Klasszikus algebra előadás

Waldhauser Tamás
2014. május 5.

Euklideszi algoritmus euklideszi gyűrűben

5.27. Tétel.

Euklideszi gyűrűben bármely két elemnek létezik legnagyobb közös osztója, és az előáll a két elem „lineáris kombinációjaként". Formálisan: ha R euklideszi gyűrű, akkor $\forall a, b \in R\ \exists x, y \in R : ax + by \sim \operatorname{lnko}(a, b)$.

Bizonyítás.

Szinte szóról szóra ugyanaz, mint számelméletből (lásd ott az 1.18. Tételt).
Ha $a = 0$, akkor $\operatorname{lnko}(a, b) \sim b$, és $a \cdot 1 + b \cdot 1 \sim \operatorname{lnko}(a, b)$. A $b = 0$ eset hasonló.
Most tfh. $a, b \neq 0$, és hajtsuk végre az $a =: r_0$ és $b =: r_1$ elemekre az euklideszi algoritmust:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 && (0 < \|r_2\| < \|r_1\|)\,; \\
r_1 &= q_2 r_2 + r_3 && (0 < \|r_3\| < \|r_2\|)\,; \\
r_2 &= q_3 r_3 + r_4 && (0 < \|r_4\| < \|r_3\|)\,; \\
&\vdots \\
r_{i-1} &= q_i r_i + r_{i+1} && (0 < \|r_{i+1}\| < \|r_i\|)\,; \\
&\vdots
\end{aligned}$$

Mivel $\|r_1\| > \|r_2\| > \|r_3\| > \cdots$, az eljárás véges számú lépés után véget ér: létezik olyan $n \in \mathbb{N}$, hogy $r_{n+1} = 0$.

Euklideszi algoritmus euklideszi gyűrűben

Biz. (folyt.)

Könnyű ellenőrizni, hogy minden i-re $D_{r_{i-1}} \cap D_{r_i} = D_{r_i} \cap D_{r_{i+1}}$. Tehát

$$D_a \cap D_b = D_{r_0} \cap D_{r_1} = D_{r_1} \cap D_{r_2} = \cdots = D_{r_n} \cap D_{r_{n+1}} = D_{r_n} \cap D_0 = D_{r_n},$$

és így $\text{lnko}\,(a, b) \sim r_n$.

Teljes indukcióval megmutatható, hogy minden i-re $\exists x_i, y_i \in R: \ ax_i + by_i = r_i$.

Kezdőlépések: $a \cdot 1 + b \cdot 0 = r_0$ és $a \cdot 0 + b \cdot 1 = r_1$.

Tfh. $j = 0, 1, \ldots, i$ esetén $\exists x_j, y_j \in R: \ ax_j + by_j = r_j$. (IH)

Fejezzük ki r_{i+1}-et a és b segítségével:

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i \cdot q_i \overset{\text{(IH)}}{=} (ax_{i-1} + by_{i-1}) - (ax_i + by_i) \cdot q_i \\ &= a \cdot (\underbrace{x_{i-1} - x_i q_i}_{x_{i+1}}) + b \cdot (\underbrace{y_{i-1} - y_i q_i}_{y_{i+1}}). \end{aligned}$$

Mivel $\text{lnko}\,(a, b) \sim r_n$, azt kapjuk, hogy $ax_n + by_n \sim \text{lnko}\,(a, b)$. □

Lineáris diofantoszi egyenlet euklideszi gyűrűben

5.28. Tétel.

Ha R euklideszi gyűrű, akkor tetszőlegesen adott $a, b, c \in R \setminus \{0\}$ elemek esetén az $ax + by = c$ egyenlet akkor és csak akkor oldható meg, ha $\text{lnko}(a, b) \mid c$.

Ha (x_0, y_0) egy megoldás, akkor bármely $t \in R$ esetén az alábbi (x, y) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t elem alkalmas megválasztásával:

$$x = x_0 + \frac{b}{\text{lnko}(a, b)} \cdot t;$$

$$y = y_0 - \frac{a}{\text{lnko}(a, b)} \cdot t.$$

Bizonyítás.

Szinte szóról szóra ugyanaz, mint számelméletből (lásd ott az 1.23. Tételt).
Legyen $d \sim \text{lnko}(a, b) \neq 0$.

Ha x, y egy megoldás, akkor $d \mid ax + by = c$.

Tudjuk, hogy $\exists x', y' \in R : ax' + by' = d$.

Ha $d \mid c$, akkor $x = x' \frac{c}{d}, y = y' \frac{c}{d}$ egy megoldás: $ax' \frac{c}{d} + by' \frac{c}{d} = c$.

Lineáris diofantoszi egyenlet euklideszi gyűrűben

Biz. (folyt.)

Tfh. x_0, y_0 egy megoldás, azaz $ax_0 + by_0 = c$.

Az világos, hogy minden $t \in R$ esetén $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ szintén megoldás:

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t = c.$$

Legyen most x, y egy tetszőleges megoldás.

$$\begin{aligned} ax + by = c = ax_0 + by_0 &\implies ax - ax_0 = by_0 - by \\ &\implies b \mid a(x - x_0) \\ &\implies \tfrac{b}{d} \mid x - x_0 \\ &\implies \exists t \in R: \; x - x_0 = \tfrac{b}{d}t \end{aligned}$$

Az y-ra vonatkozó képlet ezután már egyszerű visszahelyettesítéssel kijön:

$$by_0 - by = a(x - x_0) = \tfrac{abd}{t} \implies y = y_0 - \tfrac{a}{d}t. \qquad \square$$

Irreducibilitás és prímtulajdonság

Irreducibilis és prímelemek bármely integritástartományban definiálhatók, és a korábban tanult tulajdonságok egy része érvényes ilyen általánosságban is.

