Struktúratételek az algebrában

Szakdolgozat

Írta: Bertalan Bálint

Matematika BSc. Alkalmazott matematikus szakirány

Témavezető: Ágoston István, egyetemi docens
Algebra és számelmélet tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar

2013.

Szüleimnek; és Asztridnak

Tartalomjegyzék

Előszó

[...] *„a kényszerű absztrakció mindig bizonyos önkínzással jár,*
és matematikus az, akinek ez az önkínzás örömet okoz.”
Péter Rózsa: Játék a végtelennel

Legyen V tetszőleges $\mathbb{K}$ test feletti vektortér. Ekkor létezik bázisa. Hogy miért? Vegyünk egy $P = \{A \subseteq V \mid A \text{ lineárisan független}\}$ halmazt, majd vegyünk egy P-beli elemekből álló L láncot. Ennek egy felső korlátja $\bigcup L$, ami szintén lineárisan független. Ekkor a Zorn-lemma alapján P-ben létezik maximális elem. Könnyű látni, hogy ez bázis. Tegyük fel, hogy V bázisa n elemű: $b_1, b_2, \ldots, b_n$. Ekkor minden $v \in V$ vektor előáll ezek lineáris kombinációjaként. Tekintsük azt a $\varphi : V \to \mathbb{K}^n$ lineáris leképezést, ami minden $v \in V$ vektorhoz hozzárendel egy $\mathbb{K}$ elemeiből álló n „magas” oszlopvektort. Mivel egy bázisban az előállítás egyértelmű, egy izomorfizmust kaptunk V és $\mathbb{K}^n$ között.

Legyen G olyan csoport melyet egy g eleme generál, és tekintsük a következő szürjektív leképezést: $\varphi : \mathbb{Z} \to G$, melyre $\varphi(n) = g^n$, ami nyilván homomorfizmus. $\mathbb{Z}$ részcsoportjai 0, vagy $n\mathbb{Z}$ alakúak, amelyek n többszöröseiből állnak, tehát ciklikusak. Ekkor $\mathrm{Ker}\varphi$ vagy 0, ami azt jelenti, hogy φ injektív, tehát g minden hatványa különböző. G ekkor végetelen és a homomorfizmus tétel miatt izomorf $\mathbb{Z}$-vel. Ha $\mathrm{Ker}\varphi = n\mathbb{Z}$, akkor $G \cong \mathbb{Z}_n^+$-nel.

Legyen $\mathbf{2}$ az alábbi típusú Boole-algebra: $\mathbf{2} = \langle 2, \vee, \wedge, ', 0, 1\rangle$, ahol $\langle 2, \vee, \wedge\rangle$ a kételemű háló, melyre $0 < 1$ és $0' = 1$ és $1' = 0$. Stone tétele alapján izomorfia erejéig $\mathbf{2}$ az egyetlen nemtriviális direkt felbonthatatlan Boole-algebra. Legyen B tetszőleges, véges Boole-algebra. Ekkor $B \cong \mathbf{2}^n$-nel, valamely n természetes számra, hiszen minden véges algebra izomorf direkt felbonthatatlan algebrák direkt szorzatával, és mivel $\mathbf{2}$ az egyetlen ilyen Boole-algebra, az előző izomorfizmus fennáll. Ha B nem véges, akkor Birkhoff tétele alapján B izomorf $\mathbf{2}$ egy szubdirekt hatványával, amiből következik, hogy egy halmaztesttel.

Mi a közös a fenti egyszerű állításokban? Ezek mind egy-egy algebraosztályt leíró struktúratételnek tekinthetők, melyek segítségével egy másik reprezentációját kapjuk ugyanannak az objektumnak. Nem csak egy másfajta „megjelenítést” nyerünk, hanem lehetőségünk van a vizsgált objektumot egyszerűbb és jól ismert elemekből összerakni. Gondoljunk csak arra, hogy minden véges Abel-csoport ciklikus csoportok direkt összege, vagy, hogy egy féligegyszerű gyűrű ferdetest

feletti mátrixgyűrűk direkt összegeként áll elő. Mit jelentenek az ilyen „összerakások” és, hogy mi következik belőlük? A dolgozatban erre a kerdésre kívánunk választ adni. A teljesség igénye nelkül gyűjtöttük össze az algebrában ismeretes struktúratételnek tekintett állításokat és ezek felhasználását (lásd pl.: 3.1.14). A dolgozat három fejezetből és egy függelékből áll. A megírásához felhasznált irodalmat az Irodalomjegyzék tartalmazza. Az első fejezetben bevezetjük a direkt szorzat fogalmát, annak általánosítását, a szemidirekt szorzatot, és rámutatunk a direkt szorzat és direkt összeg közti különbségekre. A második fejezet a csoportelméletben megtalálható struktúratételeket mutatja be, kivételt teszünk azonban a véges Abel-csoportok alaptételével. Az a harmadik fejezetben kerül ismertetésre, mivel ez egyszerű következménye a főideálgyűrű feletti végesen generált torziómodulusok alaptételének. A harmadik fejezetben található többek közt Wedderburn és Artin tétele is, mely a féligegyszerű gyűrűk szerkezetébe enged betekintést. A függelék az általános algebrákról szóló Birkhoff tételt mutatja be. Megmutatjuk még, hogy ha egy Malcev-varietásban az A algebra véges sok egyszerű algebra szubdirekt szorzata, akkor előáll néhány, ezen tényezők direkt szorzataként is. Ebből következik, hogy a Jacobson-radikál szerinti faktor nem „csak” egy szubdirekt szorzat.

Ezúton szeretném köszönetemet kifejezni témavezetőmnek, Ágoston Istvánnak, aki végig segítette munkámat, felhívta figyelmemet az elkövetett hibákra, tanácsaival rámutatott, hogy mely anyagok feldolgozásával lehet gazdagabb a dolgozat (lásd pl.: 2.3.4). Mindemellett köszönöm türelmét az elhúzódó dolgozatírás kapcsán.

Budapest, 2013. április

Bertalan Bálint

1. fejezet

Struktúrák előállítása és felbontása

Megpróbálunk általánosan minél több tulajdonságot megadni a direkt szorzatról, direkt összegről mint eszközről, melynek segítségével algebraosztályok újabb elemeit készíthetjük el, vagy bonthatjuk fel őket kisebb és egyszerűbb részekre, hogy a vizsgált struktúrát jobban megérthessük.

1.1. Az algebrai struktúra fogalma

1.1.1. Definíció. Algebrai struktúrán olyan $\mathbf{A} = (A, F)$ rendezett párt értünk, ahol A elemek nemüres halmaza ($\mathbf{A}$ tartója), és minden $f \in F$ elemhez található egy n természetes szám, melyre f A-n egy n-változós műveletet jelöl ($f : A^n \to A$ függvény egy n-változós művelet).

Az A-n értelmezett műveletekről legkevesebb annyit tudhatunk, hogy hány változósak. Ez a változószámokból álló rendszer (pl.: (2,2,1,0) egy R gyűrűn értelmezett összeadás, szorzás, ellentettképzés, 0 kijelölése) megadja az algebra típusát. Tegyük fel, hogy adott a műveleti neveknek egy M halmaza és egy $\tau : M \to \mathbb{N}_0$ függvény.

1.1.2. Definíció. Az ilyen τ függvényt, ami megadja, hogy az adott művelet hány változós, *típusnak* nevezzük. Az $\mathbf{A}$ algebra τ típusú, ha létezik M-nek F-re való bijekciója. Ha $f \in M$ realizációja $\mathbf{A}$-ban f_A és $\tau(f) = n$, akkor $f_A : A^n \to A$ művelet. Ezt az n számot nevezzük a művelet *aritásának.*

Ilyen algebrai struktúrára alapvető példát szolgáltatnak a dolgozatban is vizsgált struktúrák, mint a csoportok, modulusok, gyűrűk. A dolgozatban végig egy olyan konstrukciót, vagy ennek tulajdonságait fogjuk használni a vizsgált objektumok szerkezetének feltárásához, mely lehetővé teszi, hogy a felmerülő kérdéseket meg tudjuk válaszolni. Ezt mutatjuk most be általános algebrai szemlélet mellet.

1.1.3. Definíció. Legyenek adottak az azonos típusú $\mathbf{A}_i = (A_i, F_i)$ algebrák. Ezek $\mathbf{A} = \prod \mathbf{A}_i$ direkt szorzatának elemeit képzeljük sorozatoknak (vektoroknak), $a = (\ldots, a_i, \ldots)$, melyek i-edik komponense $a_i \in \mathbf{A}_i$. A direkt szorzat tartója az $A = \prod A_i$ halmaz. Ha az $f \in M$ műveleti név $\mathbf{A}_i$-beli realizációja f_i n-változós művelet, akkor az $\mathbf{A}$-beli $\hat{f}$ realizációja az

$$\hat{f}((\ldots, a_i^{(1)}, \ldots), \ldots, (\ldots, a_i^{(n)}, \ldots)) = (\ldots, f_i(a_i^{(1)}, \ldots, a_i^{(n)}), \ldots) \quad \text{ahol } a_i^{(j)} \in \mathbf{A}_i.$$

1.2. Direkt szorzat és direkt összeg

Az eddigiek alapján beszélhetünk konkrét struktúrák, például csoportok direkt szorzatáról is. Hasonlóan legyen $\mathbf{G} = \{G_i : i \in I\}$ csoportok egy rendszere, I pedig tetszőleges indexhalmaz. Ha nem okoz félreértést a továbbiakban G_i-t azonosítjuk a tartójával. A csoportszorzást jelölje az egymásmelléírás, az egységelemet e_i míg az inverzképzést $^{-1}$. A $G = \prod G_i$ direkt szorzat elemeit, az előzőek szerint értelmezzük, a műveleteket komponensenként végezzük. A direkt szorzatbeli egységelem $e = (\ldots, e_i, \ldots)$. Véges indexhalmaz esetén szokásos az alábbi jelölés: $G = G_1 \times \times G_2 \times \ldots \times G_n$. Megjegyezzük még, hogy az i-edik komponensre való vetítést (projekciót) egy $\pi_i : G \to G_i$ szürjektív homomorfizmus ad meg, melyre $\pi_i(g) = g_i$. Ezt a konstrukciót nevezzük „külső" direkt szorzatnak.

Ha végtelen sok csoportunk van, akkor az alaphalmazaik Descartes-szorzatának azon elemeit, melyek véges sok elem kivételével mind a megfelelő csoport egységelemét tartalmazzák, nevezzük a csoportok diszkrét direkt szorzatának, vagy más néven direkt összegének. Jelölésben: $\bigoplus_{i\in I} G_i$. Ezt fogjuk majd érteni R-modulusok direkt összegén is. Ez a konstrukció az előzőekhez hasonlóan, a G_i csoportok „külső" direkt összegét jelöli. A későbbiekben értelmezzük struktúrák részstruktúráinak direkt szorzatát és direkt összegét, melyet tekintjük majd a „belső" értelmezésnek.
Véges esetben a direkt szorzat és direkt összeg megegyezik. Nézzük meg azonban, hogy általában, a végességet nem feltételezve, a két struktúra - $\prod_{i\in I} G_i$ és $\bigoplus_{i\in I} G_i$ - nem izomorf (ravasz módon konstruálható azonban olyan példa, melyre az alábbi számossági meggondolások nem alkalmazhatók). Tekintsük ezért a $\mathbb{Z}_2^\omega$ direkt hatványt ($\mathbb{Z}_2$ megszámlálhatóan sok példányban vett direkt szorzatát, ahol ω a legkisebb végtelen számosság). Belátjuk, hogy ez nem megszámlálható. Indirekt tegyük fel, hogy $\mathbb{Z}_2^\omega$-nek létezik $\{z_1, z_2, \ldots\}$ felsorolása, ahol $z_i = (a_{i0}, a_{i1}, \ldots)$ tetszőleges $0-1$ sorozat. Ekkor a Cantor-féle átlós módszer segítségével elkészíthetjük a $z = (b_0, b_1, \ldots) \in \mathbb{Z}_2^\omega$ sorozatot, amely az összes többi z_i-től is különböző: $b_i \neq a_{ii}$. Ez ellentmond annak, hogy $\mathbb{Z}_2^\omega$ minden elemét felsoroltuk.

Megmutatható továbbá, hogy $\bigoplus_{n\in\omega} \mathbb{Z}_2$ megszámlálható. Ekkor tekintsük a következő halmazt: $G_n := \{(a_0, a_1 \ldots, a_{n-1}, 0, 0, \ldots)\}$. Ennek az elemszáma minden $n \in \omega$-ra 2^n, továbbá $\bigoplus_{n\in\omega} \mathbb{Z}_2 = \bigcup_{n\in\omega} G_n$, ami véges halmazok megszámlálható uniója. Ez tehát véges. Azt kaptuk tehát, hogy a két struktúra nem lehet izomorf. Nem nehéz látni, hogy a direkt összeg részstruktúrája a direkt szorzatnak, például csoportok esetén normálosztó.

Tekintsük a $G_i, i \in I$ csoportok direkt szorzatát, vagy direkt összegét. Ekkor ez minden $i \in I$-re definiál egy ρ_i injekciót és egy π_i projekciót, melyekre $g_i \in G_i$ esetén teljesül, hogy: $\rho_i g_i = (\ldots, 0, h_i, 0, \ldots)$ és $\pi_i(\ldots, g_j, \ldots, g_i, \ldots) = g_i$, továbbá melyekre teljesül, hogy:

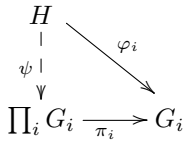
(*i*) $\pi_i\rho_j = e_{G_i}$, ha ha $i = j$, vagy 0, ha $i \neq j$.

(*ii*) Ha I véges és $G = G_1 \oplus \ldots \oplus G_n$, akkor $\rho_1\pi_1 + \ldots + \rho_n\pi_n = e_G$

(*iii*) Ha I végtelen, akkor minden $g \in \bigoplus_i G_i$-re $g = \pi_{i_1}\rho_{i_1}g + \pi_{i_2}\rho_{i_2}g + \ldots + \pi_{i_n}\rho_{i_n}g$, véges összegként írható.

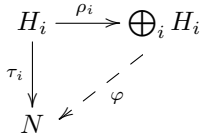
Annak ellenére, hogy a direkt szorzat elemeit vektoroknak képzeljük, jellemezhetjük őket a fenti projekciók segítségével is. Az alábbiakban közölt tételeket nem bizonyítjuk, a bizonyítások megtalálhatók pl.: [9]-ben és [3]-ben.

1.2.1. Tétel. *Legyen G a G_i csoportok direkt szorzata és π_i az i-edik komponensre való vetítés. Ekkor ez univerzális rendszer, ami azt jelenti, hogy bármely H csoport és $\varphi_i : H \to G_i$ homomorfizmus esetén egyértelműen létezik egy $\psi : H \to G$ homomorfizmus, melyre minden alábbi diagram kommutatív ($\varphi_i = \pi_i\psi$):*



Nézzük meg, hogy a direkt összeget milyen diagram jellemez:

1.2.2. Tétel. *Legyen $\tau_i : H_i \to N$ homomorfizmus minden $i \in I$-re, ρ_i az i-edik injekció H_i-ből $\bigoplus_i H_i$-be. Ekkor egyértelműen létezik egy $\varphi : \bigoplus_i H_i \to N$ homomorfizmus, melyre minden alábbi diagram kommutatív:*



Ha megfigyeljük a fenti diagram hasonló ahhoz, amit a direkt szorzatnál kaptunk, ellenben a nyilak fordított irányba mutatnak. Pongyolán fogalmazva a kategóriaelméletben objektumok *koszorzata* (II) az az objektum, az injekciókkal együtt, mely a fenti diagrammal jellemezhető. Az Abel-csoportok kategóriájában a direkt összeg éppen a koszorzat.

Térjünk vissza a kategóriaelméleti jellemzéstől a direkt szorzat néhány tulajdonságához. A most következő két tétel a direkt szorzat „belső" tulajdonságait mutatja.

1.2.3. Tétel. *Tegyük fel, hogy a G csoport a H és N csoportok direkt szorzata: $G = H \times N$. Tekintsük az alábbiakat: $H' := H \times \{e_N\}$ és $N' := N \times \{e_H\}$. Ekkor $H' \cong H$ és $N' \cong N$, továbbá normálosztók G-ben, metszetük G egységeleme, komplexusszorzatuk pedig G.*

1.2.4. Tétel. *Legyen G csoport, melyben H és N normálosztó, melyekre: $H \cap N = \{e_G\}$ és $HN = G$. Ekkor $G \cong H \times N$.*

Ha általánosan, több normálosztóról, például n-ről, tesszük fel, hogy a szorzatuk az egész G, akkor viszont nem a páronkénti metszetükről kell feltenni, hogy az csakis a csoport egységeleme, hanem bármely $n-1$ darab szorzatáról és a kimaradó metszetéről. Tehát, ha egy csoportban léteznek ilyen tulajdonságú normálosztók, akkor azok egy direkt felbontást adnak.

Igazából direkt összeggel először vektorterek esetén találkozunk. Egy véges dimenziós V vektortér U alteréhez mindig található olyan $W \leq V$, hogy minden $v \in V$-re $v = u + w$, ahol $u \in U$

és $w \in W$, és ez a felírás egyértelmű. Ekkor $V = U \oplus W$. Nem nehéz látni, hogy $U \oplus W \cong U \times W$. Hasonlóan, ha egy A Abel-csoport B és C részcsoportjaira teljesül, hogy $A = B + C$ és $B \cap C = = \{0\}$, akkor azt mondjuk, hogy A a B és C részcsoportjainak direkt összege. Modulusok esetében részmodulusok, gyűrűk esetén pedig ideálok direkt összegéről beszélünk. Ez a fajta direkt összeg, a részstruktúrák direkt összege, formálisan más, mint a struktúrák diszkrét direkt szorzata, amit szintén direkt összegnek neveztünk. Ezt a fajta direkt összeget tekintjük a „belső" direkt összegnek. Azonban nem okoz zavart, ha a „külső" és „belső" jelzőt elhagyjuk, ha a végességet is feltételezzük, hiszen, akkor a két struktúra izomorf, az egyik alaphalmaza a struktúra elemei, míg a másiké pedig rendezett párok. Ehhez például tekinstük $\mathbb{Z}_{15}^{+}$-t és két részcsoportját: $H := \{0,5,10\}$-t és $N := \{0,3,6,9,12\}$-t. Ezek csak az egységelemben metszik egymást és összegük a teljes csoport: $0,1,\ldots,14$. Tehát $\mathbb{Z}_{15}^{+} = H \oplus N$, azonban az is igaz, hogy $\mathbb{Z}_{15}^{+} \cong H \oplus N = H \times N$, ami a 1.2.4 tétel analogonja. Az előbbi a „belső", míg utóbbi a „külső" direkt összeg.

