1. Részgyűrű

Részgyűrű
A gyűrűelmélet alapfogalmait ismerjük Algebra1-ből.
HF: Ismételjük át a jegyzetből a teljes 2.2 szakaszt.

2.2.25. Definíció
Ha R gyűrű, akkor $S \subseteq R$ *részgyűrű*, ha S gyűrű R műveleteire, és *résztest*, ha maga is test R műveleteire nézve.

2.2.26. Feladat (HF)
S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik.

Egy részgyűrű egységeleme (ha van is) nem feltétlenül egyenlő a gyűrű egységelemével, de akkor igen, ha R nullosztómentes (2.2.36. Gyakorlat, 2.4.29. Feladat). Ha T test, akkor az $S \leq T$ részgyűrű akkor résztest, ha minden nem nulla elemének az T-beli inverzét is tartalmazza.

Generált részgyűrű
Ahogy csoportok esetében, egy R gyűrű X részhalmaza által generált részgyűrűje az R legszűkebb részgyűrűje, ami X-et tartalmazza, ami egyértelműen létezik, mint az X-et tartalmazó részgyűrűk metszete (5.1.1. Definíció). Ennek elemeit általános gyűrűben nehéz leírni (mint a csoportok esetében is), a kommutatív esetben azonban a generátorok egész együtthatós polinomjaiból áll.

5.1.2. Állítás (HF)
Ha R kommutatív egységelemes gyűrű és $r_1, \ldots, r_n \in R$, akkor az $r_1, \ldots, r_n$ *és az egységelem* által generált részgyűrű a $p(r_1, \ldots, r_n)$ alakú kifejezések halmaza, ahol p befutja $\mathbb{Z}[x_1, \ldots, x_n]$ elemeit.

Ahogy lineáris algebrában is, egy polinomba való behelyettesítéskor a konstans tagot R egységelemével kell megszorozni. Mindez kapcsolatban áll a polinomfüggvény fogalmával is (lásd a 2.4.30. és a 2.6.9. Gyakorlatokat).

2. Ferdetest

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak. Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Ha $z = p + qi$ és $w = r + si$, akkor $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = pE + qI + rJ + sK$ (itt E az egységmátrix). Két ilyet úgy szorozhatunk össze, hogy a disztributív szabály alapján kibontjuk a szorzatot, az E, I, J, K szorzását elvégezzük úgy, ahogy a kvaterniócsoportban tanultuk, majd összevonunk. Ezentúl E, I, J, K helyett rendre $1, i, j, k$-t fogunk írni. A kapott $p + qi + rj + sk$ elemek a *kvaterniók* ($p, q, r, s \in \mathbb{R}$).

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió *konjugáltja* $\overline{\alpha} = p - qi - rj - sk$, *normája* $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$. Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese, azaz $\left(1/\sqrt{N(\alpha)}\right)M$ unitér.

A Gyakorlat utolsó két állítása azért teljesül, mert $(MN)^* = N^*M^*$ és $\det(MN) = \det(M)\det(N)$.

Tehát ha $\alpha \neq 0$, akkor α inverze $\Big(1/N(\alpha)\Big)\overline{\alpha}$. Így $\mathbb{K}$ *ferdetest.*

Mivel $ij = k \neq -k = ji$, ezért $\mathbb{K}$ nem kommutatív, azaz nem test.

Véges nullosztómentes gyűrű test

5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben. Így elég belátni, hogy véges nullosztómentes gyűrű *ferde*test.

Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az *egyszerűsítési szabály:*
ha $ac = bc$ (vagy $ca = cb$), de $c \neq 0$, akkor $a = b$.

