete e. Ez a halmaz nem üres, mert az egyelemű $\{e\}$ részcsoport benne van ebben a halmazban. A G csoport végessége miatt ebben a halmazban van maximális elem. Jelöljön B egy ilyen részcsoportot. Tehát $\langle a\rangle \cap B = e$, és ha a G egy B' részcsoportja a B-t valódi módon tartalmazza, akkor $\langle a\rangle \cap B' \neq e$. Jelöljük G^*-gal az $\langle a\rangle$ és B által generált részcsoportot. Mivel G kommutatív, ezért $\langle a\rangle$ és B a G normális részcsoportjai. Mivel $\langle a\rangle \cap B = e$, ezért G^* előáll az $\langle a\rangle$ és B direkt szorzataként, azaz

$$G^* = \langle a\rangle \times B. \tag{2.8}$$

Elegendő azt megmutatni, hogy $G^* = G$; ehhez pedig azt, hogy $G \subseteq G^*$. Tegyük fel, indirekt módon, hogy $G \neq G^*$, azaz G-nek van olyan x eleme, amely nincs benne G^*-ban. Akkor az $x, x^p, \ldots, x^{p^k}$ sorozat kezdő eleme nincs benne G^*-ban, viszont az utolsó eleme G^*-ban van. Így van ennek a sorozatnak olyan közbülső eleme, jelöljük ezt y-nal, hogy $y \notin G^*$, de $y^p \in G^*$. A (2.8) direkt felbontás miatt $y^p = a^t b$ teljesül valamely t egész számra és valamely $b \in B$ elemre. Mivel p^k maximális volt a G elemeinek rendje között, ezért

$$e = y^{p^k} = (y^p)^{p^{k-1}} = a^{p^{k-1}t} b^{p^{k-1}}.$$

Mivel $a^{p^{k-1}t} \in \langle a\rangle$ és $b^{p^{k-1}} \in B$, ezért

$$a^{p^{k-1}t} = e = b^{p^{k-1}}$$

következik a (2.8) direkt felbontás miatt. Az a elem rendje p^k, így p^k osztja a $p^{k-1}t$ számot, amiből az következik, hogy p osztója t-nek, azaz $t = pm$ valamely m egésszel. Így $y^p = a^{pm}b$. Legyen $z = ya^{-m}$. Akkor $z^p = b \in B$. z is igaz, hogy $z \notin G^*$. Ugyanis, ha $z \in G^*$ teljesülne, akkor $a^m \in G^*$ miatt

$y7za^m \in G^*$ is következne, ami ellentmond az korábbi $y \notin G^*$ feltételnek. Tekintsük most a

$$B' = \langle B, z \rangle$$

részcsoportot. Mivel $z \notin G^*$, ezért $z \notin B$, amiből az következik, hogy B' bővebb B-nél. Mivel $z^p = b \in B$, ezért B' tetszőleges b' eleme $b' = b^* z^r$ $(b^* \in B, 0 \leq r < p)$ alakban írható. Mivel B' bővebb a B-nél, ezért $\langle a \rangle \cap B'$ tartalmaz egy etől különböző elemet. legyen ez $a^s = b^* z^r$. Itt $r \neq 0$, különben a^s az $\langle a \rangle$-nak és B-nek közös eleme lenne. Tehát $lnko(r, p) = 1$, és így az $ru + tv = 1$ diophantosi egyenlet megoldható (u-ra és v-re). Akkor viszont

$$z = z^{ru+pv} = (z^r)^u + (z^p)^v = (as(b^*)^{-1})^u b^v \in G^*,$$

ami ellentmond a $z \notin G^*$ feltételnek. Emiatt a $G \neq G^*$ indirekt feltétel nem helyes. Tehát $G = G^*$.

A bizonyítás hátralévő részében az egyértelműség bizonyítását végezzük el. A G csoport tetszőleges a és b elemeinek p^r hatványaira $(ab)^{p^r} = a^{p^r} b^{p^r}$ és $(a^{-1})^{p^r} = (a^{p^r})^{-1}$ teljesül, így $G^{(r)} = \{a^{p^r} : \ a \in G\}$ a G csoport részcsoportja minden $r = 0, 1, \ldots$ indexre. Itt $G^{(0)} = G$ és $G^{(r)} = e$, ha r elég nagy. Legyen

$$G = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle, \tag{2.9}$$

a G csoport egy direkt felbontása (p-hatványrendű) ciklikus részcsoportok direkt szorzatára. Minden $i = 1, \ldots k$ indexre $a_i^{p^r} \in \langle a_i \rangle$, ezért az $\langle a_i \rangle$ ciklikus csoportnak az $\langle a_j^{p^r} \rangle$ $(j \neq i)$ ciklikus részcsoportok által generált részcsoporttal vett metszete üres. G kommutatívitása miatt a $\langle a_1^{p^r} \rangle, \cdots \langle a_k^{p^r} \rangle$ részcsoportok mindegyike normális részcsoport a $G^{(r)}$ részcsoportban. Mivel minden $a \in G$ elem előáll

$$a = a_1^{t_1} \cdots a_k^{t_k}$$

alakban, ezért

$$a^{p^r} = (a_1^{t_1} \cdots a_k^{t_k})^{p^r} = (a_1^{t_1})^{p^r} \cdots (a_k^{t_k})^{p^r} = (a_1^{p^r})^{t_1} \cdots (a_k^{p^r})^{t_k},$$

azaz

$$a^{p^r} \in \langle a_1^{p^r} \rangle \times \cdots \times \langle a_k^{p^r} \rangle.$$

Tehát

$$G^{(r)} = \langle a_1^{p^r} \rangle \times \cdots \times \langle a_k^{p^r} \rangle. \tag{2.10}$$

Ha az a_1 elem rendje p^m, akkor a^{p^r} rendje p^{m-r} vagy 1, attól függően, hogy $m \geq r$ vagy $m \leq r$. Legyen a_i rendje p^{n_i}. Tegyük fel, az általánosság megszorítása nélkül, hogy

$$n_1 = \cdots = n_s > n_{s+1} \geq \ldots$$

Ekkor $G^{(n_1)} = e$. Tekintsük a $G^{(n_1-1)}$ csoportot. Ennek a csoportnak a (2.10) egyenlőség $r = n_1 - 1$ esetét jelentő

$$G^{(n_1-1)} = \langle a_1^{p^{n_1-1}} \rangle \times \cdots \times \langle a_k^{p^{n_1-1}} \rangle$$

felbontásában éppen s tényező lesz e-től különböző, és rendjük éppen p lesz. Így az $G^{(n_1-1)}$ részcsoport p^s elemet tartalmaz. Tekintsük most a

$$G^{(n_1-2)} = \langle a_1^{p^{n_1-2}} \rangle \times \cdots \times \langle a_k^{p^{n_1-2}} \rangle$$

részcsoportot. Ebben a felbontásban a p^{n_1}-rendű a_i elemeknek megfelelő tényezők p^2-rendűek, a p^{n_1-1}-rendűeknek megfelelő tényzők pedig p-rendűek. Így a $G^{(n_1-2)}$ részcsoportban p^{2s+s_2} elem van, ahol s_2 a p^{n_1-1} rendű a_i elemek számát jelöli. Ezt az eljárást folytatva, nyilvánvaló, hogy a felbontásban szereplő $n_1, n_1 - 1, \ldots$ rendű ciklikus csoportok száma $s, s_2, \ldots$. Ebből már következik $s, s_2, \ldots$-nek a felbontás peciális megválasztásától való függetlensége, és innen a tényezők rendjének egyértelműsége. □

Az előző két tétel következményeként megfogalmazzuk a véges Abel-csoportok alaptételét.

