12. Modulusok, féligegyszerű gyűrűk

Az alábbiakban többek közt az R egységelemes gyűrű feletti unitális baloldali modulusokkal fogunk foglalkozni. Ezek kategóriáját ${}_R\mathcal{M}$ jelöli. A morfizmusok szorzatát a kategóriáknál használt módon fogjuk jelölni, tehát az $\alpha\beta$ szorzat az ʻelőször β, majd αʻ leképezés-kompozíciót jelenti.

Megjegyzés: a vektorterekre vonatkozó alapvető defincióknál és állításoknál test feletti vektortér helyett vehetünk ferdetest feletti bal- vagy jobboldali unitális modulust is, a bizonyítások – kellő óvatosság mellett – ekkor is használhatóak. (Így gyakran e modulusokat is vektortereknek hívjuk.)

12.1 Projektív modulusok

12.1.1 Definíció: ${}_RF$ szabad modulus, ha izomorf a $\bigoplus_{\alpha\in\mathbf{I}} {}_RR$ diszkrét direkt összeggel valamely $\mathbf{I}$ indexhalmazra. Más szóval akkor, ha létezik olyan $\{e_\alpha\in F \mid \alpha\in\mathbf{I}\}$ rendszer – ezt bázisnak nevezzük – , melyre $\forall x\in F\exists!\left(n\in\mathbb{N};\alpha_1,\dots,\alpha_n\in\mathbf{I};r_1,\dots,r_n\in R\setminus\{0\}\right)$: $x=\sum_{i=1}^{n} r_k e_{\alpha_k}$, azaz minden F-beli elem egyértelműen áll elő báziselemek lineáris kombinációjaként.

Speciálisan ha R test vagy ferdetest, akkor minden R feletti modulus szabad. (Minden vektortérben van bázis.)

Például $R=\mathbb{Z}$ esetén a szabad modulusok a $\bigoplus_{\alpha\in\mathbf{I}} Z_\infty$ alakú, más néven szabad Abel-csoportok.

12.1.2 Definíció: $P\in{}_R\mathcal{M}$ projektív, ha minden

$$\begin{tikzcd} & P \arrow[d, "\varphi"] \arrow[dl, dashed, "\psi"'] & \\ A \arrow[r, "\alpha"] & B \arrow[r] & 0 \end{tikzcd}$$

diagramhoz, ahol α epimorfizmus (tehát az $A\xrightarrow{\alpha}B\longrightarrow 0$ sorozat egzakt), létezik olyan $\psi\colon P\to A$ modulus-homomorfizmus, amely kommutatívvá teszi, azaz amelyre $\alpha\psi=\varphi$.

12.1.3 Állítás: minden szabad modulus projektív.

Bizonyítás: legyen F szabad és tekintsük az alábbi diagramot:

$$\begin{tikzcd} & F \arrow[d, "\varphi"] & \\ A \arrow[r, "\vartheta"] & B \arrow[r] & 0 \end{tikzcd}$$

Jelölje az $e_\alpha\in F$ báziselem φ szerinti képét b_α. ϑ epimorfizmus, tehát $\forall\alpha\in\mathbf{I}\exists a_\alpha\in A$: $\vartheta(a_\alpha)=b_\alpha$. A kiválasztási axióma szerint tehát létezik olyan $\{a_\alpha\in A \mid \alpha\in\mathbf{I}\}$, hogy $\forall\alpha\in\mathbf{I}$: $\vartheta(a_\alpha)=b_\alpha$. Rendelje ψ e_α-hoz a_α-t. Ez egyértelműen kiterjed egy $F\to A$ homomorfizmussá: $\left(\sum_{i=1}^{n} r_i e_{\alpha(i)}\right)\psi=\sum_{i=1}^{n} r_i a_{\alpha(i)}$. Ekkor a bázisra megszorítva $\vartheta\psi=\varphi$. Ez ismét egyértelműen terjed ki $F\to B$ modulus-homomorfizmussá, tehát a két kiterjesztés, $\vartheta\psi$ és φ azonos, így a diagram valóban kommutatív.

Megjegyzés: az állítás megfordítása nem igaz. Tekintsük ugyanis az $R=\mathbb{Z}/(6)$ hatelemű gyűrű felett az $M=\mathbb{Z}/(2)$ modulust. ${}_RM$ könnyen ellenőrizhetően projektív, de nem szabad, hiszen egy R feletti szabad modulus additív csoportja $\oplus_\alpha\mathbb{Z}_6$.

12.1.4 Definíció: a $0\longrightarrow A\xrightarrow{\alpha}B$ ${}_R\mathcal{M}$-beli egzakt sorozat (azaz α mono) szétesik, ha valamely $\mu\in hom(B,A)$-ra $\mu\alpha=1_A$. Ezt néha $0\longrightarrow A\underset{\mu}{\overset{\alpha}{\rightleftarrows}}B$-vel jelölöm.

12.1.5 Definíció: a $B\xrightarrow{\beta}C\longrightarrow 0$ ${}_R\mathcal{M}$-beli egzakt sorozat (β epi) szétesik, ha $\exists\nu\in hom(C,B)$: $\beta\nu=1_C$. Néha $B\underset{\nu}{\overset{\beta}{\rightleftarrows}}C\longrightarrow 0$-val jelölöm.

12.1.6 Állítás: **(1)** $0\longrightarrow A\underset{\mu}{\overset{\alpha}{\rightleftarrows}}B$ szétesik $\Leftrightarrow$ $B=Im\,\alpha\oplus Ker\,\mu\simeq A\oplus Ker\,\mu$. (A jobbról balra irány úgy értendő, hogy ha $Im\,\alpha$ direkt összeadandó B-ben, akkor a fenti sorozat szétesik.)

(2) $B \underset{\nu}{\overset{\beta}{\rightleftarrows}} C \longrightarrow 0$ szétesik $\Leftrightarrow$ $B = Ker\,\beta \oplus Im\,\nu \simeq Ker\,\beta \oplus C$. (A jobbról balra irány úgy értendő, hogy ha B-ből kiválasztható egy C' részmodulus, amely direkt összeadandó és amelyet β kölcsönösen egyértelműen képez C-re, akkor a sorozat szétesik.)

Bizonyítás: **(2)** $\Rightarrow$: minden $b \in B$ felírható $b = \nu\beta b + (b - \nu\beta b)$ alakban. Nyilván $\nu\beta b \in Im\,\nu$. $\beta(b - \nu\beta b) = \beta b - (\beta\nu)\beta b = \beta b - 1_C \beta b = 0$, azaz $(b - \nu\beta b) \in Ker\,\beta$. Eszerint $B = Ker\,\beta + Im\,\nu$. Már csak azt kell belátnunk, hogy $(Ker\,\beta) \cap (Im\,\nu) = \{0\}$. Legyen x a metszet tetszőleges eleme. $x \in Im\,\nu$ miatt ez előáll νc : $c \in C$ alakban. Tudjuk, hogy $\beta\nu = 1_C$, amiből $c = \beta\nu c = \beta x = 0$, hiszen $x \in Ker\,\beta$. Ekkor persze $x = \nu c = \nu(0) = 0$, mint azt bizonyítani akartuk.

(2) $\Leftarrow$: $\beta|_{C'}$ egy $C' \to C$ izomorfizmus, tehát invertálható. Jelölje inverzét ν. Ekkor $Im\,\nu = C'$, azaz $\beta\nu = (\beta|_{Im\,\nu})\nu = (\beta|_{C'})\nu = \nu^{-1}\nu = 1_C$, tehát $B \underset{\nu}{\overset{\beta}{\rightleftarrows}} C \longrightarrow 0$ valóban szétesik.

(1) $\Rightarrow$: $b = \alpha\mu b + (b - \alpha\mu b)$ minden $b \in B$-re teljesül. Akár **(2)** $\Rightarrow$ bizonyításánál, itt is $\alpha\mu b \in Im\,\alpha$ és $(b - \alpha\mu b) \in Ker\,\mu$, továbbá $(Im\,\alpha) \cap (Ker\,\mu) = \{0\}$.

(1) $\Leftarrow$: $Im\,\alpha$ direkt összeadandó B-ben: $B = Im\,\alpha \oplus B_2$, azaz minden $b \in B$ egyértelműen áll elő $b = b_1 + b_2$ alakban, ahol $b_1 \in Im\,\alpha$, $b_2 \in B_2$. α mono, azaz a képén invertálható. Jelölje az inverz leképezést α^{-1}. Rendelje $\mu: B \to A$ a $b_1 + b_2$ elemhez $\alpha^{-1}(b_1)$-et. Könnyen látható, hogy $0 \longrightarrow A \underset{\mu}{\overset{\alpha}{\rightleftarrows}} B$ szétesik.

12.1.7 Definíció: a $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ ${}_R\mathcal{M}$-beli rövid egzakt sorozat szétesik, ha $0 \longrightarrow A \xrightarrow{\alpha} B$, $B \xrightarrow{\beta} C \longrightarrow 0$ valamelyike szétesik.

12.1.8 Állítás: ha az ${}_R\mathcal{M}$-beli $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ rövid egzakt sorozat egyik fele szétesik, akkor a másik fele is.

Bizonyítás: tegyük fel, hogy a jobb fél szétesik, azaz alkalmas $\nu: C \to B$-re $B = Im\,\nu \oplus Ker\,\beta$; az egzaktság miatt ekkor $B = Im\,\nu \oplus Im\,\alpha$. Tehát B minden eleme egyértelműen áll elő $b = x + y$: $x \in Im\,\nu, y \in Im\,\alpha$ alakban. Rendelje $\mu: B \to A$ a fenti b elemhez $\alpha^{-1}(y)$-t. Ez is egyértelmű (α mono) és persze homomorfizmus. Nyilván $\mu\alpha = 1_A$, azaz a bal fél is szétesik.

Most azt tegyük fel, hogy a bal fél esik szét. Ekkor alkalmas $\mu: B \to A$-ra $B = Im\,\alpha \oplus Ker\,\mu = Ker\,\beta \oplus Ker\,\mu$, azaz minden $b \in B$ egyértelműen áll elő $b = x + y$ $(\beta x = 0, \mu y = 0)$ alakban. Ekkor $\beta b = \beta x + \beta y = \beta y$ és az egzaktság miatt $Im(\beta|_{Ker\,\mu}) = Im\,\beta = C$. Továbbá $Ker(\beta|_{Ker\,\mu}) = (Ker\,\beta) \cap (Ker\,\mu) = \{0\}$ mert B direkt összege e két részmodulusnak. Összefoglalva $(\beta|_{Ker\,\mu})$ egy $Ker\,\mu \to C$ izomorfizmus. Jelölje inverzét ν. Ekkor $\beta\nu = (\beta|_{Im\,\nu})\nu = (\beta|_{Ker\,\mu})\nu = (\beta|_{Ker\,\mu})(\beta|_{Ker\,\mu})^{-1} = 1_C$, azaz a jobb fél is szétesik.

12.1.9 Tétel: $P \in {}_R\mathcal{M}$-re ekvivalensek az alábbi feltételek:

(1) P projektív,
(2) minden $M \xrightarrow{\beta} P \longrightarrow 0$ egzakt sorozat szétesik,
(3) P direkt összeadandója egy szabad modulusnak, azaz létezik $P \oplus D$ alakú szabad modulus.

Megjegyzés: a **(2)** feltétel ekvivalens azzal, hogy minden $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$ rövid egzakt sorozat szétesik. Ha ugyanis $B \longrightarrow P \longrightarrow 0$ szétesik, akkor az egész is, ha pedig minden $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$ egzakt sorozat szétesik, akkor minden $M \xrightarrow{\beta} P \longrightarrow 0$ egzakt sorozatra $0 \longrightarrow Ker\,\beta \hookrightarrow M \xrightarrow{\beta} P \longrightarrow 0$ is (vegyük észre, hogy ez is egzakt), speciálisan a jobb fele, azaz $M \xrightarrow{\beta} P \longrightarrow 0$ is.

Bizonyítás: **(1)** $\Rightarrow$ **(2)**: mivel P projektív, van olyan ν, amely kommutatívvá teszi az alábbi diagramot, azaz amelyre $\beta\nu = 1_P$. Ez éppen azt jelenti, hogy $M \longrightarrow P \longrightarrow 0$ szétesik.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\nu"'] \arrow[d, equal] & \\ M \arrow[r, "\beta"] & P \arrow[r] & 0 \end{tikzcd}$$

(2) $\Rightarrow$ **(3)**: legyen $\{b_\alpha \mid \alpha \in \mathbf{I}\}$ generátorrendszer P-ben. Legyen az ezen generátorokból képzett szabad modulus F. A $\varphi: F \to P, b_\alpha \mapsto b_\alpha$ leképezés (egyértelműen) kiterjed egy $F \to P$ epimorfizmussá, ekkor $F \xrightarrow{\varphi} P \longrightarrow 0$ egzakt. A feltételek szerint szétesik, amiből **12.1.6** szerint következik, hogy P beágyazható F-be úgy, hogy beágyazott képe direkt összeadandó legyen.

(3) ⇒ (1): legyen $F=P\oplus Q$ szabad és lássuk be, hogy az alábbi diagram kommutatívvá tehető:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\psi"'] \arrow[d, "\varphi"] & \\ A \arrow[r, "\alpha"] & B \arrow[r] & 0 \end{tikzcd}$$

Legyen $\pi: F\to P$ a vetítőleképezés, $\iota: P\to F$ a beágyazás és tekintsük a következő diagramot:

$$\begin{tikzcd} F \arrow[r, "\pi"] \arrow[d, dashed, "\omega"] & P \arrow[d, "\varphi"] & \\ A \arrow[r, "\alpha"] & B \arrow[r] & 0 \end{tikzcd}$$

F szabad és minden szabad modulus projektív, tehát létezik olyan ω, amely ezt kommutatívvá teszi, azaz $\alpha\omega=\varphi\pi$. Jobbról szorozva ι-vel (azaz megszorítva ω-t $P\le F$-re) $\alpha(\omega\iota)=\varphi(\pi\iota)=\varphi$, azaz $\psi=\omega\iota$ kommutatívvá teszi az első diagramot.

Példa: $R=\mathbb{Z}/(6)$ választással az ${}_RR={}_R(\mathbb{Z}/(2))\oplus{}_R(\mathbb{Z}/(3))$ felírásban a baloldal szabad R-modulus, így a jobb oldal mindkét tagja projektív.

12.1.10 Állítás: ha az L,L' balideálok generálják az R egységelemes gyűrűt, akkor az alábbi két külső direkt összeg izomorf: ${}_RL\oplus{}_RL'\simeq{}_RR\oplus{}_R(L\cap L')$.

Bizonyítás: tekintsük az $\varphi: L_1\oplus L_2\to R, (l_1,l_2)\mapsto l_1+l_2$ leképezést. Ez nyilván homomorfizmus és feltételeink szerint szürjektív, tehát az ${}_RL\oplus{}_RL'\xrightarrow{\varphi}{}_RR\longrightarrow 0$ sorozat egzakt. ${}_RR$ szabad, azaz projektív, tehát **12.1.9** szerint a sorozat szétesik, azaz $L\oplus L'\simeq R\oplus Ker\,\varphi$. Márpedig $Ker\,\varphi=\{(l_1,l_2)\,|\,l_1\in L_1, l_2\in L_2, l_1+l_2=0\}=\{(l,-l)\,|\,l\in L_1\cap L_2)\simeq L_1\cap L_2$.