A következőben a direkt összeg néhány fontosabb tulajdonságát ismertetjük.

(*i*) Ha $G = H \oplus N$, akkor $N \cong G/H$.

(*ii*) Ha $G = H \oplus N$ és $K \leq G$ ami tartalmazza H-t, akkor $K = H \oplus (K \cap N)$.

(*iii*) Ha $G = H \oplus N$, akkor minden $G \ni g = h + n$-re $o(g)$ az $o(h)$ és $o(n)$ legkisebb közös többszöröse.

(*iv*) Ha $G = \bigoplus_i H_i$, ahol minden $H_i = \bigoplus_j H_{ij}$, akkor $G = \bigoplus_i \bigoplus_j H_{ij}$. Ez egyfajta finomítást jelent, ami megfordítható.

1.3. Szemidirekt szorzat

Legyen $N \lhd G$-ben, H részcsoport úgy, hogy $N \cap H = \{e\}$ és $G = NH$. H-t ekkor N komplementumának nevezzük. G elemei nh alakúak, ekkor két elem szorzata a következő:

$$(n_1h_1)(n_2h_2) = (n_1(h_1n_2h_1^{-1}))(h_1h_2)$$

Az első tag N-beli hiszen N zárt a konjugálásra, az utolsó kettő elem szorzata pedig H-beli. Sikerült „tagonként" elvégezni a műveletet. Legyen $\varphi : H \to \mathrm{Aut}(N)$ homomorfizmus, melyre $\varphi(h) = \varphi_h$, ami a h-val való konjugálást jelöli: $\varphi_h(n) = hnh^{-1}$. A fenti szorzásban éppen egy h_1-gyel való konjugálás jelenik meg. Ahhoz, hogy tudjuk, hogy az $N \times H$ direkt szorzatban hogyan működik a szorzás, tudnunk kell azt is, hogy hogyan hat konjugálással a H csoport az N normálosztón. Ezt határozza meg a φ homomorfizmus.

1.3.1. Definíció. Legyenek N, H csoportok és legyen $\varphi : H \to \mathrm{Aut}(N)$ homomorfizmus. G csoport elemeit definiáljuk (n,h) rendezett pároknak, ahol a szorzást a következőképpen végezzük:

$$(n_1,h_1)(n_2,h_2) = (n_1(\varphi(h_1)(n_2)), h_1h_2).$$

Az így kapott csoportot N és H szemidirekt szorzatának nevezzük és $N \rtimes_\varphi H$-val jelöljük.

Nem nehéz megmutatni, hogy csoportot kaptunk, ahol az egységelemet az (e_N, e_H) jelöli az (n, h) elem inverzét pedig $(\varphi_{h^{-1}}(n^{-1}), h)$. Az (n, e_H) és (e_N, h) elemek részcsoportot alkotnak G-ben, melyek rendre N-nel és H-val izomorfak, így az (n, e_H) alakú elemek által alkotott részcsoport normálosztó. A szemidirekt szorzat akkor válik direkt szorzattá, ha az (e_N, h) elemek is normálosztót alkotnak, vagyis $\varphi(h)$ az N identitása, ami $\mathrm{Aut}(N)$ egységeleme. Tehát minden direkt szorzat egy szemidirekt szorzatm melynél $\varphi(h)$ minden h-ra az $\mathrm{Aut}(N)$ egységeleme. Ezért a szemidirekt szorzat a direkt szorzat egy általánosításának is tekinthető.
Tekintsük a $D_n = \langle f, t \mid f^n = t^2 = 1, tft^{-1} = f^{-1} \rangle$ diédercsoportot. D_n-et a szabályos n-szög szimmetriacsoportjaként is felfoghatjuk. A forgatások egy n rendű ciklikus csoportot generálnak, ez $\mathbb{Z}_n^+$-szal izomorf, ami viszont normálosztó, hisz az indexe 2. A tükrözések által generált részcsoport $\mathbb{Z}_2^+$-szal izomorf. Ezek szemidirekt szorzata izomorf D_n-nel, ahol egy tükrözéssel való konjugálásnak az invertálás, mint automorfizmus felel meg.

$$D_n \cong \mathbb{Z}_n^+ \rtimes_\varphi \mathbb{Z}_2^+,$$

ahol $\varphi(1) \in \mathrm{Aut}(\mathbb{Z}_n^+)$ minden $\mathbb{Z}_n^+$-beli elemet invertál.

2. fejezet

Struktúratételek a csoportelméletben

A csoportelméleti viszgálatok célja, hogy izomorfizmus erejéig az összes csoport szerkezetét fel tudjuk deríteni. Ez viszont így túl nehéz probléma. A véges Abel-csoportok szerkezete izomorfia erejéig teljesen ismert. A dolgozatban később szereplő, főideál gyűrű feletti torziómodulusok alaptételének egy speciális eseteként le tudjuk írni az összes véges Abel-csoportot. Végtelen esetben bizonyos feltételek mellett a csoport szintén előáll, mint ciklikus csoportok direkt összege. Ezt a **Kulikov és Prüfer tételei** c. részben vizsgáljuk. A nemkommutatív csoportok esetében kevés olyan ismert tétel van, mely a csoport szerkezetét visszavezetné egy egyszerűbb, ismertebb struktúrára. Az egyértelműség kérdésére a **Krull-Schmidt-tétel** c. részben kapunk választ. Továbbá megmutatjuk, hogy a véges nilpotens csoportok p-Sylowjaiknak direkt szorzatai. Az osztható Abel-csoportok szerkezete is teljesen ismert, erről is lesz szó a fejezetben.

2.1. Krull-Schmidt-tétel

Mielőtt közöljük az idekapcsolódó tételt az alapvető felhasznált fogalmakat ismertetjük.

2.1.1. Definíció. A G csoportot *felbonthatatlannak* nevezzük, ha $G \neq \{e\}$ és ha $G = H \times K$, akkor $H = \{e\}$ vagy $K = \{e\}$.

Ilyen minden egyszerű csoport, viszont a megfordítás nem igaz, nem minden felbonthatatlan csoport egyszerű. Tetszőleges p prímre és n természetes számra $\mathbb{Z}^+_{p^n}$ is felbonthatatlan, hasonlóan $\mathbb{Z}^+$, viszont ezek nem egyszerű csoportok.

2.1.2. Definíció. Azt mondjuk, hogy a G csoportban teljesül a *növőlánc-feltétel*, ha minden $H_1 \leq \leq H_2 \leq \ldots$ normális részcsoportokból álló növő lánc stabilizálódik, vagyis létezik egy $n \in \mathbb{N}$, hogy $H_i = H_n$ minden $i > n$-re. Hasonlóan G-ben teljesül a *csökkenőlánc-feltétel*, ha minden $H_1 \geq H_2 \geq \ldots$ normális részcsoportokból álló csökkenő lánc stabilizálódik.

Például a későbbi fejezetben vizsgált $\mathbb{Z}_{p^\infty}$ csak a csökkenő láncfeltételt teljesíti, míg a növőt nem, $\mathbb{Q}$ viszont egyiket sem.

A most következő tétel a két felbontás esetén fellépő komponensek izomorf voltától, egy erősebb állítást fogalmaz meg, miszerint a két felbontás megfelő módon „összeragasztható”.

2.1.3. Tétel (Krull-Schmidt)**.** *Legyen adott a G csoport, melyben a normálosztókra vonatkozó mindkét láncfeltétel teljesül. Ha $G = H_1 \times \ldots \times H_n$ és $G = K_1 \times \ldots \times K_t$, ahol H_i, K_i felbonthatalanok, akkor $n = t$, és $\{K_i\}$-t átindexelhetjük úgy, hogy $H_i \cong K_i$ minden i-re. Sőt, minden $1 \leq l \leq n$-re*

$$G = H_1 \times \ldots H_l \times K_{l+1} \times \ldots \times K_n.$$

Mielőtt elkezdenénk a bizonyítást, a bizonyításhoz felhasznált lemmákat mondjuk ki és bizonyítjuk.

2.1.4. Lemma. *(i) Ha $H \lhd G$ és H és G/H teljesíti mindkét láncfeltételt, akkor G is teljesíti.*
(ii) Ha $G = H \times K$ és G teljesíti mindkét láncfeltételt, akkor H és K is teljesíti.

Bizonyítás. (i) Legyen $G_1 \geq G_2 \geq \ldots$ normálosztókból álló lánc G-ben. Ekkor $H \cap G_1 \geq H \cap$ $\cap\, G_2 \geq \ldots$ normáloszókból álló lánc H-ban, hasonlóan $HG_1/H \geq HG_2/H \geq \ldots$ G/H-beli normálosztókból álló lánc. A feltétel alapján valamilyen n-re és s-re: $H \cap G_n = H \cap G_{n+1} = \ldots$ és $HG_s/H = HG_{s+1}/H = \ldots$ amiből $HG_s = HG_{s+1} = \ldots$ következik.
Legyen $t = \max\{n, s\}$. A moduláris szabály alapján minden $i \geq t$-re teljesül hogy:

$$G_i = G_iH \cap G_i = G_{i+1}H \cap G_i = G_{i+1}(H \cap G_i) = G_{i+1}(H \cap G_{i+1}) \leq G_{i+1}.$$

(ii) Ha $I \lhd H$, akkor $I \lhd G$ is teljesül, ezért, ha a G-beli láncok stabilizálódnak, akkor a H-beliek is. □

2.1.5. Definíció. A G csoport egy φ endomorfizmusát *normálisnak* nevezzük, ha $\varphi(hgh^{-1}) =$ $= h\varphi(g)h^{-1}$ minden $g, h \in G$-re.

Egy normális endomorfizmusra az alábbiak teljesülnek, ezek könnyen megmutathatók a definíció felhasználásával:

(i) Ha φ, ψ normálisak, akkor $\varphi \circ \psi$ is normális.

(ii) Ha φ normális és $H \lhd G$, akkor $\varphi(H) \lhd G$.

(iii) Ha φ normális automorfizmus, akkor φ^{-1} is normális.

φ és ψ endomorfizmusok $\varphi + \psi$ összegén az alábbi hozzárendeléssel adott függvényt fogjuk érteni: $g \mapsto \varphi(g)\psi(g)$. Megjegyezzük, hogy $\varphi + \psi$ nem lesz mindig endomorfizmus, és, hogy az így értelmezett összeadás nem mindig kommutatív.

2.1.6. Lemma. *Legyen $G = H_1 \times H_2 \times \ldots \times H_n$. Tekintsük a $\pi_i : G \to H_i$ i-edik projekciót és a $\lambda_i : H_i \to G$ i-edik injekciót. Ekkor bármely k különböző $\lambda_i\pi_i$ összege normális endomorfizmusa G-nek és ha $k = n$, akkor az összeg G identitása.*

Nem nehéz látni, hogy $\lambda_i\pi_i$ normális endomorfizmusa G-nek.

Bizonyítás. Legyen $\varphi = \sum_{i=1}^{k} \lambda_i \pi_i$. Mivel $\lambda_i\pi_i(h_1, h_2, \ldots, h_n) = (1, \ldots, h_i, \ldots, 1)$ ezért $\varphi(h_1, h_2, \ldots, h_n) = (h_1, h_2, \ldots, h_k, 1 \ldots, 1)$. Könnyű látni, hogy φ is normális, és ha $k = n$, akkor $\varphi = \mathrm{id}_G$. □

2.1.7. Lemma. *Ha a G csoportban teljesül a normálosztókra vonatkozó láncfeltételek valamelyike, akkor G véges sok felbonthatatlan részcsoportjának direkt szorzata.*

Bizonyítás. Egy felbonthatatlan csoport nyilván véges sok normálosztójának direkt szorzata. Legyen G olyan, melyben mindkét láncfeltétel teljesül. Indirekt tegyük fel, hogy G nem áll elő a kívánt alakban. Ekkor G nem lehet felbonthatatlan: $G = H_1 \times K_1$, ahol $H_1, K_1 \lhd G$. Mivel G rossz ebben az értelemben, legalább az egyik tényezőnek szintén rossznak kell lennie. Tegyük fel, hogy K_1 rossz, ekkor: $K_1 = H_2 \times K_2$, ahol $H_2, K_2 \lhd K_1$. Hasonlóan legyen K_2 rossz, ekkor: $K_2 = H_3 \times K_3$ stb. Kapjuk, hogy $G = H_1 \times (H_2 \times (\ldots)\ldots) \cong H_1 \times H_2 \times \ldots$. Látható, hogy két végtelen láncot kaptunk G-ben:

$$H_1 < H_1 \times H_2 < \ldots \quad \text{és} \quad G > K_1 > K_2 > \ldots,$$

melyek megsértik mindkét láncfeltételt, így ellentmondásra jutottunk, tehát G előáll véges sok részcsoportjának direkt szorzataként. □

2.1.8. Lemma. *Ha a G csoportban teljesül a normálosztókra vonatkozó mindkét láncfeltétel, és φ normális endomorfizmusa G-nek, akkor φ pontosan akkor injekció, ha szürjekció.*

Bizonyítás. Tegyük fel, hogy φ injektív, de nem szürjektív, ekkor létezik $g \in G$, melyre $g \notin \mathrm{Im}\varphi$. Mivel φ injekció, φ^n is injektív minden $n \in \mathbb{N}$-re, és $\varphi^n(g) \notin \varphi^n(\mathrm{Im}\varphi) = \mathrm{Im}\varphi^{n+1}$. Mivel φ normális $\mathrm{Im}\varphi^n \lhd G$. Ezekből következően kapunk egy végtelen, normálosztókból álló csökkenő láncot: $G > \mathrm{Im}\varphi > \mathrm{Im}\varphi^2 > \ldots$, amely nem stabilizálódik, ez pedig ellentmondás.
A másik irány igazolásához φ legyen szürjektív. Az injektivitás igazolásához azt kell megmutatnunk, hogy $\mathrm{Ker}\varphi = \{e\}$. Indirekt tegyük fel, hogy $g \in \mathrm{Ker}\varphi$ és $g \neq e$. Mivel φ szürjekció, φ^n is szürjektív minden $n \in \mathbb{N}$-re, így $g = \varphi^n(h)$ valamely $h \in G$-re. $h \notin \mathrm{Ker}\varphi^n$, de könnyen látható, hogy $h \in \mathrm{Ker}\varphi^{n+1}$. Ekkor a $\{e\} < \mathrm{Ker}\varphi < \mathrm{Ker}\varphi^2 < \ldots$ normálosztókból álló végtelen növő láncot kapjuk, ami ellentmondás. □

2.1.9. Lemma (Fitting)**.** *Ha a G csoportban a normálosztókra vonatkozó mindkét láncfeltétel teljesül és φ normális endomorfizmusa G-nek, akkor $G = Ker\varphi^n \times Im\varphi^n$ valamely $n \in \mathbb{N}$-re.*

Bizonyítás. φ normális endomorfizmusa a G csoportnak, ezért $\mathrm{Im}\varphi^n$ is normálosztó. Tekintsük a normálosztókból álló alábbi két láncot:

$$G > \mathrm{Im}\varphi > \mathrm{Im}\varphi^2 > \ldots \quad \{e\} < \mathrm{Ker}\varphi < \mathrm{Ker}\varphi^2 < \ldots$$

Mivel G-ben mindkét láncfeltétel teljesül, a két lánc stabilizálódik, legyen ez a hatvány n. Egyrészt megmutatjuk, hogy $\mathrm{Im}\varphi^n \cap \mathrm{Ker}\varphi^n = \{e\}$. Indirekt tegyük fel, hogy létezik $g \in \mathrm{Im}\varphi^n \cap \mathrm{Ker}\varphi^n$ és $g \neq e$. Mivel $g \in \mathrm{Im}\varphi^n$, létezik $h \in G$, hogy $g = \varphi^n(h)$. $e = \varphi^n(g) = \varphi^n(\varphi^n(h) = \varphi^{2n}(h)$. Kapjuk, hogy $h \in \mathrm{Ker}\varphi^{2n}$, de mivel a lánc n-nél stabilizálódik $\mathrm{Ker}\varphi^{2n} = \mathrm{Ker}\varphi^n$. Így azt kapjuk, hogy $g = \varphi^n(h) = e$, ami ellentmondás. Másrészt belátjuk, hogy $G = \mathrm{Ker}\varphi^n\mathrm{Im}\varphi^n$, ebből a két

tulajdonságból már következik, hogy G direkt szorzatként áll elő. Legyen $g \in G$ tetszőleges. Ekkor $\varphi^{2n}(h) = \varphi^n(g)$ valamely $h \in G$-re, hiszen $\mathrm{Im}\varphi^{2n} = \mathrm{Im}\varphi^n$. Ekkor $g = k\varphi^n(h)$ valamely $k \in \mathrm{Ker}\varphi^n$-re. Mindezekből következik, hogy $G = \mathrm{Ker}\varphi^n \times \mathrm{Im}\varphi^n$. □

2.1.10. Definíció. Egy G csoport φ endomorfizmusát *nilpotensnek* nevezzük, ha $\varphi^n(G) = \{e\}$ valamely $n \in \mathbb{N}$-re.

A Fitting-lemma egyik következménye, hogy ha a felbonthatatlan G csoportban a normálosztókra vonatkozó mindkét láncfeltétel teljesül, akkor minden normális endomorfizmus nilpotens vagy automorfizmus. Hiszen $G = \mathrm{Ker}\varphi^n \times \mathrm{Im}\varphi^n$ és mivel G felbonthatatlan valamelyik tényező $\{e\}$. Ha $\mathrm{Im}\varphi^n = \{e\}$ akkor φ nilpotens, ha pedig $\mathrm{Ker}\varphi^n = \{e\}$ akkor φ injektív, így a 2.1.8 lemma alapján szürjektív is, tehát automorfizmus.