2.14.6 Tétel *(véges Abel-csoportok alaptétele) Minden véges Abel-csoport felbontható véges sok prímhatványrendű ciklikus csoport direkt szorzatára. A felbontásban szereplő ciklikus csoportok rendjei (sorrendtől eltekintve) egyértelműen meg vannak határozva.*

Bizonyítás Az 2.14.4 Tétel miatt minden G véges Abel-csoport különböző primekhez tartozó p-csoportok direkt szorzata. A direkt szorzatban szereplő $G_{p_1}, \ldots, G_{p_k}$ csoportok a G által egyértelműen vannak meghatározva. Minden $i = 1, \ldots, k$ indexre a G_{p_i} részcsoport p_i-csoport, így a 2.14.5 Tétel szerint felbontható p_i-hatványrendű ciklikus csoportok direkt szorzatára. A felbontásban szereplő ciklikus csoportok rendjei (sorrendtől eltekintve) egyértelműen meg vannak határozva. □

2.14.7 Megjegyzés Először is emlékeztetünk arra, hogy elemek olyan összességét, amelyben egy elem többször is előfordulhat, az illető elemek egy rendszerének nevezzük. Ha ebben az összességben egy elem pontosan egyszer forduldul elő, akkor az illető elemek halmazáról beszélünk. A 2.14.6 Tétel szerint minden G véges Abel-csoporthoz tartozik prímhatványoknak egyértelműen meghatározott véges rendszere, tudniillik G -nek prímhatványrendű ciklikus csoportok direkt szorzatára való felbontásában a faktorok rendjeinek rendszere. (Például a 8-adrendű kommutatív csoportok a következő csoportok egyikével izomorfak: $C(2) \times C(2) \times C(2)$, $C(2) \times C(2^2)$, $c(2^3)$. Az első esethez a 2 prím hatványainak $\{2, 2, 2\}$ rendszere, a második esethez a 2 prím hatványainak $\{2, 2^2\}$ halmaza, a harmadik esethez a 2 prím egyetlen hatványából álló $\{2^3\}$ halmaza tartozik.) Könnyű látni, hogy ha két véges Abel-csoporthoz ugyanaz a prímhatvány-rendszer tartozik, akkor a két csoport egymással izomorf. Az is igaz, hogy tetszőleges véges prímhatványrendszerhez tartozik egy véges Abel-csoport (a rendszert alkotó prímhatványokkal megegyező rendű ciklikus csoportok direkt szorzata). Tehát kölcsönösen egyértelmű megfeleltetés van a véges Abel-csoportok és prímhatványok véges rendszerei között. A véges Abel-csoportok theát (izomorfia erejéig) tökéletesen jellemezhetők prímhatványok véges rendszereivel.

2.15. Sylow-tételek

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

Ludvig Sylow (1832 – 1918)

Ha a p nem szerepel ténylegesen a csoport rendjének prímtényezős felbontásában (azaz p nem osztója a G csoport rendjének), akkor a G csoport p-Sylow részcsoportja a G egységeleméből álló egyelemű részcsoport.

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

Bizonyítás A bizonyítást a csoportok n rendjére vonatkozó teljes indukcióval végezzük. Az $n = 1$ esetre az állítás nyilvánvaló. Tegyük fel, hogy n nagyobb 1-nél, és az állítás minden n-nél kisebb rendű csoportra érvényes. Legyen G egy n-edrendű csoport. Megmutatjuk, hogy az állítás igaz G-re. Legyen p tetszőleges prímszám. Feltehetjük, hogy p osztója n-nek. Tegyük fel, hogy p az n prímtényezős felbontásában p^k alakban szerepel. Két esetet fogunk vizsgálni.

Az első esetben feltesszük, hogy a G csoport $Z(G)$ centrumának rendje osztható p-vel. A Cauchy-tétel szerint ekkor a $Z(G)$ centrumnak van p-edrendű c eleme. Mivel $c \in Z(G)$, ezért a c elem által generált $\langle c \rangle$ ciklikus részcsoport a G csoport normális részcsoportja. Mivel a $\langle c \rangle$ részcsoport rendje p, ezért a $G/\langle c \rangle$ faktorcsoport rendje $\frac{n}{p}$, ami az indukciós feltétel miatt tartalmaz egy p-Sylow részcsoportot, azaz egy p^{k-1} elemet tartalmazó H' részcsoportot. A 2.7.1 Tétel szerint G-nek van egy olyan p^k-rendű H részcsoportja, amely tartalmazza a $\langle c \rangle$ részcsoportot; ez a H részcsoport a G csoport egy p-Sylow részcsoportja.

A második esetben tegyük fel, hogy a G csoport $Z(G)$ centrumának rendje nem osztható p-vel. Akkor $G \neq Z(G)$. Írjuk fel az osztályegyenletet:

$$\mid G \mid = \mid Z(G) \mid + k_1 + \cdots + k_r \quad (k_i > 1).$$

Mivel p osztja a G csoport rendjét, de nem osztja a $Z(G)$ centrum rendjét, ezért van olyan $j \in \{1, \ldots, r\}$ index, melyre p nem osztja a k_j-t, és így van a G csoportnak olyan a eleme, hogy p nem osztja az a elem $C(a)$ centralizátorának $\mid G : C(a) \mid$ indexét. A Lagrange tétel miatt $\mid G \mid = \mid C(a) \mid\mid G : C(a) \mid$, amiből az következik, hogy a $C(a)$ részcsoport rendjének primtényezős felbontásában a p prím p^k alakban szerepel. Mivel $C(a)$ rendje kisebb n-nél, ezért az indukciós feltétel miatt $C(a)$-nak van p-Sylow részcsoportja, amely rendje p^k; ez a részcsoport egybe p-Sylow részcsoportja G-nek is. □

2.15.3 Következmény *(Cauchy tétele) Ha egy p prímszám osztója a véges G csoport rendjének, akkor G-nek van p-edrendű eleme.*

Bizonyítás Ha egy p prímszám osztója a véges G csoport rendjének, akkor Sylow I. tétele szerint a G csoportnak van p-Sylow részcsoportja. Ha a ennek egy egységelemtől különböző eleme, akkor a rendje p^k, ahol k egy pozitív egész szám. Ha $k = 1$, akkor a rendje p. Tegyük fel, hogy $k > 1$. Mivel a rendje p^k, ezért $a^{p^{k-1}} \neq e$, viszont $(a^{p^{k-1}})^p = e$, és így $a^{p^{k-1}}$ a G egy p-edrendű eleme. □

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

Bizonyítás Tegyük fel, hogy a p prímszám p^k alakban szerepel a G csoport rendjének prímtényezős felbontásában, azaz a p-Sylow részcsoportok rendje p^k. Mivel egy G csoport tetszőleges H részcsoportja és tetszőleges g eleme esetén $\mid H \mid = \mid g^{-1}Hg \mid$, ezért tetszőleges véges G csoport minden p-Sylow részcsoportjának bármely konjugáltja is p-Sylow részcsoportja G-nek. A G csoport p-Sylow részcsoportjainak

$$\{P_1, P_2, \ldots, P_t\}$$

halmazán definiáljunk egy binér relációt a következőképpen: G két p-Sylow részcsoportja akkor és csak akkor áll relációban, ha P_1-nek vannak olyan elemei, amelyekkel való konjugálással egymásba mennek át. Ez a reláció ekvivalencia-reláció, amely meghatározza a G csoport p-Sylow részcsoportjaiból álló halmaz egy osztályozását. Világos, hogy P_1 osztálya csak a P_1-et tartalmazza. Megmutatjuk, hogy az összes többi osztályban lévő p-Sylow részcsoportok száma osztható p-vel. Ebből már következik a tétel állítása. Legyen P tetszőleges P-Sylow részcsoport. Akkor nincs G-nek a P-t valódi módon tartalmazó p-hatványrendű részcsoportja. P-vel egy osztályban az $a^{-1}Pa$ $(a \in P_1)$ alakú p-Sylow részcsoportok vannak. Ezek között esetleg egyenlők is vannak. A P_1 valamely a és b elemeire $a^{-1}Pa = b^{-1}Pb$ akkor és csak akkor teljesül, ha $ab^{-1} \in N(P)$, ahol $N(P)$ jelöli a P normalizátorát. Tudjuk, hogy $P \subseteq N(P)$. Megmutatjuk, hogy jelen esetben $ab^{-1} \in P$ is teljesül. Tegyük fel, indirekt módon, hogy $ab^{-1} \notin P$. Akkor $P \subset \langle P, ab^{-1} \rangle$. Mivel P egy p-Sylow részcsoport, ezért nem lehet G-nek a P-nél bővebb p-hatványrendű részcsoportja. Ellentmondásra úgy jutunk,

hogy megmutatjuk a P-nél bővebb $\langle P, ab^{-1}\rangle$ részcsoportról, hogy rendje p-hatvány. Mivel $ab^{-1} \in P_1$, ezért ab^{-1} rendje p-hatvány. Legyen ez a hatvány p^r. Akkor $(ab^{-1})^{p^r} = e$. Mivel $ab^{-1} \in N(P)$, ezért $(ab^{-1})P = P(ab^{-1})$, és így a $\langle P, ab^{-1}\rangle$ részcsoport minden eleme $x(ab^{-1})^t$ alakban írható, ahol $x \in P$ és t egy egész szám. Mivel P rendje p^k, ezért minden $y \in P$ elemre $y^{p^k} = e$. Az előzőekből következik, hogy a $\langle P, ab^{-1}\rangle$ részcsoport tetszőleges $x(ab^{-1})^t$ eleméhez megadható olyan $y \in P$ elem, hogy

$$(x(ab^{-1})^t)^{p^{r+k}} = \left(\left(x(ab^{-1})^t\right)^{p^r}\right)^{p^k} = \left(y\left((ab^{-1})^t\right)^{p^r}\right)^{p^k} =$$

$$= \left(y\left((ab^{-1})^{p^r}\right)^t\right)^{p^k} = (ye^t)^{p^k} = y^{p^k} = e$$

teljesül. Tehát a $\langle P, ab^{-1}\rangle$ részcsoport minden elemének rendje p-hatvány. Mivel $\langle P, ab^{-1}\rangle$ véges, ezért rendje p-hatvány a 2.8.12 Következmény szerint. Mint ahogy említettük, ez ellentmond annak, hogy P egy p-Sylow részcsoport. Tehát ha $a, b \in P_1$ és $a^{-1}Pa = b^{-1}Pb$, akkor $ab^{-1} \in P_1 \cap P$. Fordítva, ha $a, b \in P_1$ és $ab^{-1} \in P_1 \cap P$, akkor $P \subseteq N(P)$ miatt $ab^{-1}P = Pab^{-1}$, azaz $a^{-1}Pa = b^{-1}Pb$. Arra az redményre jutottunk, hogy P-vel egy konjugáltsági osztályban annyi különböző p-Sylow részcsoport van, amennyi a $P_1 \cap P$ részcsoport P_1-beni indexe. Mivel P_1 rendje p^k, ezért minden részcsoportjának indexe p-hatvány. Így minden P_1-től különböző p-Sylow részcsoport osztályában lévő p-Sylow részcsoportok száma osztható p-vel. Éppen ezt akartuk bizonyítani. Ahogy azt fent említettük, ebből már következik a tétel állítása. □

