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;

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. Például ilyen $\mathbb{Z}_5$ is, a mod 5 maradékok halmaza, a $+_5$ és $*_5$ műveletekre, láttuk a táblázatot.

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 $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$: *gyűrű.*

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

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

HF: 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: $b = -a$.

HF: 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 csoport definíciója

Az G *csoport* a $*$ műveletre (K2.2.13), ha

(1) $*$ asszociatív;

(2) van $*$-ra nézve egy 1 egységelem;

(3) minden elemnek van inverze.

Kommutatív csoport: a $*$ kommutatív.

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{C}[x]$, $\mathbb{R}^{n\times m}$ kommutatív csoport az összeadásra.
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$-ből a 0-t kihagyva kommutatív csoport a szorzásra.
Az n-edik egységgyökök kommutatív csoport a szorzásra.
Az S_n permutációi nemkommutatív csoport a kompozícióra ($n \geq 2$).

Az $\mathbb{R}^{n\times n}$ invertálható mátrixai nemkommutatív csoport a szorzásra.
$\mathbb{Z}_5$ elemei kommutatív csoport a mod 5 összeadásra.
$\mathbb{Z}_5$ nem nulla elemei kommutatív csoport a mod 5 szorzásra.

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

Példa: szorzatmátrix inverze.

Nullosztómentesség
Minden R gyűrű kommutatív csoport az összeadásra. Ez R *additív csoportja*, jele R^+. Ha R egységelemes, akkor az invertálható elemei csoport a szorzásra. Ez R *multiplikatív csoportja,* jele $R^\times$. Így minden test nem nulla elemei kommutatív csoport a szorzásra.

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.

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.
A $\mathbb{Z}_n^\times$ multiplikatív csoport az n-hez relatív prím elemekből áll, tehát $\varphi(n)$ eleme van. Bizonyítás: kongruenciákkal, HF.

Tétel (K2.2.29, 1.3.7): 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.

2. Összefoglaló

A 19. előadáshoz tartozó vizsgaanyag

Fogalmak
Művelet, asszociativitás, kommutativitás (K2.2.1).
Nullelem, egységelem (K2.2.6), ellentett, inverz (K2.2.9).
Csoport (K2.2.13), gyűrű (K2.2.21). Nullosztómentesség (K2.2.27).
Egységelemes, kommutatív, szokásos gyűrű, test (K2.2.23).
Gyűrű additív és multiplikatív csoportja (K2.2.10). A $\mathbb{Z}_m$ gyűrű (K2.2.31).

Tételek
Elemi számolási szabályok gyűrűkben (K2.2.10, 2.2.22),
az egyszerűsítési szabály (K2.2.28), szorzat inverze (K2.2.10).
Minden test nullosztómentes (K2.2.29, 1.3.7).
A $\mathbb{Z}_m$ mikor nullosztómentes, mikor test (K2.2.31).