2.1.11. Lemma. *Legyen G felbonthatatlan $G \neq \{e\}$, melyben a normálosztókra vonatkozó mindkét láncfeltétel teljesül, és legyenek φ_1 és φ_2 normális nilpotens endomorfizmusai. Ha $\varphi_1 + \varphi_2$ is egy endomorfizmus, akkor normális nilpotens.*

Bizonyítás. Tegyük fel, hogy $\varphi_1 + \varphi_2$ endomorfizmus és φ_1, φ_2 legyenek normálisak. Először megmutatjuk, hogy az összegük is normális:

$$(\varphi_1 + \varphi_2)(hgh^{-1}) = \varphi_1(hgh^{-1})\varphi_2(hgh^{-1}) = h\varphi_1(g)h^{-1}h\varphi_2(g)h^{-1} = h(\varphi_1 + \varphi_2)(g)h^{-1}.$$

Indirekt tegyük fel, hogy $\varphi_1 + \varphi_2$ nem nilpotens, így a(z) 2.1.9 lemma következménye alapján automorfizmus. Létezik tehát ψ inverze: $(\varphi_1 + \varphi_2)\psi = \mathrm{id}_G$ (az egymásmellé írás kompozíciót jelöl). Legyen $\psi_1 := \varphi_1\psi$ és $\psi_2 := \varphi_2\psi$, ekkor $\psi_1 + \psi_2 = \mathrm{id}_G$. Bármely $g \in G$-re $g^{-1} = (\psi_1 + \psi_2)(g^{-1}) = = \psi_1(g^{-1})\psi_2(g^{-1})$, ha invertáljuk mindkét oldalt, kapjuk, hogy $g = (\psi_2 + \psi_1)g$ vagyis ψ_1-re és ψ_2-re nézve az összeadás kommutatív. Mivel

$$\psi_1(\psi_1 + \psi_2) = \psi_1\mathrm{id}_G = \mathrm{id}_G\psi_1 = (\psi_1 + \psi_2)\psi_1,$$

kapjuk, hogy $\psi_1\psi_2 = \psi_2\psi_1$. Így tetszőleges $n \in \mathbb{N}$-re értelmezhetjük a következőt:

$$(\psi_1 + \psi_2)^n = \sum_{k=0}^{n} b_k\psi_1^k\psi_2^{n-k}, \quad \text{ahol } b_k \text{ a } k\text{-adik binomiális együttható.}$$

Mivel φ_i nilpotens a $\psi_i = \varphi_i\psi$ magja nem triviális, így a Fitting-lemma következményéből ψ_i is nilpotens. Ekkor alkalmas nagy m-re és minden $g \in G$-re:

$$(\psi_1 + \psi_2)^m(g) = \sum_{k=0}^{m} b_k\psi_1^k\psi_2^{m-k}(g) = \prod_{k=0}^{m} e^{b_k} = e.$$

Ez viszont ellentmond annak, hogy $\psi_1 + \psi_2 = \mathrm{id}_G$ és $G \neq \{e\}$. □

Hasonló feltételek mellet indukcióval, tetszőleges n-re belátható, hogy $\varphi_1 + \ldots + \varphi_n$ normális nilpotens.

A szükséges lemmák után következzen a 2.1.3 tétel bizonyítása.

Bizonyítás. Legyen adott G kétféle felbontása:

$$G = H_1 \times H_2 \times \ldots \times H_n \quad \text{és} \quad G = K_1 \times K_2 \times \ldots \times K_t,$$

a $\pi_i : G \to H_i$ projekciókkal és $\lambda_i : H_i \to G$ injekciókkal, hasonlóan $\sigma_j : G \to K_j$ és $\mu_j : K_j \to G$. Bebizonyítjuk, hogy a K_i-k alkalmas átindexelésével, $l = 1$-re:

$$G = H_1 \times K_2 \times \ldots \times K_n,$$

innen pedig indukcióval megmutatható általános l-re is, hogy:

$$G = H_1 \times H_2 \times \ldots \times H_l \times K_{l+1} \times \ldots \times K_n.$$

A 2.1.6 lemma alapján a $\sum \mu_j \sigma_j$ összeg is normális endomorfizmus, ezért egyszerű számolással adódik, hogy a:

$$\mathrm{id}_{H_1} = \pi_1\lambda_1 = \pi_1 \circ \mathrm{id}_G \circ \lambda_1 = \pi_1 \circ \sum \mu_j\sigma_j \circ \lambda_1 = \sum \pi_1\mu_j\sigma_j\lambda_1$$

is normális endomorfizmus. Mivel az id_{H_1} nem nilpotens, megmutatjuk, hogy létezik olyan j index, melyre $\pi_1\mu_j\sigma_j\lambda_1$ automorfizmus. A 2.1.4 és a 2.1.11 lemma alapján ilyen j létezik. Indexeljük át K_i-ket, j-t 1-nek megfeleltetve, ekkor tehát $\pi_1\mu_1\sigma_1\lambda_1$ automorfizmusa H_1-nek. Legyen ennek inverze α. Ekkor $(\alpha\pi_1\mu_1)\sigma_1\lambda_1 = \mathrm{id}_{H_1}$. Legyen $\beta := \sigma_1\lambda_1(\alpha\pi_1\mu_1) : K_1 \to K_1$. Nem nehéz látni, hogy $\beta^2 = \beta$. Mivel $\mathrm{id}_{H_1} = \mathrm{id}_{H_1} \circ \mathrm{id}_{H_1} = \ldots = (\alpha\pi_1\mu_1)\beta\sigma_1\lambda_1$, $\beta \neq 0$ és így nem is nilpotens. Ekkor β K_1 egy automorfizmusa, az idempotencia miatt csak $\beta = \mathrm{id}_{K_1}$ lehetséges. Ebből és a fentiekből azt nyerjük, hogy $\sigma_1\lambda_1 : H_1 \to K_1$ egy izomorfizmus (inverze $\alpha\pi_1\mu_1$). A $K_2 \times \ldots \times K_t$ σ_1-nél vett képe $\{e\}$ és $\sigma_1\lambda_1$ pedig izomorfizmus H_1 és K_1 közt, így $H_1 \cap (K_2 \times \ldots \times K_t) = \{e\}$. Definiáljuk a $\hat{G}$ csoportot a következőképpen:

$$\hat{G} := \langle H_1, K_2 \times \ldots \times K_t \rangle, \text{ ami } H_1 \times K_2 \times \ldots \times K_t$$

Könnyű látni, hogy $\hat{G} \leq G$ és, hogy a $G \ni g = k_1k_2 \ldots k_t \mapsto \pi_1\mu_1(k_1)k_2 \ldots k_t$ megfeleltetés injektív (hiszen $\pi_1\mu_1$ izomorfizmus), melynek képe $\hat{G}$. Mivel normális endomorfizmusa G-nek és injektív, ezért szürjektív is, amiből $G = \hat{G}$ következik. Azt kapjuk tehát, hogy:

$$K_2 \times \ldots \times K_t \cong G/H_1 \cong H_2 \times \ldots \times H_n.$$

Az eljárást folytatva $\max\{n, t\}$-n nyerjük a tétel állítását. □

2.2. Véges nilpotens csoportok

A következőkben a véges nilpotens csoportokat vizsgáljuk. Mielőtt kimondanánk a rájuk vonatkozó struktúratételt, ismertetjük a felhasznált fogalmakat és állításokat.

2.2.1. Definíció. Legyenek g, h egy csoport elemei, és tekintsük a következő elemet: $(gh)(hg)^{-1} = = ghg^{-1}h^{-1}$. Ha ez nem az egységelem, akkor tehát g és h nem kommutálnak. Az ilyen $ghg^{-1}h^{-1}$ elemet nevezzük g és h *kommutátorának*, jele: $[g, h]$.
Az összes kommutátor által generált részcsoport G *kommutátora*, jele: G', $(G' = [G, G])$.

Ha G egy faktorcsoportját kommutatívvá szeretnénk tenni, akkor a kommutátor részcsoportnak az egységelembe kell mennie. A kommutátor-részcsoport ezért az összes, Abel-csoportra képező $\varphi : G \to A$ homomorfizmus magjának a metszete. Könnyen megmutatható (lásd pl.: [3]), hogy $G' \lhd G$, és G/N pontosan akkor kommutatív, ha $G' \subseteq N$.

2.2.2. Definíció. A G csoport *centrális láncán* az alábbi normálláncot értjük:

$$\{e\} = N_0 \lhd N_1 \lhd \ldots \lhd N_{n-1} \lhd N_n = G,$$

melyre, minden $i = 1,2 \ldots, n$-re $[N_i, G] \subseteq N_{i-1}$. A G csoport nilpotens, ha létezik centrális lánca.

2.2.3. Definíció. Képezzük a következő G-beli $G^{(i)}$ részcsoportokat: $G^{(1)} := G$ és $G^{(i+1)} := [G^{(i)}, G]$. Az ilyen normálosztókból álló

$$G = G^{(1)} \geq G^{(2)} \geq \ldots$$

láncot nevezzük G *alsó centrális láncának*.

Hasonlóan elkészítjük G felső centrális láncát is. Jelölje G centrumát $Z(G)$. Könnyen látható, hogy $Z(G)$ normálosztó. Képezzük $Z_2(G)$-t a következő módon: legyen $\varphi : G \to G/Z(G)$ a természetes homomorfizmus, ekkor $Z_2(G)$ legyen $Z(G/Z(G))$ teljes inverz képe. Könnyen látható, hogy $Z_2(G)$ szintén normálosztó G-ben, mely tartalmazza $Z(G)$-t. $Z_1(G) := Z(G)$ és tetszőleges $n \in \mathbb{N}$-re $Z_{n+1}(G)$ legyen $Z(G/Z_n(G))$ teljes inverz képe.

2.2.4. Definíció. A G csoport *felső centrális láncán* az alábbi normálláncot értjük:

$$\{e\} \leq Z_1(G) \leq Z_2(G) \leq \ldots.$$

A nilpotenciának így két jellemzése is adódik:

2.2.5. Definíció. G nilpotens, ha valamely n-re $G^{(n)} = \{e\}$, vagy valamely k-re $Z_k(G) = G$. Ez a kétfajta jellemzés szorosan kapcsolódik egymáshoz, mivel $Z_k(G) = G$ pontosan akkor teljesül, ha $G^{(k+1)} = \{e\}$ (lásd pl.: [7]). Megjegyezzük még, hogy minden Abel-csoport nilpotens, hiszen ha G Abel, akkor $G = Z(G) = Z_1(G)$ és $G' = \{e\}$.

2.2.6. Definíció. Legyen p prím. A G véges csoport *p-csoport*, ha $|G| = p^n$, valamely $n \in \mathbb{N}$-re.

Ha a végességet nem tételezzük fel, akkor szokás a p-csoportot az elemek rendjeivel definiálni: G p-csoport, ha G minden elemének a rendje p-nek hatványa. Megmutatható, hogy véges csoportokra a két definíció ekvivalens.

2.2.7. Definíció. Legyen $|G| = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$. Ekkor G *p_i-Sylow részcsoportjai* a $p_i^{r_i}$ rendű részcsoportok, vagyis azon maximális p-csoportok, melyeket valódi módon nem tartalmazza más p_i-csoport.

2.2.8. Tétel. *Egy véges G csoport pontosan akkor nilpotens, ha p-Sylow részcsoportjainak direkt szorzata.*

Mielőtt elkezdenénk a bizonyítást, szükséges lemmákat mondunk ki és bizonyítunk.

2.2.9. Lemma. *Minden véges p-csoport nilpotens.*

Bizonyítás. Legyen G véges, nemtriviális p-csoport, és irjuk fel az osztályegyenletét:

$$|G| = |Z(G)| + |K_1| + \ldots + |K_n|.$$

Megmutatjuk, hogy $|Z(G)| \neq 1$. G rendje osztható p-vel, továbbá az osztályegyenletben szereplő nem triviális K_i konjugáltosztályok rendje is osztható p-vel, ekkor szükségképpen $Z(G)$ rendje is, így $Z(G)$ nem lehet triviális. G minden faktora is szintén p-csoport, így ezek centruma sem triviális. Ha $Z_i(G) \neq G$, akkor $Z_i(G) \subsetneq Z_{i+1}(G)$, és mivel G véges, valamely $n \in \mathbb{N}$-re $Z_n(G) = G$, vagyis G nilpotens. □

2.2.10. Lemma. *Véges sok nilpotens csoport direkt szorzata is nilpotens.*

Bizonyítás. Legyenek H és K nilpotens csoportok és $G = H \times K$ (kettőnél több tényezőre a bizonyítás indukcióval történik). Belátjuk, hogy minden i-re $G^{(i)} \leq H^{(i)} \times K^{(i)}$. $i = 2$-re $G' = H' \times$ $\times K'$, ami a direkt szorzat tulajdonsága alapján - a műveleteket tagonként végezzük - könnyen láthatóan igaz, így indukcióval megmutatható általános i-re is. Mivel H és K nilpotensek, valamely k-ra és l-re $H^{(k)} = \{e\}$ és $K^{(l)} = \{e\}$. Legyen $m := \max\{k, l\}$, ekkor $G^{(m)} \leq H^{(m)} \times K^{(m)} = \{e_H\} \times$ $\times \{e_K\}$. Ez azt jelenti, hogy G nilpotens. □

2.2.11. Definíció. Egy H részcsoport *normalizátora* azon G-beli elemekből áll, melyekre $gH =$ $= Hg$. Jele: $N_G(H)$

2.2.12. Lemma. *Ha S p-Sylow részcsoport a véges G csoportban, akkor $N_G(N_G(S)) = N_G(S)$.*

Bizonyítás. Ha S p-Sylow részcsoport, akkor Sylow II. tétele szerint minden más p-Sylow részcsoport S-nek konjugáltja (lásd pl.: [3]). Mivel $S \lhd N_G(S)$, ezért S az egyetlen p-Sylow $N_G(S)$-ben. Legyen $P := N_G(S)$. A $P \leq N_G(P)$ triviálisan teljesül. A másik irány igazolásához legyen $g \in$ $\in N_G(P)$, ekkor $gPg^{-1} = P$ és mivel $S \lhd P$, $gSg^{-1} = S$ teljesül, ekkor tehát $g \in P$. Vagyis $N_G(P) \leq P$, így kapjuk, hogy $N_G(P) = P$. □

2.2.13. Lemma. *Ha H valódi részcsoport a nilpotens G csoportban, akkor valódi részcsoport $N_G(H)$-ban is.*

Bizonyítás. Mivel G nilpotens és H valódi részcsoport, létezik $n \in \mathbb{N}$, melyre $Z_n(G) < H$ és $Z_{n+1}(G) \not\leq H$. Legyen $g \in Z_{n+1}(G)$ olyan, melyre $g \notin H$. Mivel $Z_{n+1}(G)$ definíciója szerint tartalmazza $Z_n(G)g$-t, ezért minden $h \in H$-ra $Z_n(G)gh = (Z_n(G)g)(Z_n(G)h) = (Z_n(G)h)(Z_n(G)g) =$ $= Z_n(G)hg$ ($G/Z_n(G)$-ben). Ekkor $gh = h'hg$ valamely $h' \in Z_n(G) < H$-ra, így $ghg^{-1} \in H$, ekkor $g \in N_G(H)$ és mivel $g \notin H$, H valódi részcsoport $N_G(H)$-ban. □

A szükséges lemmákat beláttuk, következzen a 2.2.8 tétel bizonyítása:

Bizonyítás. Az elégségesség a 2.2.9 és a 2.2.10 lemmákból következik.
A szükségesség igazolásához legyen G nilpotens és p-Sylow részcsoportja legyen S. Ekkor ha $S = G$ akkor kész vagyunk. Ha S valódi részcsoport, akkor a 2.2.13 lemma szerint S valódi részcsoport, sőt normálosztó $N_G(S)$-ben is, a 2.2.12 lemma miatt viszont $N_G(S)$ normalizátora önmaga, így

csak $N_G(S) = G$ lehetséges. Ekkor $S \lhd G$ és ez az egyetlen p-Sylow mivel minden más p-Sylow S-nek konjugáltja. Legyen $|G| = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ és $S_1, \dots, S_n$ a megfelelő p-Sylowok, $|S_i| = p_i^{\alpha_i}$ és minden $i \neq j$-re $S_i \cap S_j = \{e\}$. Mivel S_i és S_j diszjunkt normálosztók, egyszerű számolással megmutatható, hogy minden $x \in S_i$ és $y \in S_j$, $i \neq j$-re $xy = yx$. Ebből következik, hogy minden i-re $S_1 \dots S_{i-1} S_{i+1} \dots S_n$ részcsoport, ahol minden elem rendje osztója $p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_n^{\alpha_n}$-nek. Ekkor

$$S_i \cap (S_1 \dots S_{i-1} S_{i+1} \dots S_n) = \{e\}, \text{ így } S_1 \dots S_n = S_1 \times \dots \times S_n.$$

Mivel $|G| = p_1^{\alpha_1} \dots p_n^{\alpha_n} = |S_1 \dots S_n|$, kapjuk, hogy

$$G = S_1 \dots S_n = S_1 \times \dots \times S_n.$$

□

2.3. Kulikov és Prüfer tételei

A következő fejezetben végtelen Abel-csoportokat vizsgálunk. Arra vagyunk kíváncsiak, hogy bizonyos feltételeknek eleget tevő, Abel-féle p-csoportok mikor állnak elő ciklikus csoportok direkt összegeként.

2.3.1. Definíció. Legyen A csoport, $a \in A$, és p rögzített prím. Ekkor az a elem *p-magassága* a legnagyobb olyan nemnegatív r kitevő, melyre $p^r x = a$ megoldható A-ban. Jele: $m_p(a)$. Ha nem okoz félreértést a továbbiakban csak *magasságról* beszélünk.

2.3.2. Definíció. Az $\{a_i\}_{i \in I}$ nemnulla A-beli elemekből álló rendszert *(lineárisan) függetlennek* nevezzük, ha minden véges részrendszere (lineárisan) független, vagyis $\sum_{i=1}^{k} n_i a_i = 0$-ból $n_i a_i = 0$ következik minden $i = 1, \dots, k$-ra. (Modulusok körében az ilyen rendszert gyengén függetlennek nevezzük majd.)

2.3.3. Definíció. Egy A csoport *n-talpának* nevezzük az azon elemekből álló részcsoportot, melyek rendje n-nek osztója: $A[n] = \{a \in A : na = 0\}$.