12.2 Néhány állítás osztható Abel-csoportokról

12.2.1 Állítás: ha $A\in{}_{\mathbb{Z}}M$ (azaz Abel-csoport), $a\in A$, $o(a)=n<\infty$, p prím és $(n,p)=1$, akkor $p\,|\,a$.

Bizonyítás: $(n,p)=1 \Rightarrow px\equiv 1\ (mod\ n)$ megoldható, tehát $\exists t\in\mathbb{N}: nt=px-1 \Rightarrow nt+1=px$. Ezt jobbról megszorozva a-val $nt\cdot a+a=px\cdot a$. Itt $nt\cdot a=t\cdot(a\cdot n)=t\cdot 0=0$, hiszen a rendje n. Eszerint $d=x\cdot a$ választással $a=0+a=p\cdot d$.

12.2.2 Állítás: ha $A\in{}_{\mathbb{Z}}M$ minden eleme minden prímmel osztható, akkor A osztható.

Bizonyítás: legyen $a\in A, n\in\mathbb{Z}^+$. Legyen n prímfelbontása $\prod_{i=1}^{s}p_i$. a osztható p_1-el, azaz $\exists a_1: a=p_1\cdot a_1$. a_1 osztható p_2-vel: $a_1=p_2\cdot a_2$. Ezt folytatva $a=n\cdot a_s$.

12.2.3 Állítás: Z_{p^∞} minden p-re osztható.

Bizonyítás: $\forall a\in Z_{p^\infty}$ osztható p-vel. Ugyanis valamely k-ra $\langle a\rangle=Z_{p^k}<Z_{p^{k+1}}<Z_{p^\infty}$ és $px=a$ már $Z_{p^{k+1}}$-ban megoldható. Minden más q prímmel pedig azért osztható, mert rendje p-hatvány, azaz $(o(a),q)=1$.

Megjegyzés: $(\mathbb{Q},+)$ osztható.

12.2.4 Megjegyzés: $\oplus_{\alpha\in\mathbf{I}}D_\alpha$ pontosan akkor osztható, ha D_α osztható $\forall\alpha\in\mathbf{I}$-re, hiszen $nx=a$ pontosan akkor oldható meg, ha koordinátánként megoldható. Speciálisan: osztható csoport direkt faktora osztható.

Következmény: a szabad Abel-csoportok (szabad $\mathbb{Z}$-modulusok) nem oszthatóak, mert pl. az 1-nek nincs fele.

Megjegyzés: ha D osztható és $D\xrightarrow{\varphi}\overline{D}\longrightarrow 0$ egzakt, akkor $\overline{D}$ is osztható. Ugyanis minden $\overline{d}\in\overline{D}$ előáll $\varphi(d)$ alakban. D osztható, azaz $\forall n\in\mathbb{N}\exists x\in D: nx=d$. Ekkor persze $n\cdot\varphi(x)=\overline{d}$, azaz $\overline{d}$ osztható n-el.

12.3 Injektív modulusok

12.3.1 Definíció: a ${}_RQ\in{}_RM$ injektív, ha az alábbi diagram minden $0\longrightarrow A\xrightarrow{\alpha}B$ egzakt sorozatra kommutatívvá tehető alkalmas ψ-vel:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\varphi"] & B \arrow[dl, dashed, "\psi"] \\ & Q & \end{tikzcd}$$

Tétel: minden modulus beágyazható injektív modulusba. Egyelőre nem bizonyítjuk.

12.3.2 Állítás: $Q\in_R M$ esetén az alábbi feltételek ekvivalensek:

(1) Q injektív,

(2) minden $0\longrightarrow Q\xrightarrow{\alpha}M$ egzakt sorozat szétesik.

Bizonyítás: **(1)** $\Rightarrow$ **(2)**: legyen $0\longrightarrow Q\xrightarrow{\alpha}M$ egzakt. Mivel Q injektív, alkalmas ν homomorfizmusra az alábbi diagram kommutatív, ami épp azt jelenti, hogy a sorozat szétesik.

$$\begin{tikzcd} 0 \arrow[r] & Q \arrow[r, "\alpha"] \arrow[d, equal] & M \arrow[dl, dashed, "\nu"] \\ & Q & \end{tikzcd}$$

(2) $\Rightarrow$ **(1)**: legyen Q a feltételnek megfelelő, $0\longrightarrow A\xrightarrow{\alpha}B$ egzakt. Legyen $Q\xrightarrow{\iota}I$ beágyazás egy injektív modulusba az előző, nem bizonyított tételnek megfelelően. Tekintsük a következő diagramot:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\varphi"] & B \arrow[d, dashed, "\omega"] \\ & Q \arrow[r, "\iota"] & I \end{tikzcd}$$

Mivel I injektív, alkalmas ω-ra a diagram kommutatív. Továbbá ι monomorfizmus, tehát $0\longrightarrow Q\xrightarrow{\iota}I$ egzakt. A feltétel szerint ez szétesik, tehát $\exists\mu\in hom(I,Q)$: $\mu\iota=1_Q$. Az, hogy a fenti diagram kommutatív, azt jelenti, hogy $\omega\alpha=\iota\varphi$. Balról szorozva μ-vel $\mu(\omega\alpha)=(\mu\iota)\varphi=1_Q\varphi=\varphi$, ami azt jelenti, hogy $\psi=\mu\omega$-ra az alábbi diagram kommu tatív, azaz Q injektív.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\varphi"] & B \arrow[d, dashed, "\omega"] \arrow[dl, dashed, "\psi"] \\ & Q & I \arrow[l, "\mu"] \end{tikzcd}$$

12.3.3 Tétel (injektív teszt lemma): legyen R egységelemes gyűrű. ${}_RQ\in_R M$ pontosan akkor injektív, ha R minden L balideáljára (azaz $\forall_R L\leq_R R$-re) és $\varphi\in Hom_R(L,Q)$-ra létezik olyan $\psi\in Hom_R(R,Q)$, amelyre az alábbi diagram kommutatív (ι az $L\rightarrow R$ beágyazás). Más szóval: ha minden $L\rightarrow Q$ homomorfizmus kiterjed R-re.

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\iota"] \arrow[d, "\varphi"] & R \arrow[dl, dashed, "\psi"] \\ & Q & \end{tikzcd}$$

Bizonyítás: ha Q injektív, akkor definíció szerint található ilyen ψ.

Legyen most Q a második feltételnek megfelelő, $0\longrightarrow A\xrightarrow{\xi}B$ egzakt, $\varphi:A\rightarrow Q$. Azt kell belátnunk, hogy létezik olyan $\psi:B\rightarrow Q$, amelyre $\psi\xi=\varphi$. Mivel ξ mono, a képén invertálható. Jelölje inverzét ξ^{-1}, ez egy $Im\,\xi\rightarrow A$ homomorfizmus.

Tekintsük az olyan (B_α,ψ_α) párok $\mathcal{B}$ halmazát, ahol $Im\,\xi\leq B_\alpha\leq B$ és $\psi_\alpha:B_\alpha\rightarrow A$ kiterjesztése $\varphi\xi^{-1}$-nek (azaz $\psi_\alpha\xi=\varphi$). Ezeken definiálhatunk egy részbenrendezést: legyen $(B_\alpha,\psi_\alpha)\leq(B_\beta,\psi_\beta)$, ha $B_\alpha\leq B_\beta$ és ψ_β kiterjesztése ψ_α -nak. $\mathcal{B}$-beli párok láncának uniója is $\mathcal{B}$-beli, továbbá $\mathcal{B}$ nem üres, hiszen $(Im\,\xi,\varphi\xi^{-1})\in\mathcal{B}$. Tehát $\mathcal{B}$-re teljesülnek a Zorn-lemma feltételei, így van maximális eleme, legyen ez (B^*,ψ^*). Elég belátni, hogy $B^*=B$, hiszen ekkor $\psi^*\xi=\varphi$.

↯ $\exists b\in B\setminus B^*$. Legyen $L=\{r\in R\mid rb\in B^*\}$. Könnyen látható, hogy L balideál R-ben. Legyen $\gamma:L\rightarrow Q$ az a leképezés, melyre $\gamma(r)=\psi^*(rb)$. Minthogy $b\longmapsto rb$ és ψ^* egyaránt modulushomomorfizmus, γ is az lesz. A feltétel szerint $\exists\gamma':R\rightarrow Q$, amely kiterjesztése γ-nak. Legyen $q=\gamma'(1)$.

Jelölje $\langle B^*,b\rangle$-t B'. Definiálni akarunk egy $\psi':B'\rightarrow Q$ homomorfizmust, amelyre $(B',\psi')\in\mathcal{B}$. Írjuk fel B' egy tetszőleges elemét $b'=b^*+rb$ alakban, ahol $b^*\in B^*, r\in R$. Legyen $\psi'(b')+rq$. Ha ψ' jóldefiniált, akkor nyilvánvalóan homomorfizmus. Tegyük fel, hogy b' kétféle felírásából $\psi'(b')=a_1$ ill. $\psi'(b')=a_2$ jött ki. Véve a két felírás különbségét a 0 egy felírását kapjuk, amelyhez $\psi'(0)=a_1-a_2$ tartozik. Az egyértelműséghez tehát elég belátni, hogy ha $b^*+rb=0$, akkor $\psi^*(b^*)+rq=0$. Mivel $rb=-b^*\in B^*$ és $r\in L$, $\gamma'(r)=\gamma(r)$. Felhasználva, hogy γ' homomorfizmus: $rq=r\cdot\gamma'(1)=\gamma'(r)=\gamma(r)=\psi^*(rb)$. Eszerint $\psi^*(b^*)+rq=\psi^*(b^*)+\psi^*(rb)=\psi^*(b^*+rb)=\psi^*(0)=0$.

ψ' valóban jóldefiniált, azaz egy $B'\rightarrow Q$ homomorfizmus. Definíciójából látszik, hogy kiterjesztése ψ^*-nak, továbbá $b\notin B^*$ miatt $B^*<\langle B^*,b\rangle=B'$. Összefoglalva $(B^*,\psi^*)<(B',\psi')$, ami (B^*,ψ^*) maximalitása miatt ↯.

B^* valóban B, ezzel az állítást beláttuk.

12.3.4 Állítás: egy $\mathbb{Z}$-modulus pontosan akkor injektív, ha osztható Abel-csoport.

Bizonyítás: $\Leftarrow$: jelöljön D osztható Abel-csoportot. $\mathbb{Z}$ főideálgyűrű, tehát (bal)ideáljai az $\{(n) \mid n\in\mathbb{Z}\}$ főideálok. Legyen most $n\in\mathbb{Z}\setminus\{0\}$ és tekintsük a

$$\begin{array}{ccccc} 0 & \longrightarrow & (n) & \xrightarrow{\iota} & \mathbb{Z} \\ & & \downarrow{\scriptstyle\varphi} & \swarrow{\scriptstyle\psi} & \\ & & D & & \end{array}$$

${}_{\mathbb{Z}}\mathcal{M}$-beli diagramot. Mivel D osztható és $\varphi(n)\in D$, $\exists x\in D: nx=\varphi(n)$. Legyen ψ az a $\mathbb{Z}\to D$ homomorfizmus, amelyre $\psi(1)=x$. Ekkor $\psi(n)=n\cdot\psi(1)=nx=\varphi(n)$, azaz ψ kiterjesztése φ-nek. Ha $n=0$, akkor a $\mathbb{Z}\to D$ zérómorfizmus megfelel ψ-nek.

Eszerint minden, $\mathbb{Z}$ egy főideáljából D-be menő homomorfizmus kiterjed $\mathbb{Z}$-re. Az injektív teszt lemma szerint D injektív $\mathbb{Z}$-modulus.

$\Rightarrow$: Legyen A injektív $\mathbb{Z}$-modulus. Azt állítjuk, hogy $\forall n\in\mathbb{Z}\setminus\{0\}\,\forall a\in A: n\mid a$. Tekintsük a fenti diagramot, ahol φ az a homomorfizmus, ami n-hez a-t rendeli. A injektivitása miatt létezik olyan ψ, amely kommutatívvá teszi. Ekkor $a=\varphi(n)=\psi(n)=n\cdot\psi(1)$, azaz $n\mid a$ valóban teljesül.

Megjegyzés: az iménti tétel segítségével egyszerűen beláthatjuk egy korábbi tételünket, mely szerint Abel-csoport (jelölje A) osztható részcsoportja (D) direkt összeadandó. Tekintsük ${}_{\mathbb{Z}}\mathcal{M}$-ben a $0\longrightarrow D\hookrightarrow A$ rövid egzakt sorozatot. Mivel D injektív, ez **12.3.2** szerint szétesik, ami pedig **12.1.6** alapján éppen azt jelenti, hogy D direkt összeadandó A-ban.

12.3.5 Tétel: ha D osztható $\mathbb{Z}$-modulus, akkor előáll $D=\left(\oplus_{\alpha\in\mathbf{I}}(\mathbb{Q},+)\right)\oplus\left(\oplus_{\beta\in\mathbf{J}}Z_{p_\beta^\infty}\right)$ alakban, ahol a p_β-k nem feltétlenül különböző prímek.

Bizonyítás: legyen D torziórészcsoportja T. T is osztható, mert véges rendű elem n-edrésze is véges rendű. A fenti megjegyzésből T direkt összeadandó, alkalmas $A\le D$-re $D=T\oplus A$. A torziómentes, mert az összes véges rendű elem T-ben van. A – osztható csoport direkt faktora lévén – szintén osztható.

$T=\oplus_{p\text{ prím}}T_p$, ahol T_p a torzió-p-csoport, vagyis a p-hatvány rendű elemek halmaza (ezt a csoportelméletről szóló résznél beláttuk). A p rendű elemek (továbbá a 0) részcsoportot alkotnak, amely néhány Z_p direkt összege. Akkor persze vektortér $\mathbb{F}_p$ felett – jelölje V_p – és van egy $\{a_\beta \mid \beta\in\mathbf{J}_p\}$ bázisa.

Rögzítsük most β-t. Legyen $a_{\beta,0}=0$, $a_{\beta,1}=a_\beta$, $k\ge 1$-re pedig $a_{\beta,k+1}$ legyen olyan, hogy $p\cdot a_{\beta,k+1}=a_{\beta,k}$ teljesüljön. T_p osztható, így választható ilyen $a_{\beta,k+1}$. Ekkor $\langle a_{\beta,n} \mid n\in\mathbb{N}\rangle=H_\beta\simeq Z_{p^\infty}$. Ennek minden x eleme lényegében (k csak $\bmod p^n$ egyértelmű) egyértelműen áll elő $x=k\cdot a_{\beta,n}$ alakban, ahol $n\in\mathbb{N}$, k pedig p-vel nem osztható egész; $k=0 \Leftrightarrow x=0$. Nevezzük ezt praktikus felírásnak.