2.15.5 Tétel *(Sylow III. tétele) Véges G csoport p-Sylow részcsoportjai egymás konjugáltjai.*

Bizonyítás Legyenek a p-Sylow részcsoportok között $P_1, \dots P_r$ egymás konjugáltjai. Az előző tétel bizonyításának mintájára megmutatható, hogy ezek száma, azaz r kongruens 1-gyel modulo p. Tegyük fel, indirekt módon, hogy G-nek van olyan p-Sylow részcsoportja, amely nem szerepel ezek között. Jelöljük ezt P-vel. A $P_1, \dots P_r$ halmazon definiáljunk egy ekvivalancia-relációt a P segítségével: P_i relációban van P_j-vel $i, j \in \{1, \dots, r\}$ akkor és csak akkor, ha P_i-nek valamely P-beli elemmel képezett konjugáltja egyenlő P_j-vel. Ugyanúgy, mint az előző tétel bizonyításában, meg lehet mutatni, hogy minden osztályban az elemek száma osztható p-vel (mivel most P nincs a

$P_1, \ldots, P_r$ részcsoportok között). Így r kongruens 0-val modulo p, ami ellentmond az előző eredménynek. Tehát az indirekt feltétel nem helyes, így a p-Sylow részcsoportok egymás konjugáltjai. □

2.15.6 Tétel *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

Legyen X egy nem üres halmaz. Jelölje X^{-1} az X halmaz x elemeiből képezett x^{-1} szimbólumok halmazát. Az $X \cup X^{-1}$ halmaz elemeit betűknek fogjuk nevezni. Tetszőleges $x \in X$ elem esetén az (x, x^{-1}) és $x^{-1}, x)$ párokat tiltott betűpároknak nevezzük. Képezzük az $X \cup X^{-1}$ halmaz elemeiből (betűiből) az összes olyan véges sorozatot (más szóhasználattal élve: az összes olyan szót), amelyekben a szomszédos betűpárok egyike sem alkot tiltott betűpárt (azaz, amelyekben az x és x^{-1} elemek nincsenek egymás mellett egyetlen X-beli x elemre sem). Jelölje $\mathcal{G}_X$ ezen sorozatoknak az üres sorozattal kiegészített halmazát. Egy $\mathcal{G}_X$-beli szóban szereplő betűk számát a szó hosszának fogjuk nevezni. A $\mathcal{G}_X$ halmazon értelmezünk egy $\circ$ műveletet a következőképpen. Tetszőleges $w_1, w_2 \in \mathcal{G}$ szavak esetén jelölje $w_1 \circ w_2$ azt a $\mathcal{G}_X$-beli sorozatot, amelyet úgy kapunk meg, hogy a w_2 sorozatot a w_1 sorozat után írjuk, majd az így keletkezett sorozatból töröljük a tiltott betűpárokat (ha egyáltalán előfordulnak benne). Féldául, ha $X = \{x, y\}$ és $w_1 = yxyx^{-1}$,

$w_2 = xy^{-1}x$, akkor $w_1 \circ w_2 = yxx$. Előfordulhat, hogy a szorzat eredménye az üres szó. Például, ha $w_1 = xyx^{-1}$ és $w_2 = xy^{-1}x^{-1}$, akkor $w_1 \circ w_2$ az üres szó.

2.16.1 Tétel *Tetszőleges nem üres X halmaz esetén a $\mathcal{G}_X$ halmaz csoportot alkot az előzőekben definiált $\circ$ műveletre nézve.*

Bizonyítás A bizonyítás első részében megmutatjuk, hogy a szóban forgó művelet asszociatív. A bizonyítást a középső szó n hossza szerinti teljes indukcióval végezzük. Legyen $n = 1$, és legyenek $a \in X \cup X^{-1}, w_1, w_2 \in \mathcal{G}_X$ tetszőleges elemek. Ha $a = x \in X$, akkor jelölje a^{-1} az x^{-1} betűt. Ha $a = x^{-1} \in X^{-1}$, akkor pedig jelölje a^{-1} az x betűt. Feltehetjűk, hogy w_1 és w_2 egyike sem az üres szó. Négy esetet fogunk vizsgálni.

Az első esetben sem w_1 utolsó betűje, sem w_2 első betűje nem egyenlő az a^{-1} betűvel. Világos, hogy ekkor

$$(w_1 \circ a) \circ w_2 = w_1 a w_2 = w_1 \circ (a \circ w_2).$$

A második esetben feltesszük, hogy $w_1 = w_1' a^{-1}$ alakú, és w_2 első betűje nem egyenlő a^{-1}-gyel (emiatt $aw_2 \in \mathcal{G}_X$). Ekkor

$$(w_1 \circ a) \circ w_2 = w_1' \circ w_2 = w_1 \circ a w_2 = w_1 \circ (a \circ w_2).$$

A harmadik esetben feltesszük, hogy w_1 utolsú betűje nem egyenlő a^{-1}-gyel (emiatt $w_1 a \in \mathcal{G}_X$), és $w_2 = a^{-1} w_2'$. Ekkor

$$(w_1 \circ a) \circ w_2) = w_1 a \circ w_2 = w_1 \circ w_2' = w_1 \circ (a \circ w_2).$$

A negyedik esetben feltesszük, hogy $w_1 = w_1' a^{-1}$ és $w_2 = a^{-1} w_2'$ (emiatt w_1' utolsó betűje és w_2' első betűje nem egyenlő a-val, és így $w_1' w_2, w_1 w_2' \in \mathcal{G}_X$). Ekkor

$$(w_1 \circ a) \circ w_2 = w_1' w_2 = w_1' a^{-1} w_2' = w_1 w_2' = w_1 \circ (a \circ w_2).$$

Ezek után tegyük fel, hogy $n > 1$, és az $(w_1 \circ w') \circ w_2 = w_1 \circ (w' \circ w_2)$ teljesül minden $w_1, w_2 \in \mathcal{G}_X$ és minden n-nél kevesebb szót tartalmazó $w' \in \mathcal{G}_X$ szavakra. Legyenek $w, w_1, w_2 \in \mathcal{G}_X$ tetszőleges szavak úgy, hogy a w szó hossza n. Legyen $w = w'a$ alakú, ahol $w' \in \mathcal{G}_X$ és $a \in X \cup X^{-1}$. Mivel w'

hossza n-nél kisebb, ezért az indukciós feltétel és az egy hosszúságú szavakra az előzőekben bizonyítottak miatt kapjuk, hogy

$$(w_1 \circ w_2) \circ w_3 = (w_1 \circ (w' \circ a)) \circ w_2 = ((w_1 \circ w') \circ a) \circ w_2 = (w_1 \circ w') \circ (a \circ w_2) =$$

$$= w_1 \circ (w' \circ (a \circ w_2)) = w_1 \circ ((w' \circ a) \circ w_2) = w_1 \circ (w \circ w_2).$$

Ezzel tehát bebizonyítottuk, hogy a $\circ$ művelet asszociatív a $\mathcal{G}_X$ halmazon. Így $\mathcal{G}_X$ félcsoportot alkot a $\circ$ műveletre nézve. Ebben a félcsoportban az üres szó az egységelem. Ha egy w szóból kiindulva képezzük azt a szót, amelyet úgy kapunk meg, hogy az w-ben lévő elemeket fordított sorrendben írjuk fel, és az így keletkezett sorozatban (minden $x \in X$ esetén) az x betűt x^{-1}-re, az x^{-1} betűt x-re cseréljük, akkor ez a szó a w szó inverze. Például, ha $X = \{x, y\}$ és $w = xxyx^{-1}$, akkor $w^{-1} = xy^{-1}x^{-1}x^{-1}$. Tehát $\mathcal{G}_X$ csoportot alkot a $\circ$ műveletre nézve. □

Az előző tétel alapján a $\mathcal{G}_X$ szabad csoport minden eleme egyértelműen írható fel $x_1^{k_1} \circ x_2^{k_2} \circ x_t^{k_t}$ alakban, ahol $x_1, x_2, \ldots, x_t \in X$ és $k_1, k_2, \ldots, k_t$ egész számok. Ezért X a $\mathcal{G}_X$ csoport un. szabad generátorrendszere. A $\mathcal{G}_X$ csoportot az X szabad generátorrendszer feletti szabad csoportnak nevezzük.

