

1. Számelmélet gyűrűkben

Oszthatóság.

Definíció (Kiss-jegyzet, 3.1. szakasz)

Az R szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük.

Ha $r, s \in R$, akkor r osztója s -nek (s többszöröse r -nek), ha van olyan $t \in R$, hogy $rt = s$. **Jele:** $r \mid s$.

Példa: $2x \mid 3x^2$ igaz $\mathbb{R}[x]$ -ben, nem igaz $\mathbb{Z}[x]$ -ben.

Tulajdonságok

- (1) Ha $r \mid s$ és $r \mid t$, akkor $r \mid s \pm t$.
- (2) Ha $r \mid s$, akkor $r \mid st$, sőt $rt \mid st$. Megfordítva, ha $t \neq 0$, akkor $rt \mid st$ -ből $r \mid s$ következik (R nullosztómentes!).
- (3) *Tranzitivitás:* ha $r \mid s$ és $s \mid t$, akkor $r \mid t$.
- (4) *Reflexivitás:* $r \mid r$ minden $r \in R$ esetén (R egységelemes!).

Felbonthatatlan elem.

Emlékeztető

Az $e \in R$ egység, ha $e \mid 1$. Ez ugyanaz, mint az invertálható elem. Minden egység osztója R minden elemének.

Példa: A \mathbb{Z} gyűrű egységei ± 1 . Az egységeleme az 1.

HF: Mik a 0 osztói? Mely elemeknek osztója a 0?

Definíció

A $b = cd$ a b -nek *triviális* felbontása, ha c és d egyike egység. A $p \in R$ *felbonthatatlan* (irreducibilis), ha nem nulla, nem egység, és **nincs nemtriviális felbontása**.

Ekvivalens: p minden osztója egység, vagy p egységszerese.

Példa: A 23 felbonthatatlan \mathbb{Z} -ben, mert nem nulla, nem ± 1 , és osztói csak ± 1 és ± 23 .

Az összes felbontása: $23 = 1 \cdot 23 = 23 \cdot 1 = (-1)(-23) = (-23)(-1)$.

Alaptételes gyűrű.

Definíció

Az R gyűrűben *érvényes a számelmélet alaptétele*, ha R minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt *alaptételes* gyűrűnek nevezzük.

Tétel

A \mathbb{Z} , és minden $T[x]$ polinomgyűrű, ahol T test, alaptételes.

- elvégezhető a maradékos osztás, ezért
- létezik „legnagyobb” közös osztó, ezért
- a felbonthatatlan elemek ugyanazok, mint a prímek, ezért
- egyértelmű a felbontás.

Prímtulajdonságú elem.**Feladat**

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

Definíció

A $p \in R$ *prím* R -ben, ha nem nulla, nem egység, és tetszőleges $b, c \in R$ esetén $p \mid bc$ -ből következik, hogy $p \mid b$ vagy $p \mid c$.

Tétel

A \mathbb{Z} gyűrűben, továbbá a $T[x]$ polinomgyűrűben, ahol T test, a felbonthatatlan elemek ugyanazok, mint a prímek. **Oka:** létezik „legnagyobb” közös osztó.

HF: Minden szokásos gyűrűben minden prím felbonthatatlan.

Maradékos osztás.**Tétel (Kiss-jegyzet, 3.2.1. Tétel)**

Legyen R szokásos gyűrű. Ekkor az $R[x]$ polinomgyűrűben minden olyan $g \in R[x]$ polinommal lehet *maradékosan osztani*, amelynek *főegyütthatója invertálható* (azaz egység).

Ez azt jelenti, hogy tetszőleges $f \in R[x]$ polinomhoz léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = gq + r$, és vagy $r = 0$, vagy r foka kisebb g fokánál.

A q és r polinomok *egyértelműen* meghatározottak.

A bizonyítás ugyanaz mint komplex együtthatós polinomokra. A tétel magában foglalja azt is, hogy q és r együtthatói az f és g együtthatóiból a négy alapművelettel kaphatók.

Emlékeztető (Kiss-jegyzet, 3.2.2. Állítás)

Ha $g \mid f$ a $\mathbb{C}[x]$ -ben, és $f, g \in \mathbb{R}[x]$, akkor $g \mid f$ az $\mathbb{R}[x]$ -ben is.

Kitüntetett közös osztó.

Definíció

A b és c elemeknek d *kitüntetett közös osztója*, ha

- (1) közös osztó, azaz $d \mid b$ és $d \mid c$;
- (2) minden közös osztónak többese, azaz ha $d' \mid b$ és $d' \mid c$, akkor $d' \mid d$.

Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója, akkor a felbonthatatlanok prímelek.

Tétel

Ha egy szokásos gyűrűben „*elvégezhető a maradékos osztás*”, akkor működik az euklideszi algoritmus, és így bármely két elemnek van kitüntetett közös osztója. Az ilyen gyűrűk *alaptételesek*.

Kanonikus alak.

Definíció

A $0 \neq r$ *kanonikus alakja* $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, ahol e egység, p_1, p_2, \dots, p_k pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

Példák

\mathbb{Z} -ben $-36 = (-1)2^2 3^2$. $\mathbb{C}[x]$ -ben $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$, ahol c a főegyüttható (nem nulla konstans, így egység). Ez a gyöktényezőes alak, a k_i a b_i gyök multiplicitása.

Az *osztók száma*, a *kitüntetett közös osztó*, és a kitüntetett közös többszörös hasonló képletekkel kapható a kanonikus alakból, mint az egész számok számelméletében.

Gyökök és irreducibilitás.

Tétel (Kiss-jegyzet, 3.3. Szakasz)

Legyen T test.

- (1) Az $f \in T[x]$ akkor és csak akkor irreducibilis T fölött, ha nem konstans, és nem bontható $T[x]$ -ben *alacsonyabb fokú* polinomok szorzatára.
- (2) *Elsőfokú* polinom mindig irreducibilis $T[x]$ -ben.
- (3) *Másod- és harmadfokú* polinom akkor és csak akkor irreducibilis $T[x]$ -ben, ha *nincs gyöke* T -ben.
- (4) *Legalább negyedfokú* polinom, *HA* van gyöke T -ben, akkor biztosan *NEM* irreducibilis $T[x]$ -ben. *Ha nincs gyöke, attól még lehet reducibilis!*
Példa: $\mathbb{Q}[x]$ -ben $(x^2 + 1)^2$.
- (5) Gyök létezése *elsőfokú* irreducibilis tényezőnek felel meg.

2. Többhatározatlanú polinomok

Rekurzív definíció.

Definíció

Legyen R kommutatív, egységelemes gyűrű. Ekkor $R[x_1, \dots, x_n]$ -et n szerinti indukcióval (rekurzióval) értelmezzük: $R[x_1, x_2] = (R[x_1])[x_2]$, és így tovább, $R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n]$. Vagyis a határozatlan x_n , az együtthatók a már definiált $n - 1$ -határozatlanú polinomok gyűrűjének elemei.

Előny

Mivel $S = R[x_1, \dots, x_{n-1}]$ is kommutatív, egységelemes gyűrű, az $R[x_1, \dots, x_n] = S[x_n]$ is az. A tulajdonságokat nem kell külön ellenőrizni.

Példa: Ha R nullosztómentes, akkor indukcióval világos, hogy $R[x_1, \dots, x_n]$ is nullosztómentes.

A szimmetrikus polinomok alaptétele.

Példa

A négyzetösszeg: $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$.

Vagyis ha $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$, akkor $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$. Tehát s_2 az elemi szimmetrikus polinomok *polinomja*.

Tétel (Kiss-jegyzet, 2.7.3. Tétel)

Legyen R szokásos gyűrű. Ekkor minden $f \in R[x_1, \dots, x_n]$ szimmetrikus polinom *egyértelműen* fölírható az elemi szimmetrikus polinomok polinomjaként. Azaz létezik pontosan egy $F \in R[y_1, \dots, y_n]$ polinom, melyre

$$f(x_1, \dots, x_n) = F(\sigma_1, \dots, \sigma_n).$$

A F együtthatói a f együtthatóiból összeadás és kivonás segítségével kaphatók.

A többhatározatlanú polinomok számelmélete.

Belátható

A $\mathbb{Z}[x]$ polinomgyűrű alaptételes.

Ugyanígy: Ha R alaptételes, szokásos gyűrű, akkor $R[x]$ is az.

Bizonyítás

Alapszinten nem szerepel, lásd Kiss-jegyzet, 3.4. Szakasz.

Következmény

Ha R alaptételes, szokásos gyűrű, akkor $R[x_1, x_2, \dots, x_n]$ is az.

Speciálisan $\mathbb{Z}[x_1, x_2, \dots, x_n]$, és ha T test, akkor $T[x_1, x_2, \dots, x_n]$ is *alaptételes gyűrűk*.

Általános gyűrűkben az alaptétel vizsgálata: Kiss-jegyzet, 5.5. szakasz (a harmadik félévben).