1. Egész együtthatós polinomok

Oszthatóság egész számmal
Emlékeztető (K3.1.3): Ha $f, g \in \mathbb{Z}[x]$, akkor $f \mid g$ akkor és csak akkor, ha van olyan $h \in \mathbb{Z}[x]$, hogy $g = fh$.

Állítás (K3.1.6)
Az $f(x) \in \mathbb{Z}[x]$ akkor és csak akkor osztható $\mathbb{Z}[x]$-ben a c egész számmal, ha f minden együtthatója osztható c-vel.

Bizonyítás
Ha $c \mid f(x)$, akkor van olyan $h(x) = b_0 + b_1x + \ldots + b_nx^n \in \mathbb{Z}[x]$, melyre $ch(x) = f(x)$. Ezért $f(x)$ együtthatói a cb_i számok, amik mind c-vel oszthatók.
Megfordítva: Legyen $f(x) = a_0 + a_1x + \ldots + a_nx^n$. Ha minden a_i osztható c-vel, akkor vannak olyan b_i egészek, hogy $cb_i = a_i$ minden i-re.
Így $f(x) = c(b_0 + b_1x + \ldots + b_nx^n)$, és a zárójelben egész együtthatós polinom áll. Ezért $c \mid f(x)$. $\square$

Primitív polinomok

Emlékeztető (K3.1. szakasz)
Egység: minden polinomnak osztója. $\mathbb{Z}$-ben, $\mathbb{Z}[x]$-ben csak a ± 1. Az $f = gh$ *triviális felbontás*, ha f és g valamelyike egység. Az f *felbonthatatlan*, más szóval *irreducibilis*, ha nem nulla, nem egység, és nincs nemtriviális felbontása.

Példa: az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ irreducibilisekre bontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Definíció (K3.4.1)
Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Példa: $60x^6 + 36x^4 + 90 = 6(10x^6 + 6x^4 + 15)$. Kiemeltük az együtthatók legnagyobb közös osztóját. Nyilván $(10, 6, 15) = 1$ (de nem páronként relatív prímek). Ezért $10x^6 + 6x^4 + 15$ már primitív polinom.

Felbonthatatlan konstans polinomok

Tétel (K3.4.2)
Ha egy n egész szám $\mathbb{Z}$-ben felbonthatatlan, akkor polinomként tekintve felbonthatatlan $\mathbb{Z}[x]$-ben is.

Bizonyítás
Mivel n felbonthatatlan $\mathbb{Z}$-ben, ezért nem nulla és nem egység. Tudjuk, hogy a $\mathbb{Z}$ és a $\mathbb{Z}[x]$ egységei ugyanazok: ± 1. Ezért n a $\mathbb{Z}[x]$-ben sem egység.
Kell: n minden felbontása triviális $\mathbb{Z}[x]$-ben. Tegyük fel, hogy $n = g(x)h(x)$, ahol $g, h \in \mathbb{Z}[x]$. Mindkét oldal fokát véve $0 = \mathrm{gr}(n) = \mathrm{gr}(g) + \mathrm{gr}(h)$ adódik. Ezért g és h is nem nulla konstans, azaz egész szám. Mivel n felbonthatatlan $\mathbb{Z}$-ben, ez a felbontás triviális, vagyis g és h egyike egység $\mathbb{Z}$-ben, így $\mathbb{Z}[x]$-ben is, és ezért az $n = g(x)h(x)$ felbontás tényleg triviális $\mathbb{Z}[x]$-ben. $\square$

Prím konstans polinomok
Emlékeztető (K3.1.25): $f \in \mathbb{Z}[x]$ *prím*, ha nem nulla, nem egység, és minden $g, h \in \mathbb{Z}[x]$ esetén, *ha* $f \mid gh$, *akkor* $f \mid g$ vagy $f \mid h$.

Gauss-lemma I (K3.4.3)
Ha $p \in \mathbb{Z}$ prím, akkor p a $\mathbb{Z}[x]$-ben is prím (konstans polinomként).