Bizonyítás: Ha $ac = bc$, akkor $(a - b)c = 0$. Mivel $c \neq 0$, a nullosztómentesség miatt $a - b = 0$. □

Véges nullosztómentes gyűrűk (bizonyítás)

5.3.4. Lemma
Ha R nullosztómentes, $e \in R$, és van olyan $0 \neq r \in R$, melyre $er = r$, akkor e egységelem.

Bizonyítás: Minden t-re $ter = tr$, az r-rel egyszerűsítve $te = t$. Tehát e jobboldali egységelem. Speciálisan $re = r$. Ugyanezt balról csinálva kapjuk, hogy e bal egységelem is. □

Bizonyítás (véges nullosztómentes gyűrű test)
Legyen $R = \{r_1, \ldots, r_n\}$ és $0 \neq r$. Ekkor $r_1 r, \ldots, r_n r$ a nullosztómentesség miatt csupa különböző elem. Mivel R véges, minden elemét megkapjuk. Speciálisan $r = r_i r$ esetén a Lemma miatt $e = r_i$ egységelem. Továbbá $e = r_j r$ esetén r-nek balinverze r_j. Ugyanígy van jobbinverze is. Ezek egyenlők (Algebra1, vagy 2.2.10. Feladat). □

3. Homomorfizmus, ideál

Izomorfizmus és homomorfizmus

Definíció
Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$. Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés *gyűrűhomomorfizmus,* ha az összeadást és a szorzást is *tartja*:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.
Ha ψ kölcsönösen egyértelmű is, akkor ψ *izomorfizmus.*

Példák

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ *maradéka mod* n.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i *behelyettesítése*).

(3) A $p + qi$ alakú kvaterniók $\mathbb{C}$-vel izomorf résztestet alkotnak.

Elemi tulajdonságok

Láttuk korábban (2.2.44. Feladat)
Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor φ az *egységelemet az egységelembe* viszi, és *inverz képe a kép inverze* lesz (azaz φ az inverzképzés műveletét is tartja).

Következmény
Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi, azaz $\varphi(0) = 0$, továbbá $\varphi(-r) = -\varphi(r)$.

Példa (5.1.20. Gyakorlat)
$\varphi : \mathbb{R} \to \mathbb{R}^{2\times 2}$, $\varphi(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$ gyűrűhomomorfizmus, de $\mathbb{R}$ egységelemét nem viszi $\mathbb{R}^{2\times 2}$ egységelemébe.

Homomorfizmus képe és magja

5.1.3, 5.1.4. Definíció
Minden gyűrűhomomorfizmus csoporthomomorfizmus is az additív csoportok között, így lehet *képről* és *magról* beszélni. Mindkettő nyilván részgyűrű.

5.1.5. Tétel
Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$. Ha $a \in I = \mathrm{Ker}(\varphi)$, akkor $\varphi(a) = 0$. Ezért $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. Azaz $ra \in I$, és hasonlóan $ar \in I$. A megfordítás *faktorgyűrű* segítségével később.

Bal- és jobbideálok

5.1.6. Definíció
Egy R gyűrű egy I részhalmaza *balideál*, ha az összeadásra nézve *részcsoport*, és minden $a \in I$, $r \in R$ esetén $ra \in I$. Az I *jobbideál*, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$. Az I (kétoldali) *ideál*, ha bal- és jobbideál is. Jele: $I \triangleleft R$.

Példa
A *páros számok* ideált alkotnak $\mathbb{Z}$-ben. Mert páros számok összege is páros, a nulla is páros, és páros szám ellentettje is páros, azaz *részcsoport*; továbbá páros szám minden egész számszorosa is páros.
Általában: Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja az *n-nel osztható számok*ból álló ideál. Jele: (n).
Speciálisan $(2) = (-2) =$ az összes páros szám.

Generált ideál

5.1.8. Definíció
Ha X részhalmaza az R gyűrűnek, akkor R-nek az X-et tartalmazó legszűkebb ideálját az X által *generált* ideálnak nevezzük. Hasonlóan: generált bal-, illetve jobbideál.

Ez egyértelműen létezik, mint az X-et tartalmazó ideálok metszete.

