## 3. Integritástartományok

### Hányadostest

**3.1. Tétel.** Legyen $R = (R, +, 0, -, \cdot, 1)$ integritástartomány, és értelmezzük az $R \times (R \setminus \{0\})$ halmazon a $\oplus$ és $\odot$ műveleteket, valamint a $\sim$ relációt a következőképpen:

$$(a,b) \oplus (c,d) := (ad + bc, bd)\,, \qquad (a,b) \sim (c,d) \overset{\text{def}}{\iff} ad = bc.$$
$$(a,b) \odot (c,d) := (ac, bd)\,,$$

Ekkor $\sim$ ekvivalenciareláció, ami kompatibilis a $\oplus$ és $\odot$ műveletekkel, vagyis kongruenciája az $(R \times (R \setminus \{0\})\,; \oplus, \odot)$ algebrának; legyen $Q_R$ a megfelelő faktoralgebra. A $Q_R$ algebra a következő tulajdonságokkal rendelkezik:

(1) $Q_R$ test, amelyben az $\overline{(a,1)}$ alakú elemek egy $R$-rel izomorf részgyűrűt alkotnak;
(2) $Q_R$ minden eleme előáll „két $R$-beli elem hányadosaként", azaz $\overline{(a,1)} \odot \overline{(b,1)}^{-1}$ alakban;
(3) ha $K$ egy tetszőleges test, ami részgyűrűként tartalmazza $R$-et (vagy egy $R$-rel izomorf gyűrűt), akkor $K$-nak van $Q_R$-rel izomorf részteste.

**3.2. Definíció.** A fent megkonstruált $Q_R$ testet az $R$ integritástartomány ***hányadostestének*** nevezzük.

**3.3. Példa.** Az egész számok gyűrűjének hányadosteste a racionális számok teste: $Q_{\mathbb{Z}} \cong \mathbb{Q}$. Egy $T$ test feletti polinomgyűrű hányadosteste a $T$ feletti racionális törtek teste: $Q_{T[x]} \cong T(x)$.

**3.4. Megjegyzés.** A tételben szereplő harmadik tulajdonság így is megfogalmazható: ha $K$ egy test, és $\varphi\colon R \to K$ beágyazás (azaz injektív gyűrűhomomorfizmus), akkor $\widehat{\varphi}\colon Q_R \to K$, $\overline{(a,1)} \odot \overline{(b,1)}^{-1} \mapsto (a\varphi)\,(b\varphi)^{-1}$ is beágyazás. Ha az $\overline{(a,1)} \in Q_R$ elemet azonosítjuk az $a \in R$ elemmel, azaz $R$-et $Q_R$ részgyűrűjének tekintjük (a tételbeli első tulajdonság miatt ezt megtehetjük), akkor $\widehat{\varphi}$ kiterjesztése $\varphi$-nek: $\overline{(a,1)}\widehat{\varphi} = a\varphi = \overline{(a,1)}\varphi$. Tehát $R$ bármely testebe történő beágyazása kiterjed $Q_R$-nek ugyanabba a testbe történő beágyazásává.

**3.5. Következmény.** Minden integritástartomány beágyazható testbe. Izomorfia erejéig egyetlen olyan minimális $K$ test létezik, amibe $R$ beágyazható (a minimalitás azt jelenti, hogy $K$-nak egyetlen valódi résztestébe sem ágyazható be $R$). Ez a $K$ test izomorf $R$ hányadostestével.

### Gauss-gyűrűk

A következőkben $R = (R, +, 0, -, \cdot, 1)$ mindig tetszőleges integritástartományt jelöl.

**3.6. Definíció.** Azt mondjuk, hogy az $a \in R$ elem ***osztója*** a $b \in R$ elemnek, ha létezik olyan $c \in R$, amelyre $b = ac$. Jelölés: $a \mid b$.

**3.7. Definíció.** Azt mondjuk, hogy az $a$ és $b$ elemek ***asszociáltak***, ha $a \mid b$ és $b \mid a$. Jelölés: $a \sim b$.

**3.8. Definíció.** Az $u \in R$ elemet ***egységnek*** nevezzük, ha $u \mid 1$ (azaz $u \sim 1$). Az egységek halmazát $R^*$ jelöli.

**3.9. Állítás.** Az oszthatósági és asszociáltsági reláció, valamint az egységek minden integritástartományban rendelkeznek a szokásos tulajdonságokkal. Így például $(R^*; \cdot)$ csoport, és két elem akkor és csak akkor asszociált, ha egymástól csupán egység tényezőben különböznek. Az oszthatóság reflexív és tranzitív, valamint „asszociáltság erejéig" antiszimmetrikus. Tehát ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor egy $(R/\!\sim; |)$ részbenrendezett halmazt kapunk, amelynek legkisebb eleme $1/\!\sim = R^*$, legnagyobb eleme pedig $0/\!\sim = \{0\}$.