2.16.2 Tétel *Egy nem üres X halmaznak egy G csoportba való tetszőleges (egyértelmű) f leképezése esetén megadható a $\mathcal{G}_X$ szabad csoportnak a G csoportba való olyan φ homomorfizmusa, hogy minden $x \in X$ elemre $\varphi(x) = f(x)$ teljesül.*

Bizonyítás Tetszőleges $w = x_1^{k_1} \circ x_2^{k_2} \circ x_t^{k_t} \in \mathcal{G}_X$ szó esetén legyen

$$\varphi(w) = (f(x_1))^{k_1}(f(x_2))^{k_2} \cdots (f(x_t))^{k_t}.$$

Világos, hogy φ teljesíti a tételben megfogalmazott állításokat. □

2.16.3 Tétel *Ha X és Y azonos számosságú nem üres halmazok, akkor a $\mathcal{G}_X$ és $\mathcal{G}_Y$ szabad csoportok egymással izomorfak.*

Bizonyítás Mivel X és Y számossága megegyzik, ezért megadható X-nek Y-ra egy f bijektív leképezése. Az előző tétel szerint létezik $\mathcal{G}_X$-nek $\mathcal{G}_Y$-ba egy φ homomorfizmusa. Mivel f az X-et a $\mathcal{G}_Y$ csoport generátorrendszerére

képezi le, ezért φ szürjektív. Megmutatjuk, hogy φ injektív is. Legyenek $w, w^* \in \mathcal{G}_X$ tetszőleges elemek, mégpedig

$$w = x_1^{k_1} \circ x_2^{k_2} \circ \cdots \circ x_n^{k_n}$$

és

$$w^* = (x_1^*)^{k_1^*} \circ (x_2^*)^{k_2^*} \circ \cdots \circ (x_m^*)^{k_m^*}.$$

Tegyük fel, hogy $\varphi(w) = \varphi(w^*)$. Akkor

$$(f(x_1))^{k_1}(f(x_2))^{k_2} \cdots (f(x_n))^{k_n} = (f(x_1^*))^{k_1^*}(f(x_2^*))^{k_2^*} \cdots (f(x_m^*))^{k_m^*},$$

azaz

$$y_1^{k_1} y_2^{k_2} \cdots y_n^{k_n} = (y_1^*)^{k_1^*}(y_2^*)^{k_2^*} \cdots (y_m^*)^{k_m^*}.$$

Mivel $\mathcal{G}_Y$ minden eleme egyértelműen áll elő Y és Y^{-1}-beli elemek szorzataként, ezért $m = n$, és $y_i^{k_i} = (y_i^*)^{k_i^*}$ minden $i = 1, 2, \ldots n$ indexre. Ebből az f leképezés bijektivitása miatt $x_i^{k_i} = (x_i^*)^{k_i^*}$ következik minden $i = 1, 2, \ldots, n$ indexre, és így $w = w^*$. Tehát φ injektív. Következésképpen φ a $\mathcal{G}_X$ szabad csoportnak a $\mathcal{G}_Y$ szabad csoportra való izomorfizmusa. □

2.16.4 Tétel *Minden csoport előáll egy F szabad csoport faktorcsoportjaként.*

Bizonyítás Adott G csoport esetén jelölje X a G egy generátorrendszerét. Akkor megadható az $F = \mathcal{G}_X$ szabad csoportnak a G csoportra egy φ szürjektív homomorfizmusa. A homomorfizmus-tétel szerint G izomorf az F/N faktorcsoporttal, ahol N jelöli a φ homomorfizmus magját. □

A fejezet hátralévő részében csoportoknak definiáló relációkkal való megadásával foglalkozunk.

Az előző tétel szerint, ha G tetszőleges csoport, akkor megadható olyan F szabad csoport és annak egy N normális részcsoportja, hogy G izomorf az F/N faktorcsoporttal. Ha az F szabad generátorai $x_1, x_2, \ldots, x_n, \ldots$, és ha $g_1, g_2, \ldots, g_n, \ldots$ az ezeknek megfelelő G-beli elemek F-nek $G = F/N$-re való természetes homomorfizmusánál, akkor egy F-beli $x_{i_1}^{k_1} \circ x_{i_2}^{k_2} \circ \ldots, \circ x_{i_t}^{k_t}$ szóra pontosan akkor teljesül az

$$x_{i_1}^{k_1} \circ x_{i_2}^{k_2} \circ \ldots, \circ x_{i_t}^{k_t} \in N$$

tartalmazás, ha a G-beli $g_{i_1}^{k_1} g_{i_2}^{k_2} \ldots, g_{i_t}^{k_t}$ szorzatra teljesül a

$$g_{i_1}^{k_1} g_{i_2}^{k_2} \ldots, g_{i_t}^{k_t} = e$$

egyenlőség; ezt az egyenlőséget a $g_{i_1}, g_{i_2}, \ldots, g_{i_t}$ elemek közötti relációnak mondjuk. Ha olyan G csoportot szeretnénk konstruálni, amelyet a

$$g_1, g_2, \ldots, g_n, \ldots$$

elemek generálnak és generátorelemei között előre megadott relációk teljesülnek, akkor megkapunk egy ilyen csoportot, ha tekintjük a fenti generátorelemeknek kölcsönösen egyértelmű módon megfeleltetett

$$x_1, x_2, \ldots, x_n, \ldots$$

elemekből álló halmaz, mint szabad generátorrendszer feletti F szabad csoportot, és képezzük ezen F szabad csoportnak azon normális részcsoportja szerinti faktorcsoportját, amelyet a megadott relációknak megfeleltethető F-beli szavak generálnak. Ha a megadott relációk halmaza $\{g_{i_1}^{k_1} \cdots g_{i_t}^{k_t} = e, \ldots\}$ (az egyszerűség kedvéért csak az első relációt írtuk ki), akkor az említett G csoportot

$$G = \{g_1, g_2, \ldots, g_n, \cdots \mid g_{i_1}^{k_1} \cdots g_{i_t}^{k_t} = e, \ldots\}$$

módon is szoktuk jelölni. A megadott relációk között esetleg lehet találni olyanokat, amelyek szorzataként, hányadosaként vagy konjugáltjaként a többi is előáll. Például, ha a G csoport generálóhalmaza $\{g_1, g_2, g_3\}$, a megadott relációk pedig: $g_2g_3 = e$, $g_3g_1 = e$, $g_1g_2g_3g_1^{-1} = e$, és $g_2g_3^2g_1 = e$, akkor az első reláció g_1-gyel való konjugálásával megkapjuk a harmadikat, ha pedig az első relációt jobbról megszorozzuk a másodikkal, akkor megkapjuk a negyediket. Így a megadott relációk az első két reláció következményei. Elegendő tehát csak az első kettőt megtartani. Megjegyezzük, hogy az ezekhez tartozó F szabad csoportbeli x_2x_3 és x_3x_1 szavak által generált normális részcsoportban benne vannak a másik két relációnak megfelelő F-beli $x_1x_2x_3x_1^{-1}$ és $x_2x_3^2x_1$ szavak is.

Csoportok definiáló relációkkal való megadásánál hasznos lehet a következő tétel.

2.16.5 Tétel *(Dyck tétele) Ha G és G' csoportok ugyanazon generátorokkal vannak értelmezve úgy, hogy G-nek minden definiáló relációja szerepel G' definiáló relációi közt, akkor a G' csoport izomorf a G csoportnak egy faktorcsoportjával.*

Bizonyítás Jelölje X a G és G' közös generátorrendszerét. Akkor az $F = \mathcal{G}_X$ szabad csoportban a G definiáló relációinak megfelelő szavak által generált N normális részcsoportot tartalmazza a G' definiáló relációinak megfelelő szavak által generált N' normális részcsoport (azaz $N \subseteq N'$). A II. izomorfizmus-tétel miatt N'/N az F/N szabad csoport normális részcsoportja és $F/N' \cong (F/N)/(N'/N)$. Mivel $F/N' \cong G'$ és $F/N \cong G$, ezért $G' \cong G/(N'/N)$. Tehát G' izomorf a G egy faktorcsoportjával. □

A Dyck tételének alkalmazásával mutassuk meg, hogy

$$S_3 \cong G = \{a, b \mid a^3 = e, b^2 = e, abab = e\}.$$

Könnyen ellenőrizhető, hogy az S_3 csoportot generálják az $a = (123)$ és $b = (12)$ ciklusok, továbbá ezek a ciklusok kielégítik a megadott definiáló relációkat. A G csoportnál megadott definiáló relációkból következik, hogy $ba = a^{-1}b^{-1} = a^2b$. Így a G csoportban az a-nak b-nek minden hatványszorzata a^nb^m alakban írható; elég csak az $n = 0, 1, 2$ és $m = 0, 1$ esetekre szorítkozni. Így G-nek legfeljebb hat eleme lehet. Mivel G minden definiáló relációja szerepel S_3 definiáló relációi között, ezért Dyck tétele szerint S_3 izomorf a G egy faktorcsoportjával. Ez csak úgy lehet, ha G izomorf S_3-mal.