Bizonyítás
Mivel p prím, ezért nem nulla, és nem egység $\mathbb{Z}[x]$-ben sem. Tegyük fel, hogy $p \mid g(x)h(x)$, ahol $g(x) = a_0 + a_1x + \ldots + a_nx^n$ és $h(x) = b_0 + b_1x + \ldots + b_mx^m$. Indirekt feltevés: $p \nmid g$ és $p \nmid h$. Legyen i, illetve j a legnagyobb index, melyre $p \nmid a_i$, illetve $p \nmid b_j$. Mivel p prím $\mathbb{Z}$-ben, $p \nmid a_ib_j$. De minden más tag p-vel osztható a $c_{i+j} = a_0b_{j+i} + \ldots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \ldots + a_{i+j}b_0$ összegben, ami gh egy együtthatója. Így $p \nmid c_{i+j}$, ellentmondás. □

Az első Gauss-lemma első következménye

Gauss-lemma I, első következmény (K3.4.4)
Primitív polinomok szorzata is primitív.

Bizonyítás
Ha gh nem primitív, akkor van olyan $p \in \mathbb{Z}$ prím, amire $p \mid gh$. Ha g, h primitív, akkor $p \nmid g$ és $p \nmid h$, ez ellentmond Gauss I-nek. □

Állítás
Minden $f \in \mathbb{Q}[x]$ polinom felírható $(s/t)f_0$ alakban, ahol s és t relatív prím egészek, $f_0 \in \mathbb{Z}[x]$ pedig primitív.

Bizonyítás
Hozzuk f együtthatóit közös nevezőre, majd emeljük ki a számlálók legnagyobb közös osztóját, végül egyszerűsítsünk. □

Az első Gauss-lemma második következménye

Gauss-lemma I, második következmény (K3.4.5)
Legyen $f \in \mathbb{Z}[x]$ primitív. Ha $g \in \mathbb{Q}[x]$ és $h = fg \in \mathbb{Z}[x]$, akkor $g \in \mathbb{Z}[x]$. Így ha f osztója egy $h \in \mathbb{Z}[x]$ polinomnak $\mathbb{Q}[x]$-ben, akkor f osztója h-nak $\mathbb{Z}[x]$-ben is.

Bizonyítás
Az előző állítás szerint $g = (s/t)g_0$, ahol $(s, t) = 1$ és g_0 primitív.
Ekkor $th = sfg_0$. Ha p prímosztója t-nek, akkor $p \mid sfg_0$. Az első Gauss-lemma miatt $p \mid s$, vagy $p \mid f$, vagy $p \mid g_0$. Mindhárom lehetetlen, az első azért, mert t és s relatív prímek, a másik kettő azért, mert f és g_0 primitívek. A t számnak nincs tehát prímosztója, vagyis t egység, és így $g = (s/t)g_0$ tényleg egész együtthatós polinom. □

A második Gauss-lemma
Példa: $x^2 - 1 = \big[(2/3)x - (2/3)\big]\big[(3/2)x + (3/2)\big]$.
Ez az $x^2 - 1$ egy elbonyolított felbontása. Ki lehet javítani, ha az első tényezőt 3/2-del, a másodikat 2/3-dal szorozzuk. A második Gauss-lemma szerint ez mindig lehetséges.

Gauss-lemma II (K3.4.7)
Ha $0 \neq f \in \mathbb{Z}[x]$ és $f = gh$, ahol $g, h \in \mathbb{Q}[x]$, akkor g és h megszorozható racionális számokkal úgy, hogy a kapott g_1 és h_1 polinomok egész együtthatósak legyenek, és $f = g_1 h_1$ teljesüljön.