**Bizonyítás.** A Bevezetés az absztrakt algebrába kurzusban szerepelt (ha nem, akkor HF). □

**3.10. Definíció.** A $d \in R$ elemet az $a$ és $b$ elemek ***legnagyobb közös osztójának*** nevezzük, ha kielégíti a következő két feltételt:

(i) $d \mid a$ és $d \mid b$;
(ii) $\forall k \in R : (k \mid a \text{ és } k \mid b) \implies k \mid d$.

A $t \in R$ elem ***legkisebb közös többszöröse*** $a$-nak és $b$-nek, ha kielégíti a következő két feltételt:

(i) $a \mid t$ és $b \mid t$;
(ii) $\forall k \in R : (a \mid k \text{ és } b \mid k) \implies t \mid k$.

**3.11. Állítás.** A legnagyobb közös osztó és a legkisebb közös többszörös asszociáltság erejéig egyértelműen meghatározott, és a szokásos tulajdonságokkal rendelkezik (**ha létezik egyáltalán**). Az $(R/\!\sim; |)$ részbenrendezett halmazban $a/\!\sim$ és $b/\!\sim$ legnagyobb közös alsó korlátja $\operatorname{lnko}(a,b)/\!\sim$, legkisebb közös felső korlátjuk pedig $\operatorname{lkkt}(a,b)/\!\sim$ (amennyiben létezik $\operatorname{lnko}(a,b)$ és $\operatorname{lkkt}(a,b)$).

**Bizonyítás.** A Bevezetés az absztrakt algebrába kurzusban szerepelt (ha nem, akkor HF). □

**3.12. Definíció.** Azt mondjuk, hogy a $p \in R$ elem ***irreducibilis***, ha nem nulla és nem egység, és csak úgy bontható két elem szorzatára, hogy az egyik tényező asszociált $p$-hez. (Ekkor a másik tényező szükségképpen egység; ilyenkor ***triviális faktorizációról*** beszélünk.) Formálisan:

$$p \nsim 0, 1 \quad \text{és} \quad \forall a, b \in R : p = ab \implies (p \sim a \text{ vagy } p \sim b)\,.$$

**3.13. Definíció.** Azt mondjuk, hogy a $p \in R$ elem ***prím***, ha nem nulla és nem egység, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$p \nsim 0, 1 \quad \text{és} \quad \forall a, b \in R : p \mid ab \implies (p \mid a \text{ vagy } p \mid b)\,.$$

**3.14. Tétel.** Minden integritástartományban a prím elemek irreducibilisek.

**Bizonyítás.** Tegyük fel, hogy $p \in R$ prím elem. Ekkor $p \nsim 0, 1$, tehát azt kell ellenőriznünk, hogy $p = ab \implies (p \sim a$ vagy $p \sim b)$ minden $a, b \in R$ esetén. Tegyük fel, hogy $p = ab$; ekkor $p \mid ab$ (miért?), tehát a prímtulajdonság szerint $p \mid a$ vagy $p \mid b$. Az első esetben azt kapjuk, hogy $p \sim a$, a másodikban pedig azt, hogy $p \sim b$ (miért?). Ezzel beláttuk, hogy $p$ irreducibilis. □

**3.15. Tétel.** Ha az $R$ integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor $R$-ben minden irreducibilis elem prím.

**Bizonyítás.** Tegyük fel, hogy az $R$ integritástartományban bármely két elemnek létezik legnagyobb közös osztója, és legyen $p \in R$ irreducibilis elem. Ekkor $p \nsim 0, 1$, tehát azt kell ellenőriznünk, hogy $p \mid ab \implies (p \mid a$ vagy $p \mid b)$ minden $a, b \in R$ esetén. Tegyük fel, hogy $p \mid ab$; ekkor Euklidész lemmája[1] szerint $\frac{p}{\operatorname{lnko}(p,a)} \mid b$.[2] Mivel $p$ irreducibilis, asszociáltság erejéig csak két osztója van, így $\operatorname{lnko}(p, a) \sim 1$ vagy $\operatorname{lnko}(p, a) \sim p$. Az első esetben azt kapjuk, hogy $p \mid b$, a másodikban pedig azt, hogy $p \mid a$ (miért?). Ezzel beláttuk, hogy $p$ prím. □

**3.16. Példa.** A $\mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\right\}$ integritástartományban az $a = 6$ és $b = 2 + 2\sqrt{-5}$ elemeknek nem létezik legnagyobb közös osztója. (Asszociáltság erejéig három közös osztójuk van: 1, 2 és $1 + \sqrt{-5}$, de ezek között nincs legnagyobb az oszthatóság szerinti részbenrendezésben.) A $\mathbb{Z}[\sqrt{-5}]$ gyűrűben a 2 elem irreducibilis, de nem prím: $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, de $2 \nmid 1 + \sqrt{-5}$ és $2 \nmid 1 - \sqrt{-5}$.