2.3.4. Tétel (Kulikov)**.** *Egy A p-csoport pontosan akkor áll elő ciklikus csoportok direkt összegeként, ha $A = \bigcup_{i=1}^{\infty} A_i$, ahol $A_1 \leq A_2 \leq \dots$ egy részcsoportokból álló növő lánc, és minden nemnulla A_i-beli elem magassága egy véges K_i korlát alatt marad.*

Bizonyítás. A szükségesség igazolásához tegyük fel, hogy A ciklikus csoportok direkt összege. Minden n-re gyűjtsünk össze minden olyan direkt összeadandót melyek rendje p^n. Jelölje ezek összegét B_n. Ekkor az $A_n = B_1 \oplus B_2 \oplus \dots \oplus B_n$ részcsoport lesz A-ban, az ilyen alakú részcsoportok növő láncot alkotnak, uniójuk pedig A. Könnyű látni, hogy a K_n korlátot választhatjuk n-nek.
Az elégségességhez tegyük fel, hogy az A_i részcsoportok teljesítik a feltételeket. Készítsünk a részcsoportokból növő láncot, ha szükséges a láncot az $\{0\}$-val indítjuk és néhány tagot többször is (véges sokszor) szerepeltetünk. Így feltehetjük továbbá, hogy $K_n = n$. Ekkor $A_n \cap p^n A = \{e\}$.
Tekintsük az összes olyan $\mathcal{L}_{C_n}$ láncot, amely A részcsoportjaiból áll és:

$$C_1 \leq C_2 \leq \dots, \quad \text{és} \quad C_n \cap p^n A = 0.$$

Az ilyen láncok halmazán vezessünk be egy $\in$ rendezést a következőképpen: $\mathcal{L}_{C_n} \in \mathcal{L}_{B_n}$, ha minden n-re teljesül, hogy $C_n \leq B_n$. Az így kapott részbenrendezett halmaz induktív, így a Zorn-lemma alapján létezik benne maximális $M_1 \leq M_2 \leq \ldots$ lánc, melyre $\bigcup M_i = A$. Konstruáljuk meg a következő elemeket: minden n-re vegyünk az $M_n[p] \cap p^{n-1}A$ részcsoportból egy maximális független rendszert. Jelölje ezt L_n. Legyen $L := \bigcup L_n$. Minden $l_i \in L$-re, melyek magassága k_i, válasszunk olyan $a_i \in A$ elemeket, melyekre $p^{k_i}a_i = l_i$. Megmutatjuk, hogy $A' = \bigoplus_i \langle a_i \rangle$ megegyezik A-val.

Először belátjuk, hogy $\langle L \rangle = A[p]$. Mivel L_n maximális független rendszer, ezért $\langle L_n \rangle = M_n[p] \cap p^{n-1}A$. Továbbá L_n olyan elemeket tartalmaz, melyek magassága $n-1$, ezért $L = \bigoplus_n \langle L_n \rangle$. (Itt tényleg direkt összeget kapunk, hiszen ha az $\langle L_n \rangle$ részcsoportok nem a direkt összeget generálnák, akkor léteznének olyan $x_i \in \langle L_i \rangle$ elemek, melyekre $x_1 + x_2 + \ldots + x_n = 0$, és itt nem minden $x_i = 0$ teljesülne. Tekintsük a legkisebb indexűt, melyre $x_i \neq 0$. Ennek a magassága $i-1$, viszont $m_p(x_{i+1} + x_{i+2} + \ldots + x_n) \geq i$, hiszen $m_p(a+b) \geq \min\{m_p(a), m_p(b)\}$. Ez viszont ellentmondás.) Most n-re vonatkozó indukcióval belátjuk, hogy minden $a \in A[p]$, ami M_n-ben is benne van, része $\langle L \rangle$-nek is. Ez $n = 1$-re triviálisan teljesül, hiszen $L_1 = M_1[p] \cap p^0 A = M_1[p]$. Legyen $m \in M_{n+1}[p] - M_n$, ekkor $\langle M_n, m \rangle \cap p^n A \neq 0$, és van olyan $k \in M_n$, melyre $0 \neq k + m = r \in p^n A$. Mivel a magasságra vonatkozó K_n korlátot n-nek választottuk és $M_n \cap p^n A = 0$, $r \in M_{n+1}$, $m_p(r) = n$ és $o(r) = p$. Ezzel beláttuk, hogy $r \in \langle L_{n+1} \rangle$. Mivel $pk = pr - pm$ és $k \in M_n$, továbbá az indukciós feltevés alapján $k \in \langle L \rangle$. $m = r - k \in \langle L \rangle$, ezért $\langle L \rangle = A[p]$.

A következő lépésben egy elem rendjére vonatkozó indukcióval bizonyítjuk, hogy ha $a \in A$, akkor $a \in A'$ is teljesül. Tegyük fel, hogy az állítást minden olyan $a \in A$-ra beláttuk, melynek a rendje legfeljebb p^n. Legyen most $a \in A$ olyan, aminek a rendje p^{n+1}. Ekkor a fentiek alapján $p^n a \in \langle L \rangle$, amiből következik, hogy $p^n a = d_1 l_1 + d_2 l_2 + \ldots + d_k l_k$ valamely $l_i \in L$-re. Indexeljük úgy az l_i generátorokat, hogy az $l_1, l_2 \ldots, l_j$ elemeket magassága legalább n legyen, az $l_{j+1}, l_{j+2}, \ldots, l_k$ elemeké pedig legfeljebb $n-1$. Ekkor írhatjuk, hogy $d_i l_i = p^n m_i a_i$ minden $i = 1,2,\ldots,j$-re. Így a következőt nyerjük:

$$p^n(a - m_1 a_1 - m_2 a_2 - \ldots - m_j a_j) = d_{j+1} l_{j+1} + d_{j+2} l_{j+2} + \ldots + d_k l_k \in M_{n-1}.$$

Mivel $M_{n-1} \cap p^{n-1}A = 0$, az $a - m_1 a_1 - m_2 a_2 - \ldots - m_j a_j$ rendje legfeljebb p^n, ezért az indukciós feltétel szerint A'-beli, és mivel az $a_1, a_2 \ldots, a_j$ elemek szintén A'-ben találhatóak, szükségképpen $a \in A'$ is teljesül. Ezzel a tételt bebizonyítottuk. □

A Kulikov-tételből egyszerűen nyerünk néhány klasszikus eredményt.

2.3.5. Definíció. *Korlátosnak* nevezünk egy csoportot, ha minden elemének a rendje egy K korlát alatt marad. Például A *n-korlátos*, ha $nA = 0$.

2.3.6. Tétel (Prüfer, Baer)**.** *Minden korlátos csoport ciklikus csoportok direkt összege.*

Bizonyítás. Legyen A korlátos csoport, ekkor ennek minden p-komponense csakugyan korlátos (később precízen megmutatjuk, hogy egy torziócsoport p-kompenenseinek direkt összege). Ha a 2.3.4 tételben szereplő részcsoportoknak az A p-komponenseit választjuk, akkor ezek eleget tesznek a feltételeknek, így a tételből következően A ciklikus csoportok direkt összege. □

2.3.7. Tétel (Prüfer). *Egy megszámlálható p-csoport pontosan akkor áll elő ciklikus csoportok direkt összegeként, ha minden nem 0 elemének a magassága véges.*

Bizonyítás. Legyen A olyan megszámlálható p-csoport, melynek minden nem 0 elemének a magassága véges, ekkor választhatunk $\langle a_1, a_2, \ldots\rangle$ generátorrendszert. Az $A_n := \langle a_1, a_2, \ldots, a_n\rangle$ $(n = = 1{,}2, \ldots)$ csoportok uniója lesz A, melyek elemei triviálisan véges korlátosak. Ekkor a 2.3.4 tételből már következik az állítás. □

2.4. Osztható Abel-csoportok

A következőkben Abel-csoportok egy fontos osztályát vizsgáljuk, az osztható Abel-csoportokat. Mielőtt kimondanánk a rájuk vonakozó struktúratételt ismertetjük a felhasznált fogalmakat és állításokat.

2.4.1. Definíció. Egy G Abel-csoportot *oszthatónak* nevezünk, ha minden $n \neq 0$ egész számra és minden $g \in G$-re az $nx = g$ egyenlet megoldható G-ben. Ez azzal ekvivalens, hogy $g \in nG$, vagyis $G = nG$ minden $n \neq 0$ egészre. Jelölésben: minden $g \in G$-re $n \mid g$.

Alapvető példák osztható csoportokra: $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}, \mathbb{Z}_{p^\infty}$. Itt $\mathbb{Z}_{p^\infty}$ jelöli a *kváziciklikus csoportot*, mely az alábbi csoport: $\mathbb{Z}_{p^\infty} = \langle a_1, a_2, \ldots \mid pa_1 = 0, pa_{n+1} = a_n\rangle$. Ekkor $\mathbb{Z}_{p^\infty}$-t az alábbi növő részcsoportlánc limeszének is tekinthetjük: $0 \leq \mathbb{Z}_p \leq \mathbb{Z}_{p^2} \leq \ldots$

2.4.2. Definíció. G *torziórészcsoportjának* nevezzük a G Abel-csoport azon elemei által alkotott részcsoportot, melyek rendje véges, jelölje ezt $T(G)$.

Könnyen látható, hogy az ilyen tulajdonságú elemek tényleg részcsoportot alkotnak. Megjegyezzük, hogy $G/T(G)$ torziómentes.

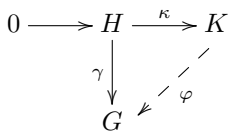
2.4.3. Definíció. G *talpának* nevezzük a G Abel-csoport azon elemeiből álló részcsoportot, melyek rendje négyzetmentes, vagyis olyan természetes szám, melynek faktorizációjában szereplő prímek első hatványon szerepelnek. Jelöljük ezt $S(G)$-vel.

A bizonyítások során felhasználjuk többek között az alábbiakat:

(*i*) Egy osztható csoport minden szürjektív homomorfizmusnál vett képe osztható. Ugyanis, ha $\varphi : A \to B$ szürjektív, akkor ha $n \mid g$-t A-ban, akkor $n \mid \varphi(g)$-t B-ben.

(*ii*) Csoportok direkt összege pontosan akkor osztható, ha az összeadandók oszthatóak. Ha $G = A \oplus B$, akkor $n \mid g = a + b$ pontosan akkor, ha $n \mid a$ és $n \mid b$.

2.4.4. Definíció. *Injektívnek* nevezünk egy G csoportot, ha minden alábbi diagram kommutatívvá tehető egy alkalmas φ homomorfizmussal:



Itt $0 \longrightarrow H \xrightarrow{\kappa} K$ azt jelöli, hogy κ injektív. Ha H-t κH-val azonosítjuk, akkor G injektivitása azt jelenti, hogy bármely $\gamma : H \to G$ homomorfizmus kiterjeszthető K-ból G-be képező homomorfizmussá (K tartalmazza H-t).

(*iii*) (Baer) Minden osztható csoport injektív (a bizonyítást lásd pl. [9]-ben).

2.4.5. Tétel. *Ha G osztható Abel-csoport, akkor $G \cong \bigoplus_I \mathbb{Z}_{p^\infty} \oplus \bigoplus_n \mathbb{Q}$.*

Mielőtt elkezdenénk a bizonyítást, szükséges lemmákat mondunk ki és bizonyítunk:

2.4.6. Lemma. *(Baer) Ha H osztható részcsoport a G csoportban, akkor $G = H \oplus K$, alkalmas K részcsoporttal.*

Bizonyítás. Mivel H osztható, így injektív is, ezért létezik $\varphi : G \to H$ homomorfizmus (projekció), hogy az alábbi diagram kommutatív:

$$\begin{array}{ccc} H & \xrightarrow{\rho} & G \\ \| & \swarrow_{\varphi} & \\ H & & \end{array}$$

Itt ρ injekció H-ból G-be. Legyen $\theta = \mathrm{id}_G - \varphi$. Ekkor $G = H + \theta G$, $\theta G = \mathrm{Ker}\varphi$. Mivel a mag és a projekció képe „diszjunkt", $G = H \oplus \mathrm{Ker}\varphi$. □

2.4.7. Lemma. *Ha $G = T(G)$-vel, akkor $G = \bigoplus_p T_p$, ahol T_p p-csoport.*

Bizonyítás. T_p G azon elemeiből áll, melyek rendje p-nek hatványa. Könnyen látható, hogy ez tényleg részcsoport. Mivel $o(a_1+\ldots+a_n)$ osztója az $\mathrm{lkkt}(o(a_1), \ldots, o(a_n))$-nek, ezért $T_{p_i} \cap \bigoplus_{i \neq j} T_{p_j} = 0$, így T_p-k generálják a direkt összeget, és $\bigoplus_p T_p \subseteq G$. Legyen $g \in G$, mivel G torziócsoport, g rendje véges, tegyük fel, hogy ez n és, hogy n faktorizációja $\prod_i p_i^{\alpha_i}$. n-et osszuk el $p_i^{\alpha_i}$-vel: $n_i := np_i^{-\alpha_i}$, ekkor könnyen látható hogy az n_i-k összességükben relatív prímek. Számelméleti meggondolás, hogy a legkisebb közös osztót alkalmas egész s_i-k segítségével, az n_i-k lineáris kombinációjaként írhatjuk: $1 = \sum_i s_i n_i$, így $g = \sum_i s_i n_i g$. Mivel $p_i^{\alpha_i} n_i g = ng = 0$, kapjuk, hogy $n_i g \in T_{p_i}$ minden p_i-re, vagyis $g \in \bigoplus_p T_p$, és így $G \subseteq \bigoplus_p T_p$, vagyis $G = \bigoplus_p T_p$. □

2.4.8. Lemma. *Ha G osztható p-csoport, akkor $G \cong \bigoplus_I \mathbb{Z}_{p^\infty}$.*

Bizonyítás. Válasszunk egy maximális $\{a_i\}_{i \in I}$ lineárisan független rendszert G talpában (a Zorn-lemma biztosítja, hogy ilyen létezik). Mivel G osztható, minden $\{a_i\}$-re létezik egy $\{a_{i,n}\}_{n \in \mathbb{N}}$ végtelen sorozat, melyre: $a_{i,1} = a_i, pa_{i,j+1} = a_{i,j}$. Legyen $H_i := \langle a_{i,n} \rangle_{n \in \mathbb{N}}$, könnyen látható, hogy $H_i \cong \mathbb{Z}_{p^\infty}$. A $\langle a_i \rangle$ talpa a H_i csoportnak és a_i-k függetlenségéből következően H_i-k a $H = \bigoplus_{i \in I} H_i$ direkt összeget generálják. H osztható, hiszen egy direkt összeg, melynek komponensei egy osztható csoporttal izomorfak: $H \cong \bigoplus_I \mathbb{Z}_{p^\infty}$, ekkor $G = H \oplus K$ (alkalmas K részcsoporttal). Mivel $\{a_i\}_{i \in I}$ rendszer maximális, így csak $K = \{0\}$ lehetséges, ekkor $G \cong \bigoplus_I \mathbb{Z}_{p^\infty}$. □

2.4.9. Lemma. *Legyen G torziómentes osztható csoport. Ekkor $G \cong \bigoplus_n \mathbb{Q}$.*

Bizonyítás. Válasszunk G-ben egy maximális független $\{a_i\}_{i\in I}$ rendszert (a Zorn-lemmát felhasználva megmutatható, hogy ilyen létezik). Mivel G osztható és torziómentes az $ny = x$ egyértelműen megoldható, ekkor $y = \frac{1}{n}x$ jóldefiniált. Legyen $\mathbb{Q}a_i := \{ra_i : r \in \mathbb{Q}\}$. Könnyen látható, hogy $\mathbb{Q}a_i$ részcsoport G-ben és $\mathbb{Q}a_i \cap \mathbb{Q}a_j = 0$ minden $i \neq j$-re, hiszen, ha $\frac{s}{t}a_i = \frac{p}{q}a_j$, akkor $qsa_i - tpa_j = 0$ ami ellentmond a_i-k függetlenségének. Legyen $H := \bigoplus_{i\in I} \mathbb{Q}a_i$, ekkor $H \leq G$. Tekintsük az alábbi $\varphi : \mathbb{Q}a_i \to \mathbb{Q}$ homomorfizmust: $\frac{s}{t}a_i \mapsto \frac{s}{t}$ hozzárendeléssel. Könnyen látható, hogy ez izomorfizmus, így $\mathbb{Q}a_i \cong \mathbb{Q}$, vagyis $H \cong \bigoplus_I \mathbb{Q}$. Mivel H osztható csoport $G = H \oplus K$ (alkalmas K részcsoporttal). Mivel $\{a_i\}_{i\in I}$ rendszer maximális, így csak $K = \{0\}$ lehetséges, ekkor $G \cong \bigoplus_n \mathbb{Q}$. □

Mivel a szükséges lemmákat beláttuk, következzen a 2.4.5 tétel bizonyítása:

Bizonyítás. Ha $x \in T(G)$, akkor mivel G osztható csoport, bármely $n \in \mathbb{N}$ esetén létezik $y \in G$, hogy $ny = x$. Könnyen látható, hogy $y \in T(G)$, hiszen $o(x)ny = o(x)x = 0$, vagyis $T(G)$ osztható. Ekkor az 1. lemma (Baer) szerint $G = T(G) \oplus H$ valamely H részcsoportra. A direkt összeg tulajdonságai alapján $H \cong G/T(G)$-vel. Ekkor H torziómentes és osztható, így a 2.4.9 lemma alapján $H \cong \bigoplus_n \mathbb{Q}$. $T(G)$ torziócsoport, így a 2.4.7 lemma alapján $T(G) = \bigoplus_p T_p$. T_p p-csoport és osztható, hiszen $T(G)$ osztható, ekkor viszont a 2.4.8 lemma miatt $T(G) \cong \bigoplus_I \mathbb{Z}_{p^\infty}$. Ezekből következik, hogy $G \cong \bigoplus_I \mathbb{Z}_{p^\infty} \oplus \bigoplus_n \mathbb{Q}$, amivel a tételt beláttuk. □

3. fejezet

Struktúratételek a gyűrű - és moduluselméletben

A gyűrűk szerkezetének felderítésében nagy segítséget kapunk, ha a felettük vett modulusokat vizsgáljuk (lásd pl.: 3.2.15). A csoportok reprezentációjánál pedig a csoportgyűrűk, csoportalgebrák feletti modulusok kerülnek a vizsgálat középpontjába. A fejezetben bemutatjuk a főideálgyűrű feletti végesen generált torziómodulusok alaptételét, melyből speciális esetként következik a véges **Abel-csoportok alaptétele**. A tételt felhasználva megmutatjuk, hogy minden komplex elemű mátrixnak létezik **Jordan-normálalakja**. Bemutatjuk a **Wedderburn-Artin-struktúratételt**, a hozzá kapcsolódó, speciális ideál, a **Jacobson-radikál** és teljes mátrixgyűrűk kapcsolatát. A véges csoportok reprezentációjáról is lesz szó a fejezetben.