Azt állítjuk, hogy amit az így megadott T_p-beli H_β-k generálnak, az a direkt összegük. $\nmid$ nem ez a helyzet, ekkor néhány (véges sok!), páronként más-más H_β-ba tartozó nem 0 elem összege 0, azaz $\sum_{i=0}^{r}x_i=0\ :\ x_i\in H_{\beta(i)}\setminus\{0\}$. Tekintsük az x_i elemek praktikus felírását. Azt kapjuk, hogy $\sum_{i=0}^{r}k_i\cdot a_{\beta(i),n(i)}=0\ :\ k_i\in\mathbb{N}, p\nmid k_i, n(i)\in\mathbb{Z}^+$. Legyen n az $n(i)$ számok legnagyobbika és szorozzuk meg az egyenletet p^{n-1}-el. Ha $n(i)<n$, akkor $p^{n-1}k_i\cdot a_{\beta(i),n(i)}=p^{n-n(i)}k_i\cdot a_{\beta(i)}=0$, ha pedig $n(i)=n$, akkor $p^{n-1}k_i\cdot a_{\beta(i),n(i)}=k_i\cdot a_{\beta(i)}$. Így tehát $\sum_{n(i)=n}k_i\cdot a_{\beta(i)}=0$. A bal oldal a megfelelő $a_{\beta(i)}$ vektorok lineáris kombinációja, egyik együttható sem osztható p-vel és az összeg legalább egytagú. Viszont az $a_{\beta(i)}$-k az $\mathbb{F}_p$ feletti V_p vektortér lineárisan független elemei, $\lightning$.

Valóban, $\langle H_\beta \mid \beta\in\mathbf{J}_p\rangle=\oplus_{\beta\in\mathbf{J}_p}H_\beta$. Jelölje ezt T_p'.

T_p' osztható, mert Z_{p^∞}-ek direkt összege. $\nmid$ $T_p\ne T_p'$. Ekkor $T_p=T_p'\oplus T^*$, mert Abel-csoport osztható részcsoportja direkt összeadandó (ld. csoportelmélet). T^* rendje is p-hatvány, tehát van p-edrendű eleme. Ez benne van $V_p\subseteq T_p$-ben, $\lightning$. Így $T_p=T_p'=\oplus_{\beta\in\mathbf{J}_p}H_\beta\simeq\oplus_{\beta\in\mathbf{J}_p}Z_{p^\infty}$.

Tekintsük most az A torziómentes, osztható csoportot. Minden $v\in A, n\in\mathbb{Z}\setminus\{0\}$ esetén pontosan egy $x\in A$-ra lesz $n\cdot x=v$. Ugyanis legalább egy ilyen van az oszthatóság miatt, ha pedig $nx=nx'=v$, akkor $n(x-x')=0$ és a torziómentességből $x=x'$. Azaz tetszőleges $v\in A, q\in\mathbb{Q}$-ra jóldefiniált a $q\cdot v\in A$ elem. Triviális, hogy az imént megadott művelettel A egy $\mathbb{Q}$ feletti vektortér, ennek additív csoportja $\oplus_{\alpha\in\mathbf{I}}(\mathbb{Q},+)$ alakú.

Tehát $D=T\oplus A=A\oplus\left(\oplus_{p\text{ prím}}T_p\right)\simeq\left(\oplus_{\alpha\in\mathbf{I}}(\mathbb{Q},+)\right)\oplus\left(\oplus_{p\text{ prím}}\left(\oplus_{\beta\in\mathbf{J}_p}Z_{p^\infty}\right)\right)$, ezzel az állítást beláttuk.

12.3.6 Állítás: minden $\mathbb{Z}$-modulus beágyazható egy injektív $\mathbb{Z}$-modulusba.

Bizonyítás: a $\mathbb{Z}$-modulusok az Abel-csoportok, az injektívek az oszthatóak. Azt kell tehát belátni, hogy minden Abel-csoport beágyazható egy osztható Abel-csoportba. $\oplus_{\alpha\in\mathbf{I}}\mathbb{Q}$ osztható, tehát $\oplus_{\alpha\in\mathbf{I}}\mathbb{Z}\leq\oplus_{\alpha\in\mathbf{I}}\mathbb{Q}$ miatt minden szabad Abel-csoport beágyazható oszthatóba. Minden A Abel-csoport előáll valamilyen F szabad Abel-csoport faktorcsoportjaként, azaz $A\simeq F/B$. Ágyazzuk be F-et a D osztható csoportba, ez megad egy $F/B\hookrightarrow D/B$ beágyazást. Osztható csoport homomorf képe is osztható, így $A\xrightarrow{\sim}F/B\hookrightarrow D/B$ megfelel.

Megjegyzés: legyen $A,B\in{}_R\mathcal{M}$ és tekintsük $Hom_R({}_RA,{}_RB)$-t. Ebből szeretnénk jobboldali modulust csinálni. Mindenképp Abel-csoport, azaz $\mathbb{Z}$-modulus. Ha R kommutatív, akkor a $(\varphi\cdot r):a\longmapsto r\cdot\varphi(a)$ művelettel jobboldali R-modulus is lesz, mert $((\varphi\cdot r)\cdot s)(a)=s\cdot((\varphi\cdot r)(a))=sr\cdot\varphi(a)=rs\cdot\varphi(a)=(\varphi\cdot rs)(a)$ miatt $(\varphi\cdot r)\cdot s=\varphi\cdot rs$, a többi axióma pedig triviálisan teljesül.

Legyen most $M\in{}_R\mathcal{M}$, $A\in{}_{\mathbb{Z}}\mathcal{M}$. Persze M-et tekinthetjük csupán Abel-csoportnak, azaz ${}_{\mathbb{Z}}\mathcal{M}$ egy elemének. Készítsünk a $H=Hom_{\mathbb{Z}}(M,A)$ Abel-csoportból jobboldali R-modulust. Legyen a szorzás a következő: $\varphi\in H, r\in R$-re $(\varphi r)(m):=\varphi(rm)$. Lássuk be, hogy ez valóban egy $H\times R\to H$ művelet és teljesülnek rá a modulusaxiómák.

$(\varphi r)(m_1+m_2)=\varphi(rm_1+rm_2)\underset{\varphi\text{ összegtartó}}{=}\varphi(rm_1)+\varphi(rm_2)=(\varphi r)(m_1)+(\varphi r)(m_2)$, azaz φr összegtartó, valóban $\mathbb{Z}$-modulus-homomorfizmus. H Abel-csoport és a fent definiált szorzás nyilván disztributív az összeadásra, így ahhoz, hogy $H\in\mathcal{M}_R$, elég, hogy $\forall r,s\in R\,\forall\varphi\in H$: $(\varphi r)s=\varphi(rs)$. Márpedig $((\varphi r)s)(m)=(\varphi r)(sm)=\varphi(r(sm))=\varphi((rs)m)=(\varphi(rs))(m)$. Valóban jobboldali R-modulust definiáltunk.

Hasonlóan, ha $M\in\mathcal{M}_R$ és A Abel-csoport, akkor $Hom_{\mathbb{Z}}(M,A)$ baloldali R-modulussá tehető az $r\cdot\varphi: m\longmapsto\varphi(mr)$ definícióval.

12.3.7 Lemma: ha D injektív $\mathbb{Z}$-modulus, akkor $H=Hom_{\mathbb{Z}}(R_{\mathbb{Z}},D)$ injektív baloldali R-modulus a fenti művelettel.

Bizonyítás: az injektív teszt lemma szerint elég belátni, hogy az alábbi ${}_R\mathcal{M}$-beli diagram alkalmas ψ-vel kommutatívvá tehető, ha L balideál R-ben.

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\iota"] \arrow[d, "\varphi"] & R \arrow[dl, dashed, "\psi"] \\ & Hom_{\mathbb{Z}}(R_{\mathbb{Z}},D) & \end{tikzcd}$$

Jelölje $x\in L$ φ szerinti képét φ_x. Ekkor $\varphi_x: R\to D$ összegtartó leképezés. Tekintsük azt az $f: L\times R\to D$ leképezést, amelyre $f(x,y)=\varphi_x(y)$. f-re az alábbiak fognak teljesülni:

⚀ $f(x,y_1+y_2)=f(x,y_1)+f(x,y_2)$, mert φ_x összegtartó.

⚁ $f(x_1+x_2,y)=f(x_1,y)+f(x_2,y)$, mert φ homomorfizmus, azaz $\varphi_{x_1+x_2}=\varphi_{x_1}+\varphi_{x_2}$.

φ R-modulusok homomorfizmusa, így $\varphi_{rx}=r\cdot\varphi_x$. H-ban a szorzást úgy definiáltuk, hogy $\forall\vartheta\in H$: $(r\cdot\vartheta)(y)=\vartheta(y\cdot r)$. Speciálisan $\vartheta=\varphi_x$-re $\varphi_{rx}(y)=(r\cdot\varphi_x)(y)=\varphi_x(y\cdot r)$. Ebből

⚂ $f(rx,y)=f(x,yr)$.

Legyen $g(x)=f(x,1)$. Ez egy értelmes (R egységelemes) $L\to D$ leképezés, sőt, f fenti tulajdonságai alapján összegtartó, azaz ${}_{\mathbb{Z}}\mathcal{M}$-beli homomorfizmus. D osztható, más néven injektív $\mathbb{Z}$-modulus, így g kiterjeszthető ${}_{\mathbb{Z}}L$-ről ${}_{\mathbb{Z}}R$-re, legyen a kiterjesztés $\hat{g}: R\to D$. Legyen most $\hat{f}: R\times R\to D$, $\hat{f}(x,y)=\hat{g}(y\cdot x)$.

⚀′ $\hat{f}(x,y_1+y_2)=\hat{f}(x,y_1)+\hat{f}(x,y_2)$ ha $x,y_1,y_2\in R$. Ugyanis $\hat{g}$ összegtartó és R-ben a szorzás disztributív az összeadásra, azaz $\hat{g}((y_1+y_2)\cdot x)=\hat{g}(y_1x)+\hat{g}(y_2x)$.

⚁′ $\hat{f}(x_1+x_2,y)=\hat{f}(x_1,y)+\hat{f}(x_2,y)$ ugyanígy.

⚂′ $\hat{f}(rx,y)=\hat{f}(x,yr)$, hiszen $\hat{g}(y\cdot rx)=\hat{g}(yr\cdot x)$.

⚃′ $\hat{f}(x,y)=f(x,y)$, ha $x\in L, y\in R$. A bal oldal ugyanis definíció szerint $\hat{g}(yx)$, a jobb oldal pedig ⚂ szerint $f(yx,1)$. $x\in L$ és L balideál, tehát $yx\in L$, így g definíciójából $f(yx,1)=g(yx)$. Márpedig $\hat{g}(yx)=g(yx)$ mindenütt, ahol g értelmezve van, hiszen $\hat{g}$ kiterjesztése g-nek.

Legyen most $\hat{\varphi}(x)$ az az $R\to D$ leképezés, amelyre $\hat{\varphi}(x)(y)=\hat{f}(x,y)$. ⚀′ szerint $\hat{\varphi}(x)$ összegtartó, azaz $\hat{\varphi}(x)\in H$. ⚁′ és ⚂′ szerint $\hat{\varphi}$ művelettartó, azaz ${}_R\mathcal{M}$-beli homomorfizmus. ⚃′ szerint $x\in L$ esetén $\hat{\varphi}(x)=\varphi(x)$, tehát $\hat{\varphi}$ kiterjesztése φ-nek.

$\hat{\varphi}$ kommutatívvá teszi a vizsgált diagramot, eszerint H valóban injektív.

Megjegyzés: legyen R egységelemes gyűrű, $\varphi: {}_RA \to {}_RB$ homomorfizmus, ${}_RM \in {}_R\mathcal{M}$ rögzített. Ekkor φ indukál egy $\varphi_*: Hom_R(M,A) \to Hom_R(M,B)$ $\mathbb{Z}$-modulus-homomorfizmust; ez nem más, mint $\varphi_*: \alpha \mapsto \varphi \circ \alpha$. Azt állítjuk, hogy $*: {}_RA \mapsto Hom_R(M,A); \varphi \mapsto \varphi_*$ egy ${}_R\mathcal{M} \to {}_{\mathbb{Z}}\mathcal{M}$ kovariáns funktor. Valóban, ha ${}_R\mathcal{M}$-ben tekintjük $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$-t, akkor $Hom_R(M,A) \xrightarrow{\alpha_*} Hom_R(M,B) \xrightarrow{\beta_*} Hom_R(M,C)$ egy ${}_{\mathbb{Z}}\mathcal{M}$-beli diagram és $\beta_*\alpha_* = (\beta\alpha)_*$. Ezt úgy is megfogalmazhatjuk, hogy $Hom_R(M,\cdot): {}_R\mathcal{M} \to {}_{\mathbb{Z}}\mathcal{M}$ kovariáns funktor. Hasonlóan $Hom_R(\cdot, N)$ kontravariáns funktor, azaz $Hom_R(\cdot,\cdot)$ első változójában kontravariáns, második változójában kovariáns bifunktor ${}_R\mathcal{M} \times {}_R\mathcal{M}$-ből ${}_{\mathbb{Z}}\mathcal{M}$-be.

12.3.8 Tétel: minden M R-modulus beágyazható injektív R-modulusba.

$R=\mathbb{Z}$ esetére az állítást már beláttuk. Legyen most R tetszőleges. Tekintsük M-et $\mathbb{Z}$-modulusként, ekkor a tétel első fele szerint van olyan $0 \to M \xrightarrow{\iota} D$ egzakt sorozat ${}_{\mathbb{Z}}\mathcal{M}$-ben, ahol D injektív. Alkalmazzuk erre a fent definiált $*$ funktort, a rögzített modulus legyen R. Ekkor a $0 \to Hom_{\mathbb{Z}}(R_{\mathbb{Z}}, M_{\mathbb{Z}}) \xrightarrow{\iota_*} Hom_{\mathbb{Z}}(R_{\mathbb{Z}}, D_{\mathbb{Z}})$ diagramot kapjuk.

Azt állítjuk, hogy ez is egzakt sorozat, azaz ι_* injektív. Valóban, ha $\iota_*(\alpha) = \iota_*(\beta)$, akkor $\iota\alpha = \iota\beta$, amiből – tekintve, hogy ι monomorfizmus, így balról lehet vele egyszerűsíteni – $\alpha = \beta$.