**3.17. Definíció.** ***Gauss-gyűrűnek*** nevezzük az olyan integritástartományokat, amelyekben minden a nullától és az egységektől[3] különböző elem irreducibilis elemek szorzatára bomlik, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű. Tehát az $R$ integritástartomány Gauss-gyűrű, ha minden $a \in R$ $(a \neq 0, a \nsim 1)$ esetén léteznek olyan $p_1, \ldots, p_n \in R$ irreducibilis elemek, amelyekre $a = p_1 \cdot \ldots \cdot p_n$; továbbá amennyiben $a = q_1 \cdot \ldots \cdot q_m$ egy másik irreducibilis faktorizáció, akkor $n = m$, és létezik olyan $\pi \in S_n$, amelyre $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

**3.18. Példa.** Az egész számok gyűrűje, a Gauss-egészek gyűrűje, és bármely test feletti polinomgyűrű Gauss-gyűrű. (A testek is Gauss-gyűrűk: a definíció üresen teljesül rájuk.)

**3.19. Tétel.** Legyen $R$ Gauss-gyűrű, és legyen $a, b \in R$ irreducibilis felbontása $a \sim p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ és $b \sim p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$. (Az $\alpha_i, \beta_i$ kitevők nemnegatív egész számok; ha valamelyik $p_i$ csak $a$ vagy csak $b$ felbontásában szerepel, akkor a másikban 0 kitevővel vesszük.) Ekkor teljesülnek az alábbiak:

(1) $a \mid b \iff \alpha_i \leq \beta_i$ $(i = 1, \ldots, n)$;

(2) $\operatorname{lnko}(a, b) \sim p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$;

(3) $\operatorname{lkkt}(a, b) \sim p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

**Bizonyítás.** Tegyük fel, hogy $R$ Gauss-gyűrű, és legyen $a, b \in R$ irreducibilis felbontása $a \sim \prod p_i^{\alpha_i}$ és $b \sim \prod p_i^{\beta_i}$.

(1) Ha $a \mid b$, akkor van olyan $c \in R$ elem, amelyre $b = ac$. Legyen $c$ irreducibilis felbontása $c \sim \prod p_i^{\gamma_i}$ (ha $p_i$ nem szerepel $c$ felbontásában, akkor $\gamma_i = 0$). Az $ac = b$ egyenlőségből azt kapjuk, hogy $\prod p_i^{\alpha_i + \gamma_i} = \prod p_i^{\beta_i}$. A felbontás egyértelműségéből következik, hogy minden $i$-re $\alpha_i + \gamma_i = \beta_i$. Mivel $\gamma_i \geq 0$, ebből megkapjuk, hogy $\alpha_i \leq \beta_i$.

A másik irány igazolásához tegyük fel, hogy $\alpha_i \leq \beta_i$ minden $i$-re, és legyen $c = \prod p_i^{\beta_i - \alpha_i}$ (itt fontos, hogy $\beta_i - \alpha_i \geq 0$, mert ha negatív kitevős hatvány jelenne meg, az multiplikatív inverzet jelentene, márpedig multiplikatív inverze csak az egységeknek van). Világos, hogy az így megadott $c$ elemmel $b = ac$, azaz $a \mid b$.

(2) Jelöljük $d$-vel a jobb oldalon lévő elemet, és az egyszerűség kedvéért vezessük be a $\delta_i = \min(\alpha_i, \beta_i)$ jelölést: $d = \prod p_i^{\delta_i}$. Meg fogjuk mutatni, hogy $d \sim \operatorname{lnko}(a, b)$. Hogy $d \mid a$ és $d \mid b$, az következik abból, hogy minden $i$-re $\delta_i \leq \alpha_i$ és $\delta_i \leq \beta_i$ (miért?). Az lnko definíciójában szereplő (ii) feltétel bizonyításához tegyük fel, hogy $k \in R$ egy tetszőleges elem,

[1] A legnagyobb közös osztó szokásos tulajdonságai, és azok következményeként Euklidész lemmája is bebizonyítható minden olyan integritástartományban, ahol bármely két elemnek létezik legnagyobb közös osztója.

[2] Itt a tört igazából nem osztást jelent. Mivel $\operatorname{lnko}(p, a) \mid p$, van olyan $? \in R$ elem, amelyre $p = ? \cdot \operatorname{lnko}(p, a)$. A kérdőjel helyére kerülő elemet jelöli $\frac{p}{\operatorname{lnko}(p,a)}$.