Bizonyítás
Legyen $g = rg_0$ és $h = sh_0$, ahol $r, s \in \mathbb{Q}$ és $g_0, h_0 \in \mathbb{Z}[x]$ primitív. Ekkor $f = (rs)(g_0 h_0)$. A Gauss-lemma I első következménye miatt $g_0 h_0$ primitív, így a második következménye miatt $rs \in \mathbb{Z}[x]$, azaz rs egész szám. Így a $g_1 = rsg_0$ és $h_1 = h_0$ jó választás. $\square$

Az irreducibilitás kapcsolata $\mathbb{Z}$ és $\mathbb{Q}$ fölött

(1) Ha $f \in \mathbb{Z}[x]$ nem konstans és irreducibilis $\mathbb{Z}$ fölött, akkor f irreducibilis $\mathbb{Q}$ fölött is.

(2) Ha f primitív és irreducibilis $\mathbb{Q}$ fölött, akkor $\mathbb{Z}$ fölött is.

Bizonyítás
(1): Mivel f nem konstans, ezért nem 0 és nem egység $\mathbb{Q}$ fölött.
Tegyük föl, hogy $f = gh$ nemtriviális felbontás $\mathbb{Q}$ fölött, tehát g és h nem konstans. A második Gauss-lemma miatt $f = g_1 h_1$, ahol $g_1, h_1 \in \mathbb{Z}[x]$, és $\mathrm{gr}(g_1) = \mathrm{gr}(g)$, $\mathrm{gr}(h_1) = \mathrm{gr}(h)$. Az $f = g_1 h_1$ felbontás triviális $\mathbb{Z}$ fölött, mert f irreducibilis $\mathbb{Z}[x]$-ben. Így g_1 és h_1 egyike ± 1, de akkor f és g egyike konstans, ami ellentmond annak, hogy $f = gh$ nemtriviális felbontás.
(2): Ha f primitív, irreducibilis $\mathbb{Q}$ fölött és $f = gh$, ahol $g, h \in \mathbb{Z}[x]$, akkor a $\mathbb{Q}$ fölötti irreducibilitás miatt g és h egyike konstans, és így egész szám. Mivel f primitív, ez az egész szám csak ± 1 lehet. $\square$

$\mathbb{Z}[x]$ irreducibilis polinomjainak jellemzése

Tétel (K3.4.8)
Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Bizonyítás
A felsorolt polinomokról már beláttuk, hogy $\mathbb{Z}[x]$-ben irreducibilisek. Tegyük fel, hogy $f \in \mathbb{Z}[x]$ irreduciblis. Emeljük ki együtthatóinak legnagyobb közös osztóját: $f = nf_0$, ahol f_0 primitív és n egész. Ez triviális felbontás kell, hogy legyen, ezért vagy $f_0 = \pm 1$, vagy $n = \pm 1$. Az első esetben $f = \pm n$ egy $\mathbb{Z}$-beli prímszám. A második esetben f primitív, és nem konstans, különben f egység lenne $\mathbb{Z}[x]$-ben. Láttuk, hogy ekkor f irreducibilis $\mathbb{Q}$ fölött. $\square$

$\mathbb{Z}[x]$ alaptételes: egyértelműség

Tétel (K3.4.10)
$\mathbb{Z}[x]$-ben érvényes a számelmélet alaptétele.

Bizonyítás
Az *egyértelműség* igazolásához elég megmutatni, hogy minden irreducibilis prím (a bizonyítás ugyanaz, mint egész számokra).

Legyen $f \in \mathbb{Z}[x]$ irreducibilis. Ha f konstans prímszám, akkor az első Gauss-lemma miatt f prím $\mathbb{Z}[x]$-ben. A másik esetben f primitív és irreducibilis $\mathbb{Q}$ fölött. Tegyük föl, hogy f osztója $\mathbb{Z}[x]$-ben gh-nak, ahol $g, h \in \mathbb{Z}[x]$. Mivel $\mathbb{Q}[x]$ alaptételes, f prímtulajdonságú $\mathbb{Q}[x]$-ben, tehát f osztója g-nek vagy h-nak $\mathbb{Q}[x]$-ben. Az első Gauss-lemma második következménye miatt ez az oszthatóság $\mathbb{Z}[x]$-ben is fönnáll. Így f prím $\mathbb{Z}[x]$-ben.