3.1. Végesen generált torziómodulusok

Mielőtt közölnénk és bizonyítanánk a tételt, a felhasznált fogalmakat definiáljuk és bizonyítjuk. A továbbiakban az R gyűrűről feltesszük, hogy kommutatív, egységelemes és nullosztómentes, továbbá, hogy főideálgyűrű, ebből következően igaz benne a számelmélet alaptétele.

3.1.1. Definíció. Egy bal oldali R-modulus egy m elemének a *rendje* azon $r \in R$ elemekből álló halmaz, melyek m-et 0-ba szorozzák.

Nem nehéz látni, hogy ez az $\{r \in R : rm = 0\}$ halmaz balideál R-ben, esetünkben pedig főideál.

3.1.2. Definíció. Az M R-modulust *torziómodulusnak* nevezzük, ha minden elemének nem nulla a rendje, vagyis minden eleme végesrendű.

3.1.3. Definíció. Az M R-modulus *exponensének* nevezzük az M modulus annulátorának (azon R-beli elemek által alkotott ideál, melyek M elemeit 0-ba szorozzák) egyik generátorelemét. Az m által generált modulus exponense $o(m)$. Ez m rendjének generátoreleme, mivel R főideálgyűrű.

Megjegyezzük, hogy egy ciklikus modulus exponense megegyezik a generátorelemének a rendjével.

Az alaptétel azt mondja ki, hogy bármely főideálgyűrű feletti végesen generált torziómodulus felbontható ciklikus részmodulusainak direkt összegére, ahol az összeadandók rendje prímhatvány, és a felbontás egyértelmű. Mielőtt eljutnánk a teljes tételhez, megmutatjuk, hogy létezik olyan részmodulusokra történő felbontás, melyek még nem biztos, hogy ciklikusak.

3.1.4. Tétel. *Bármely R főideálgyűrű feletti, végesen generált M torziómodulus, melynek exponense az $r_1, \ldots, r_n$ páronként relatív prím elemek szorzata, felírható részmodulusainak direkt összegeként: $M = M_1 \oplus \ldots \oplus M_n$. Az M_i részmodulusok szintén végesen generáltak, M_i exponense r_i. Ha az r_i elemek egyetlen felbonthatatlan elem hatványai, akkor a direkt összegként történő felírás egyértelmű abban az értelemben, hogy bármely más felbontásban csak a tagok sorrendje változhat.*

Bizonyítás. Legyen $G = \{g_1, \ldots, g_n\}$ az M egy generátorrendszere. Mivel M torziómodulus, léteznek $r_1, \ldots, r_n$ R-beli nemnulla elemek, melyekre $r_i g_i = 0$. Legyen r az r_i-k legkisebb közös többszöröse, ekkor bármely $m \in M$-re $rm = 0$, hiszen m-et a g_i generátorok előállítják, R kommutatív és nullosztómentes, így r sem 0. Bontsuk fel az M modulus r exponensét relatív prím p, q elemek szorzatára, és tekintsük az $M_p = \{qm : m \in M\}$ és $M_q = \{pm : m \in M\}$ részmodulusokat. Mivel r-t az egymáshoz relatív prím p, q elemekre tudtuk felbontani, ezért léteznek olyan $x, y \in R$ elemek, melyekre $px + qy = 1$ teljesül. Ekkor minden $m \in M$-re $m = 1m = (px + qy)m = x(pm) + + y(qm)$, vagyis $M = M_p + M_q$. Könnyen látható, hogy $pM_p = \{0\}$ és hasonlóan $qM_q = \{0\}$. Az egyértelmű felírás bizonyításához tekintsünk egy tetszőleges $n \in M_p \cap M_q$ elemet. Megmutatjuk, hogy ez csak a 0 lehet: $pn = qn = 0$, melyből $n = 1n = (px + qy)n = x(pn) + y(qn) = x0 + y0 = 0$, tehát $M_p \cap M_q = \{0\}$. Ebből már következik, hogy $M = M_p \oplus M_q$. Legyen M_p exponense p' és M_q exponense q'. Ekkor $p' \mid p$ és $p'qM = \{0\}$ miatt $pq \mid p'q$, amiből $p \mid p'$ következik, vagyis M_p exponense tényleg p. M_q exponense hasonlóan számítható. M_p generátorrendszere szintén véges, innen indukcióval megmutatható az állítás több összeadandóra.

Tegyük fel, hogy r_i már tovább nem bontható relatív prímek szorzatára, ekkor $M = M_1 \oplus \ldots \oplus \oplus M_n$. Tekintsünk egy másik felbontást. Legyen $M = N_1 \oplus \ldots \oplus N_k$. Itt hasonlóan N_i exponense s_i. Mivel R alaptételes, érvényes benne az egyértelmű faktorizáció, így $n = k$. Az s_i-k csak sorrendben térhetnek el az r_i-ktől, ezért feltehetjük, hogy $s_i = r_i$. Tekintsük a $t_i = \frac{r}{r_i}$ elemeket. Könnyen látható, hogy r_i és t_i relatív prímek, és t_i az M_i kihagyásával keletkező direkt összeg exponense, r_i tehát csak az M_i elemeti viheti 0-ba, $M_i = \{m \in M : r_i m = 0\}$. Ez hasonlóan áll fent N_i-re, így szükségképpen $M_i = N_i$, mivel az $\{m \in M : r_i m = 0\}$ független az így definiált részmodulustól. Ezzel a bizonyítást befejeztük. □

A továbbiakban be fogjuk látni, hogy M-nek létezik egy olyan $B = \{b_1, \ldots, b_n\}$ bázisa, melyre M a b_i-k által generált ciklikus modulusok direkt összege, és olyan $r_1, \ldots, r_n$ R-beli elemek, melyek egy felbonthatatlan elem hatványai, és ahol b_i-k rendje a megfelelő r_i. Mielőtt ezt belátnánk, bebizonyítjuk az alábbi lemmát.

3.1.5. Lemma. *Legyen R főideálgyűrű, és tekintsük az M végesen generált R-modulust, melynek bázisa $B = \{b_1, \ldots, b_n\}$. Ekkor bármely N, M-beli részmodulusra létezik M-nek olyan $C = = \{c_1, \ldots, c_n\}$ elemekből álló bázisa, és léteznek olyan R-beli $r_1, \ldots, r_n$ elemek, melyekre $r_1 \mid r_2 \mid | \ldots \mid r_n$, hogy a $d_1 = r_1 c_1, \ldots, d_n = r_n c_n$ elemek közül a 0-tól különbözőek N egy bázisát alkotják.*

A bizonyítás előtt definiáljunk két fontos fogalmat:

3.1.6. Definíció. *Normálalakúnak* nevezünk egy $A = (a_{ij})$ mátrixot, ha a főátlón kívül minden elem 0 és minden i-re $a_{ii} \mid a_{i+1,i+1}$

3.1.7. Definíció. *Elemi átalakításnak* nevezzük a következőket:

(i) Az i-edik oszlop r-szeresét hozzáadjuk a j-edik oszlophoz ($i \neq j, \quad r \in R$).

(ii) Egy oszlopot egy r egységgel megszorzunk.

(iii) Megcserélünk két oszlopot.

(iv) Elhagyunk egy sort vagy/és egy oszlopot.

Hasonló érvényes sorokra is.

A (konstruktív) bizonyításhoz még szükségünk van két lemmára.

3.1.8. Lemma. *Legyen $A \in R^{k\times k}$. Ekkor A-nak pontosan akkor létezik $R^{k\times k}$-ban inverze, ha determinánsa R-nek egysége.*

Bizonyítás. Tegyük fel, hogy létezik $A^{-1} \in R^{k\times k}$. Ekkor a determinánsok szorzástétele alapján $\det(A) \cdot \det(A^{-1}) = 1$, így A determinánsa tényleg egység.
A megfordításhoz tegyük fel, hogy $\det(A)$ egység R-ben, vagyis R minden elemének az osztója. A inverzét A elemeinek összeadással, kivonással, szorzással és $\det(A)$-val való osztással kapjuk, így az inverz szintén $R^{k\times k}$-beli. □

3.1.9. Lemma. *Legyen M végesen generált R-modulus, melynek az egyik generátorrendszere $g_1, \ldots, g_n$. Legyen $A = (a_{ij}) \in R^{n\times n}$, melynek determinánsa R-nek egysége. Ekkor a $b_i = a_{i1}g_1 + + \ldots + a_{in}g_n$ $(i = 1, \ldots, n)$ szintén generátorrendszere M-nek, és ha a g_i-k bázist alkottak, akkor a b_i-k is.*

Bizonyítás. Tegyük bele g_i-ket formálisan egy v vektorba. Ekkor $Av = w$, ahol w tartalmazza b_i-ket. Mivel A determinánsa egység, létezik $A^{-1} = (s_{ij}) \in R^{n\times n}$. Ekkor az inverzzel beszorozva azt kapjuk, hogy $g_i = s_{i1}b_1 + \ldots + s_{in}b_n$. A b_i-k tehát generátorrendszert alkotnak. Tegyük fel, hogy g_i-k bázist alkotnak. Tekintsük b_i-k egy lineáris kombinációját. Legyen $c_1b_1 + \ldots + c_nb_n = 0$. Ha visszahelyettesítjük a g_i-ket és kihasználjuk, hogy függetlenek, akkor azt kapjuk, hogy A sorainak a c_i együtthatókkal vett lineáris kombinációja 0, ami azt jelentené, hogy a sorok összefüggenek, így a determinánsa 0. Ez viszont ellentmondás, így szükségképpen $c_1 = \ldots = c_n = 0$. A b_i-k tehát bázist alkotnak. □

És most elkezdhetjük a 3.1.5 lemma bizonyítását:

Bizonyítás. Készítsük el azt az n oszlopból álló mátrixot, melynek sorai azok $(s_1, \ldots, s_n)$ R-beli sorvektorok, melyre az $s_{i1}b_1 + \ldots + s_{in}b_n = g_i$, ahol g_i generátor N-ben. A g_i elemeket egy I halmaz elemeivel indexeljük. Az így kapott mátrixot elemi átalakításokkal normálalakra fogjuk hozni. Legyen s_{11} és s_{12} legnagyobb közös osztója d. Mivel R főideálgyűrű, alkalmas $x, y \in R$ elemekkel $s_{11}x + s_{12}y = d$. A kapott mátrixunkat szorozzuk jobbról az alábbi B mátrixszal:

$$\begin{pmatrix} x & -\frac{s_{12}}{d} & 0 & \dots & 0 \\ y & \frac{s_{11}}{d} & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Ekkor az újonnan keletkező mátrix első sorának első eleme d lesz a második pedig 0. Mivel az oszlopokkal végzett elemi átalakítások elemi bázistranszformációnak felelnek meg és a fenti mátrix determinánsa 1, az előző lemma alapján az a keletkező új c_i-k szintén bázist alkotnak. Ekkor a sorok elemei már ugyanannak a g_i-nek az új bázisban felírt kordinátái lesznek. Ezt az eljárást folytatva, alkalmas mátrixokkal való szorzással elérhető, hogy az első sor első eleme, az első sor elemeinek egyik legnagyobb közös osztója legyen, míg a többi elem 0. Hasonlóan kinullázhatjuk az első oszlopot. Mivel mindig osztókat nyerünk, az egyértelmű faktorizáció miatt az eljárás véget ér. Legyen tehát az első sor és oszlop minden eleme 0, kivéve r_{11}-et. Tegyük most fel, hogy van a mátrixunkban egy olyan elem, ami nem osztható r_{11}-gyel. Legyen ez például r_{ij}. Ekkor adjuk hozzá az első sorhoz a i-ediket, az első sor j-edik eleme r_{ij} lesz, majd ismét folytassuk az eljárást elölről. Ha az elemi átalakítások során a mátrixunkban az r_{11} minden más elemnek osztója, és az első sorban és oszlopban az első elemen kívül minden elem 0, akkor hagyjuk el a mátrix első sorát és oszlopát, majd folytassuk az eljárást az eggyel kevesebb oszloppal (és sorral) rendelkező mátrixszal. Mivel n oszlopunk van az eljárás véges. A keletkező mátrix négyzetes ($n \times n$, mivel a csupa 0 sorokat elhagyhatjuk), a főátlóban álló elemekre teljesül az oszthatósági feltétel, az újonnan keletkező N-beli generátorelemek pedig rendre $r_{ii}c_i$ alakúak, melyek N egy bázisát alkotják. Ezzel a bizonyítást befejeztük. □

3.1.10. Definíció. Az M modulusban az X *gyengén független* rendszer, ha X-beli elemek egy lineáris kombinációja csak úgy lehet 0, ha minden összeadandó 0. *Gyenge bázisnak* a gyengén független generátorrendszert nevezzük.

3.1.11. Tétel. *Legyen R főideálgyűrű és M pedig végesen generált, torzió R-modulus. Ekkor M-nek létezik olyan $B = \{b_1, \dots, b_n\}$ elemekből álló (gyenge) bázisa, és olyan $r_i \in R$ elemek, melyek mindegyike egy felbonthatatlan elem hatványa és $o(b_i) = r_i$.*

A bázis létezéséből már következik, hogy M felbontásában az összeadandók ciklikus részmodulusok, melyek rendje r_i. Tudjuk, hogy egyfajta felbontás létezik, ezeket az összeadandókat (részmodulusokat) szeretnénk tovább bontani a megfelelő módon.

Bizonyítás. Legyen M R-modulus, melynek generátorrendszere $G = \{g_1, \dots, g_n\}$ és exponense p^k, ahol $p \in R$ egy felbonthatatlan elem. Tekintsünk most R-et mint önmaga feletti R-modulust. Készítsük el az R^n-beli n hosszú e_i sorvektorokat, melyek i-edik helyén 1, a többi helyen pedig 0 áll. Világos, hogy $e_1, \dots, e_n$ R^n egy bázisát alkotják. Mivel e_i bázis, létezik egy egyértelműen meghatározott $\varphi : R^n \to M$ modulushomomorfizmus, melyre $\varphi(e_i) = g_i$. φ-nek szürjektívnek kell lennie, hiszen G generátorrendszer, így $M \cong R^n/\mathrm{Ker}\varphi$. Tekintsük Ker$\varphi$-t, R^n egy részmodulusát. A(z) 3.1.5 szerint R^n-nek létezik egy olyan $C = \{c_1, \dots, c_n\}$ bázisa és olyan $r_1, \dots, r_n$ R-beli elemek,

melyekre $r_1 \mid r_2 \mid \ldots \mid r_n$ teljesül, hogy a $d_1 = r_1c_1, \ldots, d_n = r_nc_n$ elemek közül a nem 0-k $\mathrm{Ker}\varphi$ egy bázisát alkotják. Legyen $\varphi(c_i) = b_i$, ekkor $r_ib_i = 0$ hiszen $r_ic_i \in \mathrm{Ker}\varphi$. A most kapott b_i elemek generátorrendszert alkotnak a faktorban, hiszen c_i bázis és φ szürjektív. b_i-k egy lineáris kombinációja csak úgy lehet 0, ha a megfelelő együtthatók oszthatók r_i-vel. b_i-k ekkor egy gyenge bázist alkotnak, így $M \cong \langle b_1\rangle \oplus \ldots \oplus \langle b_n\rangle$. r_i-k osztják az M exponensét, így minden r_i a felbonthatatlan p-nek egy hatványa. A(z) 3.1.4 tétel alapján M felbontható olyan részmodulusainak direkt összegére, melyek exponense már nem bontható relatív prímek szorzatára, ekkor ez prímhatvány kell, hogy legyen. Az ilyen össezadandókat bontottuk olyan ciklikus modulusok direkt összegére, melyek exponense ennek a prímhatványnak osztója. A direkt összeg „finomítási" tulajdonsága alapján M tényleg olyan ciklikus modulusok direkt összege, melyek rendje prímhatvány. Ezzel a főideálgyűrű feletti végesen generált torziómodulusok alaptételét bebizonyítottuk. □

3.1.1. Véges Abel-csoportok alaptétele

A most következő tétel speciális esete az előzőeknek.

3.1.12. Tétel. *Minden véges Abel-csoport prímhatványrendű ciklikus csoportok direkt összege. Az ilyen felbontásban szereplő összeadandók rendjei egyértelműen meghatározottak. Kétféle felbontás esetén egy q prímhatványhoz tartozó összeadandók száma mindkét felbontásban ugyanannyi lesz.*

Legyen G véges Abel-csoport. Ekkor G $\mathbb{Z}$-modulussá válik a szokásos G-beli műveletekre, a $\mathbb{Z}$ elemeivel történő szorzást a következőképpen értelmezzük:

$$ng := \begin{cases} \underbrace{g + \ldots + g}_{n} & n > 0 \\ 0 & n = 0 \\ -(\underbrace{g + \ldots + g}_{n}) & n < 0 \end{cases}$$

Természetesen ha a csoportművelet a szorzás, akkor hatványozásról beszélhetünk.
Mivel $\mathbb{Z}$ főideálgyűrű és G véges, így végesen generált és torziócsoport, alkalmazhatjuk a főideálgyűrű feletti végesen generált torziómodulusok alaptételét. Ekkor G prímhatványrendű ciklikus csoportok direkt összege. Legyen például G rendje 60. Ekkor 60 prímhatványtényezőiből kell a 60-at megkapni. A következő csoportokat nyerjük:

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

Tekintsük például $\mathbb{Z}_{32}^{\times}$-t, melynek rendje 16. Ebben $\langle 3\rangle$ egy 8 elemű részcsoport. Ennek az indexe 2. Mivel az 5 nem található $\langle 3\rangle$-ban, a $\{3{,}5\}$ már generálják az egész csoportot. A(z) 3.1.5 lemma alapján elkészítünk egy olyan mátrixot, melyben olyan r, s elemek találhatól, melyekre $3^r \cdot 5^s = 1$, majd ezt a mátrixot hozzuk normálalakra. Mivel euklideszi gyűrű felett vagyunk, alkalmazhatjuk az euklideszi normát és a maradékos osztást a sorok és oszlopok kinullázására.

$$\begin{pmatrix} 8 & 0 \\ 0 & 8 \\ 2 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 8 \\ 0 & 0 \end{pmatrix}$$

Amiből azt kapjuk, hogy $\mathbb{Z}_{32}^{\times} \cong \mathbb{Z}_2^+ \oplus \mathbb{Z}_8^+$.