Lássuk be, hogy ι_* mint a $Hom_{\mathbb{Z}}(R,M)$ és $Hom_{\mathbb{Z}}(R,D)$ baloldali R-modulusok közti leképezés is homomorfizmus. Összegtartó, mert ${}_{\mathbb{Z}}\mathcal{M}$-ben homomorfizmus. Az kell még, hogy ha $\varphi \in Hom_{\mathbb{Z}}(R,M)$, akkor $r \cdot \iota_*(\varphi) = \iota_*(r \cdot \varphi)$. Legyen $x \in R$ tetszőleges és nézzük meg, mit vesz fel a két leképezés x-ben:

$$\big(r \cdot \iota_*(\varphi)\big)(x) = \big(\iota_*(\varphi)\big)(xr) = (\iota \circ \varphi)(xr) = \iota\big(\varphi(xr)\big) = \iota\big((r \cdot \varphi)(x)\big) = \big(\iota \circ (r \cdot \varphi)\big)(x) = \big(\iota_*(r \cdot \varphi)\big)(x) \text{ , ugyanazt.}$$

Tehát $Hom_{\mathbb{Z}}(R,M)$ mint baloldali R-modulus beágyazható a $Hom_{\mathbb{Z}}(R,D)$ – a lemma szerint injektív – modulusba. Továbbá $Hom_R(R,M) \subseteq Hom_{\mathbb{Z}}(R,M)$, hiszen ami összeg- és szorzattartó ($\in Hom_R$), az összegtartó ($\in Hom_{\mathbb{Z}}$). Mindkettő baloldali R-modulus, azaz $Hom_R(R,M) \le Hom_{\mathbb{Z}}(R,M)$, így $Hom_{\mathbb{Z}}(R,M)$-el $Hom_R(R,M)$-et is be tudtuk ágyazni egy injektív modulusba. Most már csak azt kell észrevennünk, hogy $Hom_R(R,M) \simeq M$. Valóban, $\varphi \rightleftharpoons \varphi(1)$ művelettartó bijekció a két modulus között.

Összefoglalva $M \simeq Hom_R(R,M) \le Hom_{\mathbb{Z}}(R,M) \le Hom_{\mathbb{Z}}(R,D)$ és ez utóbbi injektív.

12.4 Féligegyszerű gyűrűk

12.4.1 Tétel (Wedderburn-Artin): legyen R egységelemes gyűrű. Ekkor az alábbi feltételek ekvivalensek:

- **(F1)** $\forall$ baloldali R-modulus projektív,
- **(F2)** $\forall$ baloldali R-modulus injektív,
- **(F3)** $\forall$ baloldali R-modulus féligegyszerű,
- **(F4)** $\forall$ ${}_R\mathcal{M}$-beli rövid egzakt sorozat szétesik,
- **(F5)** ${}_RR$ féligegyszerű,
- **(F6)** R előáll $R = \bigoplus_{i=1}^{n} M_{n(i)}(D_i)$ alakban, ahol D_i ferdetest.
- **(F7)** $\forall$ jobboldali R-modulus projektív,
- **(F8)** $\forall$ jobboldali R-modulus injektív,
- **(F9)** $\forall$ jobboldali R-modulus féligegyszerű,
- **(F10)** $\forall$ $\mathcal{M}_R$-beli rövid egzakt sorozat szétesik,
- **(F11)** R_R féligegyszerű,

12.4.2 Definíció: a fenti feltételeknek eleget tevő gyűrűket (minimumfeltételes) féligegyszerű gyűrűnek nevezzük. (A minimumfeltételt az helyettesíti, hogy R egységelemes.)

Bizonyítás: mivel **(F6)**-ban szó sincs jobb- és baloldali modulusokról, elég belátni az első hat feltétel ekvivalenciáját, hiszen ugyanúgy a második hat is ekvivalens lesz.

(F1) $\Leftrightarrow$ **(F4)**: használjuk **12.1.9**-t. Ha ${}_R\mathcal{M}$ minden eleme projektív, akkor minden $0 \to A \to B \to C \to 0$ rövid egzakt sorozat szétesik, hiszen C projektív. Ha minden ${}_R\mathcal{M}$-beli rövid egzakt sorozat szétesik, akkor minden $0 \to Ker\,\beta \hookrightarrow M \xrightarrow{\beta} P \to 0$, azaz minden $M \xrightarrow{\beta} P \to 0$ egzakt sorozat szétesik, így minden $P \in {}_R\mathcal{M}$ projektív.

(F2) $\Leftrightarrow$ **(F4)**: használjuk **12.3.2**-t. Ha ${}_R\mathcal{M}$ minden eleme injektív, akkor minden $0 \to A \to B \to C \to 0$ rövid egzakt sorozat szétesik, hiszen A projektív. Ha minden ${}_R\mathcal{M}$-beli rövid egzakt sorozat szétesik, akkor minden $0 \to Q \xrightarrow{\alpha} M \to M/Im\,\alpha \to 0$, azaz minden $0 \to Q \to M$ egzakt sorozat szétesik, így minden $Q \in {}_R\mathcal{M}$ projektív.

(F3) $\Leftrightarrow$ **(F4)**: használjuk **12.1.6**-t. Ha minden $B \in {}_R\mathcal{M}$ féligegyszerű, akkor egy $0 \to A \xrightarrow{\alpha} B \to C \to 0$ rövid egzakt sorozat mindig szétesik, mert $Im\,\alpha$ mindig direkt összeadandó. Ha pedig minden ${}_R\mathcal{M}$-beli rövid egzakt sorozat szétesik, akkor minden B-re és minden $A \le B$-re $0 \to A \hookrightarrow B$ szétesik, azaz minden $A \le B$ direkt összeadandó, B féligegyszerű.

(F3) $\Leftrightarrow$ (F5): a balról jobbra irány triviális. Tekintsük $\Leftarrow$-t. Legyen ${}_RR=\oplus_{\alpha\in\mathbf{I}}L_\alpha$, ahol az L_α-k ${}_RR$ egyszerű részmodulusai, azaz minimális balideálok. Ekkor $1\in R$ egyértelműen áll elő $1=e_{\alpha(1)}+e_{\alpha(2)}+\ldots+e_{\alpha(n)}$ alakban, ahol $n\in\mathbb{Z}^+$, az $\alpha(i)$-k $\mathbf{I}$ páronként különböző elemei, $e_{\alpha(i)}\in L_{\alpha(i)}\setminus\{0\}$. Ekkor tetszőleges $r\in R$ előáll $r\cdot 1=r\cdot e_{\alpha(1)}+\ldots+r\cdot e_{\alpha(n)}$ alakban. $r\cdot e_{\alpha(i)}\in L_{\alpha(i)}$, mert balideálok, tehát $R=\bigoplus_{i=1}^{n}L_i$. Tekintsük az $R\cdot e_i$ halmazokat. Ezek rendre L_i-beli balideálok és $1\in R$, $e_i\neq 0$ miatt egyik sem $\{0\}$. L_i egyszerű, azaz $L_i=Re_i$. Szorozzuk most meg az $1=\sum_{i=1}^{n}e_i$ egyenlőséget balról e_i-vel. Kapjuk, hogy $e_i=\sum_{j=1}^{n}e_ie_j$, ahol $e_ie_j\in L_j$. Direkt összegben az előállítás egyértelmű, tehát $e_i=e_i^2$ és $\forall j\neq i$: $e_ie_j=0$.

Most lássuk be, hogy ${}_RM\in{}_R\mathcal{M}$ minden A részmodulusa direkt összeadandó. Legyen $\mathcal{B}=\{B\leq M\,|\,A\cap B=\{0\}\}$. $\mathcal{B}$-beli elemek láncának uniója is ilyen, továbbá $\{0\}\in\mathcal{B}$. A Zorn-lemma szerint van tehát maximális elem $\mathcal{B}$-ben. Legyen B ilyen. Ekkor $A+B=A\oplus B$.

↯ $A\oplus B\neq M$, ekkor $\exists x\in M\setminus(A\oplus B)$. Mivel R egységelemes, $x\in Rx=\sum(L_i\cdot x)$. $x\notin A\oplus B$ miatt $\exists i$: $L_ix\nsubseteq A\oplus B$. Jelölje L_i -t L. $Lx\neq\{0\}$, mert $\{0\}\subseteq A\oplus B$, azaz a $\varphi: L\to M, r\mapsto r\cdot x$ modulushomomorfizmus magja nem L. $Ker\,\varphi<L\Rightarrow Ker\,\varphi=\{0\}$, hiszen L egyszerű. Így $L\simeq Lx$. Tekintsük $Lx\cap(A\oplus B)$-t, ez Lx részmodulusa. Nem lehet Lx, mert $Lx\nsubseteq A\oplus B$, így $\{1\}$ kell legyen, mert $Lx\simeq L$ egyszerű. Tehát $Lx+A\oplus B=Lx\oplus A\oplus B$, azaz $Lx\oplus B=B'\in\mathcal{B}$ és $B<B'$. Ez B választása miatt ↯.

(F5) $\Leftarrow$ (F6): legyen $R=\bigoplus_{i=1}^{n}M_{n(i)}(D_i)$ és lássuk be, hogy R féligegyszerű. Féligegyszerű gyűrűk direkt összege is az, tehát elég belátni, hogy $M_n(D)$ feligegyszerű, ha $n\in\mathbb{Z}^+$ és D ferdetest. Állítsuk elő $M_n(D)$-t n minimális balideáljának direkt összegeként.

Legyen $L_i\subseteq M_n(D)$ azon mátrixok halmaza, melyek az i-edik oszlop kivételével csak 0 elemeket tartalmaznak. L_i zárt az összeadásra és egy $\mathbf{A}$ elemét balról szorozva $\mathbf{B}\in M_n(D)$-vel a kapott mátrix minden sora lineáris kombinációja lesz $\mathbf{A}$ sorainak, tehát az i-edik oszlopon kívül csak 0 elemeket tartalmaz $\Rightarrow$ L_i-beli $\Rightarrow$ L_i balideál $M_n(D)$-ben. Legyen most $\mathbf{A}\in L_i\setminus\{0\}$ és $\mathbf{A}'\in L_i$ tetszőleges. $\mathbf{A}'$ i-edik oszlopvektorát jelölje v. $\mathbf{A}\neq 0$ $\Rightarrow$ $\exists j$: $a_{ji}\neq 0$. Legyen $\mathbf{B}$ az a mátrix, melynek j-edik oszlopában $v\cdot a_{ji}^{-1}$ van, minden más 0. Így $\mathbf{B}\cdot\mathbf{A}$ i-edik oszlopában $v\cdot a_{ji}^{-1}\cdot a_{ji}=v$ jelenik meg, minden más 0 lesz, azaz $\mathbf{B}\cdot\mathbf{A}=\mathbf{A}'$. Így L_i minden 0-tól különböző $\mathbf{A}$ elemére az $\mathbf{A}$ által generált balideál már L_i. Azaz L_i egyszerű. $M_n(D)=\bigoplus_{i=1}^{n}L_i$ valóban féligegyszerű.

(F5) $\Rightarrow$ (F6): legyen R véges sok minimális balideál direkt összege: $\boxdot$ ${}_RR=\bigoplus_{i=1}^{n}{}_R(L_i)$. Tudjuk, hogy ekkor L_i előáll $L_i=Re_i$ alakban, ahol az e_i elemek ortogonális idempotens rendszert alkotnak. Csoportosítsuk az ${}_R(L_i)\in{}_R\mathcal{M}$ modulusokat izomorfia szerint és minden egyes izomorfiaosztály elemeinek vegyük a direkt összegét. Jelölje az így kapott direkt összegeket $R_1,R_2,\ldots,R_m$. Ekkor persze $\square$ ${}_RR=\bigoplus_{k=1}^{m}{}_R(R_k)$, hiszen ez $\boxdot$ átcsoportosított alakja.

Azt állítjuk, hogy R_k jobbideál is, azaz $R_k\triangleleft R$. Ez pontosan akkor igaz, ha $l\neq k$ esetén $R_kR_l=\{0\}$. (Ha R_k jobbideál, akkor ez benne van $R_k\cap R_l$ -ben, ami $\square$ miatt 0. Ha pedig ez minden $l\neq k$-ra fennáll, akkor ismét $\square$ szerint $R_kR=R_k(\sum_{l=1}^{m}R_l)=R_kR_k+(\sum_{l\neq k}R_kR_l)\subseteq R_k+\{0\}=R_k$, azaz R_k jobbideál.) Legyen L az R_k-t, L^* az R_l-t adó minimális balideálok egyike. Elég belátni, hogy $LL^*=\{0\}$, hiszen ebből $R_kR_l=(\sum_{i\in ?}L_i)(\sum_{j\in ?^*}L_j^*)=\sum\sum_{i,j}\{0\}=\{0\}$. ↯ $LL^*\neq\{0\}$, ekkor $\exists z\in L^*$: $Lz\neq\{0\}$. Tekintsük a $\varphi: {}_RL\to{}_RL^*, x\mapsto xz$ homomorfizmust. z választása miatt $Im\,\varphi\neq\{0\}$, ekkor persze $Ker\,\varphi\neq L$. Ezek részmodulusok L-ben ill. L^*-ban, melyek egyszerű modulusok. Így hát $Im\,\varphi=L^*$ és $Ker\,\varphi=\{0\}$, ebből $L\underset{\varphi}{\simeq}L^*$. Akkor viszont L^*-nak is R_k-ban kellene lennie, ↯.

Tehát $R=\bigoplus_{k=1}^{m}R_k$ előáll ideáljai direkt összegeként. Ekkor R_k balideáljai R-nek is balideáljai, ugyanis ha L balideál R_k-ban, akkor $RL=(\sum_{l=1}^{m}R_l)L=(\sum_{l\neq k}\{0\})+R_kL\subseteq L$. Így hát az L_i-k a megfelelő R_k ideálokban mint részgyűrűben is minimális balideálok, továbbá R_k egységelemes ($1\in R$ megfelelő koordinátája egységelem R_k-ban). Alkalmazva a most következő lemmát $R_k\simeq M_{n(k)}(D_k)$, amiből következik a bizonyítandó az állítás.

Lemma: legyen R egységelemes és álljon elő véges sok páronként izomorf minimális balideáljának direkt összegeként: ${}_RR=\bigoplus_{i=1}^{n}{}_R(L_i)$. Ekkor alkalmas D ferdetestre és n pozitív egészre $R\simeq M_n(D)$.

Bizonyítás: tudjuk, hogy $L_i=Re_i$, ahol az e_i-k …, továbbá $\boxdot$ $(\sum_{j=1}^{n}e_j)=1$. Tekintsük $Hom_R(L_1,L_1)=End_R(L_1)$-et és jelöljük D-vel. Ez az összeadásra és a kompozícióra gyűrűt alkot.

Azt állítjuk (ezt egyébként Schur-lemma néven is szokták emlegetni), hogy ha R egységelemes és ${}_RM\in{}_R\mathcal{M}$ egyszerű, akkor $End_R({}_RM)$ ferdetest. Valóban, $id_M\in End_R({}_RM)$ miatt egységelemes, továbbá $\psi\in End_R({}_RM)\setminus\{0\}$-ra $Im\,\psi\neq\{0\}$, $Ker\,\psi\neq M$. Az egyszerűségből $Im\,\psi=M$, $Ker\,\psi=\{0\}$, azaz ψ invertálható, mint azt bizonyítani kívántuk.