5.29. Definíció.

Azt mondjuk, hogy a $p \in R$ elem *irreducibilis*, ha nem nulla és nem egység, és csak úgy bontható két elem szorzatára, hogy az egyik tényező asszociált p-hez. (Ekkor a másik tényező szükségképpen egység; ilyenkor *triviális faktorizáció*ról beszélünk.) Formálisan:

$$\forall a, b \in R : p = ab \implies (p \sim a \text{ vagy } p \sim b) .$$

5.30. Definíció.

Azt mondjuk, hogy a $p \in R$ elem *prím*, ha nem nulla és nem egység, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall a, b \in R : p \mid ab \implies (p \mid a \text{ vagy } p \mid b) .$$

Prímtulajdonság

5.31. Állítás.

Ha $p \in R$ rendelkezik a prímtulajdonsággal, $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$ és $p \mid a_1 \cdot \ldots \cdot a_n$, akkor $p \mid a_i$ valamely $i \in \{1, \ldots, n\}$-re.

Bizonyítás.

$$p \mid a_1 \cdot (a_2 \cdot \ldots \cdot a_n) \Longrightarrow p \mid a_1 \text{ vagy } p \mid a_2 \cdot \ldots \cdot a_n = a_2 \cdot (a_3 \cdot \ldots \cdot a_n)$$

$$\Longrightarrow p \mid a_1 \text{ vagy } p \mid a_2 \text{ vagy } p \mid a_3 \cdot \ldots \cdot a_n = a_3 \cdot (a_4 \cdot \ldots \cdot a_n)$$

$$\Longrightarrow \ldots$$

$$\Longrightarrow p \mid a_1 \text{ vagy } p \mid a_2 \text{ vagy } p \mid a_3 \text{ vagy } \ldots \text{ vagy } p \mid a_n$$

□

Irreducibilitás vs. prímtulajdonság

5.32. Tétel.

Minden integritástartományban a prímelemek irreducibilisek.

Bizonyítás.

Legyen R egy tetszőleges integritástartomány és $p \in R$ egy prímtulajdonságú elem. Ekkor $p \nsim 0, 1$, így csak azt kell belátnunk, hogy p-nek minden felbontása triviális.

Tekintsük p egy tetszőleges felbontását: $p = ab$.
Világos, hogy ekkor $a \mid p$ és $b \mid p$.

Az is világos, hogy $p \mid ab$, tehát p prímtulajdonsága miatt $p \mid a$ vagy $p \mid b$.
Az első esetben $p \sim a$, a második esetben $p \sim b$, azaz a felbontás triviális. □

Irreducibilitás vs. prímtulajdonság

A másik irányú, „irreducibilis $\Longrightarrow$ prím” implikáció bizonyításánál már kihasználjuk a legnagyobb közös osztók létezését (de mást nem).

5.33. Tétel.

Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor R-ben minden irreducibilis elem prím.

Bizonyítás.

Legyen R egy olyan integritástartomány, amelyben bármely két elemnek létezik legnagyobb közös osztója, és legyen $p \in R$ irreducibilis. Ekkor $p \notin R^* \cup \{0\}$, így csak azt kell belátnunk, hogy p rendelkezik a prímtulajdonsággal.

Ha $p \mid ab$, akkor $\frac{p}{(p,a)} \mid b$. Mivel p felbonthatatlan, $(p, a) \sim 1$ vagy $(p, a) \sim p$.
Az első esetben $p \mid b$, a második esetben $p \mid a$. □

Példa.

A $\mathbb{Z}\left[\sqrt{-5}\right]$ gyűrűben a 2 irreducibilis, de nem prím:

$$2 \mid (1+\sqrt{-5})(1-\sqrt{-5}), \text{ de } \quad 2 \nmid 1+\sqrt{-5} \quad \text{és} \quad 2 \nmid 1-\sqrt{-5}.$$

Gauss-gyűrűk

A végső cél természetesen a számelmélet alaptételének általánosítása integritástartományokra, vagyis egyértelmű irreducibilis faktorizáció létezésének igazolása. Külön nevet is érdemelnek azok az integritástartományok, amelyekben ez megtehető.

5.34. Definíció.

*Gauss-gyűrű*nek nevezzük az olyan integritástartományokat, amelyekben minden a nullától és az egységektől különböző elem irreducibilis elemek szorzatára bomlik, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű.

Tehát az R integritástartomány Gauss-gyűrű, ha minden $a \in R$ $(a \neq 0, a \not\sim 1)$ esetén léteznek olyan $p_1, \ldots, p_n \in R$ irreducibilis elemek, hogy $a = p_1 \cdot \ldots \cdot p_n$; továbbá amennyiben $a = q_1 \cdot \ldots \cdot q_m$ egy másik irreducibilis faktorizáció, akkor $n = m$, és létezik olyan $\pi \in S_n$, amelyre $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

5.35. Tétel.

Minden euklideszi gyűrű Gauss-gyűrű.

5.38. Megjegyzés.

Az 5.35. Tétel megfordítása nem igaz: az egész együtthatós polinomok gyűrűje Gauss-gyűrű, de nem euklideszi gyűrű.

Gauss-gyűrűk

5.36. Következmény.

Az egész számok gyűrűje, minden test feletti polinomgyűrű, valamint a Gauss-egészek gyűrűje Gauss-gyűrű.