3.1.2. Jordan-féle normálalak

A következőkben a Jordan-féle normálalakot tárgyaljuk. Alapvető igény lehet, hogy egy A mátrixot alkalmas bázisban „szép" alakra hozzunk, melyből könnyen leolvashatók a sajátértékek és magával a mátrixszal is könnyebb számolni, például hatványozni. Megmutatjuk, hogy a Jordan-féle normálalak létezése következik a főideálgyűrű feletti végesen generált torziómodulusok alaptételéből. Az alaptétel felhasználásával V-ben egy olyan bázist szeretnénk kiválasztani, melyben az A mátrixa főátlóra fűzött blokkokból áll. Mielőtt kimondanánk és bizonyítanánk a tételt, definiáljunk egy alkalmas modulust, mellyel dolgozni szeretnénk.

3.1.13. Definíció. Legyen V egy algebrailag zárt $\mathbb{K}$ test feletti n dimenziós vektortér és $A \in$ $\in \mathrm{End}(V)$, a V egy lineáris transzformációja. Tekintsük a következő homomorfizmust: $\Phi_A : \mathbb{K}[x] \to \mathrm{End}(V)$, melyre $\Phi_A(f) = f(A)$, azaz az A lineáris transzformáció behelyettesítése az $f \in \mathbb{K}[x]$ polinomba. Ekkor V $\mathbb{K}[x]$-modulussá tehető a következőképpen: a modulusösszeadás a V-beli összeadással egyezzen meg, míg egy $\mathbb{K}[x]$-beli f elemmel való szorzásra pedig: $fu := f(A)u$ teljesüljön. A kapott modulust jelöljük $M(A, V)$-vel.

Azt könnyű igazolni, hogy $M(A, V)$ végesen generált és torziómodulus, hiszen V bázisa $\mathbb{K}[x]$ felett is generátorrendszer, és például A minimálpolinomja minden elemet 0-ba visz. Ezért alkalmazhatjuk az alaptételt. Részmodulusai pontosan a V vektortér A-invariáns alterei. Legyen ugyanis $W \leq V$ részmodulus, ekkor $xw \in W$ és így Aw is W-beli. A megfordításhoz legyen W A-invariáns altér, ekkor könnyen láthatóan A minden hatványa is W-be képez, így bármely $w \in W$-re az fw is W-beli, hiszen egy altér zárt a lineáris kombináció képzésére. W tehát részmodulus.

3.1.14. Tétel (Jordan-féle normálalak)**.** *Legyen V egy algebrailag zárt test feletti véges dimenziós vektortér és A V egy lineáris transzformációja. Jelölje $m_A(x) = (x - \alpha_1)^{k_1} \dots (x - \alpha_n)^{k_n}$ az A minimálpolinomját $\mathbb{K}$ felett. Ekkor V-nek létezik olyan bázisa, melyben A mátrixa a főátlóra helyezett Jordan-blokkokból áll, minden más elem pedig 0. Egy α_i sajátértékhez tartozó Jordan-blokk a következő alakú: a főátlóban α_i szerepel, a főátló alatt ferdén minden elem 1, minden más 0. Egy ilyen blokk mérete legfeljebb k_i, és van pontosan k_i méretű is, annyi ilyen blokk van ahány dimenziós az α_i-hez tartozó sajátaltér. Ez az alak egyértelmű abban az értelemben, hogy akárhogy is választjuk a bázist, a Jordan-normálalak csak a blokkok permutációjában térhet el.*

Mielőtt bizonyítanánk a tételt, a bizonyításhoz felhasznált állításokat és lemmákat mondjuk ki és látjuk be.
A most következő lineáris algebrai tétel alapján megkapjuk a részmodulusokat, melyek direkt összeadandók, ezekhez az alterekhez tartozó részmodulusokban keressük azt a bázist, amiben a mátrix a kívánt alakú.

3.1.15. Lemma. *Legyen V n dimenziós vektortér, melynek $b_1, \dots, b_n$ olyan bázisa, melyre a $b_1, \dots, b_k$ által generált U altér A-invariáns. Hasonlóan $b_{k+1}, \dots, b_n$ által generált W altér is A-*

invariáns. Ekkor A mátrixa a $b_1, \dots, b_n$ bázisban a következő alakú:

$$\begin{pmatrix} A_1 & O \\ O & A_2 \end{pmatrix},$$

ahol A_1 az A mátrixa az U altérre történő megszorítással adódik, A_2 pedig W-re történő megszorítással, O pedig a csupa 0 mátrix.

Bizonyítás. Világos, hogy $V = U \oplus W$. Ekkor bármely $v \in V$-re $v = u + w$ egyértelmű felírás adódik. Tekintsük Av-t. Ekkor $Av = v' = u' + w'$, ahol u' és w' rendre U és W-beli, mivel ezek A-invariáns alterek. Ekkor A mátrixa szükségképpen a kívánt blokkdiagonális alakú. □

Tegyük fel, hogy $W = \langle m \rangle$, m rendje egy $\mathbb{K}[x]$-beli irreducibilis polinom hatványa, p^k. Mivel $\mathbb{K}$ algebrailag zárt, $\mathbb{K}[x]$ minden irreducibilis polinomja elsőfokú: $p(x) = x - \alpha$ (feltehetjük, hogy p normált). „Megkeressük" a kívánt bázist.

3.1.16. Lemma. *Legyen $m \in M(A, V)$ olyan, hogy $p^{k-1}m \neq 0$, de $p^k m = 0$ és legyen $m_1 := m, m_2 := pm, \dots,$*
$m_k := p^{k-1}m$. Ekkor $\langle m \rangle_{\mathbb{K}[x]} = \langle m_1, \dots, m_k \rangle_{\mathbb{K}}$, és $m_1, \dots, m_k$ független $\mathbb{K}$ felett.

Bizonyítás. Először lássuk be, hogy $m_1, \dots, m_k$ generátorrendszer. A bal oldal elemei fm alakúak, ahol $f \in \mathbb{K}[x]$. Mivel f egyértelműen írható $x - \alpha$ polinomjaként, vagyis $f(x) = a_0 + a_1(x - \alpha) + + \dots + a_n(x - \alpha)^n$, továbbá a 0 együtthatókat is beírva feltehető, hogy $n \geq k - 1$ (elég lesz csak k tagot kiírni), azt kapjuk, hogy:

$$fm = a_0 m + a_1(x - \alpha)m + \dots + a_n(x - \alpha)^n m = a_0 m + a_1(pm) + \dots + a_{k-1}(p^{k-1}m).$$

A függetlenség igazolásához megmutatjuk, hogy a 0 csakis triviális lineáris kombinációként áll elő. Ha

$$0 = a_0 m_1 + a_1 m_2 \dots + a_{k-1} m_k = a_0 m + a_1(pm) + \dots + a_{k-1}(p^{k-1}m) = fm,$$

akkor m rendje osztja f-et, vagyis $p^k \mid f$. Mivel p^k foka k és f foka legfeljebb $k - 1$, $f = 0$, vagyis minden $a_i = 0$. Ekkor $m_1, \dots, m_k$ tényleg független generátorrendszer. □

Hogy néz ki A mátrixa az $m_1, \dots, m_k$ bázisban? Legyen $B = A - \alpha I$, ahol I az identitás (a megfelelő méretű egységmátrix). Ekkor $p(A) = A - \alpha I = B$. Nézzük, hova viszi B az i-edik báziselemet:

$$B(m_i) = B(p^{i-1}m) = B(B^{i-1}(m)) = B^i(m) = p^i m.$$

Az m_i-edik báziselem tehát az m_{i+1}-edikbe kerül, a k-adik pedig 0-ba. B mátrixa tehát a következő alakú $k \times k$-as mátrix:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \quad \text{amiből} \quad A = B + \alpha I = \begin{pmatrix} \alpha & 0 & \dots & 0 & 0 \\ 1 & \alpha & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \alpha \end{pmatrix}$$

Így egy α-hoz tartozó $k \times k$-as Jordan-blokkot kaptunk.
Ezekből az eredményekből már összerakhatjuk a(z) 3.1.14 tétel bizonyítását:

Bizonyítás. Az alaptétel szerint $M(A,V)$ felbontható prímhatványrendű ciklikus modulusok direkt összegére. Ezek a részmodulusok pontosan az A-invariáns alterek, melyekben választhatjuk a(z) 3.1.16 lemmában megkonstruált bázist. Az invariáns alterek bázisainak egyesítésében, mint bázisban, az A mátrixa a megfelelő blokkdiagonális alakú lesz.
Tegyük fel, hogy A mátrixa a megfelelő alakú, Jordan-blokkokból álló mátrix. Ekkor a(z) 3.1.15 lemma alapján az egyes blokkok egy W, A-invariáns alteret, tehát részmodulust határoznak meg. Legyen $m_1, \ldots, m_k$ bázis W-ben. $B := A - \alpha I$, a fenti mátrixok. Ekkor $m_i = B^{i-1}(m_1)$ és $B^k(m_1) = = 0$. Ha $p(x) = (x - \alpha)$ egy $\mathbb{K}[x]$- beli polinom, akkor egyrészt $p(A) = B$, másrést $m_i = p^{i-1}m_1$, ha $i < k$ és $p^k m_1 = 0$. Ekkor a(z) 3.1.16 lemma alapján m_1 generálja W-t $\mathbb{K}[x]$ felett, melynek rendje $(x-\alpha)^k$. W tehát ciklikus, prímhatványrendű, így az alaptétel szerint a Jordan-normálalak is egyértelmű. □

A következő eljárással kiszámíthatjuk egy mátrix Jordan-normálalakját (az eljárás helyességét nem bizonyítjuk, megtalálható pl.:[3]-ben). Egy $\mathbb{K}$ test fölötti véges dimenziós V vektortér A transzformációjának a mátrixa a standard bázisban legyen adott. Tekintsük A transzponáltját, majd ebből vonjuk ki az xI-t. $A^T - xI$-t A karakterisztikus mátrixának nevezzük. Ezt fogjuk normálalakra hozni, a főátlóban megjelenő s_i polinomok, melyekre $s_1 \mid s_2 \mid \ldots \mid s_n$ teljesül, a következő tulajdonságokkal bírnak:

(*i*) Az $s_1 \ldots s_n$ az A karakterisztikus polinomja.

(*ii*) s_n az A minimálpolinomjának asszociáltja.

(*iii*) Ha mindegyik s_i polinom gyökténye zőkre bomlik $\mathbb{K}$ felett, akkor egy $\alpha_i \in T$ gyökhöz tartozó blokkok mérete $t_1, \ldots, t_n$, ahol t_i jelöli a s_i polinomban az α_i multiplicitását.

Legyen $A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$. Készítsük el A karakterisztikus mátrixát, melyet normálalakra hozunk. Az eleminációs lépések után:

$$\begin{pmatrix} 1-x & 2 & 0 \\ 0 & 1-x & 0 \\ 0 & 2 & 1-x \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & (x-1)^2 \end{pmatrix}$$

A normálalakból leolvasható a minimálpolinom és a karakterisztikuspolinom is. Az 1 kétszeres és egyszeres gyök, így A Jordan-normálalakja a következő:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

3.2. Féligegyszerű gyűrűk szerkezete

A következőkben a féligegyszerű gyűrűket vizsgáljuk. Szeretnénk az R gyűrűt mátrixok segítségével ábrázolni, ezért a féligegyszerű gyűrűk szerkezetét visszavezetjük a teljes mátrixgyűrűre. Az

R gyűrűről a továbiakban feltesszük, hogy egységelemes, azonban nem feltétlenül kommutatív, és a szóba kerülő modulusokról pedig azt, hogy unitérek. Mielőtt kimondanánk és bizonyítanánk az ide kapcsolódó struktúratételt, az eddigiekhez hasonlóan a felhasznált fogalmakat és állításokat mondjuk ki és látjuk be.

3.2.1. Definíció. Az R gyűrűt *radikálmentesnek* nevezzük, ha nincs olyan $B \neq \{0\}$ balideálja, hogy $B^n = \{0\}$ valamely $n \in \mathbb{N}$-re.

3.2.2. Definíció. Az R gyűrűt bal oldali *Artin-gyűrűnek* nevezzük, ha balideáljaira teljesül a minimumfeltétel, vagyis minden balideálokból álló csökkenő lánc stabilizálódik.

3.2.3. Definíció. Az R gyűrűt *féligegyszerűnek* nevezzük, ha radikálmentes és bal Artin-féle.

3.2.4. Tétel (Wedderburn-Artin)**.** *Legyen R tetszőleges egységelemes gyűrű, ekkor az alábbiak ekvivalensek:*

(i) A bal oldali R-modulusok minden részmodulusa direkt összeadandó.

(ii) Tekintsük R-et mint R-modulust. Ekkor R minden balideálja R-nek direkt összeadandója.

(iii) R féligegyszerű.

(iv) R véges sok ferdetest feletti mátrixgyűrű direkt összege.

(v) R mint önmaga feletti R-modulus véges sok minimális balideáljának direkt összege.

A bizonyítás megkezdése előtt a felhasznált lemmákat mondjuk ki és bizonyítjuk. Ezen állítások a Schur-lemmából és a sűrűségi tételből következnek.

3.2.5. Lemma (Schur)**.** *Legyen M egyszerű bal oldali R-modulus és $\mathbb{D} = End_R(M)$, vagyis M R-endomorfizmusainak gyűrűje, ekkor $\mathbb{D}$ ferdetest.*

Bizonyítás. Legyen M a szóban forgó egyszerű bal R-modulus és $\alpha \in \mathrm{End}_R(M)$, melyre $\alpha \neq 0$. Ekkor $\mathrm{Im}\alpha$ nem 0 és $\mathrm{Ker}\alpha$ nem az egész M. Mivel ezek részmodulusok és M egyszerű, $\mathrm{Im}\alpha = M$ és $\mathrm{Ker}\alpha = 0$, vagyis α bijekció, így létezik inverze. Könnyen láthatóan α^{-1} is R-homomorfizmus, tehát $\mathbb{D}$ test (ferdetest). □

3.2.6. Tétel (sűrűségi tétel)**.** *Legyen M egyszerű R-modulus. Tekintsük M-et mint $\mathbb{D}$ vektorteret, és legyenek ennek $u_1, \ldots, u_n$ független elemei. Tetszőleges $u'_1, \ldots, u'_n$ M-beli elemekre létezik $a \in R$, hogy $au_i = u'_i$ minden $i = 1 \ldots n$-re.*

Bizonyítás. Jelölje $l(u_1, \ldots, u_i)$ az $u_1, \ldots, u_i$ elemek bal annullátorát. Legyen $B_i = l(u_1, \ldots, u_{i-1}, u_{i+1} \ldots, u_n)$. Tekintsük a $B_i u_i$ M-beli részhalmazt. Mivel u_i független a többi u_j-től, ez nemcsak a 0-ból áll. Tetszőleges $r, s \in B_i$-re az $ru_i - su_i = (r-s)u_i \in B_i u_i$ és tetszőleges $p \in R$-re $p(ru_i) = = (pr)u_i \in B_i u_i$, hiszen B_i balideál. Látható tehát, hogy a $B_i u_i$ halmaz M-nek részmodulusa. Mivel M egyszerű, $B_i u_i = M$, vagyis létezik $a_i \in B_i$, melyre $a_i u_i = u'_i$. Ekkor viszont az $a := a_1 + + \ldots + a_n$-re $au_i = u'_i$ minden $i = 1, \ldots, n$-re. □

3.2.7. Lemma. *Legyen R bal Artin-féle. Ha M egyszerű bal R-modulus, akkor M mint $\mathbb{D}$ vektortér véges dimemnziós.*

Bizonyítás. Képezzük a $\mathbb{D}$-vektortér független $u_1, \ldots, u_n, \ldots$ elemeit, majd tekintsük a $B_i = l(u_1, \ldots, u_i)$ balideálokat. Erről látható, hogy $B_i \supset B_{i+1}$ és mivel R bal Artin, a lánc stabilizálódik. Kimutatható, hogy M mint $\mathbb{D}$-vektortér egy v eleme pontosan akkor függ az M-beli $u_1, \ldots u_n$ elemektől, ha minden $r \in R$-re az $ru_1 = 0, \ldots, ru_n = 0$ feltételeből $rv = 0$ következik (a bizonyítást lásd [2]). Esetünkben $B_{n+1} = B_n$ így az u_{n+1} már lineárisan függ az első n független elemtől. M tehát tényleg véges dimenziós. □

3.2.8. Lemma. *Ha M egyszerű bal oldali R-modulus véges dimenziós mint $\mathbb{D}$-vektortér, akkor $R/l(M) \cong End_{\mathbb{D}}(M)$.*

Bizonyítás. Tekintsük az alábbi megfeleltetést: tetszőleges $r \in R$-re legyen $\varphi_r : u \to ru$ hozzárendeléssel értelmezett függvény. Ekkor az $r \mapsto \varphi_r$ megfeleltetés egy $\Phi : R \to \mathrm{End}(M)$ gyűrűhomomorfizmust indukál. KerΦ pontosan azon R-beli elemekből áll, melyek M-et 0-ba szorozzák, ez éppen $l(M)$. $\mathrm{End}_{\mathbb{D}}(M)$ elemei $\mathbb{D}$-endomorfizmusok, ha $\alpha \in \mathbb{D}$, akkor $\varphi(\alpha m) = \alpha\varphi(m)$, itt α egy R-beli elemmel való szorzás. A homomorfizmustétel miatt $\mathrm{Im}\Phi \cong R/l(M)$, és mivel a 3.2.6 tétel biztosítja, hogy Φ szürjektív, így $R/l(M) \cong \mathrm{End}_{\mathbb{D}}(M)$ teljesül. □

3.2.9. Lemma. *Ha M n dimenziós $\mathbb{D}$-vektortér, akkor $End_{\mathbb{D}}(M) \cong \mathbb{D}^{n\times n}$.*

Bizonyítás. Legyen M egy bázisa $u_1, \ldots, u_n$ és $\alpha \in \mathrm{End}_{\mathbb{D}}(M)$. Rendeljünk α-hoz egy A mátrixot. Ha $\alpha u_i = a_{1,i}u_i + \ldots + a_{n,i}u_n$, akkor legyen $A = (a_{i,j})$. Endomorfizmusok összege a mátrixok összege, szorzatuk pedig $\gamma = \alpha\beta$ endomorfizmusok esetén egyszerű számolással megmutatható, hogy $C = BA$ (sor-oszlop szorzás helyett, oszlop-sor szorzás szerepel). Kaptunk tehát egy „duális" izomorfizmust a teljes mátrixgyűrűvel. □