Hasonlóan igazolható, hogy

$$Q \cong G = \{a, b \mid a^4 = e, abab^{-1} = e, a^2b^{-2} = e\},$$

éa

$$D_n \cong G = \{a, b \mid a^n = e, b^2 = e, abab = e\}.$$

2.17. Kis elemszámú csoportok

Használni fogjuk a következő tételt.

2.17.1 Tétel *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 $e, t, ff^2, \ldots, f^{n-1}, tf, tf^2, \ldots, tf^{n-1}$, 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 $b \notin \langle a \rangle$, akkor $\langle a, b \rangle$ rendje nagyobb, mint négy, tehát ez az egész csoport. Mivel a centrum szerinti faktorcsoport nem lehet ciklikus, ezért $\langle a \rangle$ képe ebben a faktorcsoportban nem lehet az egész csoport. Ez azt jelenti, hogy $\langle a \rangle$-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.

3. fejezet

GYŰRŰK

3.1. A gyűrű fogalma

3.1.1 Definíció *(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

3.2.1 Definíció *(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.

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

3.2.3 Tétel *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. □

3.2.4 Definíció *(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.*

3.2.5 Definíció *(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.*

3.2.6 Tétel *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

3.3.1 Definíció *(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 $ab \in S$.

3.3.2 Definíció *(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.

3.3.3 Definíció *(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. Faktorgyűrűk

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.

3.4.1 Tétel *Egy R gyűrű tetszőleges ideálja szerinti mellékosztályai a gyűrű kompatibilis osztályozását adják. Megfordítva, gyűrű tetszőleges kompatibilis osztályozásának osztályai valamely ideál szerinti mellékosztályok.*

Bizonyítás. Legyen I egy R gyűrű ideálja. Az R gyűrű I szerinti $a + I$ mellékosztályai 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 mellékosztályok 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 mellékosztályok. 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.

3.4.2 Tétel *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

3.5.1 Definíció *(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.

3.5.2 Definíció *(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.*

3.5.3 Tétel *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. □

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

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

3.5.6 Tétel *(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

3.6.1 Tétel *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. □

3.6.2 Tétel *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 öszeadást 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.

3.6.3 Tétel *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

3.7.1 Definíció *(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.

3.7.2 Tétel *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. □

3.7.3 Tétel *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.

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

3.7.5 Tétel *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

3.8.1 Definíció *(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.

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

3.8.3 Tétel *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 $(a) = (b)$. □

3.8.4 Definíció *(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.

3.8.5 Tétel *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. □

3.8.6 Definíció *(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.*

3.8.7 Megjegyzés 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. $d' = d\epsilon$.

3.8.8 Definíció *(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.

3.8.9 Tétel *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. □

3.8.10 Definíció *(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.

3.8.11 Tétel *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. □

3.8.12 Tétel *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

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

Carl Fridrich Gauss (1777 – 1855)

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.

3.9.2 Lemma *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.

3.9.3 Tétel *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 $(a_i) = (a_{i+1}) = \ldots$. 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

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

3.10.2 Definíció *(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.*

3.10.3 Tétel *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. □

3.10.4 Tétel *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

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

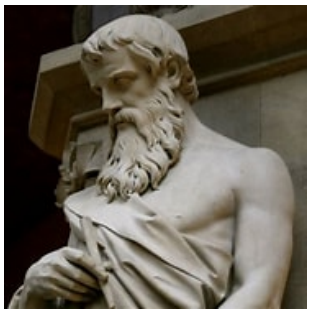
szigorúan növekvő lánca. Legyen $I = \cup_{i=1}^{\infty}(a_i)$. Ha $a, b \in I$, akkor $a, b \in (a_j)$ valamely j indexre, és ezérz $a - b \in (a_j)$, amiből $a - b \in I$ következik. Ha $a \in I$, akkor $a \in (a_j)$ valamely j indexre, és ezért tetszőleges $r \in R$ elemre

$ar \in (a_j) \subseteq I$ 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 elemények 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 $p|b$. □



A. Eukleidész

3.10.5 Definíció *(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 $\varphi(r) < \varphi(b)$.

3.10.6 Tétel *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

3.11.1 Definíció *(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.*

3.11.2 Megjegyzés 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.

Emmy Noether (1882 – 1935)

3.11.3 Tétel *(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 $L_m = L_{m+1} = \cdots$ □

3.11.4 Definíció *(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.*

David Hilbert (1862 – 1943)

3.11.5 Tétel *(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 teszőleges 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

3.12.1 Definíció *(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.

3.12.2 Tétel *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 $AB = (a_1b_1, \ldots a_1b_m, a_2b_1, \ldots a_nb_1, \ldots, a_nb_m)$, vagyis végesen generált ideálok szorzata is végesen generált.*

3.12.3 Definíció *(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.*

3.12.4 Tétel *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. □

3.12.5 Tétel *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. □

3.12.6 Tétel *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. □

3.12.7 Tétel *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. □

3.12.8 Tétel *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.

□

Richard Dedekind (1831 – 1916)

3.12.9 Definíció *(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.

3.12.10 Tétel *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.

3.13.1 Tétel *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.*

3.13.2 Tétel *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. □

3.13.3 Definíció *(Ferdetest feletti vektortér) Legyen $(V; +)$ egy kommutatív csoport $(F; +.\cdot)$ pedig egy ferdetest. Azt mondjuk, hogy V bal oldali vektortér az F ferdetest felett, ha minden $(\alpha, a) \in F \times V$ elempárhoz hozzá van rendelve egy αa-vel jelölt F-beli elm úgy, hogy tetszőleges $\alpha, \beta \in F$ és $a, b \in V$ elemekre az alábbiak teljesülnek*

- $\alpha(a + b) = \alpha a + \alpha b$,
- $(\alpha + \beta)a = \alpha a + \beta a$,

- $(\alpha\beta)a = \alpha(\beta a)$,
- $1a = a$, *ahol* 1 *az* F *ferdetest egységeleme.*

A V elemeit vektoroknak, az F elemeit skalároknak is nevezzük. Ha az F elemeivel való szorzást jobbról írjuk, akkor a jobb oldali vektortér fogalmához jutunk. Ekkor az $\alpha\beta$ skalárral való szorzásra $a(\alpha\beta) = (a\alpha)\beta$ teljesülését írjuk elő.

Egyszerűen igazolható, hogy egy F ferdetest elemeiből képezett n-elemű sorozatok F^n halmaza bal oldali vektorteret alkot F felett, ha egy $a \in F$ skalárnak egy $[a_1, \ldots, a_n]$ sorozattal képezett szorzatát a következőképpen értelmezzük:

$$a[a_1, \ldots, a_n] = [aa_1, \ldots, aa_n].$$

Az előzőekben használt fogalmakkal élve, egy F ferdetest elemeiből képezett $n \times n$-típusú mátrixok sorait az F ferdetest feletti F^n bal oldali vektortér vektoraiként is tekinthetjük, és használhatjuk a "mátrix sorvektorai" kifejezést.

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

Bizonyítás Legyen L az $M_n(F)$ mátrixgyűrű bal oldali ideálja. Ha $\underline{a}, \underline{b} \in F^n(L)$, akkor vannak L-ben olyan A és B mátrixok, hogy $\underline{a}$ az A mátrix i-dik, $\underline{b}$ pedig a B mátrix j-dik sorvektora. Legyenek $\alpha, \beta \in F$ tetszőleges skalárok, és legyen k tetszőleges sorindex. Akkor az L-beli $(E_{ki}\alpha)A + (E_{kj}\beta)B$ mátrix k-dik sorvektora $\alpha\underline{a} + \beta\underline{b}$, amiből következik, hogy $F^n(L)$ az F^n bal oldali vektortér egy altere.