Tekintsünk most egy $\varphi: L_i \to L_k$ homomorfizmust. $\varphi(e_i) \in L_k = Re_k$ miatt $\exists r \in R$: $\varphi(e_i) = re_k$. Rendelje a $\Theta: Hom_R(L_i, L_k) \to e_i Re_k$ leképezés φ-hez az $e_i \cdot \varphi(e_i) = e_i re_k$ elemet. Vegyük észre, hogy $\forall x \in L_i$ elemre $\varphi(x) = \varphi(xe_i) = x \cdot \varphi(e_i) = xe_i \cdot \varphi(e_i) = x \cdot \Theta(\varphi)$.

$Hom_R(L_i, L_k)$ és $e_i Re_k$ egyaránt Abel-csoport az összeadásra. Azt állítjuk, hogy a fenti Θ leképezés izomorfizmust ad a két csoport között. Szürjektív, mert $e_i re_k \in e_i Re_k$ előáll a $\varphi: x \mapsto x \cdot e_i re_k$ homomorfizmus Θ szerinti képeként. Injektív, mert ha $\Theta(\varphi) = \Theta(\psi)$, akkor $\forall x \in L_i$: $\varphi(x) = x \cdot \Theta(\varphi) = x \cdot \Theta(\psi) = \psi(x)$, amiből $\varphi = \psi$.

Ha a $\varphi: L_i \to L_k$ és $\psi: L_k \to L_m$ modulushomomorfizmusok Θ szerinti képei (Θ-t definiáljuk minden egyes L_a, L_b párra) $e_i re_k$ és $e_k se_m$, akkor $\forall x \in L_i$: $(\psi\varphi)(x) = \varphi(x) \cdot e_k se_m = x \cdot e_i (re_k^2 s) e_m = x \cdot e_i r^* e_m \in e_i Re_m$, így a $\psi\varphi: L_i \to L_m$ homomorfizmus Θ szerinti képe $\Theta(\psi\varphi) = e_i re_k \cdot e_k se_m = \Theta(\varphi) \cdot \Theta(\psi)$. Tehát az $\bigcup_{i,k=1}^n Hom_R(L_i, L_k)$ homomorfizmusok az összeadás (ahol értelmes) és kompozíció műveletekkel adott struktúrája helyett tekinthetjük $\left(\bigcup_{i,k=1}^n e_i Re_k\right)$-t az összeadás és R-beli szorzás műveletekkel. Jelölje Θ inverzét Φ és $e_1 Le_1$-et D', ekkor $D' \underset{\Phi}{\simeq} D$. Rögzítsünk minden egyes i-re egy $\gamma_i: L_1 \to L_i$ izomorfizmust. Jelölje a hozzátartozó $\Theta(\gamma_i) \in e_1 Re_i$ elemet g_i. (Ekkor γ_i éppen a jobbról g_i-vel való szorzás.) Mivel γ_i invertálható, g_i is az.

⚁ $g_i e_k = e_i g_k^{-1} = 0$ ha $i \neq k$, hiszen $i \neq k$-ra $e_i e_k = 0$, így $g_i e_k \in e_1 R(e_i e_k) = e_1 R \cdot 0 = \{0\}$ és $e_i g_k^{-1} \in (e_i e_k) Re_1 = \{0\}$. Persze $g_i e_i = g_i$.

Legyen most $r \in R$ tetszőleges és tekintsük $g_i \cdot e_i re_k \cdot g_k^{-1}$-et. Ezzel jobbról szorozva az L_1-ből L_1-be képező $\gamma_k^{-1} \circ \left(\Phi(e_i re_k)\right) \circ \gamma_i$ homomorfizmust kapjuk, azaz D egy elemét. Legyen $\mathbf{M}(r) \in M_n(D')$ az a mátrix, melyben az i-edik sor k-adik eleme $g_i \cdot e_i re_k \cdot g_k^{-1} \in D'$. Azt állítjuk, hogy az $\mathbf{M}: R \to M_n(D'), r \mapsto \mathbf{M}(r)$ leképezés izomomorfizmus. Jelölje az $\mathbf{M}(.)$ mátrix i-edik sorának k-adik elemét $m_{ik}(.)$.

⚂ $\mathbf{M}(r+s) = \mathbf{M}(r) + \mathbf{M}(s)$, mert a disztibutivitásból $m_{ik}(r+s) = g_i e_i (r+s) e_k g_k^{-1} = g_i e_i re_k g_k^{-1} + g_i e_i (se_k g_k^{-1} = m_{ik}(r) + m_{ik}(s)$.

⚃ $\mathbf{M}(r \cdot s) = \mathbf{M}(r) \cdot \mathbf{M}(s)$. Ugyanis a jobb oldal i, k eleme

$$\textstyle\sum_{j=1}^n m_{ij} \cdot m_{jk} = \sum_{j=1}^n (g_i e_i re_j g_j^{-1})(g_j e_j re_k g_k^{-1}) = g_i e_i r \cdot \left(\sum_{j=1}^n e_j^2\right) \cdot se_k g_k^{-1} \underset{\boxdot}{=} g_i e_i (rs) e_k g_k^{-1} = m_{ik}(rs)$$

megegyezik a bal oldal megfelelő elemével.

⚄ $\mathbf{M}$ injektív, azaz $\mathbf{M}(r) = 0 \Rightarrow r = 0$. Valóban, ha $\mathbf{M}(r) = 0$, akkor $\forall i, k$: $0 = \Phi(m_{ik}) = \Phi(g_i e_i re_k g_k^{-1}) = \gamma_k^{-1} \circ \Phi(e_i re_k) \circ \gamma_i$. Mivel γ_i és γ_k^{-1} izomorfizmusok, ez a szorzat csak akkor lesz az $L_1 \to L_1$ zérómorfizmus, ha $\Phi(e_i re_k): L_i \to L_k$ a zérómorfizmus, azaz $\forall i, k$: $e_i re_k = 0$. Így $0 = \sum_{i,k=1}^n e_i re_k = (\sum_{i=1}^n e_i) r (\sum_{k=1}^n e_k) \underset{\boxdot}{=} 1 \cdot r \cdot 1 = r$, mint azt bizonyítani akartuk.

⚅ M szürjektív, azaz $\forall \mathbf{A} \in M_n(D') \exists r \in R$: $\mathbf{A} = \mathbf{M}(r)$. Elég belátni, hogy azon $\mathbf{E} = \mathbf{E}_{ik}(d)$ mátrix, melyben az i-edik sor k-adik eleme $d \in D' \setminus \{0\}$ (d tetszőleges), előáll képként, hiszen ilyen mátrixok összegeként $M_n(D')$ minden eleme előáll és $Im\,\mathbf{M}$ részgyűrű. Jelölje $\Theta(d)$-t δ. Ha $d \in D \setminus \{0\}$, akkor δ egy $L_1 \to L_1$ izomorfizmus. Ezért $\gamma_k \delta \gamma_i^{-1}: L_i \to L_k$ is izomorfizmus, így előáll $\Phi(e_i re_k)$ alakban, azaz $g_i^{-1} dg_k = e_i re_k$ és $d = g_i \cdot (g_i^{-1} dg_k) \cdot g_k^{-1} = g_i \cdot e_i re_k \cdot g_k^{-1}$. Tekintsük $\mathbf{M}(e_i re_k)$-t. Ennek (l, m) eleme $g_l e_i re_k g_m^{-1}$, ez ⚁ szerint $l = i, m = k$ kivételével 0. Az (i, k) elem a fentiek szerint d, azaz $\mathbf{M}(e_i re_k) = \mathbf{E}$. $\mathbf{M}$ tényleg szürjektív.

$R \underset{\mathbf{M}}{\simeq} M_n(D') \simeq M_n(D)$, ezzel a lemmát igazoltuk.

12.4.3 Definíció: $M \in {}_R M$ noether-modulus, ha részmodulusai teljesítik a maximumfeltétel; ez ekvivalens azzal, hogy minden részmodulusa végesen generált. M artin-modulus, ha részmodulusai teljesítik a minimumfeltételt. (Azaz ha M részmodulushálója noether- ill. artin-háló.)

12.4.4 Állítás: legyen $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ egzakt sorozat ${}_R M$-ben. Ekkor B artin-modulus $\Leftrightarrow$ A és C is az.

Bizonyítás: $\Rightarrow$: A részmodulusai részmodulusai B-nek is, C részmodulusait pedig β^{-1} (mint teljes inverz kép) injektíven és rendezéstartóan emeli vissza B részmodulusaiba. Ha tehát B részmodulusai közt nincs végtelen leszálló lánc, akkor ugyanez A-ra és C-re is áll. (Másképp: A ill. C részmodulushálója éppen a $[\{0\}, A]$ ill. az $[A, B]$ intervallum B részmodulushálójában (a beágyazások α és β^{-1}), artin-hálónak pedig a részhálója is artin.)

$\Leftarrow$: legyen $A \leq B$, A és $C = B/A$ artin, és lássuk be, hogy B is az. Legyen $(M_n)_{i=1}^{\infty}$ B részmodulusainak végtelen (nem feltétlenül szigorúan) csökkenő lánca. Elég igazolni, hogy M_n idővel stabilizálódik. Tekintsük az $(M_n + A)/A$ részmodulusok (ezek az M_n-ek képei a $B \to C$ természetes homomorfizmusban) végtelen csökkenő láncát C-ben. Ez egy n' index felett stabilizálódik, mert C artin. Azaz $\forall k \in \mathbb{N}$: $M_{n'+k} + A = M_{n'} + A$. Vegyük most az $M_{n'+k} \cap A$ leszálló láncot A részmodulusai közt. Ez is stabilizálódik, azaz alkalmas $n'' \geq n'$-re $\forall k \in \mathbb{N}$: $M_{n''+k} \cap A = M_{n''} \cap A$. Ekkor

$$\forall k \in \mathbb{N}:\ M_{n''} = M_{n''} \cap (A + M_{n''}) = M_{n''} \cap (A + M_{n''+k}) = (M_{n''} \cap A) + M_{n''+k} = (M_{n''} \cap A) + M_{n''+k} = (M_{n''+k} \cap A) + M_{n''+k} = M_{n''+k}.$$

(A harmadik átalakításnál azt használtuk, hogy részmodulusháló moduláris.) Így n'' után az M_n lánc is stabilizálódik.

Megjegyzés: a fentivel azonos állítás mondható noether-modulusokról és ugyanígy bizonyítható. (Tulajdonképpen azt láttuk be, hogy egy korlátos moduláris háló pontosan akkor artin, ha véve valamely a elemére a $[0,a]$ és $[a,1]$ intervallumokat, ezek artin-hálót alkotnak. A noether-háló az artin-háló duálisa, a modularitás önmaga duálisa, így ugyanez noether-hálóval is igaz.)

Megjegyzés: az egységelemes gyűrűkkel ellentétben, modulusokra nem teljesül az artin $\Rightarrow$ noether implikáció.

12.4.5 Definíció: az M modulusnak $0=M_0<M_1<\ldots<M_{n-1}<M_n=M$ kompozíciólánca, ha a lánc tagjai részmodulusok és a lánc nem finomítható, azaz $\forall i\in\{1\ldots n\}:\nexists N: M_{i-1}<N<M_i$. Ez nyilván ekvivalens azzal, hogy $\forall i$: M_i/M_{i-1} egyszerű modulus.

12.4.6 Állítás: M-nek van kompozíciólánca $\Leftrightarrow$ artin és noether.

Bizonyítás: $\Leftarrow$: legyen M artin és noether. Legyen $M_0=0$, majd $i\geq 0$, $M_i\neq M$ esetén M_{i+1} legyen az M_i-t szigorúan tartalmazó részmodulusok nemüres (M benne van) halmazának egy minimális eleme. Ekkor $M_0<M_1<M_2<\ldots$ részmodulusok szigorúan növekvő lánca, azaz véges hosszú. Ez csak úgy lehetséges, ha idővel $M_n=M$ lesz, ekkor nyilván kompozícióláncot kaptunk.

$\Rightarrow$: ha M-nek van kompozícióolanca, akkor a $\{0\}$ modulusból megkapható véges sok lépésben úgy, hogy minden lépésben egyszerű modulussal bővítünk. Minden egyszerű modulus artin és noether, mert igen kevés részmodulusa van. **12.4.4** és az azt követő megjegyzés szerint mindkét tulajdonság megmarad a lépések során.

12.4.7 Megjegyzés: a Wedderburn-Artin tétel szerint minden R féligegyszerű gyűrű véges sok minimális balideáljának direkt összege, azaz ${}_RR$-nek van kompozícióolánca. Így R balartin és balnoether. A **(6)** feltétel szimmetriája miatt persze jobbartin és jobbnoether is.

12.4.8 Definíció: az R gyűrű I bal-/jobb-/kétoldali ideálja nilpotens, ha $\exists n\in\mathbb{N}: I^n=\{0\}$. Ez azt jelenti, hogy minden n tényezős I-beli szorzat értéke 0. I nil-ideál/-balideál/-jobbideál, ha minden eleme nilpotens. Nyilván minden nilpotens ~~ nil-~~, de a megfordítás csak artin-gyűrűben igaz (ezt majd belátjuk).

12.5 Féligegyszerű gyűrűk klasszikus tárgyalásmódja

Tudjuk, hogy tetszőleges R gyűrűre és n pozitív egészre az $M_n(R)$ teljes mátrixgyűrű is gyűrű lesz; továbbá ha R egységelemes, akkor $M_n(R)$ is az és egységeleme az az $\mathbf{I}$ diagonális mátrix, melynek minden átlóeleme R egységeleme. Definiáljuk $\mathbf{A}$ skalárszorosait az alábbi módon: $\mathbf{A}\in M_n(R)$, $r\in R$ esetén $r\cdot\mathbf{A}$ ill. $\mathbf{A}\cdot r$ legyen az a mátrix, melynek (i,k) eleme $r\cdot a_{ik}$ ill. $a_{ik}\cdot r$, ahol a_{ik} az $\mathbf{A}$ mátrix (i,k) eleme. Ezen műveletekre nézve $M_n(R)$ (R,R)-bimodulus lesz.

Jelölje $r\in R$-re $\mathbf{D}_r$ azt a mátrixot, melynek átlójában mindenütt r van, többi eleme 0. Ekkor tetszőleges $\mathbf{M}\in M_n(R)$-re $r\cdot\mathbf{M}=\mathbf{D}_r\cdot\mathbf{M}$ és $\mathbf{M}\cdot r=\mathbf{M}\cdot\mathbf{D}_r$. Ez azért jó, mert így $M_n(R)$ egy bal-, jobb- ill. kétoldali ideálja minden elemének bal- vagy jobboldali ill. tetszőleges skalárszorosát is tartalmazza. Továbbá $\delta: r\rightarrow\mathbf{D}_r$ az R gyűrű beágyazása $M_n(R)$-be.

Ha R kommutatív, akkor a szokott módon definiálhatjuk $\mathbf{A}\in M_n(R)$-re $\mathbf{A}$ determinánsát. Az a_{ik} elemhez tartozó előjeles aldeterminánst A_{ik}-val jelölve $\mathbf{A}$ adjungáltja az a mátrix, melyben az i-edik sor k-adik eleme A_{ki}. Jelölése **adj A** vagy $\mathbf{A}^*$. Akárcsak a test feletti mátrixgyűrűknél, $\mathbf{A}^*\cdot\mathbf{A}=\mathbf{A}\cdot\mathbf{A}^*=(\det\mathbf{A})\cdot\mathbf{I}$. Ha $\det\mathbf{A}\in R$ egység, akkor $(\det\mathbf{A})^{-1}\cdot\mathbf{A}^*$ kétoldali inverze lesz $\mathbf{A}$-nak, különben a determinánsok szorzásszabálya értelmében $\mathbf{A}$-nak nem lehet inverze.