[3] Ha megállapodunk abban, hogy az üres (nulla darab tényezőből álló) szorzat értéke 1 (hasonlóan ahhoz, hogy az üres összeg 0), akkor az egységeket is fel lehet bontani irreducibilis elemek szorzatára, és ez a felbontás egyértelmű is lesz. A nullát viszont mindenképp ki kell zárni, azt nem lehet irreducibilis elemek szorzataként felírni.

amire $k \mid a$ és $k \mid b$ teljesül. Legyen $k$ irreducibilis felbontása $k \sim \prod p_i^{\varkappa_i}$. Mivel $k \mid a$ és $k \mid b$, ezért minden $i$-re $\varkappa_i \leq \alpha_i$ és $\varkappa_i \leq \beta_i$ (miért?). Ebből következik, hogy $\varkappa_i \leq \delta_i$ minden $i$-re (miért?), tehát $k \mid d$ (miért?). Ezzel beláttuk, hogy $d \sim \operatorname{lnko}(a, b)$.

(3) A bizonyítás nagyon hasonló az előzőhöz, csak mindent a „feje tetejére kell állítani". □

**3.20. Definíció.** Az $(A; \leq)$ részbenrendezett halmaz teljesíti a ***leszállólánc-feltételt***, ha $A$-ban nem létezik végtelen szigorúan csökkenő sorozat, azaz nem léteznek olyan $a_1, a_2, \ldots \in A$ elemek, amelyekre $a_1 > a_2 > \cdots$. Másképpen fogalmazva, minden csökkenő sorozat előbb-utóbb stabilizálódik: ha $a_1 \geq a_2 \geq \cdots$, akkor $a_k = a_{k+1} = \cdots$ valamely $k$ természetes számra. Hasonlóan definiálható a ***felszállólánc-feltétel*** is.

**3.21. Tétel.** Tetszőleges $R$ integritástartomány esetén ekvivalensek az alábbiak:

(1) $R$ Gauss-gyűrű;
(2) az $(R/\sim; |)$ részbenrendezett halmaz teljesíti a leszállólánc-feltételt, és $R$-ben bármely két elemnek létezik legnagyobb közös osztója;
(3) az $(R/\sim; |)$ részbenrendezett halmaz teljesíti a leszállólánc-feltételt, és $R$-ben minden irreducibilis elem prím.

**Bizonyítás.** (1) $\Longrightarrow$ (2): Tegyük fel, hogy $R$ Gauss-gyűrű. A 3.19. Tételben beláttuk, hogy bármely két $R$-beli elemnek létezik legnagyobb közös osztója. Tegyük fel, hogy $a_1, a_2, a_3 \ldots \in R$ egy végtelen szigorúan csökkenő sorozat az oszthatóság szerinti részbenrendezésben: $\cdots \mid a_3 \mid a_2 \mid a_1$, és itt mindegyik oszthatóságnál valódi osztóról van szó (azaz $a_{i+1} \nsim a_i$). Legyen $a_1$ irreducibilis felbontása $a_1 \sim \prod p_i^{\alpha_i}$. A 3.19. Tétel (1) állítása szerint $a_1$-nek asszociáltság erejéig csak véges sok osztója van (hány darab?). Ez ellentmondás, mert $a_1, a_2, a_3, \ldots$ mind osztói $a_1$-nek (miért?), és páronként nem asszociáltak (miért?). (Hogyan kell módosítani a bizonyítást akkor, ha $a_1$ egység, illetve akkor, ha $a_1 = 0$?)

(2) $\Longrightarrow$ (3): Ez rögtön következik a 3.15. Tételből.

(3) $\Longrightarrow$ (1): Tegyük fel, hogy az $(R/\sim; |)$ részbenrendezett halmaz teljesíti a leszállólánc-feltételt, és $R$-ben minden irreducibilis elem prím. Először azt bizonyítjuk, hogy minden nemnulla elem irreducibilisek szorzatára bontható. Legyen NIF azon nemnulla $R$-beli elemek halmaza, amelyeknek nincs irreducibilis faktorizációja. Tegyük fel, hogy NIF $\neq \emptyset$ (indirekt feltevés), és legyen $a_1 \in$ NIF. Ekkor $a_1$ nem egység (hiszen az egységeknek van irreducibilis faktorizációjuk, mégpedig az üres szorzat), és $a_1$ nem is irreducibilis (hiszen az irreducibilis elemeknek van irreducibilis faktorizációjuk, mégpedig egytényezős szorzat). Tehát $a_1 \nsim 0, 1$ és nem is irreducibilis, így (a 3.12. Definíció szerint) van nemtriviális faktorizációja: léteznek olyan $b, c \in R$ elemek, amelyekre $a_1 = bc$ és $b \nsim a_1$, $c \nsim a_1$. A $b$ és $c$ elemek közül legalább az egyik NIF-ben van, ugyanis ellenkező esetben $b$-nek és $c$-nek is lenne irreducibilis faktorizációja, és ezeket egymás mellé biggyesztve megkapnánk $a_1$ egy irreducibilis faktorizációját, ami ellentmond annak, hogy $a_1 \in$ NIF. Jelölje $a_2$ azt az elemet $b$ és $c$ közül, amelyik NIF-ben van (ha mindkettő NIF-beli, akkor bármelyiket választhatjuk $a_2$-nek). Ekkor $a_2$ egy NIF-beli valódi osztója $a_1$-nek (miért?). Ezzel beláttuk, hogy minden NIF-beli elemnek van NIF-beli valódi osztója. Így tehát $a_2$-nek is van NIF-beli valódi osztója, legyen ez $a_3$. Hasonlóképpen $a_3$-nak is van NIF-beli valódi osztója, és így tovább. Az $a_1, a_2, a_3, \ldots$ elemek egy végtelen, szigorúan csökkenő sorozatot alkotnak az $(R/\sim; |)$ részbenrendezett halmazban, tehát az mégsem teljesíti a leszállólánc-feltételt. Ez az ellentmondás azt mutatja, hogy az indirekt feltevésünk hamis volt: NIF $= \emptyset$, vagyis minden nemnulla $R$-beli elemnek van irreducibilis faktorizációja.

