1. 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.

Példák

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

(2) Analízisben tárgyalt függvények: gyűrű.

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

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

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

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

(7) Páratlan nevezőjű törtek: gyűrű.

Számolás maradékokkal.

Definíció
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

$+_5$	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
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 sokténye zős 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
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
Legyen $+$ művelet az R halmazon és $0 \in R$ nullelem. Az $a \in R$ *ellentettje* b, ha $a + b = 0$. 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*, ha értelmezve van rajta 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.
Test: egységelemes, kommutatív gyűrű, amelyben minden nem nulla elemnek van inverze.

Elemi számolási szabályok.

Állítás (Kiss-jegyzet, 2.2.20. Feladat)
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 $(ab)b^{-1}a^{-1} = 1$.

asszociativitás
ellentett definíciója
nullelem definíciója

Nullosztómentesség.

Definíció
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 (lásd Kiss-jegyzet, 2.2.29. Állítás)
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.

Tétel (Kiss-jegyzet, 2.2.27. Tétel)
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 (lásd Kiss-jegyzet, 2.2.26. Gyakorlat)
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 balról is lehet egyszerűsíteni: Ha $ca = cb$ és $c \neq 0$, akkor $a = b$.

Ezzel befejeztük a Kiss-jegyzet első három fejezetét (nem minden témát érintettünk, és kevés bizonyítás szerepelt). Mostantól: *lineáris algebra*. A félév végén átismételjük a polinomokat immár „gyűrűs" szemszögből.