3.2.10. Lemma. *Test fölötti teljes mátrixgyűrű egyszerű.*

Bizonyítás. Tekintsünk egy $A \neq 0$ mátrix által generált ideált. Megmutatjuk, hogy ez tartalmazza az egységmátrixot, így csak az egész gyűrű lehet. Mivel A nem a nullmátrix, van egy nem 0 eleme. Ekkor alkalmas mátrixokkal balról és jobbról szorozva elérhető, hogy ez az elem a főátló egyik helyére kerüljön, és minden más elem 0 legyen. Ennek az elemnek az inverzével szorozva ezen a helyen 1 fog szerepelni. Hasonlóan átvisszük az elemet a többi kívánt helyre, normálunk, így olyan mátrixokat kapunk, melyek egy eleme 1 a többi pedig 0. Ezek összege a kívánt alakú, tehát az A által generált ideál tartalmazza az egységmátrixot, így az ideál az egész gyűrű. □

A szükséges lemmákat ismertettük, így elkezdhetjük a *Wedderburn-Artin-tétel* bizonyítását:

Bizonyítás. $(i) \Rightarrow (ii)$ R egységelemes, és mivel önmaga feletti bal R-modulus, ezért unitér. E tulajdonságok miatt a részmodulusoknak megfelelő balideálok direkt összeadandók R-ben.
$(ii) \Rightarrow (iii)$ Belátjuk, hogy R radikálmentes és minimumfeltételes a balideálokra. Ha e az R egységeleme, akkor a feltevés szerinti direkt összegre való bontásból ($R = B \oplus C$, ahol $B \neq \{0\}$ balideál) $e = f + g$ adódik. Ekkor bármely $r \in R$ esetén $re = rf + rg$. Meg szeretnénk mutatni, hogy

B nem nilpotens. Ha $r \in B$, akkor a direkt összeg tulajdonságai miatt $r = rf$ és $rg = 0$. Az f tehát B jobbegységeleme és $B \subseteq B^2 \neq \{0\}$, így B nem nilpotens. Mivel minden balideál direkt összeadandó, és mint láttuk nem nilpotensek, R radikálmentes.
Legyen B és C olyan balideáljai R-nek, hogy $C \subseteq B$ teljesül. Megmutatjuk, hogy C-nek létezik olyan D komplementuma B-ben, melyre $B = C \oplus D$. A fentiek alapján létezik C-nek jobbegységeleme, legyen ez g, D pedig álljon B azon b elemeiből, melyre $bg = 0$ (D nyilván nem üres hiszen például $0 \in D$). Könnyen látható, hogy D balideál és tetszőleges $b \in B$-re $b = (b - bg) + bg$ és $(b - bg)g = 0$, így $(b - bg) \in D$. Ha $x \in C \cap D$, akkor egyrészt $xg = x$, másrészt $xg = 0$, tehát a két balideál diszjunkt és mivel generálják B-t, $B = C \oplus D$.

Tekintsünk most egy $R = B_0 \supseteq B_1 \supseteq \ldots$ balideálokból álló csökkenő láncot. Az előzőek alapján minden $B_{i-1} = B_i \oplus C_i$, alkalmas C_i-vel. Legyen $C = \langle C_i : i = 1, \ldots \rangle$. Ekkor $R = C \oplus C_0$, alkalmas C_0-val. Megmutatjuk, hogy azon felül, hogy a C_i-k generálják R-et, direkt összeadandók is, tehát minden C_i metszete a többi generátumával csak a 0-ból áll. Ez azt jelenti, hogy $c_1 + \ldots + c_n = 0$-ból $c_i = 0$ következik minden $i = 1, \ldots, n$-re (a 0 indexet elhagyhatjuk, hiszen az összegben szereplő c_0 0-val egyenlő, C_0 definíciója miatt). Ez viszont teljesül, hiszen $B_{i-1} = B_i \oplus C_i$ és $C_j \subseteq B_i$ minden $j \geq i$-re. Ekkor $R = C_1 \oplus \ldots \oplus C_n$. Ha e az R egységeleme, akkor természetesen e eleme a direkt összegnek is, továbbá ha e_i jelöli e C_i-be eső részét, akkor e_i szintén eleme a direkt összegnek. Minden $i > n$-re $e_i = 0$, így $C_i = \{0\}$, tehát az $R = B_0 \supseteq B_1 \supseteq \ldots$ lánc stabilizálódik. Ekkor R bal Artin-féle (is), vagyis féligegyszerű.
$(iii) \Rightarrow (iv)$ Legyen R féligegyszerű, ekkor létezik egy B minimális balideálja. Mivel $BB \neq \{0\}$, így B sem triviális. Ekkor $l(B)$ és $r(l(B))$ ideálok, melyek metszete nilpotens. R féligegyszerű, így a metszet csak 0 lehet. Tekintsük a $\varphi : R \to R/l(B)$ természetes homomorfizmust. Mivel $l(B)$ és $r(l(B))$ diszjunktak φ az $r(l(B))$-t injektíven képezi le a faktorgyűrű egy nem triviális ideáljára. A 3.2.8 lemma szerint ez a faktorgyűrű egyszerű, így $\varphi(r(l(B)))$ csakis az egész lehet. Ebből következik, hogy $R = l(B) \oplus r(l(B))$. Az $r(l(B))$ viszont izomorf egy test feletti teljes mátrixgyűrűvel. Konstruáljunk R-ben egy ideálokból álló csökkenő láncot úgy, hogy $R = R_0 \supset R_1 \supset \ldots \supset R_n$ teljesüljön és mindegyik R_i direkt összeadandó legyen. Megmutatható, hogy R féligegyszerűségéből következik, hogy a direkt összeadandók is féligegyszerűek. Ekkor tehát $R_n = R_{n+1} \oplus S_{n+1}$, ahol S_{n+1} már izomorf egy test feletti teljes mátrixgyűrűvel. A minimumfeltétel miatt indukcióval kapjuk, hogy $R = S_1 \oplus \ldots \oplus S_k$ a kívánt felbontás.
$(iv) \Rightarrow (v)$ A mátrixgyűrűben azok a mátrixok, melyek valamely oszlopán kívül csupa 0-ból állnak egy minimális balideált alkotnak, ezek direkt összege kiadja az egész gyűrűt. Ebből már következik, hogy R minimális balideáljainak direkt összege.
$(v) \Rightarrow (i)$ Legyen $R = B_1 \oplus \ldots \oplus B_n$ minimális balideálokra való felbontás és M legyen unitér bal oldali R-modulus. Legyen $N \leq M$ és K olyan maximális részmodulusa M-nek, melyre $N \cap K = \{0\}$ (a Zorn-lemma biztosítja, hogy ilyen létezik). Megmutatjuk, hogy $M = N \oplus K$. Először belátjuk, hogy M minden eleme benne van véges sok minimális részmodulus generátumában. Ha $0 \neq m \in M$, akkor tekintsük a $B_i m = \{rm : r \in B_i\}$ részmodulust. Mivel M unitér, m eleme a $B_1 m, \ldots, B_n m$ részmodulusok generátumának. Ha $n = rm$ a $B_i m$ egy tetszőleges nem nulla eleme, akkor $Rn = Rrm = B_i m$, vagyis $B_i m$ minimális részmodulus. Ezek után megmutatjuk, hogy $N \oplus K$ tartalmaz minden minimális részmodulust. Legyen ugyanis $N' \leq M$ minimális, és tegyük

fel, hogy $N' \not\subseteq K$. Tekintsük az $\langle N', K\rangle \cap N$ halmazt. Mivel K maximális, a metszet tartalmaz egy $t \neq 0$ elemet. $t \in \langle N', K\rangle$, így $t = n' + k$ és $t \in N$ is teljesül. Mivel N és K diszjunktak és $t \neq 0$, kapjuk, hogy $n' \neq 0$, így $n' = t - k \in N \oplus K$. $Rn' = N'$ mivel N' minimális és eleme a generátumnak. Ezzel beláttuk, hogy az M unitér modulus minden részmodulusa direkt összeadandó, így a ciklikus bizonyítással pedig bebizonyítottuk, hogy a tétel állításai ekvivalensek. □

3.2.1. A Jacobson-radikál

A következőkben egy tetszőleges, egységelemes R gyűrű *Jacobson-radikálját* és annak tulajdonságait vizsgáljuk. Megmutatjuk, hogy *Artin-gyűrű* esetén, hogy kapcsolódik a féligegyszerűség-hez, hasonlóan a szerinte vett faktor milyen tulajdonságokkal rendelkezik.

3.2.11. Definíció. Legyen R tetszőleges egységelemes gyűrű. Azon $a \in R$ elemek halmazát, melyekre bármely $r \in R$ esetén az $1 - ra$ invertálható, az R gyűrű *Jacobson-radikáljának* nevezzük, jele: $J(R)$.

Legyen $r \in R$ nilpotens, vagyis $r^n = 0$ valamely $n \in \mathbb{N}$-re. Megmutatjuk, hogy $1-r$ invertálható: $1 = 1 - r^n = (1 - r)(1 + r + \ldots + r^{n-1})$.

3.2.12. Lemma. *Legyen B olyan balideálja R-nek, melynek minden eleme nilpotens. Ekkor $B \subseteq$ $\subseteq J(R)$.*

Bizonyítás. Ha $b \in B$, akkor $rb \in B$ tetszőleges $r \in R$-re hiszen B balideál, így rb is nilpotens. A fentiek alapján $1 - rb$ invertálható, így $B \subseteq J(R)$. □

3.2.13. Tétel. *$J(R)$ az R maximális balideáljainak a metszete, és kétoldali ideál R-ben.*

Bizonyítás. Legyen M az R-nek egy tetszőleges maximális balideálja, $r \in J(R)$ és tegyük fel, hogy $r \notin M$. Legyen $m \in M$ és tekintsük az $m + ar$ alakú elemeket, ahol $a \in R$. Ezek egy balideált alkotnak, mely tartalmazza M-et és r-t. Mivel M maximális ez az ideál csak az egész R lehet, így tartalmazza 1-et is. Ezek alapján $1 = m + ar$, amiből $m = 1 - ar$, és mivel $r \in J(R)$, az $1 - ar$-nek létezik egy s balinverze. $1 = s(1 - ar) = sm$. Ez azt jelenti, hogy $1 \in M$, így $M = R$, ami viszont ellentmondás. Ebből következik, hogy $J(R) \subseteq M$ minden maximális balideálra.

Legyen most $r \in R$ olyan, amely része minden maximális balideálnak. Meg kell mutatnunk, hogy $1 - r$ invertálható (igazából azt kell megmutatni, hogy $1 - ar$ invertálható minden $a \in R$-re, de mivel r benne van minden maximális balideálban, ar is benne van). A bizonyításhoz felhasználjuk *Krull-tételét*, mely szerint egységelemes gyűrűben minden ideál benne van egy maximális ideálban (esetünkben balideálokat tekintünk). Tegyük fel indirekt, hogy az $1 - r$ elemnek nincs balinverze, tehát $1 \notin R(1 - r)$, így ez nem az egész R. Az eddig elmondottak szerint $R(1 - r) \subseteq M$, ahol M maximális. Mivel $r \in M$ és $1 - r \in R(1 - r) \subseteq M$, $1 - r + r = 1 \in M$, ami azt jelenti, hogy $M = R$, ez viszont ellentmondás. $1 - r$-nek létezik tehát egy s balinverze. Azt kapjuk tehát, hogy $1 - s = -sr$, amit minden maximális balideál tartalmaz. Ekkor az $1 - (1 - s) = s$-nek létezik egy t balinverze. Az s-nek az $1 - r$ jobbinverze és a bal-, jobbinverz egyenlőségéből következik $t = 1 - r$ kétoldali inverze s-nek, tehát s jobbinverze is $1 - r$-nek. Megmutattuk tehát, hogy egy r elemre,

mely benne van minden maximális balideálban, az $1-r$ invertálható, így $r \in J(R)$. Ezzel azt kaptuk, hogy $J(R) = \bigcap M$. Ez azt is jelenti, hogy $J(R)$ balideál. □

Még szükséges belátnunk, hogy $J(R)$ jobbideál is.

Tekintsük az alábbi B halmazt. Legyen M maximális balideálja az R gyűrűnek, $b \in R$ és $B := \{r \in R : rb \in M\}$.

3.2.14. Lemma. *Ha $b \notin M$, akkor B maximális balideálja az R gyűrűnek.*

Bizonyítás. M balideál, ezért B is az. Legyen $K = {}_RR/_RM$. A faktormodulus részmodulusainak egyértelműen megfeleltethetők az M-et tartalmazó R-beli balideálok. Mivel M maximális K egyszerű. Legyen K egy eleme $b+M$. Mivel $b \notin M$, $b+M \neq 0$. A B-beli elemek viszont annullálják $b+M$-et, hiszen minden B-beli elem M-be szorozza b-t. Legyen $\varphi : {}_RR \to K$ modulushomomorfizmus, melyre $\varphi(s) = s(b+M)$. Ennek magja B és szürjektív, hiszen K egyszerű és az 1 nem a 0-ba megy ($1 \notin B$). A homomorfizmus tétel alapján $K \cong_R R/_RB$, amiből következik, hogy ${}_RR/_RB$ is egyszerű, vagyis B maximális balideál. □

3.2.15. Tétel. *Legyen R (egységelemes) gyűrű. Ekkor $J(R)$ az egyszerű R-modulusok annullátorainak metszete.*

Bizonyítás. Legyen K egyszerű R-modulus, $0 \neq k \in K$. Az előző lemma alapján tudjuk, hogy k annullátora R-nek maximális balideálja. Ha $r \in J(R)$, akkor $r \in B$ (a fentiekben definiált B) is teljesül, így $J(R)$ benne van K annullátorában. A másik irány bizonyításához $r \in R$ legyen olyan, ami minden egyszerű R-modulust annullál. Legyen M maximális balideál R-ben és $K = {}_RR/_RM$ egyszerű modulus. Ennek $1+M$ eleme, melyre $r(1+M) = 0$ amiből $r \in M$ következik. Látjuk tehát, hogy az annulláló elem benne van minden M maximális balideálban, így $J(R)$-ben is. □

Mivel egy modulus annulátora kétoldali ideál, és ezek metszete is szintén kétoldali ideál, ami éppen $J(R)$-rel egyezik meg, azt kaptuk, hogy $J(R)$ tényleg kétoldali ideálja R-nek. Ezzel a 3.2.13 tétel bizonyítását befejeztük.
Megmutatjuk a *Jacobson-radikál* és a féligegyszerűség közti szoros kapcsolatot:

3.2.16. Tétel. *Legyen R (egységelemes) Artin-gyűrű. Ekkor:*

(i) R pontosan akkor féligegyszerű, ha $J(R) = \{0\}$.

(ii) $R/J(R)$ ferdetest feletti teljes mátrixgyűrűk direkt szorzata.

Bizonyítás. (i) Legyen $J(R) = \{0\}$ és B R-nek egy nilpotens ideálja. Ekkor $B^n = \{0\} \subseteq J(R)$, ezért a 3.2.12 lemma alapján $B \subseteq J(R)$, így $B = \{0\}$, R tehát radikálmentes és így féligegyszerű. Legyen R féligegyszerű, ekkor a 3.2.4 tétel alapján R minimális ideáljainak a direkt összege. Tekintsük az ${}_RR_i$ egyszerű modulust (R_i a direkt összeg egy tagja), melyet minden R_j annullál. Ezek metszete a direkt összeg tulajdonsága miatt $\{0\}$. A 3.2.15 tétel miatt $J(R) = \{0\}$.
(ii) Soroljuk fel az egyszerű R-modulusokat. Legyenek ezek M_i-k ($i \in I$ indexhalmaz). Jelölje l_i az M_i annullátorát. A 3.2.8 és 3.2.9 lemmákban beláttuk, hogy R/l_i izomorf egy alkalmas ferdetest feletti teljes mátrixgyűrűvel. Készítsük el az R/l_i gyűrűk direkt szorzatát. Legyen $\varphi : R \to \prod R/l_i$,

amelyre $\varphi(r) = (\ldots, r + l_i, \ldots)$. Ker$\varphi$ azon R-beli elemekből áll, melyek benne vannak minden l_i-ben. Ez pont $J(R)$. Ekkor a homomorfizmustétel alapján $R/J(R) \cong S \leq \prod R/l_i$. A *Jacobson-radikál* szerinti faktor tehát egy szubdirekt szorzat. Az, hogy véges sok tényezős szubdirekt szorzatot kaptunk, abból következik, hogy az l_i ideálok véges metszeteinek halmazában is van minimális. A dolgozat függelékében megmutatjuk, hogy így igazából egy direkt szorzatról beszélhetünk. □

3.2.2. A véges csoportok reprezentációjának kiindulópontja

Legyen R algebra egy $\mathbb{K}$ test felett, V pedig egy $\mathbb{K}$-vektortér. Ekkor R egy reprezentációján egy $\Phi : R \to \mathrm{End}_{\mathbb{K}}(V)$ homomorfizmust értünk. Egy $r \in R$-nek egy φ_r transzformáció felel meg, hasonlóan a 3.2.8 lemma bizonyításában elmondottakhoz. Könnyen láthatóan V R-modulussá válik a következő művelettel: bármely $v \in V$-re $rv := \varphi_r(v)$.
Ha G véges csoport, melynek rendje n, és $R = \mathbb{K}[G]$ a G-hez tartozó csoportalgebra, akkor a reprezentáció a következő tulajdonságokkal rendelkezik: $\varphi_1 = E$, ahol E a vektortér identikus leképezése, $\varphi_{g_1 g_2} = \varphi_{g_1}\varphi_{g_2}$. Ezekből következően bármely φ_g transzformáció invertálható. Mivel a vektortér $\mathbb{K}[G]$-modulussá válik a $(k_1 g_1 + \ldots + k_n g_n)v := k_1(g_1 v) + \ldots + k_n(g_n v)$ művelettel, definiálhatjuk G egy hatását a vektortéren. Bizonyos feltételek mellett, Maschke tétele alapján, a csoportalgebra előáll véges sok teljes mátrixgyűrű direkt összegeként, így G elemeit mátrixok segítségével is „ábrázolhatjuk". Eljutunk tehát egy $G \to \mathrm{GL}(n, \mathbb{K})$ reprezentációhoz, melynek egy ilyen $\mathbb{K}[G]$ modulus felel meg. Ezek vizsgálata a véges csoportok reprezentációelméletének fontos tárgyát képezik.