Az unicitás bizonyítása hasonló módszerrel történik: legyen NEF azon nemnulla $R$-beli elemek halmaza, amelyeknek nem egyértelmű az irreducibilis faktorizációja. Tegyük fel, hogy NEF $\neq \emptyset$ (indirekt feltevés); ebből fogunk egy végtelen leszálló láncot konstruálni. Legyen $a_1 \in$ NEF, ekkor $a_1$-nek van két lényegesen különböző irreducibilis faktorizációja (azaz nem csak sorrendben és/vagy asszociáltságban térnek el egymástól): $a_1 \sim p_1 \cdot \ldots \cdot p_n$, illetve $a_1 \sim q_1 \cdot \ldots \cdot q_m$. Ekkor

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n \sim q_1 \cdot q_2 \cdot \ldots \cdot q_m, \qquad (\clubsuit)$$

és itt a bal oldal szemlátomást osztható $p_1$-gyel, így a jobb oldal is osztható vele: $p_1 \mid q_1 \cdot \ldots \cdot q_m$. Mivel $p_1$ irreducibilis, a tételbeli (3) feltevés miatt prím is. Ekkor tehát van olyan $i \in \{1, \ldots, m\}$, amelyre $p_1 \mid q_i$ (a prímtulajdonságból könnyen levezethető, hogy kettőnél több tényezős szorzatokra is igaz, hogy ha $p_1$ osztója egy szorzatnak, akkor osztója valamelyik tényezőjének). A jelölés megkönnyítése céljából (és az általánosság megszorítása nélkül) tegyük fel, hogy $i = 1$. Mivel $q_1$ irreducibilis (és $p_1$ nem egység), a $p_1 \mid q_1$ oszthatóság nem lehet valódi, azaz $p_1 \sim q_1$. Így ($\clubsuit$) mindkét oldalát egyszerűsíthetjük $p_1$-gyel (vagy $q_1$-gyel, ízlés szerint), és a két oldal még mindig asszociált marad: $a_1/p_1 \sim p_2 \cdot \ldots \cdot p_n \sim q_2 \cdot \ldots \cdot q_m$ (miért?). (Itt $a_1/p_1$ nem osztást jelöl, hanem azt, hogy „hányszor van meg" $a_1$-ben $p_1$). Ez a két faktorizációja az $a_2 := a_1/p_1$ elemnek lényegesen különböző (miért?), tehát $a_2 \in$ NEF, és $a_2$ valódi osztója $a_1$-nek (miért?). Ezzel beláttuk, hogy minden NEF-beli elemnek van NEF-beli valódi osztója, és innen ugyanúgy juthatunk ellentmondásra, mint az egzisztencia bizonyításánál. □

**3.22. Tétel.** Ha $R$ Gauss-gyűrű, akkor $R[x]$ is az.

**Bizonyítás.** Nem bizonyítjuk. □

**3.23. Következmény.** Ha $K$ test, akkor $K[x]$ és $K[x, y] \cong K[x][y]$ Gauss-gyűrűk (és hasonlóan $K[x_1, \ldots, x_n]$ is minden $n$ természetes számra). Az egész együtthatós polinomok $\mathbb{Z}[x]$ gyűrűje is Gauss-gyűrű.

**Bizonyítás.** Következik a fenti tételből, és abból, hogy $K$ és $\mathbb{Z}$ Gauss-gyűrűk. □

## Főideálgyűrűk

**3.24. Állítás.** Bármely $a, b \in R$ esetén érvényesek az alábbi ekvivalenciák:

(1) $a \mid b \iff \langle a \rangle \supseteq \langle b \rangle$;

(2) $a \sim b \iff \langle a \rangle = \langle b \rangle$;

(3) $a \sim 1 \iff \langle a \rangle = R$.