$\mathbb{Z}[x]$ alaptételes: a felbontás létezése

Először megmutatjuk, hogy minden nem konstans primitív polinom felbontható felbonthatatlanok szorzatára.

Legyen g minimális fokú ellenpélda. Ha g irreducibilis, akkor az egytényezős felbontás jó. Ha nem, akkor $g = hk$ ahol h és k nem egység. Mivel g primitív, h és k is az. Így egyikük sem konstans (mert akkor egység lenne), és ezért mindketten g-nél alacsonyabb fokúak. Mivel g foka minimális, h és k már felbomlik irreducibilisek szorzatára. A két felbontást összeszorozva g felbontását kapjuk.

Ha $f \in \mathbb{Z}[x]$ tetszőleges, akkor legyen $f = nf_0$, ahol f_0 primitív polinom és n egész. Ekkor n felbontható prím egész számok szorzatára, f_0 pedig a fentiek szerint irreducibilisek szorzatára. $\square$

A Schönemann–Eisenstein-kritérium

Schönemann–Eisenstein-kritérium (K3.5.2)
Legyen f egész együtthatós, nem konstans polinom. *HA* van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Bizonyítás
Tegyük föl, hogy f mégsem irreducibilis $\mathbb{Q}$ fölött, vagyis az f-nél alacsonyabb fokú, racionális együtthatós g és h polinomok szorzatára bontható. A második Gauss-lemma miatt feltehetjük, hogy g és h egész együtthatós.

A Schönemann–Eisenstein-kritérium bizonyítása

Legyen $f(x) = a_0 + \ldots + a_n x^n$, $g(x) = b_0 + \ldots + b_k x^k$ és $h(x) = c_0 + \ldots + c_\ell x^\ell$, ahol $\mathrm{gr}(g) = k < n$ és $\mathrm{gr}(h) = \ell < n$. Mivel $a_n = b_k c_\ell$, a b_k és c_ℓ egészek egyike sem osztható p-vel. Továbbá $a_0 = b_0 c_0$, és mivel a_0 osztható p-vel, de p^2-tel nem, ezért a b_0 és c_0 számok közül pontosan az egyik osztható p-vel. A g és a h esetleges cseréjével feltehetjük, hogy ez a b_0. Legyen i a legkisebb olyan index, amelyre b_i nem osztható p-vel. Ilyen i van, hiszen b_0 osztható p-vel, de b_k nem, és $0 < i \leq k$. Mivel $f = gh$, ezért $a_i = b_0 c_i + b_1 c_{i-1} + \ldots + b_{i-1} c_1 + b_i c_0$. Ez az együttható nem osztható p-vel, mert az összeg mindegyik tagja osztható vele, kivéve az utolsó tagot. A feltétel szerint f együtthatói oszthatók p-vel, kivéve a_n-et. Ezért $i = n$, azaz $i \leq k$ miatt $k \geq n$. Ez ellentmond a $k < n$ feltételnek. $\square$

A Schönemann–Eisenstein-kritérium: megjegyzések

(1) Az állítás megfordítása nem igaz! Például $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nincs hozzá megfelelő p prím. Tehát a kritérium nem ad eljárást az irreducibilitás eldöntésére: ha nem alkalmazható, akkor az irreducibilitást nem tudjuk, új ötlet után kell néznünk, lásd K 111. oldal (pl. eltolt, fordított Schönemann–Eisenstein).

(2) A kritérium racionális együtthatós polinomokra is alkalmazható lehet, ha a nevezőkkel felszorzunk.

(3) A feltételek teljesülése csak $\mathbb{Q}$ fölötti (és nem $\mathbb{Z}$ fölötti) irreducibilitást biztosít. Pl. a $9x + 18$ polinomra érvényes a feltétel ha $p = 2$, és ez a polinom irreducibilis is $\mathbb{Q}$ fölött, de nem irreducibilis $\mathbb{Z}$ fölött (nem primitív).