5.1.9. Állítás (HF)
Ha R egységelemes gyűrű és $s_1, \ldots, s_n \in R$, akkor az $s_1, \ldots, s_n$ által generált balideál az $r_1 s_1 + \ldots + r_n s_n$ alakú elemek halmaza, ahol $r_1, \ldots, r_n$ befutja R elemeit. Jele: $(s_1, \ldots, s_n)$.

A bizonyítás nagyon hasonló ahhoz, ahogy Abel-csoportok generált részcsoportjainak elemeit írtuk le (4.6.1. Állítás). Ha R kommutatív, akkor a balidálok pontosan az ideálok, ezért az előző állítás a generált ideál elemeit adja meg.

Főideál

5.1.10. Definíció
Legyen R *kommutatív, egységelemes* gyűrű és $s \in R$ rögzített. Az s által generált ideál, azaz s összes többszöröseinek halmaza: $(s) = \{rs \ : \ r \in R\}$ az s által generált *főideál*.

Példa
$R = \mathbb{R}[x]$. Az $(x-1)$ az $x-1$-gyel osztható polinomokból áll.
Ezek azok, melyeknek gyöke az 1 (gyöktényező kiemelhető).
Ezért ha $\varphi : \mathbb{R}[x] \to \mathbb{R}$, $\varphi(f) = f(1)$ (φ az 1 behelyettesítése),
akkor $\mathrm{Ker}(\varphi) = (x-1)$.

HF: Legyen $\varphi : \mathbb{R}[x] \to \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Ekkor $\mathrm{Ker}(\varphi) = (x^2+1)$.
Segítség: ha i gyöke $f \in \mathbb{R}[x]$-nek, akkor a konjugáltja, azaz $-i$ is gyöke f-nek (4.7.7. Gyakorlat).

4. Főideálgyűrűk

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.
Állítás: A $\mathbb{Z}$ gyűrűben nincs más ideál.

Bizonyítás
Legyen I nem nulla ideál $\mathbb{Z}$-ben, és n a legkisebb *abszolút értékű nem nulla* eleme. Belátjuk, hogy $I = (n)$.
Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.
Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$. De $r = k - nq \in I$, mert I zárt a többszörözésre és a kivonásra. Mivel $|n|$ minimális volt, így r csak nulla lehet. Tehát $k \in (n)$, azaz $I \subseteq (n)$. □

HF: Hasonlítsuk össze ezt annak bizonyításával, hogy ciklikus csoport részcsoportja is ciklikus (4.3.26. Lemma).

Ideálok a polinomok között

Legyen R *kommutatív, egységelemes* gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).
Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás
Legyen I nem nulla ideál $T[x]$-ben, és g a legkisebb *fokú nem nulla* eleme. Belátjuk, hogy $I = (g)$.
Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.
Legyen $f \in I$, ekkor $f = qq+r$, ahol $\mathrm{gr}(r) < \mathrm{gr}(g)$ vagy $r = 0$. De $r = f - gq \in I$, mert I zárt a többszörözésre és a kivonásra. Mivel $\mathrm{gr}(g)$ minimális volt, így r csak nulla lehet. Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Nyilvánvaló a hasonlóság a $\mathbb{Z}$-beli bizonyítással: *maradékos osztásra* van szükség.

Euklideszi gyűrű

5.5.1. Definíció
Euklideszi gyűrű: „elvégezhető benne a maradékos osztás."
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák
$\mathbb{Z}$ euklideszi: $\varphi(k) = |k|$.
$T[x]$ euklideszi, ha T test: $\varphi(f) = \mathrm{gr}(f)$.
Gauss-egészek: $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.
Ez is euklideszi gyűrű: $\varphi(a + bi) = a^2 + b^2$.
Bizonyítás: Freud Róbert és Gyarmati Edit számelmélet könyve.