Ha egy A mátrix benne van az L bal oldali ideálban, akkor annak összes sorvektora benne van az $F^n(L)$ altérben. Megmutatható az is, hogy minden olyan $B \in M_n(F)$ mátrix, melynek minden sorvektora $F^n(L)$-hez tartozik benne van az L bal oldali ideálban. Ugyanis, ha a B mátrix sorvektorai

$\underline{b}_1, \ldots, \underline{b}_n$, akkor léternek olyan L-beli $A_1, \ldots, A_n$ mátrixok, hogy az A_i mátrix k_i-dik sorvektora $\underline{b}_i$. Ekkor viszont

$$B = E_{1k_1}A_1 + \cdots + E_{nk_n}A_n \in L,$$

mert az $E_{ik_i}A_i$ mátrix i-dik sorvektora $\underline{b}_i$, a többi sorvektora pedig a nullvektor.

Ha az F^n bal oldali vektortér tetszőleges W alteréhez elkészítjük $M_n(F)$ mindazon mátrixait, amelyeknek valamennyi sorvektora W-ben van, akkor ezek L halmaza az $M_n(F)$ gyűrű egy bal oldali ideálja. Az evidens, hogy tetszőleges $A_1, A_2 \in L$ esetén $A_1 - A_2 \in L$, mert az $A_1 - A_2$ mátrix i-dik sorvektora az A_1 és az A_2 mátrixok i-dik sorvektorainak különbsége (és így két W altérbeli vektor különbsége), amely benne van a W altérben. Ha A egy L-beli mátrix (azaz minden sorvektora W-hez tartozik), akkor tetszőleges $B \in M_n(F)$ mátrix esetén a BA mátrix i-dik sorvektora (minden i sorindex esetén) megegyezik az A mátrix sorvektorainak a B mátrix i-dik sorában álló elemek lineáris kombinációjával, amely lineáris kombináció eleme W-nek. Így $BA \in L$. Tehát L valóban bal oldali ideálja az $M_n(F)$ mátrixgyűrűnek. Az, hogy a W altérrel konstruált L bal oldali ideálhoz tartozó $F^n(L)$ altér éppen W, az előzőek alapján nyilvánvaló. □

Megjegyezzük, hogy analóg tétel érvényes az $M_n(F)$ mátrixgyűrű jobb oldali ideáljaira (amely tételben a mátrixok oszlopvektorai szerepelnek)

.

3.14. Féligegyszerű gyűrűk

3.14.1 Definíció *(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.*

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

$$L_1 \supseteq L_2 \supseteq \cdots \supseteq L_n \supseteq \ldots$$

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.

A 3.13.4 Tétel szerint, ha L_1 és L_2 az $M_n(F)$ mátrixgyűrű olyan bal oldali ideáljai, amelyekre az $L_1 \subset L_2$ valódi tartalmazás teljesül, akkor $F^n(L_1) \subset F^n(L_2)$. Mivel az F^n bal oldali vektortér dimenziója n, és nagyobb altér dimenziója is nagyobb, ezért az F^n bal oldali vektortér altereinek egyetlen szigorúan csökkenő lánca sem lehet végtelen. Ebből következően, az $M_n(F)$ mátrixgyűrű bal oldali ideáljainak egyetlen szigorúan csökkenő lánca sem lehet végtele, azaz az $M_n(F)$ mátrixgyűrűben a bal oldali ideálokra teljesül a minimum-feltétel.

3.14.3 Definíció *(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.

3.14.4 Definíció *(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.

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

3.14.6 Lemma *Ha L egy R féligegyszerű gyűrűnek minimális bal oldali ideálja, akkor R-nek van olyan e idempotens eleme, amelyre $L = Re$ teljesül.*

Bizonyítás Legyen L az R féligegyszerű gyűrű minimális bal oldali ideálja. Mivel $L \neq \{0\}$, ezért $L^2 \neq \{0\}$, és így van olyan $a \in L$ elem, melyre $La \neq \{0\}$ teljesül. Mivel La az R bal oldali ideálja és $La \subseteq$, ezért $La = L$, mert L minimális bal oldali ideál. Tehát L-nek minde eleme xa alakú ($x \in L$). Ezért van L-nek olan e eleme, amelyre $ea = a$. Mivel $a \neq 0$, ezért $e \neq 0$. Ha $b \in L$ tetszőleges elem, akkor $bea = ba$, azaz $(be-b)a = 0$. Jelölje X az L bal oldali ideál mindazon x elemeinek halmazát, amelyekre $xa = 0$ teljesül. Nem nehéz belátni, hogy X az R egy bal oldali ideálja. Mivel $La \neq \{0\}$, ezért $X \subset L$, amiből L minimalitása miatt $X = \{0\}$ következik. Mivel $be - b \in X$, ezért $be-b = 0$, azaz $be = b$. Tehát $be = b$ az L tetszőleges b elemére. Mivel $e \in L$, ezért $e^2 = e$, azaz e egy idempotens elem. Ebből viszont az is adódik, hogy $Le = L$ (ugyanis $be = b$ minden $b \in L$ elemre). Mivel $e \in L$, ezért $Re \subseteq L$ (mivel L az R bal oldali ideálja). Így $L = Le \subseteq Re \subseteq L$, amiből $L = Re$ következik. □

Az előző lemma lényegében azt mondja ki, hogy féligegyszerű gyűrű minden minimális bal oldali ideálja idempotenssel generálható. A következő tétel szerint ez féligegyszerű gyűrűknek nem csak minimális bal oldali ideáljára, hanem tetszőleges bal oldali ideáljára érvényes.

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

Bizonyítás Legyen L egy R féligegyszerű gyűrű tetszőleges bal oldali ideálja. L tartalmaz idempotens elemeket; ilyen például a 0 nullelem. Tetszőleges $f \in L$ idempotens elem esetén jelölje A_f az L minazon x elemeinek halmazát, melyekre $xf = 0$ teljesü. Az A_f halmazok mindegyike az R bal oldali ideáljai, így ezek között van minimális: A_e. Megjegyezzük, hogy A_e nem az R-nek minimális bal oldali ideálja hanem csak az A_f alakúak között minimális a tartalmazásra nézve. Megmutatjuk, hogy $A_e = \{0\}$. Tegyük fel, indirekt módon, hogy $A_e \neq \{0\}$. Mivel A_e az R bal oldali ideálja, ezért az általa tartalmazott nem nulla bal oldali ideálok között van minimális, ami az R gyűrű minimális ideálja, s ezért (a 3.14.6 Lemma szerint) A_e tartalmaz egy $e_1 \neq 0$ idempotens elemet. Erre $e_1 e = 0$ teljesül. Tekintsük az L-beli $e_2 = e + e_1 - ee_1$ elemet. Igen egyszerűen ellenőrizhető, hogy teljesülnek az alábbiak:

$$ee_2 = e_0, \quad e_2 e = e, \quad e_1 e_2 = e_1, \quad e_2 e_1 = e_1.$$

Ezekből adódóan $e_2^2 = (e + e_1 - ee_1)e_2 = e_2$, azaz e_2 idempotens elem. Ha $xe_2 = 0$, akkor $xe = x(e_2e) = (xe_2)e = 0e = 0$, ezért $A_{e_2} \subseteq A_e$. Az $e_1e_2 = e_1 \neq 0$ miatt $e_1 \neq A_{e_2}$, így A_{e_2} valódim része A_e-nek. Ez ellentmond az A_e megválasztásának. Tehát $A_e = \{0\}$, ahogy azt eredetileg állítottuk. Mivel e idempotens elem, ezért az L minden b eleme setén $(be-b)e = 0$, és így $be - b \in A_e$. Mivel $A_e = \{0\}$, ezért $be = b$. Ugyanúgy, mint az előző lemma bizonyításának utolsó szakaszában, ebből már következik, hogy $L = Re$. □

3.14.8 Definíció *(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.*

3.14.9 Tétel *(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 a 3.14.7 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. □

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

Bizonyítás Legyen A egy R féligegyszerű gyűrű kétoldali ideálja. A 3.14.7 Lemma szerint $A = Re$ alkú valamely $e \in R$ idempotenssel. Emiatt e jobb oldali egységeleme A-nak. Megmutatjuk, hogy e bal oldali egységelem is. Legyen $J = \{a \in A \mid \ ea = 0\}$. Mivel $eJ = \{0\}$, ezért

$$J^2 = (Je)J = J(eJ) = \{0\},$$

azaz J nilpotens jobb oldali ideál. Mivel RJ ideál és $(RJ)^2 = R(JR)J \subseteq RJJ = \{0\}$, ezért $RJ = \{0\}$ a R gyűrű féligegyszerűsége miatt. Ez azt eredményezi, hogy J bal oldali ideál is. Mivel $J^2 = \{0\}$, ezért $J = \{0\}$ az R gyűrű féligegyszerűsége miatt. Mivel minden $b \in A$ elemre

$$0 = eb - eb = e^2b - eb = e(eb - b),$$

ezért $eb - b \in J$, amiből $eb - b = 0$, azaz $eb = b$ következik. Tehát e az A-nak bal oldali egységeleme is, és így e az A egységeleme. A 3.14.9 Tétel bizonyításában szereplő felbontást L_1 helyett A-ra alkalmazva, $R = A \oplus B$ adódik, ahol B az $x - xe$ $(x \in R)$ alakú elemek összessége. Megmutatható, hogy B nem csak bal oldali, hanem jobb oldali ideál is. Ugyanis tetszőleges $r \in R$ elem $r = re + (r - re)$ alakban írható, és ezért (használva azt is, hogy $re = ere$)

$$(x - xe)r = (x - xe)re + (x - xe)(r - re) = x(re - ere) =$$

$$= (x - xe)(r - re) = (x - xe)(r - re) \in B.$$

Tehát $BR \subseteq B$, azaz B az R-nek jobb oldali ideálja. Következésképpen B az R-nek kétoldali idálja. □

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, illetve 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 R-nek is kétoldali ideálja.