12.5.1 Tétel: ha D ferdetest, akkor $M_n(D)$ egyszerű gyűrű.

Bizonyítás: legyen I az $R=M_n(D)$ gyűrű $\{0\}$-tól különböző ideálja. Elegendő megmutatni, hogy $I=R$. Jelölje $\mathbf{E}_{kl}$ azt a mátrixot, melynek (k,l) eleme 1, minden más eleme 0. Legyen $\mathbf{A}$ az I ideál nemnulla eleme. Legyen (i,j) olyan, hogy $a_{ij}\neq 0$. Így $I\lhd R$, $\mathbf{A}\in I$, $a_{ij}^{-1}\cdot\mathbf{E}_{ki}\in R$ és $\mathbf{E}_{jl}\in R$ $\Rightarrow$ $(a_{ij}^{-1}\cdot\mathbf{E}_{ki})\mathbf{A}\cdot\mathbf{E}_{jl}\in I$. Ez a szorzat viszont épp $\mathbf{E}_{kl}$, azaz $\mathbf{E}_{kl}\in I$. Az $\{\mathbf{E}_{kl}\}_{k,l=1}^n$ elemek már generálják R-t (például generált balideálként), hiszen tetszőleges $\mathbf{B}\in R$ $\mathbf{B}=\sum_{k,l=1}^n b_{kl}\cdot\mathbf{E}_{kl}$. Tehát $\forall\mathbf{B}\in R$ előáll I-beli elemek (baloldali) skalárszorosai összegeként, azaz $R\subseteq I$.

12.5.2 Tétel: legyen D ferdetest. Ekkor $M_n(D)$ balideáljai bijektív módon megfeleltethetőek a $V=D^n$ vektortér altereinek és a megfeleltetés tartalmazástartó.

Megjegyzés: jelölje $M_n(D)$ balideálhálóját $\mathcal{L}$, V altérhálóját $\mathcal{V}$. (A részbenrendezés mindkét esetben a tartalmazás, a $\wedge$ művelet a metszet, az $\vee$ művelet az összeadás.) A tétel azt mondja ki, hogy $\mathcal{L}\simeq\mathcal{V}$.

Bizonyítás: rendelje a $\varphi:\mathcal{L}\to\mathcal{V}$ leképezés $L\in\mathcal{L}$-hez az L-beli elemek sorvektorainak halmazát V-ben, $\psi:\mathcal{V}\to\mathcal{L}$ pedig $U\leq V$-hez azon R-beli elemek halmazát, melyeknek minden sorvektora U-beli. Elég belátni, hogy φ szürjektív és kölcsönösen rendezéstartó, azaz $L\varphi\leq L'\varphi \Leftrightarrow L\leq L'$.

Először is lássuk be, hogy φ és ψ valóban $\mathcal{V}$-be és $\mathcal{L}$-be képez, azaz $L\varphi\in\mathcal{V}$ és $U\varphi\in\mathcal{L}$.

Legyen $L\in\mathcal{L}$; $u,v\in L\varphi$; $\lambda\in D$ és lássuk be, hogy $\lambda u+v\in L\varphi$. u és v választása miatt találhatóak olyan $\mathbf{A},\mathbf{B}\in L$ mátrixok, melyek i-edik illetve j-edik sora u illetve v. $\mathbf{M}=(\lambda\cdot\mathbf{E}_{1i})\cdot\mathbf{A}+\mathbf{E}_{1j}\cdot\mathbf{B}\in L$, mert L balideál. $\mathbf{M}$ első sora $\lambda u+v$, így ez valóban $L\varphi$-beli.

Legyen most $U\in\mathcal{V}$; $\mathbf{A},\mathbf{B}\in U\psi$; $\mathbf{M}\in M_n(D)$. Azt kell belátni, hogy ekkor $\mathbf{M}\cdot\mathbf{A},\mathbf{A}+\mathbf{B}\in U\psi$. A mátrixszorzás definíciójából látszik, hogy $\mathbf{M}\cdot\mathbf{A}$ sorai $\mathbf{A}$ sorainak lineáris kombinációi, azaz U-beliek: $\mathbf{M}\cdot\mathbf{A}\in U\psi$. $\mathbf{A}+\mathbf{B}$ sorait generálják $\mathbf{A}$ és $\mathbf{B}$ sorai, így ezek is U-beliek: $\mathbf{A}+\mathbf{B}\in U\psi$.

Ha $L\leq L'$ balideálok, akkor φ definíciója szerint $L\varphi\leq L'\varphi$. Lássuk most be, hogy $L\varphi\leq L'\varphi \Rightarrow L\leq L'$. Legyen $\mathbf{A}\in L$ tetszőleges, sorvektorai rendre $v_1,v_2,\ldots,v_n$. Ezek $L\varphi$-beli, azaz $L'\varphi$-beli elemek, tehát találhatóak olyan $\mathbf{A}_k\in L'$ elemek és i_k indexek, hogy $k=1,\ldots,n$-re $\mathbf{A}_k$ i_k-adik sora v_k. Ekkor az $\mathbf{A}=\sum_{k=1}^{n}\mathbf{E}_{k,i_k}\cdot\mathbf{A}_k$ előállítás szerint $\mathbf{A}\in L'$.

Ezzel beláttuk, hogy φ injektív, hiszen $L\varphi=L'\varphi$ esetén $L\varphi\leq L'\varphi$ és $L'\varphi\leq L\varphi$ folytán $L\leq L'$ és $L'\leq L$, összefoglalva $L=L'$.

Könnyen látható, hogy $\forall U\in\mathcal{V}$: $U\psi\varphi=U$, speciálisan φ szürjektív is, azaz hálóizomorfizmus (bijekció). Ekkor invertálható és $U\psi=(U\psi\varphi)\varphi^{-1}=U\varphi^{-1}$ miatt persze $\varphi^{-1}=\psi$.

Megjegyzés: ha sorvektorok helyett oszlopvektorokat tekintettünk volna és V-t nem bal-, hanem jobboldali D-modulusként kezeltük volna, akkor azt kaptuk volna, ho gy R jobbideálhálója izomorf $\mathcal{V}$-vel.

12.5.3 Következmény: $M_n(D)$-ben bal- vagy jobbideálok szigorúan monoton lánca legfeljebb $n+1$ elemű. Ugyanis alkalmazva a fenti φ-vel a $\dim(.)\circ\varphi$ leképezést egy ilyen láncra először D^n-beli alterek szigorúan monoton láncát kapjuk, majd 0 és n közötti egész számok szigorúan monoton láncát, ez utóbbi pedig legfeljebb $n+1$ elemű lehet.

Speciálisan $M_n(D)$ bal- és jobbideáljai eleget tesznek mind a minimum-, mind a maximumfeltételnek.

12.5.4 Definíció: R féligegyszerű, ha balartin és nem tartalmaz 0-tól különböző nilpotens balideált.

Megjegyzés: látni fogjuk, hogy azonos fogalomhoz jutunk, ha a feltételeket jobbideálokra kötjük ki.

12.5.5 Lemma: ha L az R féligegyszerű gyűrű minimális balideálja, akkor előáll $L=Re$ alakban, ahol e idempotens. Ekkor persze e jobboldali egységelem L-ben, hiszen $\forall(re)\in L$: $re\cdot e=r\cdot e^2=re$.

Bizonyítás: legyen $a\in L$ olyan, hogy $La\neq\{0\}$. (Létezik ilyen a, mert L nem nilpotens, azaz $L^2\neq\{0\}$). La balideál R-ben, része L-nek és nem $\{0\}$, L minimalitása miatt tehát csak $La=L$ lehetséges. Így hát L minden eleme előáll xa : $x\in L$ alakban. Speciálisan $\exists e\in L$: $ea=a$. Ekkor $e\neq0$, mert $a\neq0$.

L tetszőleges b elemére $bea=ba$, azaz $(be-a)=0$. Tekintsük azon L-beli x elemek halmazát, melyekre $xa=0$. Ez is balideál R-ben és $ea=a\neq0$ miatt nem az egész L. L minimalitása folytán csak $\{0\}$ lehet, azaz $\forall b\in L$: $(be-b)a=0$ azt jelenti, hogy $\forall v\in L$: $be=b$. Tekintsük Re-t. $e\in L$ miatt $Re\subseteq L$ és $\forall b\in L$: $b=be\in Re$ miatt $L\subseteq Re$, azaz $Re=L$, mint azt bizonyítani akartuk.

12.5.6 Lemma: az R féligegyszerű gyűrű L balideálja előáll Re alakban, ahol e idempotens. Ekkor persze e jobboldali egységelem L-ben.

Bizonyítás: minden L-beli e' idempotens elemhez tekintsük az $A_{e'}=\{x\in L \mid xe'=0\}$ halmazt. Ez persze balideál R-ben. $0\in L$ idempotens, tehát az $\{A_{e'} \mid e'\in L \text{ idempotens}\}$ nemüres halmazban van minimális elem, hiszen R balideáljai teljesítik a minimumfeltételt. Legyen ez A_e.

$\uparrow$ $A_e\neq\{0\}$. Ekkor A_e tartalmaz minimális balideált, amely az előző lemma szerint Re_1 alakba írható, ahol $e_1\in Re_1\subseteq A_e$ idempotens. $e_1\in A_e$-ből $e_1e=0$. Legyen $e_2=e+e_1-ee_1\in L$. Könnyen ellenőrizhető, hogy $ee_2=e_2e=e$ és $e_1e_2=e_2e_1=e_1$, amiből $e_2^2=(e+e_1-ee_1)e_2=e_2$, azaz e_2 idempotens. Ha $xe_2=0$, akkor $xe=xe_2e=0\cdot e=0$, azaz $A_{e_2}\subseteq A_e$. Mivel $e_1e_2=e_1\neq 0$, $e_1\in A_e\setminus A_{e_2}$, így $A_{e_2}\subseteq A_e$ valódi tartalmazás. Ez A_e választása miatt $\lightning$.

Tehát alkalmas $e\in L$ idempotens elemre $A_e=\{0\}$. Így $\forall b\in L$: $(be-b)e=0$-ból következik $\forall b\in L$: $be=b$. Eszerint $L=Le\subseteq Re$, míg L balideál voltából $Re\subseteq L$, összefoglalva $L=Re$.

12.5.7 Tétel (Noether): ha az R gyűrű féligegyszerű, akkor előáll véges sok minimális balideáljának direkt összegeként és ezen balideálok mindegyike idempotenssel generálható (értsd: Re alakú, ahol $e^2=e$ alakú).

Bizonyítás: R-ben van minimális balideál, legyen ez L_1. Az első lemma szerint $L_1=Re_1$, ahol e_1 idempotens. Legyen $L_1'=\{r-re_1\mid r\in R\}$, ez persze balideál R-ben. $x\in L_1\cap L_1'$ esetén egyrészt $xe_1=x$, mert e_1 jobboldali egységelem L_1-ben, másrészt $xe_1=0$, mert $x\in L_1'$ miatt $\exists r$: $xe_1=(r-re_1)e_1=re_1-re_1^2=0$. Tehát $x=0$, $L_1\cap L_1'=\{0\}$. Továbbá $\forall r\in R$ előáll $r=re_1+(r-re_1)\in L_1+L_1'$ alakban, azaz $R=L_1\oplus L_1'$. Így R minden minimális balideálja direkt összeadandó.

Ha $L_1'=\{0\}$, akkor az állítás igaz. Ha nem, akkor legyen L_2 egy L_1' által tartalmazott minimális balideál. A fenti módon $R=L_2\oplus L_2'$. Ebből $L_2\leq L_1'$ alapján – felhasználva, hogy balideálháló moduláris – $L_1'=L_2\oplus(L_1'\cap L_2')$, azaz $R=L_1\oplus L_2\oplus(L_1'\cap L_2')$. Folytassuk ezt mindaddig, amíg $\bigcap_{k=1}^{n}L_k'=\{0\}$ lesz. Ez idővel bekövetkezik, mert $L_1'\supseteq(L_1'\cap L_2')\supseteq\ldots\supseteq(\bigcap_{k=1}^{i}L_k')\supseteq\ldots$ R-beli balideálok szigorúan monoton csökkenő lánca, tehát véges hosszú. Ekkor $R=\bigoplus_{k=1}^{n}L_k$, a tétel állításának megfelelően.

12.5.8 Lemma: legyen R féligegyszerű gyűrű, $A\lhd R$. Ekkor A előáll Re alakban, ahol e kétoldali egységelem A-ban, továbbá alkalmas $B\lhd R$-re $R=A\oplus B$.

Bizonyítás: A balideál, így előáll Re alakban, ahol e idempotens, tehát jobboldali egységelem A-ban. Igazolni fogjuk, hogy e baloldali egységeleme is A-nak. Legyen $J=\{a\in A\mid ea=0\}$. Ez nyilván jobbideál, mert $a\in J, r\in R$ esetén $ar\in A$ és $ear=0\cdot r=0$, azaz $ar\in J$ definíció szerint. Ekkor $J^2=Je\cdot J=J\cdot eJ=J\cdot\{0\}=\{0\}$, így J nilpotens. Az RJ kétoldali ideálra $(RJ)^2=R(JR)J=RJJ=0$. Mivel R féligegyszerű, egyetlen nilpotens balideálja $\{0\}$, azaz $RJ=\{0\}$. Ez persze része J-nek, így J kétoldali ideál. J is nilpotens, így maga is $\{0\}$.

Legyen most $b\in A$ tetszőleges, ekkor $0=e^2b-eb=e(eb-b)$. $A\lhd R$ miatt $(eb-b)\in A$, így definíció szerint J-beli, azaz $\forall b\in A$: $eb-b=0$. Pontosan ekkor nevezzük e-t A baloldali egységelemének.

Legyen most $B=\{r-re\mid r\in R\}$. Akárcsak az előbbi lemmánál, B balideál R-ben és $R=A\oplus B$. Már csak azt kell igazolnunk, hogy B jobbideál is. Legyen $r,s\in R$ tetszőleges, ekkor $(r-re)s\in B$ bizonyítandó. Tekintve az $(r-re)s=(r-re)se+(r-re)(s-se)=r(se-ese)+(r-re)(s-se)$ előállítást az első tag 0, hiszen $se\in A$ miatt $ese=se$, a második tag pedig két B-beli elem szorzata lévén maga is B-beli. Ekkor persze az összeg is B-beli.