**Bizonyítás.** Emlékeztető: mivel $R$ integritástartomány, az 1.74. Következmény szerint $\langle a \rangle = \{ra : r \in R\}$. Tehát $\langle a \rangle$ nem más, mint $\langle a \rangle$ többszöröseinek, vagyis az $a$-val osztható elemeknek) a halmaza:

$$\langle a \rangle = \{t \in R : a \mid t\}. \qquad (\spadesuit)$$

(1) Tegyük fel, hogy $a \mid b$, és legyen $t \in \langle b \rangle$. Ekkor ($\spadesuit$) szerint $b \mid t$. Így tehát $a \mid t$ (miért?), ami ($\spadesuit$) alapján azt jelenti, hogy $t \in \langle a \rangle$. Ezzel beláttuk, hogy $\langle a \rangle \supseteq \langle b \rangle$.

A másik irány igazolásához tegyük fel, hogy $\langle a \rangle \supseteq \langle b \rangle$. Ebből $b \in \langle b \rangle$ miatt rögtön következik, hogy $b \in \langle a \rangle$. Ez pedig ($\spadesuit$) szerint azt jelenti, hogy $a \mid b$.

(2) Ez egyszerű következménye az első résznek:

$$a \sim b \overset{3.7}{\iff} a \mid b \text{ és } b \mid a \overset{3.24/(1)}{\iff} \langle a \rangle \supseteq \langle b \rangle \text{ és } \langle b \rangle \supseteq \langle a \rangle \iff \langle a \rangle = \langle b \rangle.$$

(3) Ez egyszerű speciális esete az előzőnek ($b = 1$), hiszen $\langle 1 \rangle = R$ (miért?). □

**3.25. Következmény.** Az $a, b \in R$ elemeknek a $d \in R$ elem akkor és csak akkor legnagyobb közös osztója, ha $\langle d \rangle$ a legszűkebb olyan főideál, ami tartalmazza $\langle a \rangle$-t is és $\langle b \rangle$-t is.

**Bizonyítás.** Nem kell mást tennünk, mint a 3.24. Állítás segítségével átfogalmazni a legnagyobb közös osztó definícióját főideálokkal: $d \sim \operatorname{lnko}(a, b)$ akkor és csak akkor teljesül, ha

(i) $\langle d \rangle \supseteq \langle a \rangle$ és $\langle d \rangle \supseteq \langle b \rangle$;

(ii) $\forall k \in R : (\langle k \rangle \supseteq \langle a \rangle \text{ és } \langle k \rangle \supseteq \langle b \rangle) \implies \langle k \rangle \supseteq \langle d \rangle$.

Az (i) feltétel azt jelenti, hogy $\langle d \rangle$ tartalmazza az $\langle a \rangle$-t és $\langle b \rangle$-t is, a (ii) feltétel pedig azt jelenti, hogy az ilyen tulajdonságú főideálok között $\langle d \rangle$ a legszűkebb. □

**3.26. Megjegyzés.** A legszűkebb ideál (nemcsak a főideálok, hanem az összes ideálok között), ami tartalmazza $\langle a \rangle$-t és $\langle b \rangle$-t is, nem más, mint $\langle a \rangle + \langle b \rangle$ (ez az ideálhálóbeli egyesítés, lásd az 1.76. Tételt és az 1.77. Megjegyzést). Csakhogy $\langle a \rangle + \langle b \rangle$ nem biztos, hogy főideál, és az sem biztos, hogy létezik $\operatorname{lnko}(a, b)$.

**3.27. Definíció.** Az $R$ integritástartományt ***főideálgyűrűnek*** nevezzük, ha minden ideálja főideál, azaz minden $I \lhd R$ ideálhoz létezik olyan $a \in R$ elem, amelyre $I = \langle a \rangle$.

**3.28. Állítás.** Főideálgyűrűben bármely két elemnek létezik legnagyobb közös osztója (és így legkisebb közös többszöröse is), és az előáll a két elem „lineáris kombinációjaként”: $\forall a, b \in R\ \exists x, y \in R$: $ax + by \sim \operatorname{lnko}(a, b)$.