J.H.M.Wedderburn (1882˘1948)

E.Martin (1898 – 1962)

3.14.11 Tétel *(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 a 3.14.10 Lemma szerint. 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.

3.14.12 Tétel *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 is jellemzi a következő tétel (amelyet bizonyítás nélkül ismertetünk).

3.14.13 Tétel *(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.*

4. fejezet

MODULUSOK, VEKTORTEREK

4.1. A modulus fogalma

4.1.1 Definíció *(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.

4.1.2 Megjegyzés 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 moduluson 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.

4.1.3 Definíció *(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 $ra \in N$.*

4.1.4 Tétel *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.*

4.1.5 Definíció *(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.

4.1.6 Tétel *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 $a_i \in M$ $(i = 1, \ldots, n)$.*

4.1.7 Definíció *(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

4.2.1 Definíció *(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.

4.2.2 Tétel *(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.*

4.2.3 Tétel *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.

4.2.4 Definíció *(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.*

4.2.5 Definíció *(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.*

4.2.6 Megjegyzés 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

4.3.1 Definíció *(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.*

4.3.2 Tétel *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 egységelemének 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. □

4.3.3 Definíció *(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.

4.3.4 Megjegyzés 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.

4.3.5 Megjegyzés 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.

4.3.6 Megjegyzés 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.

4.3.7 Megjegyzés A

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

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

4.3.8 Tétel *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.

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

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

diagramm, amelyben a

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

sor egzakt, kiegészíthető olyan

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

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

4.3.10 Tétel *Minden szabad R-modulus projektív.*

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

5. fejezet

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

5.1.1 Tétel *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 $\mid L \mid = \mid K \mid^n$. □

5.1.2 Tétel *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. Az 5.1.1 Tétel felhasználásával kapjuk az $\mid L \mid = p^n$ eredményt valamely n pozitív egész számmal. □

5.1.3 Tétel *(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. Az 5.1.2 Tétel szerint $Z(F)$ elemszáma p-nek valamely hatványa. Jelölje ezt a hatványt q. Mivel $Z(F)$ az F részteste, ezért a Tétel 5.1.1 szerint $\mid F \mid = q^n$ valamely n pozitív egész számra. Ha meg tudjuk mutatni, hogy az n kitevő egyenlő 1-gyel, akkor abból $F = K$ következik, ami bizonyítaná a tétel állítását. Tegyük fel, indirekt módon, hogy $n \geq 2$. 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 $\mid Z(G) \mid = q - 1$. Tehát az osztályegyenlet a következő alakú:

$$q^n - 1 = q - 1 + \mid K_1 \mid + \cdots + \mid K_m \mid .$$

Legyen $j \in \{1, 2, \ldots, m\}$ tetszőleges index. A K_j elemszáma megegyezik tetszőleges $f \in K_j$ elem különböző G-beli konjugáltjainak számával, azaz az f elem G-beli centralizátorának indexével. Az f elem F testbeli $C(f)$ centralizátora F-nek részferdeteste, amely résztestként tartalmazza F centrumát. Így $C(f)$ elemszáma $Z(F)$ elemszámának, q-nak egy q^{n_j} hatványa. Így

$$\mid K_j \mid = \frac{\mid G \mid}{\mid C(f) \mid - 1} = \frac{q^n - 1}{q^{n_j} - 1}.$$

Ezek szerint a fenti osztályegyenlet a következő alakú:

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

Tudjuk, hogy

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

minden pozitív egész n-re és minden valós x-re, ahol $\Phi_d(x)$ jelöli a d-dik körosztási polinomot. Mivel n_j osztója n-nek minden $j = 1, 2, \ldots, m$ 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 $\Phi_n(q)$ osztja $q^n - 1$ különbséget és a $\frac{q^n-1}{q^{n_j}-1}$ tagokat minden $j = 1, 2, \ldots, m$ indexre. Ebből következik, hogy $\Phi_n(q)$ osztja $q - 1$-et.

Ellentmondásra úgy fogunk jutni, hogy megmutatjuk azt is, hogy $\Phi_n(q)$ nem osztja a $q - 1$ különbséget. 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. Ez ellentmod 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. □

5.1.4 Tétel *Minden véges test multiplikatív csoportja ciklikus.*

Bizonyítás. Legyen T $k+1$ elemet tartalmazó test. Jelölje G a T multiplikatív csoportját. Akkor $\mid G \mid = k$. 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. □

5.1.5 Tétel *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

5.2.1 Tétel *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. □

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

Bizonyítás. A tétel az előző tétel következménye. □

5.2.3 Tétel *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)

5.3.1 Definíció *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.

5.3.2 Definíció *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.*

5.3.3 Tétel *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. □

5.3.4 Definíció *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.

5.3.5 Tétel *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

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

elemek lineárisan függetlenek. Ugyanis, ha lineárisan függők lennének, akkor meg lehetne adni olyan $c_i \in K$ $(i = 0, \dots, n-1)$ 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

$$f(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$$

polinomnak. Ez viszont ellentmondás. Megmutatható, hogy az $1, \dots, \alpha^{n-1}$ 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 $1, \alpha, \dots, \alpha^{n-1}$ elemek lineáris kombinációjaként. Tehát az $1, \alpha, \dots, \alpha^{n-1}$ 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 $c_0, c_1, \dots, c_{n-1}$ elemekkel. □

5.3.6 Tétel *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 $K(\alpha) \cong K(x)$. □

5.3.7 Definíció *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.*

5.3.8 Tétel *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. □

5.3.9 Tétel *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. □

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

5.3.11 Tétel *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

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

5.4.2 Tétel *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. □

5.4.3 Tétel *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. □

5.4.4 Tétel *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. □

5.4.5 Következmény *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.

5.5.1 Definíció *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.

5.5.2 Tétel *(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 $K_{i+1} = K_i(\alpha_{i+1}) = K(\alpha_1, \dots \alpha_i, \alpha_{i+1})$ bővítést a q_{i+1} valamely α_{i+1} gyöke segítségével. Tovább haladva, véges sok lépés után eljutunk egy kívánt $K(\alpha_1, \dots, \alpha_n)$ bővítéshez, amely az $f(x)$ polinom felbontási teste.

5.5.3 Tétel *(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

5.6.1 Definíció *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.

5.6.2 Tétel *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.*

5.6.3 Tétel *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

Az 5.1.2 Tétel szerint minden véges test elemszáma prímhatvány.

5.7.1 Tétel *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. □

5.7.2 Tétel *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. □

5.7.3 Tétel *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 $a \mapsto a^p$ műveletartó 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. □

5.7.4 Tétel *Tetszőleges p prím és tetzőleges n pozitív egész szám esetén a p^n elemszámú K testnek csak olyan p^k elemszámú résztestei vannak, ahol k az n osztója. Továbbá az is igaz, hogy a K testnek pontosan egy p^k elemszámú részteste van.*

Bizonyítás Ha T a p^n elemszámú K test egy részteste, akkor K és T karakterisztikája p, és $Z_p \subseteq T \subseteq K$. Mivel T véges dimenziós vektortér Z_p felett (jelöljük ezt a dimenziót k-val), ezért $\mid T \mid = p^k$. Így a $T \mid_{Z_p}$ testbővítés foka k. Jelölje t a $K \mid_T$ testbővítés fokát. Mivel a $K \mid_{Z_p}$ testbővítés foka megegyezik a $T \mid_{Z_p}$ testbővítés fokának és a $K \mid_T$ testbővítés fokának szorzatával, ezért $= kt$. Tehát k az n egy osztója.

