1. Faktorgyűrű

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 $ab = 0$.

Faktorcsoport.

Állítás
Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés
Legyen G kommutatív csoport a $+$ műveletre. Ha N részcsoport G-ben, akkor tehát normálosztó is. A G/N *faktorcsoport* elemei az N szerinti mellékosztályok
(ezek a $g + N$ halmazok, ahol g befutja G-t).
Az összeadás: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$. A G/N csoport *egységeleme* az $N = 0 + N$ mellékosztály, a $g + N$ *inverze* $(-g) + N$. A $\psi : g \mapsto (g + N)$ leképezés a *természetes homomorfizmus* G-ből G/N-re. Ennek *képe* az egész G/N, *magja* N.

Faktorgyűrű.

Állítás
Ha I ideál R-ben, akkor az R^+/I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I *faktorgyűrűt* kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)
Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy *jóldefiniált*.
Azaz ha $r_1 + I = r_1' + I$ és $r_2 + I = r_2' + I$, akkor $r_1 r_2 + I = r_1' r_2' + I$.
$r_1 + I = r_1' + I \implies r_1 - r_1' \in I$ és $r_2 + I = r_2' + I \implies r_2 - r_2' \in I$.
De akkor $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$.
HF: Igazak erre a szorzásra a gyűrűaxiómák (szorzás asszociativitása, mindkét oldali disztributivitás); az $r \mapsto r + I$ természetes homomorfizmus szorzattartó is. □

Az egész számok faktorgyűrűi.

Állítás
$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás
$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\ (n)$. Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.
Másrészt $\psi(k_1)\psi(k_2) = \big(k_1+(n)\big)\big(k_2+(n)\big) = k_1 k_2 + (n)$.
Azaz $\psi(k_1 *_n k_2) = \psi(k_1)\psi(k_2)$. Összegtartás hasonló, HF. □

Példa a polinomgyűrűben.

Példa (5.2.6. Állítás)
„Számítsuk ki" az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt. $\quad I := (x^2+1)$.

$f+I = g+I \iff f-g \in I \iff x^2+1 \mid f-g$. Vagyis két polinom akkor van ugyanabban a mellékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják. A lehetséges maradékok a legfeljebb elsőfokú polinomok. Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b \in \mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I) = x^2+I = -1+\big((x^2+1)+I\big) = -1+I$.
HF: $\big((a+bx)+I\big)\big((c+dx)+I\big) = \big((ac-bd)+(ad+bc)x\big)+I$.
HF: $\big((a+bx)+I\big)+\big((c+dx)+I\big) = \big((a+c)+(b+d)x\big)+I$.
Azaz $a+bi \mapsto (a+bx)+I$ *izomorfizmus* $\mathbb{C} \to \mathbb{R}[x]/(x^2+1)$.

A homomorfizmustétel.

5.2.5 Homomorfizmustétel
Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ izomorf *csoportok*. Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (HF).

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése). Itt $\mathrm{Im}(\varphi) = \mathbb{C}$ és $\mathrm{Ker}(\varphi) = (x^2+1)$, ezért $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Megjegyzés: Ez csak akkor működik, ha $\mathbb{C}$ *már ismert!* Ha *meg akarjuk konstruálni* $\mathbb{C}$-t (vagy más testeket), akkor érdemes a faktorgyűrűt használni.

Négyelemű test.

5.2.10 Gyakorlat
A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,
mert $x^2+x=1+(x^2+x+1)$ és $x^2+x+1\in I$ (azaz x^2+x-nek az x^2+x+1-gyel való *osztási maradéka* 1).
Test, mert a táblázat szerint $A^{-1}=B$, $B^{-1}=A$, $E^{-1}=E$.

2. 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 $0\le r<|n|$. 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, alkalmazás és további példák legközelebb.

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 $f = qq + r$, 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 (legközelebb).