**Bizonyítás.** Tegyük fel, hogy $R$ főideálgyűrű, és legyen $a, b \in R$. Ekkor a legszűkebb olyan (fő)ideál, ami tartalmazza $\langle a \rangle$-t is és $\langle b \rangle$-t is, nem más, mint $\langle a \rangle \vee \langle b \rangle = \langle a \rangle + \langle b \rangle$ (lásd a 3.26. Megjegyzést). Mivel $R$-ben minden ideál főideál, van olyan $d \in R$, amelyre $\langle a \rangle + \langle b \rangle = \langle d \rangle$. A 3.25. Következmény szerint $d \sim \operatorname{lnko}(a, b)$, továbbá $d \in \langle a \rangle + \langle b \rangle$ miatt $d$ előáll $ax + by$ $(x, y \in R)$ alakban. □

**3.29. Következmény.** Főideálgyűrűben az $ax + by = c$ „diofantoszi egyenletnek” akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a, b) \mid c$. Az általános megoldás ugyanúgy kapható meg egy partikuláris megoldásból, mint az egész számok gyűrűjében.

**Bizonyítás.** A bizonyítás szinte szó szerint ugyanaz, mint az egész számok gyűrűjében (lásd Algebra és számelmélet 3), csak itt a partikuláris megoldást nem az euklideszi algoritmusból, hanem a 3.28. Állításból kapjuk. □

**3.30. Definíció.** Az $R$ integritástartományt ***euklideszi gyűrűnek*** nevezzük, ha létezik olyan $\|\cdot\| : R \to \mathbb{N}_0$, $a \mapsto \|a\|$ leképezés (úgynevezett ***euklideszi norma***), amire teljesülnek az alábbiak tetszőleges $a \in R$ és $b \in R \setminus \{0\}$ esetén:

(1) $\|a\| = 0 \iff a = 0$;

(2) $a \mid b \implies \|a\| \leq \|b\|$;

(3) $\exists q, r \in R : a = bq + r$ és $\|r\| < \|b\|$.

**3.31. Tétel.** Minden euklideszi gyűrű főideálgyűrű.

**Bizonyítás.** Legyen $R$ eulideszi gyűrű az $\|\cdot\|$ euklideszi normával, és legyen $I \lhd R$. Ha $I = \{0\}$, akkor $I$ nyilván főideál (miért?) tehát feltehetjük, hogy $I \neq \{0\}$. Legyen $d \in I \setminus \{0\}$ az $I$-beli nemnulla elemek közül a legkisebb normájú (ha több olyan elem van, aminek a normája a lehető legkisebb, akkor bármelyiket választhatjuk). Meg fogjuk mutatni, hogy $I = \langle d \rangle$. Az $I \subseteq \langle d \rangle$ tartalmazás igazolásához tekintsünk egy tetszőleges $a \in I$ elemet. Az euklideszi gyűrű definíciója szerint vannak olyan $q, r \in R$ elemek, amelyekre $a = dq + r$ és $\|r\| < \|d\|$ ($a$-t osztjuk $d$-vel maradékosan). Ekkor $r = a - dq$, tehát $r \in I$ (miért?). Mivel $\|r\| < \|d\|$, és $d$ normája volt a legkisebb az $I$-beli nemnulla elemek között, csak

$r = 0$ lehetséges. Így tehát $a = dq$, ami azt jelenti, hogy $a \in \langle d \rangle$. Ezzel beláttuk, hogy $I \subseteq \langle d \rangle$, a más irányú tartalmazás pedig világos (miért?), tehát $I = \langle d \rangle$. □

**3.32. Megjegyzés.** A tétel megfordítása nem igaz: létezik olyan főideálgyűrű, amely nem euklideszi. Ilyen például a $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ gyűrű, ahol $\omega = \frac{1+\sqrt{19}i}{2}$.

**3.33. Következmény.** Az egész számok gyűrűje, minden test feletti polinomgyűrű, valamint a Gauss-egészek gyűrűje főideálgyűrű.