Megjegyzés: ideálok direkt összegét azért kedveljük jobban bal- vagy jobbideálok direkt összegénél, mert az előbbiben az összeadás mellett a szorzás is végezhető koordinátánként. Ugyanis $R=\bigoplus_{k=1}^{n}I_k$: $I_k\lhd R$, $r=\sum_{k=1}^{n}r_k$, $s=\sum_{k=1}^{n}s_k$: $r_k,s_k\in I_k$ esetén $rs=\sum_{k=1}^{n}r_ks_k+\sum_{k\neq m}r_ks_m$-ben a második összeg egy tagjára $r_ks_m\in I_kI_m\subseteq I_k\cap I_m=\{0\}$, így az egész összeg 0. Ez alapján

12.5.9 Megjegyzés: az $R=\bigoplus_{k=1}^{n}I_k$ gyűrűben I_k (egyoldali) ideáljai R-nek is (egyoldali) ideáljai.

12.5.10 Következmény: féligegyszerű gyűrű ideálja is féligegyszerű.

Bizonyítás: a **12.5.8** lemma szerint féligegyszerű gyűrű ideálja direkt összeadandó, így balideáljai egyben R-nek is balideáljai. Ezért sem $\{0\}$-tól különböző nilpotens balideál, sem végtelen leszálló lánc nincs köztük.

12.5.11 Tétel (Wedderburn, Artin I.): ha R féligegyszerű, akkor egységelemes és előáll véges sok minimális ideáljának (ezek egyszerű gyűrűk) direkt összegeként, melyek mindegyikének mint gyűrűnek balideáljaira teljesül a minimum-feltétel. Továbbá ez az előállítás egyértelmű.

Bizonyítás: az $R\lhd R$ ideálra alkalmazva az előbbi lemmát kapjuk, hogy egységelemes. Lássuk most be, hogy előáll véges sok minimális balideáljának direkt összegeként.

Ha R egyszerű, akkor kész vagyunk. Ha nem, akkor legyen $A\lhd R$ nem-triviális ideál. A lemma szerint alkalmas B ideálra $R=A\oplus B$ és $A,B\ntrianglelefteq R$. Ha A és B egyaránt egyszerű, akkor mindkettő minimális ideál és kész vagyunk. Ellenkező esetben valamelyik tovább bontható, hiszen az előbbi következmény szerint féligegyszerű. Folytassuk a tovább-bontást, amíg lehet. Ha véges sok lépéssel kész vagyunk, akkor előállítottuk R-t véges sok minimális ideál direkt összegeként.

↯ Sikerül az algoritmust végtelen sokáig folytatni. Ekkor A és B valamelyike is végtelen sokáig bontható, jelölje A_1. Hasonlóan A_1-nek is van végtelen sokáig bontható valódi ideálja, legyen ez A_2, stb. $A_1 > A_2 > A_3 > \ldots > A_k > \ldots$ ideálok végtelen, szigorúan monoton csökkenő lánca, ↯.

Már csak az egyértelműség van hátra. Ehhez elég, hogy $R = \bigoplus_{k=1}^{n} I_k$ minden A minimális ideálja az I_k-k valamelyike. Legyen $a \in A \setminus \{0\}$ és állítsuk elő a direkt összegből $a = \sum_{k=1}^{n} a_k \,:\, a_k \in I_k$. Az a_k-k valamelyike nem 0, legyen ez a_1. I_1 egységelemét e_1-el jelölve $ae_1 = a_1 e_1 = a_1$. Így az a által generált ideál tartalmazza a_1-et. I_1 minimális ideál, tehát $I_1 \subseteq (a) \subseteq A$. A is minimális ideál, így $A = I_1$.

12.5.12 Tétel: legyen L az R féligegyszerű gyűrűben e idempotens, Re minimális balideál. Ekkor $D = eRe$ ferdetest.

Bizonyítás: világos, hogy ere alakú elemek összege, különbsége és szorzata is ilyen, tehát D gyűrű, amelyben e kétoldali egységelem. Legyen most $x = ere \in D \setminus \{0\}$ és lássuk be, hogy van baloldali inverze. Tekintsük $Re \cdot (ere)$-t. Ez része az Re minimális balideálnak és maga is balideál, így vagy $\{0\}$, vagy a teljes Re. $\{0\}$ nem lehet, mert $0 \neq ere = ee \cdot ere \in Re(ere)$. Ezért $Re \cdot x = Re$, amiből $Dx = D$. Speciálisan $e \in D = Dx$, azaz $\exists x' \in D$: $x'x = e$. Ezt kerestük.

12.5.13 Tétel (Wedderburn, Artin II.): az R $(\neq \{0\})$ gyűrű pontosan akkor egyszerű és balartin, ha prímszámrendű zérógyűrű, vagy alkalmas D ferdetestre és n pozitív egészre $R \simeq M_n(D)$.

Bizonyítás: $\Rightarrow$: legyen R a feltételeknek megfelelő.

Tegyük fel, hogy R-nek van $L \neq \{0\}$ nilpotens balideálja, $L^m = \{0\}$. Tekintsük $I = L + LR$-t. Könnyen ellenőrizhető, hogy $I \triangleleft R$. Mivel R egyszerű és $\{0\} \neq L \subseteq I \triangleleft R$, $I = R$. Ebből $RL \subseteq L$ felhasználásával

$$R^m = (L+LR)^m = \sum_{k=0}^{m} L^k (LR)^{m-k} = L^m + \sum_{k=0}^{m-1} L^k (LR)^{m-k} = \{0\} + \sum_{k=0}^{m-1} L^{k+1} (RL)^{m-k-1} R \subseteq \sum_{k=1}^{m} L^m R = \sum_{k=1}^{m} \{0\} \cdot R = \{0\}$$

Eszerint R nilpotens. R^2 ideál az R egyszerű gyűrűben, tehát vagy $\{0\}$, vagy R. Ez utóbbi nem lehetséges, mert akkor R minden hatványa R lenne, holott nilpotens. Azaz $R^2 = \{0\}$, R zérógyűrű. Zérógyűrűben az additív csoport minden részcsoportja ideál, így $(R,+)$-nak nincs valódi részcsoportja. Eszerint prímrendű ciklikus csoport, R pedig prímrendű zérógyűrű.

Tekintsük most azt az esetet, amikor R-ben nincs nilpotens balideál. Ekkor féligegyszerű, azaz Noether tétele szerint előáll véges sok minimális balideáljának direkt összegeként és egységelemes. Legyen $R = \bigoplus_{k=1}^{n} L_k$ ez az előállítás, e az egységelem. Állítsuk elő e-t a direkt összeg szerint: $e = \sum_{k=1}^{n} e_k$, ahol $e_k \in L_k$. Tetszőleges $a_m \in L_m$-re $a_m = a_m e = \sum_{k=1}^{n} a_m e_k$. A két oldalon r két – a direkt összeg szerinti – előállítása található, így egyrészt $a_m e_m = a_m$, másrészt $k \neq m$ esetén $a_m e_k = 0$. Ezek szerint e_m jobboldali egységelem L_m-ben (speciálisan idempotens), másrészt $a_m = e_m$ választással $e_m e_k = 0$, ha $k \neq m$. Utóbbit úgy mondjuk, hogy az e_k elemek ortogonálisak.

$L_k \supseteq Re_k \supseteq L_k e_k = L_k$, mert L balideál és e_k jobboldali egységelem L-ben, így $L_k = Re_k$. Tehát $R = \bigoplus_{k=1}^{n} Re_k$, ahol az e_k elemek ortogonális idempotensek, összegük R egységeleme és Re_k minimális balideál R-ben.

Jelölje az $e_1 R e_1$ ferdetestet D. $\{x \in R \mid xRe_1 = \{0\}\}$ láthatóan ideált alkot R-ben, ami $e_1 R e_1 \neq \{0\}$ miatt nem az egész R. Azaz $xRe_1 = \{0\} \Leftrightarrow x = 0$, speciálisan $e_k R e_1 \neq \{0\}$. Legyen $d_k \in e_k R e_1$ nemnulla elem, erre $e_k d_k = d_k e_1 = d_k$. Az $Ry = \{0\}$ egyenletet kielégítő $y \in R$ elemek ideált alkotnak, mely R egyszerűsége és $R^2 \neq 0$ folytán csak $\{0\}$ lehet, így $e_k d_k = d_k \neq 0$-ból $Re_k d_k \neq \{0\}$. $Re_k d_k$ balideál R-ben, $d_k \in Re_1$ folytán része Re_1-nek és az előbbiekből nem $\{0\}$. Re_1 minimális balideál, azaz csak $Re_k d_k = Re_1$ lehetséges. Ezért $e_1 R e_k d_k = e_1 R e_1$, tehát alkalmas $d_k^* \in e_1 R e_k$ elemre $d_k^* d_k = e_1$. Mármost $(d_k d_k^*)^2 = d_k (d_k^* d_k) d_k^* = (d_k e_1) d_k^* = d_k d_k^*$ és $d_k d_k^* \in e_k R e_1 e_1 R e_k \in e_k R e_k$. Így hát $d_k d_k^*$ az $e_k R e_k$ ferdetest egy idempotens eleme.

> A $p(x) = x^2 - x$ polinomnak ferdetestben is csak 0 és 1 lehet gyöke, mert a $p(x) = x \cdot (x-1)$ felírásban minden együttható centrumbeli, így a szorzás és a behelyettesítés felcserélhető $\Rightarrow$ a ferdetest minden α elemére $p(\alpha) = \alpha \cdot (\alpha - 1)$, ami tényleg csak $\alpha \in \{0,1\}$ esetben lesz 0 $\Rightarrow$ csak ezek idempotensek.

Ezek szerint $d_k d_k^*$ vagy 0, vagy e_k. $d_k d_k^* d_k = d_k e_1 \neq 0$ miatt csak e_k lehet. Ebből és $d_k \in e_k R e_1$, $d_k^* \in e_1 R e_k$-ból:

$$e_k d_k = d_k, \quad d_k^* e_k = d_k^*, \quad d_k d_k^* = e_k, \quad d_k e_1 = d_k, \quad e_1 d_k^* = d_k^*, \quad d_k^* d_k = e_1.$$

Válasszunk ki ilyen d_k elemeket minden egyes $k\in\{1,\dots,n\}$-re és rendelje $\varphi: R\to M_n(D)$ az R gyűrű tetszőleges a eleméhez azt az $\mathbf{A}\in M_n(D)$ mátrixot, melyben $a_{ik}=d_i^* a d_k$ (ez valóban D eleme, hiszen $a_{ik}=e_1 a_{ik} e_1$). Azt akarjuk belátni, hogy φ gyűrűizomorfizmus.

$\varphi(a+b)$ és $\varphi(a)+\varphi(b)$ i-edik sorának k-adik eleme egyaránt $d_i^*(a+b)d_k=d_i^* a d_k+d_i^* b d_k$, így φ összegtartó.

$\varphi(a)\cdot\varphi(b)$ i-edik sorának k-adik eleme $\sum_{s=1}^{n}(d_i^* a d_s)(d_s^* b d_k)=d_i^* a\cdot(\sum_{s=1}^{n} e_s)\cdot b d_k=d_i^* aebd_k=d_i^*(ab)d_k$, szerencsére megegyezik $\varphi(ab)$ megfelelő elemével.

A $\sum_{i,k} d_i a_{ik} d_k^*=\sum_{i,k}(d_i d_i^*)a(d_k d_k^*)=(\sum_i e_i)a(\sum_k e_k)=eae=a$ előállításból φ injektív, hiszen $\varphi(a)$ megadja a-t.

Legyen $\mathbf{M}\in M_n(D)$ tetszőleges, i-edik sorának k-adik elemét jelölje m_{ik}. Ekkor $a=\sum_{s,t} d_s m_{st} d_t^*\in R$ választással $\varphi(a)$ i-edik sorának k-adik eleme $d_i^* a d_k=\sum_{s,t} d_i^* d_s m_{st} d_t^* d_k$. Ha $i\neq s$, akkor $d_i^* d_s=d_i^*(e_i e_s)d_s=0$ és hasonlóan $t=k$ kivételével $d_t^* d_k=0$. Tehát az összegnek egyetlen nem 0 tagja van; ezt beírva $d_i^* a d_k=d_i^* d_i m_{ik} d_k^* d_k=e_1 m_{ik} e_1$, ami $m_{ik}\in e_1 R e_1$ miatt éppen m_{ik}. Azaz $\varphi(a)=\mathbf{M}$, így $\mathbf{M}\in Im\,\varphi$. Ezek szerint φ szürjektív is.

Összegezve a fentieket $\varphi: R\to M_n(D)$ művelettartó bijekció, $R\simeq M_n(D)$.

$\Leftarrow$: ferdetest feletti mátrixgyűrű egyszerű és bal-artin, ezt már beláttuk. Prímrendű zérógyűrű ugyancsak, ez triviális.

12.5.14 *Megjegyzés: a fenti tételben D és n izomorfia erejéig egyértelmű.

Ehhez azt kell belátnunk, hogy $M_n(D)$ egyértelműen meghatározza n-t és izomorfia erejéig D-t. $M_n(D)$-ben balideálok szigorúan monoton lánca lehet $n+1$ elemű, de hosszabb nem, ez meghatározza n-t. Legyen most L minimális balideál, J minimális jobbideál $M_n(D)$-ben. Legyen az L sorvektorai által generált részmodulus (altér) a baloldali D-modulusként tekintett D^n-ben U, a J oszlopvektorai által generált részmodulus a jobboldali D-modulusként tekintett D^n-ben W. Tudjuk, hogy ezek minimális részmodulusok (hálóizomorfizmus), azaz egy elem által generáltak: $U=D\cdot u$ és $W=w\cdot D$, ahol $u=(u_1,\dots,u_n)$, $w=(w_1,\dots,w_n)$ D^n-beli nem 0 vektorok. Feltehetjük, hogy például u_1 és w_1 nem 0, sőt, pont 1. Tekintsük $Q=L\cap J$ egy tetszőleges $\mathbf{A}$ elemét, ennek elemei legyenek $((a_{ik}))_{i,k=1}^{n}$. Ekkor $a_{1k}=a_{11}\cdot u_k$, hiszen $\mathbf{A}\in L$ és $u_1=1$. Hasonlóan $a_{ik}=w_i\cdot a_{1k}$, hiszen $\mathbf{A}\in J$ és $w_1=1$. Tehát $a_{ik}=w_i\cdot a_{11}\cdot u_k$. Másrészt ha egy $\mathbf{A}$ mátrix ilyen alakú, akkor eleme Q-nak. Tehát Q épp azon $\mathbf{A}$ mátrixok halmaza, ahol ahol $a_{11}\in D$ tetszőleges és $a_{ik}=w_i\cdot a_{11}\cdot u_k$.