Most megmutatjuk, hogy n minden k osztója esetén létezik a K testnek p^k elemszámú részteste. Tegyük fel tehát, hogy k az n egy osztója. Akkor $n = kt$ valamely pozitív egész t-vel. Mivel

$$p^n - 1 = p^{kt} - 1 = (p^k)^t - 1 = (p^k - 1)((p^k)^{t-1} + \cdots p^k + 1),$$

ezért $p^k - 1$ a $p^n - 1$ egy osztója. Mivel $p^n - 1$ a K test multiplikatív csoportjának rendje és $p^k - 1$ ennek a rendnek egy osztója, ezért ebben a csoportban van $p^k - 1$-edrendű b elem. A b elem által generált ciklikus részcsoport rendje $p^k - 1$. Ennek a ciklikus részcsoportnak minden b^t elemére teljesül a $(b^t)^{p^k-1} = (b^{p^k-1})^t = 1^t = 1$ egyenlőség (itt 1 jelöli a K csoport egységelemét). Jelölje T a b által generált ciklikus csoportot, kiegészítve a K test nullelemével. Az előzőek miatt T elemei az $x^{p^k} - x$ polinom zérushelyei, így T az $x^{p^k} - x$ polinom felbontási teste. T elemszáma p^k.

Ha K két résztestének azonos az elemszáma (tegyük fel, hogy ez az elemszám p^k, ahol k az n egy osztója), akkor mindkét résztest az $x^{p^k} - x$ polinom gyökeiből áll (az előzőek szerint). Így a két résztest egymással egyenlő. □

5.7.5 Tétel *Tetszőleges p prím és tetzőleges n pozitív egész szám esetén mindig létezik Z_p test feletti n-dimenziós irreducibilis f polinom. Az ilyen*

f polinomok mindegyikének felbontási teste izomorf a p^n elemszámú testtel, valamint az is teljesül rájuk, hogy osztói az $x^{p^n} - x$ polinomnak.

Bizonyítás Jelöljön K egy p^n elemszámú testet. Mivel K multiplikatív csoportja ciklikus, ezért van ebben a csoportban olyan b elem, ami generálja ezt a csoportot. Mivel a Z_p testnek a b elemmel való $Z_p(b)$ bővítésére $Z_p(b) = Z_p[b]$ teljesül, ezért $Z_p(b) = K$, mert K nem nulla elemei már a b hatványaiként is előállnak. Így a $Z_p(b) \mid_{Z_p}$ testbővítés foka n (mert $\mid K \mid = p^n$), amiből az adódik, hogy a b elem $m_b(x)$ irreducibilis minimálpolinomjának foka n.

Legyen f tetszőleges Z_p test feletti n-edfokú irreducibilis polinom. Jelölje F ennek a polinomnak a felbontási testét. Mivel F tartalmazza résztestként Z_p-t, ezért F elemszáma p-nek valamely pozitív egész kitevős hatványa. Ha $b \in F$ egy zérushelye f-nek, akkor b minimálpolinomjának fokszáma megegyezik f fokszámával, azaz n-nel. Így a $Z_p(b) \mid_{Z_p}$ testbővítés foka is n. Ez azt jelenti, hogy az F felbontási test $Z_p(b)$ részteste p^n elemet tartalmaz. Mivel ez az f polinom tetszőleges b zérushelyére igaz, ezért $Z_p(b_1) = Z_p(b_2)$ teljesül f tetszőleges b_1 és b_2 zérushelyére, mivel $Z_p(b_1)$ és $Z_p(b_2)$ a p-hatvány elemszámú F test két azonos elemszámú részteste (lásd az előző tételt). Tehát az f minden zérushelye benne van az F test egyetlen p^n elemszámú résztestében, és ez a résztest előáll a Z_p testnek egyetlen zérushelyével való bővítésével. Így ez a p^n elemszámú test az f polinom felbontási testével izomorf.

Legyen b az $f(x)$ polinom egy zérushelye. Az előző rész szerint a $Z_p(b)$ test elemszáma p^n, és ezért a $Z_p(b)$ test multiplikatív csoportjának rendje $p^n - 1$. Így b zérushelye az $x^{p^n} - x$ polinomnak is. Végezzük el az $x^{p^n} - x$ polinomnak az $f(x)$ polinommal való maradékos osztását. Akkor megadhatók olyan Z_p feletti $q(x)$ és $r(x)$ polinomok, hogy $x^{p^n} - x = f(x)q(x) = r(x)$, amelyben szereplő $r(x)$ polinom vagy azonosan nulla, vagy fokszáma kisebb az $f(x)$ polinom fokszámánál. Ha $r(x)$ nem lenne az azonosan nulla polinom, akkor az előző egyenlőség miatt $0 = b^{p^n} - b = f(b)q(b) - r(b) = r(b)$ teljesülne, ami azt jelentené, hogy b az $r(x)$ polinom zérushelye. Mivel az $r(x)$ polinom fokszáma kisebb az $f(x)$ polinom fokszámánál, ez utóbbi eredmény lehetetlen, hiszen az irreducibilis $f(x)$ polinomnál kisebb fokszámú polinomnak nem lehet b zérushelye. Tehát $r(x)$ csak az azonosan nulla polinom lehet, amiből már adódik, hogy $f(x)$ az $x^{p^n} - x$ polinom egy osztója. □

5.7.6 Példa *Határozzuk meg a négyelemű testet!*

Megoldás.Mivel a négyelemű test a Z_2 test másodfokú bővítése, ezért az

a Z_2 testből egy másodfokú irreducibilis polinom segítségével állítható elő. Világos, hogy $x^4 - x = x(x^3 - 1) = x(x - 1)(x^2 + x + 1)$. Az $x^2 + x + 1$ polinom irreducibilis a Z_p test felett, mert nincs zérushelye Z_2-ben. Jelölje a az $x^2 + x + 1$ polinom egy zérushelyét a polinom felbontási testében. Akkor $Z_2(a)$ egy négyelemű test, melyben 1 és a egy bázis, azaz $Z_2(a)$ minden eleme egy és csak egyféleképpen előállítható $\alpha + \beta a$ alakban ($\alpha, \beta \in Z_2$). Tehát

$$Z_2(a) = \{0, 1, a, 1 + a\}.$$

Jelöljük az $1 + a$ elemet b-vel. Akkor az összeadás és a szorzás művelettáblái a következők (használva azt is, hogy $a^2 + a + 1 = 0$).

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

5.7.7 Példa *Határozzuk meg a nyolcelemű testet!*

Megoldás.Mivel a nyolcelemű test a Z_2 test harmadfokú bővítése, ezért az a Z_2 testből egy harmadfokú irreducibilis polinom segítségével állítható elő. Világos, hogy $x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$. Az $x^3 + x + 1$ és $x^3 + x^2 + 1$ polinomik mindegyike irreducibilis Z_2 felett, mert nincs zérushelyük Z_2-ben. Így ezen két irreducibilis polinom bármelyikének zérushelyével való bővítésként megkapjuk a nyocelemű testet. Használjuk az $x^3 + x + 1$ polinomot. Jelölje a az $x^3 + x + 1$ polinom egy zérushelyét a polinom felbontási testében. Akkor $Z_2(a)$ egy nyolcelemű test, melyben az 1, a és a^2 elemek egy bázist alkotnak, azaz $Z_2(a)$ minden eleme egy és csak egyféleképpen előállítható $\alpha + \beta a + \gamma a^2$ alakban ($\alpha, \beta, \gamma \in Z_2$). Tehát

$$Z_2(a) = \{0, 1, a, 1 + a, a^2, 1 + a^2, a + a^2, 1 + a + a^2\}.$$

Vezessük be a következő jelöléseket:

$$b = 1 + a, c = a^2, d = 1 + a^2, u = a + a^2, v = 1 + a + a^2.$$

Akkor az összeadás és a szorzás művelettáblái a következők (használva azt is, hogy $a^3 + a + 1 = 0$).

$+$	0	1	a	b	c	d	u	v
0	0	1	a	b	c	d	u	v
1	1	0	b	a	d	c	v	u
a	a	b	0	1	u	v	c	d
b	b	a	1	0	v	u	d	c
c	c	d	u	v	0	1	a	b
d	d	c	v	u	1	0	b	a
u	u	v	c	d	a	b	0	1
v	v	u	d	c	b	a	1	0

$+$	0	1	a	b	c	d	u	v
0	0	0	0	0	0	0	0	0
1	0	1	a	b	c	d	u	v
a	0	a	c	u	b	1	v	d
b	0	b	u	d	v	c	1	a
c	0	c	b	v	u	a	d	1
d	0	d	1	c	a	v	b	u
u	0	u	v	1	d	b	a	c
v	0	v	d	a	1	u	c	b

6. fejezet

FÜGGELÉK

6.1. Körosztási polinomok

6.1.1 Definíció *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:

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

6.1.2 Definíció *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.*

6.1.3 Tétel *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.*

6.1.4 Definíció *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:

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

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

6.1.5 Tétel *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

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

6.1.6 Tétel *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.

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

6.2. Csoportok szemidirekt szorzata

6.2.1 Definíció *(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.*

6.2.2 Tétel *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.*

6.2.3 Definíció *(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.

6.2.4 Tétel *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.*

Irodalomjegyzék

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