3.2.17. Tétel (Maschke)**.** *A $\mathbb{K}[G]$ csoportalgebra pontosan akkor féligegyszerű gyűrű, ha $\mathbb{K}$ karakterisztikája nem osztója a csoport rendjének.*

Bizonyítás. A szükségesség igazolásához tegyük fel, hogy a $\mathbb{K}$ karakterisztikája, p, osztója G rendjének, n-nek. Legyen $h = \sum_{g_i \in G} g_i$. Könnyen láthatóan $h^2 = nh$, ami a feltétel miatt 0. Továbbá $h \in Z(\mathbb{K}[G])$, így a h által generált ideál nilpotens. A 3.2.12 lemma alapján része a Jacobson-radikálnak, ami így nem triviális. Ekkor a 3.2.16 tétel alapján a csoportalgebra nem lehet féligegyszerű.
Az elégségesség igazolásához a 3.2.4 tétel miatt elég azt belátni, hogy $\mathbb{K}[G]$ minden balideálja direkt összeadandó. Legyen I balideálja a csoportalgebrának, mivel $\mathbb{K}[G]$ vektortér $\mathbb{K}$ felett, I altér (a csoportalgebra, mint önmaga feletti $\mathbb{K}[G]$-modulus esetén pedig részmodulus), ezért egy alkalmas W altérrel (például I merőleges kiegészítő alterével) $\mathbb{K}[G] = I \oplus W$ alakban írható. Legyen π_I az I irányába történő projekció, vagyis $\pi_I(g) = i$ és Ker$\pi_I = W$, ahol $g \in \mathbb{K}[G]$ és $i \in I$. Tekintsük az alábbi leképezést: $P : \mathbb{K}[G] \to \mathbb{K}[G]$, ahol

$$P(h) = \frac{1}{n} \sum_{g \in G} g\pi_I(g^{-1}h) \quad h \in \mathbb{K}[G]$$

Mivel G rendje egység $\mathbb{K}$-ban, a definíció értelmes. Megmutatjuk, hogy Im$P \subseteq I$. Ha $h \in \mathbb{K}[G]$ és $g \in G$, akkor egyrészt $\pi_I(g^{-1}h) \in I$, másrészt $g\pi_I(g^{-1}h) \in I$, mivel I balideál. Ekkor tehát $P(h) \in I$ is teljesül. P fixen hagyja I elemeit, ugyanis, ha $i \in I$, akkor I balideál tulajdonságát kishasználva, $g^{-1}i \in I$, melyből $\pi_I(g^{-1}i) = g^{-1}i$, ekkor viszont $g\pi_I(g^{-1}i) = i$. P definícióját

felhasználva kapjuk, hogy $P(i) = i$. A kettő együtt mutatja, hogy $\mathrm{Im}P = I$. Megmutatjuk, hogy P $\mathbb{K}[G]$-homomorfizmus, vagyis $P(gh) = gP(h)$. Ezt elég megmutatni tetszőleges $g \in G$-re, hiszen G elemei a csoportalgebra bázisát alkotják.

$$gP(h) = \frac{1}{n}\sum_{x\in G} gx\pi_I(x^{-1}h) = \frac{1}{n}\sum_{x\in G} gx\pi_I(x^{-1}g^{-1}gh) = \frac{1}{n}\sum_{y=gx\in G} y\pi_I(y^{-1}gh) = P(gh)$$

Ebből következően $\mathrm{Ker}P$ részmodulus. Bármely $h \in \mathbb{K}[G]$ esetén $h = P(h) + (h - P(h))$. Könnyen láthatóan $(h - P(h)) \in \mathrm{Ker}P$, amiből könnyen láthatóan I direkt kiegészítője $\mathrm{Ker}P$, az I balideál tehát direkt összeadandó. □

Függelék

Az első fejezetben már láttuk, hogy hogy realizálódnak műveleti nevek az azonos típusú algebrák direkt szorzatában. A Függelékben definiáljuk a szubdirekt szorzatot, megvizsgáljuk, hogy milyen feltételek mellett lesznek egyes algebrák szubdirekt irreducibilisek, és ismertetjük Birkhoff ide kapcsolódó tételét. Továbbá megmutajuk, hogy az olyan algebrák osztályában, melyeknek bármely két kongruenciája felcserélhető, bizonyos feltételek mellett a szubdirekt szorzat direkt szorzatként is előáll.

4.1. Definíció. Legyenek $\mathbf{A}$ és $\mathbf{B}$ τ típusú algebrák. A $\varphi : A \to B$ leképezést homomorfizmusnak nevezzük $\mathbf{A}$ és $\mathbf{B}$ között, ha bármely n-változós τ típusú f műveletre és bármely A-beli $a_1, a_2, \ldots, a_n$ elemekre:

$$\varphi(f_{\mathbf{A}}(a_1, a_2, \ldots, a_n)) = f_{\mathbf{B}}(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n))$$

Egy csoporthomomorfizmus magja, az egységelem teljes inverz képe, normálosztó. A modulushomomorfizmusok magjai pedig pontosan a részmodulusok. Mi lesz ebben az esetben φ magja? Most nem csak egy elem teljes inverz képét kell megadnunk, hanem az összes elemét. Tehát szükségünk lesz egy ekvivalenciarelációra, aminek az osztályai az $\mathbf{A}$ algebra egy partícióját fogják adni.

4.2. Definíció. Legyen $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfizmus, ekkor Kerφ az alábbi reláció által definiált partíciók halmaza: $(a, b) \in A^2$-re $(a, b) \in \text{Ker}\varphi \Leftrightarrow \varphi(a) = \varphi(b)$.

Az összes $\mathbf{A}$-beli ekvivalenciareláció halmazát Eq(A)-val jelöljük.

4.3. Definíció. Legyen $\Theta \in \text{Eq}(A)$. Ekkor Θ-t *kongruenciának* nevezzük, ha kompatibilis $\mathbf{A}$ műveleteivel, vagyis bármely n változós $\mathbf{A}$-beli f műveletre és $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ A-beli elemekre, ha:

$$a_1 \Theta b_1, a_2 \Theta b_2, \ldots, a_n \Theta b_n, \text{ akkor } f_{\mathbf{A}}(a_1, a_2, \ldots, a_n) \Theta f_{\mathbf{A}}(b_1, b_2, \ldots, b_n)$$

$\mathbf{A}$ kongruenciahálóját Con$(\mathbf{A})$-val jelöljük. Nem nehéz látni, hogy Con$(\mathbf{A})$ elemei pontosan az $\mathbf{A}$-n értelmezett homomorfizmusok magjai. Egy Θ kongruencia szerinti faktoralgebra elemeit a/Θ jelöli, ez a Θ partíciónak az a elemet tartalmazó osztálya.

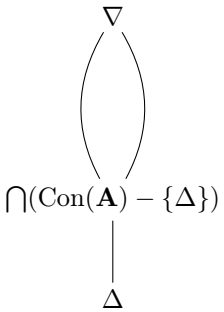
Ahhoz, hogy egy algebra szerkezetét feltárjuk, megpróbáltuk direkt szorzatra bontani addig, amíg direkt felbonthatatlan tényezőket nem kaptunk. Ez az eljárás nem alkalmazható minden típusú algebrára, egy sokkal általánosabb módszerre van szükségünk, amivel már minden algebrát elő tudunk állítani egyszerűbb építőkövekből.

4.4. Definíció. Egy $\mathbf{A}$ algebra az $\mathbf{A}_i$ $(i \in I)$ algebrák *szubdirekt szorzata*, ha $\mathbf{A} \leq \prod_{i\in I} \mathbf{A}_i$ és $\pi_i(\mathbf{A}) = \mathbf{A}_i$ minden $i \in I$-re. Egy $\varphi : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$ injektív leképezés *szubdirekt beágyazás*, ha $\varphi(\mathbf{A})$ az $\mathbf{A}_i$ algebrák szubdirekt szorzata.

4.5. Definíció. Egy $\mathbf{A}$ algebra *szubdirekt irreducibilis*, ha minden $\varphi : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$ szubdirekt beágyazásra létezik $i \in I$, melyre a $\pi_i \circ \varphi : \mathbf{A} \to \mathbf{A}_i$ izomorfizmus.

Tekintsük például a $\mathbb{Z}_4^+ \times \mathbb{Z}_4^+$ algebra átlóját, azon (a, a) alakú elemeket, ahol $a \in \mathbb{Z}_4^+$. Jelölje ezt $\mathbf{D}$. Könnyen láthatóan ez szubdirekt szorzata $\mathbb{Z}_4^+$ két példányának. Viszont a felbontás triviális, hiszen minden φ beágyazásra például $\pi_1 \circ \varphi$ izomorfizmus $\mathbf{D}$ és $\mathbb{Z}_4^+$ között.

4.6. Tétel. *Egy $\boldsymbol{A}$ algebra pontosan akkor szubdirekt irreducibilis, ha triviális, vagy $Con(\boldsymbol{A}) - \{\Delta\}$ tartalmaz legkisebb elemet, ahol Δ jelöli a triviális, „diagonális" relációt (az ábrán található ∇ jelöli azt a relációt, amely minden elemet tartalmaz).*



A bizonyításhoz használjuk az alábbi lemmát.

4.7. Lemma. *Ha Θ_i az $\boldsymbol{A}$ algebra olyan kongruenciái, melyek metszete Δ, akkor a $\varphi : \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{A}/\Theta_i$, $\varphi(a)_i = a/\Theta_i$ által definiált természetes homomorfizmus szubdirekt beágyazás.*

Bizonyítás. Legyen $\varphi_i : \mathbf{A} \to \mathbf{A}/\Theta_i$ a természetes homomorfizmus, ekkor ennek a magja éppen Θ_i, φ pedig ezen φ_i-kből „áll". A magok metszete Δ, így φ injektív, és mivel a természetes homomorfizmus szürjektív, φ szubdirekt is. □

Bizonyítás. A szükségességhez tegyük fel, hogy $\mathbf{A}$ kongruenciahálója nem tartalmaz Δ fölött legkisebb elemet. Legyen $I = \mathbf{A} - \{\Delta\}$. Ekkor a $\varphi : \mathbf{A} \to \prod_{\Theta\in I} \mathbf{A}/\Theta$ a 4.7 lemma alapján egy szubdirekt beágyazás, és mivel $\Theta \in I$-re az $\mathbf{A} \to \mathbf{A}/\Theta$ nem injektív, $\mathbf{A}$ szubdirekt felbontható.
Az elégségességhez tegyük fel, hogy $\Theta = \bigcap(\mathrm{Con}\mathbf{A} - \{\Delta\}) \neq \Delta$ és legyen $a \neq b$ olyan, amire $(a, b) \in \Theta$. Ha $\varphi : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$ egy szubdirekt beágyazás, akkor valamely $i \in I$-re, $\varphi(a)_i \neq \varphi(b)_i$, ekkor viszont $(\pi_i \circ \varphi)(a) \neq (\pi_i \circ \varphi)(b)$, amiből következően $(a, b) \notin \mathrm{Ker}(\pi_i \circ \varphi)$. Ez azt jelenti, hogy $\Theta \not\subseteq \mathrm{Ker}(\pi_i \circ \varphi)$. Mivel Θ a Δ-n kívüli, összes kongruencia metszete, és nem része $\pi_i \circ \varphi$ magjának, a mag csak Δ lehet, ami azt jelenti, hogy a $\pi_i \circ \varphi : \mathbf{A} \to \mathbf{A}_i$ hozzárendelés izomorfizmus, így $\mathbf{A}$ szubdirekt irreducibilis. □

A 2. fejezetben említettük, hogy az egyszerű csoportok, vagy például tetszőleges p prímre a p^n rendű ciklikus csopotok direkt felbonthatatlanok. Ezek a csoportok szubdirekt felbonthatatlanok is.

4.8. Tétel (Birkhoff)**.** *Minden algebra izomorf szubdirekt irreducibilis algebrák szubdirekt szorzatával. A tényezők az algebra homomorf képei.*

Bizonyítás. Feltehetjük, hogy az $\mathbf{A}$ algebra nem triviális. Legyenek a, b különböző $\mathbf{A}$-beli elemek. A Zorn-lemma alapján létezik olyan maximális $\Theta_{a,b}$ kongruencia $\mathbf{A}$-n, melyre $(a,b) \notin \Theta_{a,b}$. Jelölje η azt a legkisebb kongruenciát, mely szerint a és b egy ekvivalenciaosztályba esnek. Ekkor az $\eta \vee$ $\vee \Theta_{a,b}$ a legkisebb kongruencia $[\Theta_{a,b} \vee \nabla] - \{\Theta_{a,b}\}$-ben (Con$\mathbf{A}$ részhálójában). Fel fogjuk használni azt az állítást, bizonyítását lásd pl.:[12]-ben, hogy egy tetszőleges ρ kongruenciára a $[\rho, \nabla_{\mathbf{A}}]$ részháló izomorf $\mathrm{Con}(\mathbf{A}/\rho)$-val. Mivel a $[\Theta_{a,b} \vee \nabla] - \{\Theta_{a,b}\}$-nek van legkisebb eleme, a vele izomorf kongruenciahálónak is van, ezért a 4.6 tétel alapján, $\mathbf{A}/\Theta_{a,b}$ szubdirekt irreducibilis. Az ilyen $\Theta_{a,b}$ kongruenciák metszete Δ, hiszen minden (a,b) pár kimarad valamelyikből, így a beágyazásról szóló 4.7 lemma alapján $\mathbf{A}$ beágyazható szubdirekt irreducibilis $(\mathbf{A}/\Theta_{a,b})$ algebrák szorzatába. □

A 3. fejezetben láttuk, hogy egy R gyűrű Jacobson-radikál szerinti faktora véges sok teljes mátrixgyűrű szubdirekt szorzata. Megmutatjuk, hogy Malcev-varietásban ez direkt szorzatot jelent. Emlékeztetünk rá, hogy *varietásnak* neveztük azonos típusú algebrák azon osztályát, mely azonosságokkal definiálható.

4.9. Definíció. Egy $\mathcal{V}$ varietás *Malcev-varietás*, ha minden algebrájának bármely két kongruenciája felcserélhető.

Malcev tétele szerint ez azzal ekvivalens, hogy a varietásnak van Malcev-kifejezése. Ez egy olyan $p(x,y,z)$ kifejezés, amire a varietás minden elemére:

$$\mathbf{A} \models p(x,x,y) \approx y \text{ és } \mathbf{A} \models p(x,y,y) \approx x$$

Egy R gyűrűre ilyen az $x - y + z$, tehát a gyűrűk varietása Malcev.

4.10. Tétel. *Ha $\boldsymbol{A}$ algebra egy Malcev-varietásban, mely előáll véges sok egyszerű algebra szubdirekt szorzataként, akkor izomorf a tényezők közül néhány direkt szorzatával.*

Bizonyítás. A bizonyítás során fel fogjuk használni, hogy, ha egy Malcev-varietásban az $\mathbf{A}$ algebra $\mathbf{B}$ és $\mathbf{C}$ algebrák szubdirekt szorzata, akkor van olyan $\mathbf{B}$-beli Θ és $\mathbf{C}$-beli ρ kongruencia, és $\varphi : \mathbf{B}/\Theta \to \mathbf{C}/\rho$ izomorfizmus, hogy $\mathbf{A}$ minden eleme olyan (b,c) párokból áll, melyekre $\varphi(b/\Theta) =$ $= c/\rho$.
Tegyük fel, hogy az $\mathbf{A}$ algebra a $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_n$ egyszerű algebrák szubdirekt szorzata. A bizonyítást indukcióval végezzük. Egy tényező esetén $\mathbf{A}$ izomorf az egyetlen tényezővel. Tegyük fel, hogy $n-1$-re már igaz az állítás. Ekkor, ha $\mathbf{A}$-t az első $n-1$ komponensére vetítjük, akkor az így nyert $\mathbf{B}$ algebra szubdirekt szorzata lesz ennek az első $n-1$ tényezőnek, és így az indukciós feltétel miatt ezek közül néhány direkt szorzatával fog megegyezni. Azt kapjuk, hogy $\mathbf{A} \leq \mathbf{B} \times \mathbf{C}_n$. Mivel $\mathbf{C}_n$ egyszerű, kongruenciái csak a Δ és ∇. A fentiek szerint van olyan Θ kongruenciája $\mathbf{B}$-nek, amire $\mathbf{B}/\Theta \cong \mathbf{C}/\nabla$, így azt kapjuk, hogy $\mathbf{B}/\Theta$ szintén egyelemű, vagyis $\mathbf{A} = \mathbf{B} \times \mathbf{C}_n$. Ha $\mathbf{C}/\Delta$-hoz keresünk $\mathbf{B}$-nek megfelelő Θ kongruenciáját, akkor viszont az első projekció izomorfizmus lesz $\mathbf{A}$ és $\mathbf{B}$ között, hiszen bármely $b \in$ B-re pontosan egy olyan $c \in \mathbf{C}_n$ elem van, amire $(b,c) \in \mathbf{A}$. □

Irodalomjegyzék

[1] Fried Ervin: *Algebra I. - Elemi és lineáris algebra*, Nemzeti Tankönyvkiadó, 2000

[2] Fried Ervin: *Algebra II. - Algebrai struktúrák*, Nemzeti Tankönyvkiadó, 2002

[3] Kiss Emil: *Bevezetés az algebrába*, Typotex, 2007

[4] Kiss Emil: *Bevezetés az algebrába: A gyakorlatok és feladatok megoldásai*, Typotex, 2007

[5] Freud Róbert: *Lineáris algebra*, ELTE Eötvös Kiadó, 2007

[6] I. R. Safarevics: *Algebra: Az algebra alapfogalmai*, Typotex, 2000

[7] Joseph J. Rotman: *An Introduction to the Theory of Groups*, Springer, 1995

[8] Thomas W. Hungerford: *Algebra*, Springer, 2003

[9] Fuchs László: *Infinite Abelian groups I.*, Academic Press, 1970

[10] Daniel Miller: *The Structure of Divisibel Abelian Groups*, arXiv:1010.5836 [math.GR], 2010

[11] Joseph J. Rotman: *Advanced Modern Algebra*, Prentice Hall, 2003

[12] Stanley Burris, H. P. Sankappanavar: *A Course in Universal Algebra*, szabadon letölthető: http://www.math.sc.edu/ mcnulty/alglatvar/burrissanka.pdf 2012