(4) A kritérium alapján $x^n - 2$ irreducibilis $\mathbb{Q}$ fölött (és így $\mathbb{Z}$ fölött is, hiszen primitív). Vagyis létezik akármilyen fokú irreducibilis polinom $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

2. A körosztási polinom

A körosztási polinom

Definíció (K3.9.1)
Ha $n \geq 1$ egész, akkor Φ_n az *n-edik körosztási polinom:*

$$\Phi_n(x) = (x - \xi_1) \dots (x - \xi_{\varphi(n)}),$$

ahol $\xi_1, \dots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes olyan komplex szám, melynek rendje n. Tehát Φ_n-nek egyszeres gyökei a primitív n-edik egységgyökök.

Példák:
$\Phi_1(x) = x - 1.$ $\quad \Phi_2(x) = x - (-1) = x + 1.$
$\Phi_4(x) = (x - i)\big(x - (-i)\big) = (x - i)(x + i) = x^2 + 1.$

$$\Phi_3(x) = \left(x - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right) = x^2 + x + 1.$$

$$\Phi_6(x) = \left(x - \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - \left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right) = x^2 - x + 1.$$

A körosztási polinom kiszámítása

Tétel (K3.9.5, K3.9.7), nem bizonyítjuk
Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$. Ezért mindegyik körosztási polinom egész együtthatós.

Példa (K3.9.11): Legyen p prím, ekkor $\Phi_1(x)\Phi_p(x) = x^p - 1$. Így

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \ldots + x^{p-1}\,.$$

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6 - 1}{(x+1)(x^3 - 1)} = x^2 - x + 1\,.$$

HF: Számítsuk ki rekurzívan $\Phi_4(x)$-et és $\Phi_{12}(x)$-et.

Tétel (K3.9.9, nehéz)
Mindegyik *körosztási polinom irreducibilis* $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Hasznos képlet: K3.9.15. feladat.

3. Gyűrűk és testek

Hasonló tételek

Láttuk:
Legyen T a $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ egyike. Ekkor $T[x]$-ben

(1) ki lehet emelni a gyöktényezőket;

(2) érvényes a polinomok azonossági tétele;

(3) elvégezhető az interpoláció, a maradékos osztás;

(4) ugyanaz a gyökök és irreducibilitás kapcsolata;

és így tovább. *Nagyon hasonlóan viselkednek.* Oka: a négy alapművelet a szokásos szabályok szerint elvégezhető, és *ennyi elég az állítások bizonyításához.*
$\mathbb{Z}$ hasonló, de nem lehet minden nem nulla számmal osztani.

Nem érdemes ugyanazt a bizonyítást külön elmondani $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ esetén.
Hátha *más fontos számkör* is van, ahol a négy alapművelet elvégezhető, és így a fenti tételek érvényesek.

Gyűrűk és testek

Definíció-kísérlet
Az R *gyűrű*, ha az összeadás kivonás, szorzás *a szokásos szabályok szerint* elvégezhető. A T *test*, ha ezen felül még minden nem nulla számmal lehet osztani.
Motiváló példák (K2.2.35):

(1) A polinomok, azaz $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{C}[x, y]$: *gyűrű.*

(2) A négyzetes mátrixok $\mathbb{C}^{n\times n}$, $\mathbb{R}^{n\times n}$, $\mathbb{Q}^{n\times n}$: *gyűrű.*

(3) Folytonos (differenciálható) $\mathbb{R} \to \mathbb{R}$ függvények: *gyűrű.*

(4) Az $a + bi$ alakú számok ($a, b \in \mathbb{Z}$): *gyűrű.*

(5) Az $a + bi$ alakú számok ($a, b \in \mathbb{Q}$): *test.*

(6) Az $a + b\sqrt{2}$ alakú számok ($a, b \in \mathbb{Z}$): *gyűrű.*

(7) Az $a + b\sqrt{2}$ alakú számok ($a, b \in \mathbb{Q}$): *test.*

(8) Páratlan nevezőjű törtek: *gyűrű.*

Számolás maradékokkal

Definíció (K1.1.4)
Ha $n \geq 1$ egész, akkor legyen $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Összeadás: $a +_n b$ az $a + b$ maradéka n-nel osztva. Szorzás: $a *_n b$ az ab maradéka n-nel osztva.