**Bizonyítás.** A fenti gyűrűk mindegyikéről tudjuk, hogy euklideszi. (Honnan tudjuk? Mi az euklideszi norma?) □

**3.34. Tétel.** Minden főideálgyűrű Gauss-gyűrű.

**Bizonyítás.** Ha $R$ főideálgyűrű, akkor a 3.28. Állítás szerint bármely két elemének van legnagyobb közös osztója, így a 3.21. Tétel szerint elég azt megmutatnunk, hogy az $(R/\sim; |)$ részbenrendezett halmaz teljesíti a leszállólánc-feltételt. Tegyük fel tehát, hogy $a_1, a_2, \ldots$ egy leszálló lánc az oszthatóság szerinti részbenrendezésben: $\cdots \mid a_3 \mid a_2 \mid a_1$. Azt kell igazolnunk, hogy van olyan $k$ index, hogy $a_k \sim a_{k+1} \sim \cdots$. Legyen $I_j = \langle a_j \rangle$ minden $j \in \mathbb{N}$ esetén; a 3.24. Állítás szerint $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, és azt kell igazolnunk, hogy van olyan $k$ index, hogy $I_k = I_{k+1} = \cdots$. Ideálok uniója általában nem ideál (ugye?), de mivel itt „egymásba skatulyázott" ideálokról van szó, $I = I_1 \cup I_2 \cup I_3 \cup \cdots$ ideál $R$-ben. (Az összeadásra való zártság például így ellenőrizhető: ha $a, b \in I$, akkor van olyan $i$ és $j$, hogy $a \in I_i$ és $b \in I_j$. Ekkor $k = \max(i, j)$ esetén $a, b \in I_k$. Mivel $I_k$ ideál, $a + b \in I_k$, és ebből következik, hogy $a + b \in I$. Az ideál definíciójában szereplő többi feltétel hasonlóan, sőt még egyszerűbben ellenőrizhető (HF).) Tudjuk, hogy $R$-ben minden ideál főideál, tehát $I = \langle d \rangle$ alkalmas $d \in I$ elemre. Mivel $d \in I_1 \cup I_2 \cup I_3 \cup \cdots$, van olyan $k$, amelyre $d \in I_k$. Ebből következik, hogy $I = \langle d \rangle \subseteq I_k \subseteq I$, ez pedig csak akkor lehetséges, ha $I = \langle d \rangle = I_k = I$. Ez pedig azt jelenti, hogy $I_k = I_{k+1} = \cdots = I$ (miért?). □

**3.35. Megjegyzés.** A tétel megfordítása nem igaz: létezik olyan Gauss-gyűrű, ami nem főideálgyűrű. Ilyenek például a $\mathbb{Z}[x]$ és $K[x, y]$ gyűrűk (tetszőleges $K$ test esetén).

**Bizonyítás.** A 3.23. Következmény szerint $\mathbb{Z}[x]$ és $K[x, y]$ Gauss-gyűrűk. A $\mathbb{Z}[x]$ gyűrűben $\langle 2, x \rangle$ olyan ideál, ami nem főideál, a $K[x, y]$ gyűrűben pedig $\langle x, y \rangle$ nem főideál. Csak az elsőt ellenőrizzük, a másik HF. Tegyük fel, hogy $\langle d \rangle = \langle 2, x \rangle$ valamilyen $d \in \mathbb{Z}[x]$ polinomra. A 3.24. Állítás alapján $\langle d \rangle = \langle 2, x \rangle \supseteq \langle 2 \rangle \implies d \mid 2$, és hasonlóan $\langle d \rangle = \langle 2, x \rangle \supseteq \langle x \rangle \implies d \mid x$. Olyan $d \in \mathbb{Z}[x]$ polinom, amire $d \mid 2$ és $d \mid x$ teljesül, csak kettő van: $d = \pm 1$ (miért?). Azt kaptuk tehát, hogy $\langle \pm 1 \rangle = \langle 2, x \rangle$, ami lehetetlen (miért?). □

**3.36. Következmény.** Az egész számok gyűrűje, minden test feletti polinomgyűrű, valamint a Gauss-egészek gyűrűje Gauss-gyűrű.

**3.37. Tétel.** Ha $R$ főideálgyűrű és $m \in R \setminus \{0\}$, akkor az $R/\langle m \rangle$ faktorgyűrű akkor és csak akkor test, ha $m$ irreducibilis.

**Bizonyítás.** Ha $m \sim 1$, akkor $R/\langle m \rangle$ egyelemű gyűrű (miért?), így nem lehet test. Ha $m \nsim 1$, akkor $R/\langle m \rangle$ legalább kételemű kommutatív egységelemes gyűrű (miért?), tehát azt kell megvizsgálnunk, hogy van-e minden nemnulla elemének multiplikatív inverze. Tekintsük először azt az esetet, amikor $m$ nem irreducibilis, azaz van nemtriviális faktorizációja: $m = ab$, ahol $a \nsim m$ és $b \nsim m$. Ekkor $\overline{a} = a + \langle m \rangle$ és $\overline{b} = b + \langle m \rangle$ zérusosztók az $R/\langle m \rangle$ gyűrűben (miért?), így az nem test (sőt, még csak nem is integritástartomány). Most tegyük fel, hogy $m$ irreducibilis, és legyen $\overline{a} = a + \langle m \rangle \in R/\langle m \rangle$. Ha $\overline{a} \neq \overline{0}$, akkor $m \nmid a$, és $m$ irreducibilitása miatt ez azt jelenti, hogy $a$ és $m$ relatív prímek: $\operatorname{lnko}(a, m) \sim 1$ (miért?). A 3.28. Állítás szerint vannak olyan $x, y \in R$ elemek, amelyekre $ax + my = 1$. Ebből következik, hogy $\overline{a} \cdot \overline{x} = \overline{1}$ (miért?), vagyis $\overline{a}$ multiplikatív inverze $\overline{x}$. Ezzel megmutattuk, hogy $R/\langle m \rangle$ minden nemnulla elemének van multiplikatív inverze, tehát $R/\langle m \rangle$ test. □