Euklideszi gyűrű főideálgyűrű

5.5.3. Tétel
Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás
Legyen I nem nulla ideál R-ben, és g a legkisebb φ-*értékű nem nulla* eleme. Belátjuk, hogy $I = (g)$.
Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.
Legyen $f \in I$, ekkor $f = gq+r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$. De $r = f - gq \in I$, mert I zárt a többszörözésre és a kivonásra. Mivel $\varphi(g)$ minimális volt, így r csak nulla lehet. Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Főideálgyűrű: szokásos gyűrű, melynek minden ideálja főideál. Ezekben érvényes a *számelmélet alaptétele*.

5. Ideálok és számelmélet

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)
Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r *osztója* s-nek, ha van olyan t *a gyűrűben*, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ *nem nulla, nem egység.*
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r *felbonthatatlan*: nincs *nemtriviális* felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r *prím:* ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R *alaptételes*: minden nullától és egységtől különböző elem *egyértelműen* előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$, $T[x]$ (T test), $\mathbb{Z}[x]$.
$a, b \in R$ *kitüntetett közös osztója* d, ha

(1) d közös osztó, azaz $d \mid a$ és $d \mid b$;

(2) d mindegyik közös osztónak többszöröse.

Az alapfogalmak összefüggései

3.1.27. Gyakorlat
Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

3.1.28. Gyakorlat
Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel *egyértelműségi* állítása.

3.1.22. és 3.1.26. Gyakorlatok
Alaptételes gyűrűben

(1) bármely két elemnek van kitüntetett közös osztója;

(2) minden felbonthatatlan elem prím.

Ideálok és oszthatóság

5.1.10. Definíció: (r) az r összes többszöröséből áll: *főideál.*

5.5.4. Lemma
$r \mid s \iff (r) \supseteq (s)$. □

„Megfordul"! Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

5.5.5. Lemma
Legyen R szokásos gyűrű és $a, b \in R$. Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója. (A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás
Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$. Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

Euklideszi és főideálgyűrű alaptételes

Tétel (5.5.9. Következmény)
Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

Bizonyítás
Ha $(a, b) = (d)$, akkor d az a és b *kitüntetett közös osztója.* Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek *van* kitüntetett közös osztója. Így érvényes az alaptétel egyértelműségi állítása.
A felbontás *létezését* nem bizonyítjuk.

$R = \mathbb{Z}[x]$ *alaptételes* gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ± 1, ± 2, és $2 \nmid x$.
$(2, x)$ azokból a polinomokból áll, melyek konstans tagja páros. Az 1 nem ilyen, tehát $(2, x) \neq (1)$, ezért $(2, x)$ *nem főideál.*
Tehát $\mathbb{Z}[x]$ nem főideálgyűrű, és így nem is euklideszi, noha alaptételes.

Példa nem alaptételes gyűrűre

3.1.34. Feladat
Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek *nincs kitüntetett közös osztója.*
A 3 *felbonthatatlan, de nem prím.*
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan, de 3 nem egységszerese $2 \pm i\sqrt{5}$-nek, így ez a 9-nek két, lényegesen különböző felbontása. Ezért ez a gyűrű *nem alaptételes.*

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához. A kiút az, hogy a $(9, 3(2 + i\sqrt{5}))$ *ideál* veszi át a hiányzó kitüntetett közös osztó szerepét. Ez a témakör az *algebrai számelmélet.*

Direkt szorzat

5.1.17. Definíció
Az R és S gyűrűk *direkt szorzatának* alaphalmaza $R \times S$, ahol a műveleteket *komponensenként* végezzük:
$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ és $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$.

HF: Ez tényleg gyűrű. Hasonló a definíció kettőnél több tényező esetében is.
A belső jellemzés mint csoportokra (normálosztó helyett ideál):

5.1.18. Állítás
Ha I és J ideálok az R gyűrűben, a csoportelméleti $I + J$ komplexusösszeg az egész R, továbbá $I \cap J = 0$, akkor $R \cong I \times J$.

A bizonyítás ötlete: Ha $I \cap J = 0$, $a \in I$, $b \in J$, akkor $ab = 0$.