Példa (K, 4. oldal)

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ezek a *modulo* 5 *műveleti táblázatok. Ez gyűrű, sőt test!*

A szokásos tulajdonságok
Definiálni kell, hogy mik a „szokásos" tulajdonságok.

Definíció (K2.2.1)
Művelet egy R halmazon: bármely $a, b \in R$-hez $a * b \in R$.
Asszociativitás: $(a * b) * c = a * (b * c)$ bármely a, b, c-re. (Ilyenkor a soktényezős szorzatot is akárhogy zárójelezhetjük.)
Kommutativitás: $a * b = b * a$ bármely a, b-re. (Ilyenkor sok tényezőt is akárhogy cserélgethetünk.)

Példák
A $\mathbb{C}$-beli összeadás és szorzás asszociatív és kommutatív. A $+_n$ és $*_n$ műveletek asszociatívak és kommutatívak. A halmazelméleti *unió* és *metszet* is asszociatív és kommutatív. Függvények *kompozíciója* asszociatív, de általában nem kommutatív. $(f \circ g)(x) = f\big(g(x)\big)$.

Nullelem, egységelem, ellentett, inverz

Definíció (K2.2.6)
Legyen $+$ művelet az R halmazon. A $0 \in R$ elemet *nullelemnek* nevezzük, ha minden $a \in R$ esetén $a + 0 = 0 + a = a$.

Házi Feladat: legfeljebb egy nullelem lehet.

Definíció (K2.2.9)
Legyen $+$ művelet az R halmazon és $0 \in R$ nullelem. Az $a \in R$ *ellentettje* b, ha $a + b = b + a = 0$. Jele: $b = -a$.

Házi Feladat: Minden elemnek legfeljebb egy ellentettje van.

Az előző definíciók szorzás művelet esetén:
Jelölje R-en a műveletet egymás mellé írás. Ekkor:
Az $1 \in R$ *egységelem*, ha $1a = a1 = a$ minden $a \in R$-re.
Az $a \in R$ *inverze* b, ha $ab = ba = 1$. Jele: $b = a^{-1}$.

A gyűrű és test definíciója

Az R *gyűrű* (K2.2.21), ha értelmezett az összeadás $+$-szal, és a szorzás egymás mellé írással jelölt művelete úgy, hogy

(1) Az összeadás asszociatív.

(2) Az összeadás kommutatív.

(3) Van az összeadásra nézve egy 0 nullelem.

(4) Minden elemnek van ellentettje.

(5) A szorzás asszociatív.

(6) Tetszőleges $x, y, z \in R$ esetén igaz a *disztributivitás*: $(x+y)z = xz + yz$ és $z(x+y) = zx + zy$.

Kommutatív gyűrű: a szorzás kommutatív.
Egységelemes gyűrű: a szorzásra nézve van egységelem (jele 1).
Test: egységelemes, kommutatív gyűrű, amelyben minden nem nulla elemnek van (a szorzásra) inverze (K2.2.23).

Elemi számolási szabályok

Állítás (K2.2.22, K2.2.10)
Legyen R gyűrű és $a, b \in R$ tetszőleges elemek.

(1) $0a = a0 = 0$.

(2) $(-a)b = a(-b) = -(ab)$.

(3) Ha a és b invertálható, akkor ab is, és inverze $b^{-1}a^{-1}$.

Mintabizonyítás

(1) A disztributivitás miatt $a0 = a(0+0) = a0 + a0$. Mindkét oldalhoz adjuk hozzá $a0$ ellentettjét.
$0 = (a0 + a0) + (-a0) = a0 + \big(a0 + (-a0)\big) = a0 + 0 = a0$.