Azt állítjuk, hogy Q vagy zérógyűrű, vagy D-vel izomorf részgyűrűje $M_n(D)$-nek és mindkét eset előfordulhat alkalmas L,J-re. Legyen $\varrho=\sum_{j=1}^{n} u_j w_j$, jelölje továbbá $\mathbf{A}_\alpha$ Q azon elemét, melynek bal felső eleme $\alpha\in D$. Ekkor $\mathbf{A}_\alpha\cdot\mathbf{A}_\beta$ i-edik sorának k-adik eleme $\sum_{j=1}^{n}(w_i\alpha u_j)(w_j\alpha u_k)=w_i\alpha(\sum_{j=1}^{n} u_j w_j)\beta u_k=w_i(\alpha\varrho\beta)u_k$. Tehát $\mathbf{A}_\alpha\cdot\mathbf{A}_\beta=\mathbf{A}_{\alpha\varrho\beta}$. Ha $\varrho=0$, akkor ez mindig 0, tehát Q zérógyűrű. Ha $\varrho\neq 0$, akkor $\exists\varrho^{-1}\in D$ és $\alpha\mapsto\mathbf{A}_{\alpha\varrho^{-1}}$ művelettartó bijekció D és Q között, mint az könnyen ellenőrizhető.

Ezek szerint $M_n(D)$ ismeretében D az az egyetlen gyűrű, amely előáll egy minimális balideál és egy minimális jobbideál metszeteként, de nem zérógyűrű.

Megjegyzés: ha R kommutatív egyszerű gyűrű, akkor az $R\simeq M_n(D)$ előállításban $n=1$ és D test, hiszen $n>2$ esetén $M_n(D)$ soha nem kommutatív. Eszerint minden kommutatív egyszerű gyűrű test, eltekintve persze az érdektelen prímrendű zérógyűrűktől.

Megjegyzés: mivel $M_n(D)$-ben jobbideálokra is teljesül a minimumfeltétel és az egyetlen nilpotens jobbideál a $\{0\}$, a féligegyszerű gyűrű definíciójában a balideálokat jobbideálokra cserélve azonos fogalomhoz jutunk.

Következmény: további két ekivalens feltételt kaptunk arra, hogy az R gyűrű féligegyszerű legyen:
(F12) R balartin és nincs $\neq\{0\}$ nilpotens balideálja, **(F13)** R jobbartin és nincs $\neq\{0\}$ nilpotens jobbideálja.

12.6 Nemkommutatív gyűrű Jacobson-radikálja

12.6.1 Definíció: legyen $\mathcal{I}$ olyan leképezés, ami gyűrűk egy $\mathcal{R}$ osztályán értelmezett és $\mathcal{R}$ minden R eleméhez annak egy $\mathcal{I}(R)$ ideálját rendeli. $\mathcal{I}$-t radikálnak nevezzük, ha $\forall R\in\mathcal{R}$: $\mathcal{I}\left(R/\mathcal{I}(R)\right)=\{0\}$.

A Jacobson-radikált egységelemes, kommutatív gyűrűben már definiáltuk, ez a maximális ideálok metszete volt. Most ki szeretnénk terjeszteni a definíciót nemkommutatívakra is.

12.6.2 Állítás: az R egységelemes gyűrű $I<R$ (bal)ideálja belefoglalható maximális (bal)ideálba.

Bizonyítás: legyen H az I-t fedő, de 1-et nem tartalmazó (bal)ideálok halmaz. H-beli lánc uniója könnyen láthatóan szintén H-beli és $I\in H$. Így a Zorn-lemma szerint H-nak van maximális elem.

12.6.3 Definíció: az R egységelemes gyűrű $J(R)$ Jacobson-radikálja a R-beli maximális balideálok metszete.

Látszólag az imént a „bal-Jacobson-radikál” fogalmát definiáltuk és ez balideál R-ben. Szerencsére $J(R)$ kétoldali ideál és megegyezik a „jobb-Jacobson-radikál”-lal.

12.6.4 Tétel: legyen R egységelemes. Ekkor $y\in R$-re ekvivalensek az alábbi feltételek:

(1) $y\in J(R)$,
(2) $(1-xy)$-nak $\forall x\in R$-re van balinverze,
(3) minden $M\in{}_R\mathcal{M}$ egyszerű modulusra $yM=\{0\}$,
(4) $(1-xyz)\in U(R)$ minden $x,z\in R$-re (van kétoldali inverze)
(5) y eleme a maximális jobbideálok metszetének,
(6) $(1-yz)$-nek minden $z\in R$-re van jobbinverze,
(7) minden $M\in\mathcal{M}_R$ egyszerű modulusra $My=\{0\}$,

Speciálisan, a maximális balideálok és a maximális jobbideálok metszete megegyezik és kétoldali ideál R-ben.

Bizonyítás: mivel a **(4)** feltétel változatlan, az **(1)**…**(3)** és **(5)**…**(7)** feltételek pedig felcserélődnek, ha R-ről áttérünk az oppozit gyűrűjére, elegendő az első négy feltétel ekvivalenciáját belátni.

(1) $\Rightarrow$ **(2)**: $\uparrow$ $y\in J(R)$, de valamely $x\in R$-re $R(1-xy)\neq R$. Ekkor $R(1-xy)$ egy R-nél szűkebb balideál, így belefoglalható egy L maximális balideálba. $y\in J(R)\subseteq L$ miatt $xy\in L$ és $(1-xy)=1\cdot(1-xy)\in R\cdot(1-xy)\subseteq L$ miatt $(1-xy)\in L$. Ekkor összegük, $xy+(1-xy)=1$ is L-beli, ami $L\neq R$ szerint $\lightning$.

(2) $\Rightarrow$ **(3)**: $\uparrow$ $(1-xy)$-nak minden $x\in R$-re van balinverze, de valamely $M\in{}_R\mathcal{M}$ egyszerű modulusra $yM\neq\{0\}$. Ekkor M valamely m elemére $ym\neq 0$, azaz $Rym\neq\{0\}$. Ez részmodulusa M-nek, M pedig egyszerű, így $Rym=M$. Ekkor $m\in M$ alkalmas $x\in R$ elemre előáll $xym=m$ alakban $\Rightarrow$ $(1-xy)m=0$. Balról szorozva $(1-xy)$ balinverzével $m=0$, azaz $ym=0$, $\lightning$.

(3) $\Rightarrow$ **(1)**: legyen L tetszőleges maximális balideál R-ben. Ekkor $M={}^{R}\!/_{L}$ egyszerű modulus, azaz $y\cdot\left({}^{R}\!/_{L}\right)=\{0\}$ $\Rightarrow$ $y\in L$. Így y eleme az összes maximális balideál metszetének.

(4) $\Rightarrow$ **(1)**: triviális (rögzítsük $z=1$-et). A megfordításhoz még néhány lépésre szükségünk van.

12.6.5 Definíció: legyen $M\in{}_R\mathcal{M}$. Ekkor M annulátor-ideálja $Ann(M)=\{r\in R\,|\,rM=\{0\}\}$. Ez nyilván balideál, de jobbideál is, mert ha $r\in Ann(M)$, $s\in R$, akkor $(rs)M=r(sM)\subseteq rM=\{0\}$.

12.6.6 Állítás: $M\in{}_R\mathcal{M}$ egyszerű $\Leftrightarrow$ $\{0\}$, Z_p feletti zérómodulus vagy alkalmas L maximális balideálra $M\simeq{}^{R}\!/_{L}$.

Bizonyítás: $\Rightarrow$: legyen M egyszerű. Ha zérómodulus, akkor additív csoportja vagy $\{0\}$, vagy egyszerű, tehát Z_p. Ha nem zérómodulus, akkor valamely $m\in M$-re $Rm\neq\{0\}$. Rm részmodulus, így csak M lehet. Tehát $\varphi: R\to M, r\mapsto rm$ epimorfizmus, azaz $L=Ker\,\varphi$ jelöléssel $M=Im\,\varphi\simeq{}^{R}\!/_{L}$. Ha lenne L és R között balideál, akkor annak φ szerinti képe $\{0\}$ és M közötti részmodulus lenne, ami lehetetlen, azaz L maximális balideál. Hogy a felsorolt modulusok valóban egyszerűek, az egyszerű.

12.6.7 Állítás: legyen R egységelemes, L balideál R-ben. Ekkor $Ann\left({}^{R}\!/_{L}\right)$ a legnagyobb kétoldali ideál, amely része L-nek.

Bizonyítás: $Ann\left({}^{R}\!/_{L}\right)=\{r\in R\,|\,r\cdot(R/L)=\{0\}\}=\{r\in R\,|\,rR\subseteq L\}$. $1\in R$ miatt $r\in rR$, tehát $Ann\left({}^{R}\!/_{L}\right)\subseteq L$. Így $Ann\left({}^{R}\!/_{L}\right)=\{r\in L\,|\,rR\subseteq L\}$. Ezen felírásból látszik, hogy $Ann\left({}^{R}\!/_{L}\right)$ minden L-beli elemet tartalmaz, amely egyáltalán belekerülhet L-beli jobbideálba. Mivel $Ann\left({}^{R}\!/_{L}\right)$ kétoldali ideál, tényleg ez a legnagyobb.

Megjegyzés: az ${}^{R}\!/_{L}$ alakú modulusok éppen a ciklikus R-modulusok.

Bizonyítás *(folytatás)*: **(1)**, **(3)** $\Rightarrow$ **(4)**: az iménti definíciót használva **(3)** szerint $J(R)$ éppen az összes egyszerű R-modulus annulátorának metszete. Ezek mind kétoldali ideálok, azaz mets zetük is az. Legyen most $y\in J(R)$; $x,z\in R$. Ekkor yz-t is tartalmazza $J(R)$, mert ideál. **(1)** szerint alkalmas $u\in R$-re $u\cdot\left(1-x(yz)\right)=1$. Ebből $u=1+uxyz$. Mivel y eleme a $J(R)$ kétoldali ideálnak, $-uxyz\in J(R)$. Ekkor $u=1-(-uxyz)$-nek van baloldali inverze is, $u\in U(R)$. Ekkor persze az inverze, $1-xyz$ is $U(R)$-beli, mint azt bizonyítani akartuk.

Ezzel befejeztük **12.6.4** bizonyítását.

Példa: legyen R_0 a $\mathbb{Z}[x_n|n\in\mathbb{N}]$ megszámlálható változós polinomgyűrű, I_0 ebben az $\{x_n^{n+1}|n\in\mathbb{N}\}$ elemek által generált ideál, $R=R_0/I_0$. A természetes homomorfizmust jelölje felülvonás. Minden $\bar{x}_n$ nilpotens, hiszen $x_n^{n+1}\in I_0$. Tehát R nilradikálja (R kommutatív) tartalmazza $\{\bar{x}_n|n\in\mathbb{N}\}$-t (sőt, éppen az általa generált ideál). Márpedig $N=N(R)$ nem nilpotens, hiszen $0\neq x_n^n\in N^n$ szerint $N^n\neq\{0\}$ minden $n\in\mathbb{N}$-re teljesül. Eszerint valóban nem minden nilideál nilpotens.

12.6.8 Lemma: véges sok nilpotens balideál összege is nilpotens.

Bizonyítás: elegendő két tagra belátni. Legyen tehát $L_1^n=L_2^k=\{0\}$ és lássuk be, hogy L_1+L_2 is nilpotens. Tekintsünk először egy $S_\varepsilon=L_{\varepsilon(1)}L_{\varepsilon(2)}\cdot\ldots\cdot L_{\varepsilon(n+k-1)}$ szorzatot, ahol $\varepsilon(i)\in\{1,2\}$. Ha legalább n helyen $\varepsilon(i)=1$, akkor $L_2L_1\subseteq L_1$ felhasználásával kiejthetjük az n-edik L_1 tényező előtt álló L_2 tényezőket és kapjuk, hogy $S_\varepsilon\subseteq L_1^n\cdot(\ldots)=\{0\}\cdot(\ldots)=\{0\}$. Ellenkező esetben $L_1L_2\subseteq L_2$-vel $S_\varepsilon\subseteq L_2^k\cdot(\ldots)=\{0\}$. Ennek segítségével $(L_1+L_2)^{n+k-1}=\sum_{\varepsilon:\{1,\ldots,n-k-1\}\to\{1,2\}}S_\varepsilon=\sum_\varepsilon\{0\}=\{0\}$, azaz L_1+L_2 is nilpotens.

12.6.9 Lemma: ha L nilbalideál az R egységelemes gyűrűben, akkor $L\leq J(R)$.

Bizonyítás: legyen $y\in L$. Elég belátni, hogy $(1-xy)$-nak van balinverze $\forall x\in R$ esetén. $xy\in L$, mert L balideál, így xy nilpotens. Tehát az $s=\sum_{k=0}^{\infty}(xy)^k$ végtelen tagúnak tűnő összeg valójában véges, azaz értelmes és R-beli eredményt szolgáltat. Ekkor $s(1-xy)=(1-xy)s=1$.

12.6.10 Állítás: ha R egységelemes és balartin, akkor $J(R)$ a legnagyobb nilpotens balideál R-ben.

Bizonyítás: az előző lemma szerint $J=J(R)$ minden nil-, speciálisan minden nilpotens balideált tartalmaz. Elegendő tehát belátni, hogy J nilpotens. Tekintsük az $J\supseteq J^2\supseteq J^3\supseteq\ldots$ leszálló láncot R ideáljai közt. Ez feltételeink szerint stabilizálódik, azaz alkalmas $k\in\mathbb{N}$-re $J^k=J^{k+m}$ teljesül minden $m\in\mathbb{N}$ esetén.

↑ $J^k\neq\{0\}$. Ekkor $J^k\cdot J^k\neq\{0\}$, így a $J^k\cdot L\neq\{0\}$ feltételnek eleget tevő L balideálok halmaza nemüres. Legyen L_0 ezek között minimális. Legyen $a\in L$ olyan, melyre $J^k\cdot a\neq\{0\}$. Ekkor $J^k\cdot(Ja)=J^k\cdot a\neq\{0\}$ miatt Ja-ra is teljesül a feltétel. $Ja\subseteq L_0$ és L_0 minimális volta miatt $Ja=L_0\ni a$, azaz $\exists y\in J$: $y\cdot a=a$. Átrendezve $(1-y)a=0$. Ezt megszorozva $(1-y)$ – $y\in J$ szerint létező – balinverzével $a=0$, ami $J^k\cdot a\neq\{0\}$-ból ↯.

Tehát $J^k=\{0\}$, J valóban nilpotens.

Következmény: újabb ekvivalens ($\Leftrightarrow$ **(F12)** az előző állításból) feltételt kaptunk arra, hogy az R egységelemes gyűrű féligegyszerű legyen:

(F14) R balartin és $J(R)=\{0\}$.

Megjegyzés: a Jacobson-radikálról szóló részben végig egységelemes gyűrűkkel foglalkoztunk. Az egységelem létezése azonban néhány trükkel kikerülhető. Az első Jacobsontól származik. Vegyük észre, hogy $(1-y)$-nak pontosan akkor balinverze $(1-x)$, ha $x+y=xy$. Ha az R – nem feltétlenül egységelemes – gyűrűben y-hoz található olyan x, melyre teljesül ez utóbbi feltétel, akkor y-t bal-kváziregulárisnak hívjuk. A kváziregularitás segítségével is megfogalmazhatóak és bizonyíthatóak a Jacobson-radikállal kapcsolatos állítások.

A másik: x-nek a általánosított inverze, ha $axa=a$ (ez egységelemes gyűrűben x bármelyik oldali inverzére teljesül). R Neumann-reguláris, ha minden $x\in R$-hez található ilyen elem.