(3) $b^{-1}a^{-1}(ab) = b^{-1}1b = 1$. Hasonlóan $(ab)b^{-1}a^{-1} = 1$.

<u>Példa:</u> szorzatmátrix inverze.

Nullosztómentesség

Definíció (K2.2.27)
Az R gyűrű *nullosztómentes*, ha egy szorzat csak akkor nulla, ha valamelyik tényezője nulla: $ab = 0 \implies a = 0$ vagy $b = 0$.
Szokásos gyűrű: kommutatív, egységelemes, nullosztómentes.

Példák
Mindegyik eddig tanult polinomgyűrű szokásos gyűrű (a többhatározatlanúak is).
A $\mathbb{Z}_6$ nem nullosztómentes: $2 *_6 3 = 0$, de $2 \neq 0$ és $3 \neq 0$.
A $\mathbb{Z}_5$ test, például a „2-*ben a* 3" osztás eredménye 4, mert $3 *_5 4 = 2$.
A 3 inverze 2, mert $3 *_5 2 = 1$.
Ha $n = ab$, ahol $0 < a, b < n$, akkor $a *_n b = 0$, de $a, b \neq 0$. Ezért ha n nem prím, akkor $\mathbb{Z}_n$ *nem* nullosztómentes.

Test nullosztómentes

Tétel (K2.2.31)
A $\mathbb{Z}_n$ a $+_n$ és $*_n$ műveletekre egységelemes, kommutatív gyűrű. A $\mathbb{Z}_n$ pontosan akkor nullosztómentes, ha n prímszám, és ebben az esetben test is.
Bizonyítás: kongruenciákkal.

Tétel (K2.2.29)
Minden test nullosztómentes.

Bizonyítás
Legyen T test, és $z, w \in T$. Tegyük föl, hogy $zw = 0$, de $z \neq 0$. Meg kell mutatnunk, hogy akkor $w = 0$. Mivel $z \neq 0$, van inverze: $uz = 1$. Ezzel szorozva

$$w = 1 \cdot w = (uz)w = u(zw) = u \cdot 0 = 0.$$

Példa: Az egész számok gyűrűje nullosztómentes, de nem test.

Az egyszerűsítési szabály

Tétel (K2.2.28)
Nullosztómentes gyűrűben érvényes az *egyszerűsítési szabály*: ha $ac = bc$ és $c \neq 0$, akkor $a = b$.

Bizonyítás
$ac = bc \implies 0 = ac - bc = (a - b)c$. Mivel $c \neq 0$, a nullosztómentesség miatt $a - b = 0$, azaz $a = b$.

Hasonlóképpen nullosztómentes gyűrűben balról is lehet egyszerűsíteni:
ha $ca = cb$ és $c \neq 0$, akkor $a = b$.

Minden lineáris algebrából eddig kimondott állítás tetszőleges test fölött is érvényes, ugyanazzal a bizonyítással.
Legközelebb átismételjük a polinomokat „gyűrűs" szemszögből.

4. Összefoglaló

A 10. előadáshoz tartozó vizsgaanyag

Fogalmak
Primitív polinom. Prímtulajdonságú polinom. Körosztási polinom.
Művelet, asszociativitás, kommutativitás. Nullelem, egységelem, ellentett, inverz. Gyűrű, nullosztómentesség. Egységelemes, kommutatív, szokásos gyűrű, test. A $\mathbb{Z}_m$ gyűrű.

Tételek
Gauss-lemma I, ennek két következménye, Gauss-lemma II. A $\mathbb{Z}[x]$ irreducibiliseinek visszavezetése $\mathbb{Q}[x]$-re, $\mathbb{Z}[x]$ alaptételes.
A körosztási polinom rekurzív képlete. A körosztási polinom egész együtthatós és irreducibilis.
Elemi számolási szabályok gyűrűkben, az egyszerűsítési szabály, szorzat inverze. Minden test nullosztómentes. A $\mathbb{Z}_m$ mikor nullosztómentes, mikor test.