Gyűrűk

Waldhauser Tamás

2021 őszi félév


MIÉRT AZ ALGEBRA A MATEMATIKA LEGSZEMÉRMESEBB ÁGA?
MERT OTT A TESTHEZ MINDIG A GYŰRŰN KERESZTÜL VEZET AZ ÚT

Oszthatóság, asszociáltság, egységek

Legnagyobb közös osztó

Irreducibilitás és prímtulajdonság

Euklideszi gyűrűk

Gauss-gyűrűk

Oszthatóság, asszociáltság, egységek

Legnagyobb közös osztó

Irreducibilitás és prímtulajdonság

Euklideszi gyűrűk

Gauss-gyűrűk

Oszthatóság

Mostantól R mindig tetszőleges integritástartományt (azaz kommutatív, egységelemes, zérusosztómentes gyűrűt) jelöl.

Definíció.

Azt mondjuk, hogy az $a \in R$ elem *osztója* a $b \in R$ elemnek (b *többszöröse* a-nak), ha létezik olyan $c \in R$, amelyre $b = ac$.

Jelölés.

Az oszthatósági relációt $\mid$ jelöli: $a \mid b \iff \exists c \in R : b = ac$.
Ha $a \neq 0$, akkor egyetlen ilyen c létezik (mert R zérusosztómentes), ilyenkor használjuk a $c = \frac{b}{a}$ jelölést. Ha $a \nmid b$, akkor a $\frac{b}{a}$ törtet (egyelőre) nem értelmezzük.

Tétel.

Tetszőleges $a, b, c \in R$ esetén érvényesek az alábbiak:

(1) $a \mid a$

Biz: $a = a \cdot 1$

(2) $(a \mid b \text{ és } b \mid c) \implies a \mid c$

Biz: $(b = au \text{ és } c = bv) \implies c = (au)\,v = a\,(uv)$

Oszthatóság

Tétel (folyt.).

Tetszőleges $a, b, c \in R$ esetén érvényesek az alábbiak:

(3) $1 \mid a$

Biz: $a = 1 \cdot a$

(4) $a \mid 0$

Biz: $0 = a \cdot 0$

(5) $0 \mid a \iff a = 0$

Biz: $0 \mid a \iff \exists u \in R : a = 0 \cdot u \iff a = 0$

(6) $(a \mid b \text{ és } a \mid c) \implies a \mid b \pm c$

Biz: $(b = au \text{ és } c = av) \implies b \pm c = au \pm av = a(u \pm v)$

(7) $a \mid b \iff ac \mid bc$, ha $c \neq 0$

Biz: $b = au \implies bc = (ac)\, u$

$bc = auc \overset{c \neq 0}{\implies} b = au$

Egységek

Definíció.

Azt mondjuk, hogy az $u \in R$ elem *egység*, ha $u \mid 1$.

Jelölés.

Az egységek halmazát R^* jelöli: $R^* = \{u \in R : u \mid 1\}$.

Tétel.

Az egységek pontosan a multiplikatív inverzzel rendelkező elemek. Következésképp $(R^*, \cdot)$ csoport.

Bizonyítás.

$$u \mid 1 \iff \exists v \in R\colon uv = 1 \iff u\text{-nak van multiplikatív inverze}$$

Az egységek halmaza zárt a szorzásra: ha u-nak és v-nek van inverze, akkor uv-nek is van: $(uv)^{-1} = v^{-1}u^{-1} \quad (= u^{-1}v^{-1})$.

Az egységelem nyilván egység, és egység inverze is egység, tehát $(R^*, \cdot)$ valóban csoport. □

Egységek

Példa.

Néhány nevezetes gyűrű egységcsoportja:

- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, és általában tetszőleges T test esetén $T^* = T \setminus \{0\}$;
- $T[x]^* = T^* = T \setminus \{0\}$;
- $\mathbb{Z}^* = \{1, -1\}$;
- $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$ (itt $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ a *Gauss-egészek* gyűrűje);
- $\mathbb{Z}[\sqrt{-5}]^* = \{1, -1\}$ (itt $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$);
- $\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m : a \perp m\}$;
- $(T^{n\times n})^* = \mathrm{GL}_n(T) = \{A \in T^{n\times n} : \det(A) \neq 0\}$.

Asszociáltság

Definíció.

Azt mondjuk, hogy az a és b elemek *asszociáltak*, ha $a \mid b$ és $b \mid a$.

Jelölés.

Az asszociáltsági relációt $\sim$ jelöli: $a \sim b \iff a \mid b$ és $b \mid a$.

Tétel.

Az asszociáltság ekvivalenciareláció R-en. Két elem akkor és csak akkor asszociált, ha egymástól csupán egység tényezőben különböznek.

Bizonyítás.

Az asszociáltság nyilván szimmetrikus reláció, a reflexivitása és tranzitivitása pedig következik az oszthatóság reflexivitásából és tranzitivitásából.

Be kell még látni, hogy $(a \mid b \text{ és } b \mid a) \iff \exists u \in R^* : b = ua$.

$$(b = au \text{ és } a = bv) \implies a = a(uv) \overset{a \neq 0}{\implies} 1 = uv \implies u, v \in R^*$$

$$b = ua \implies a = u^{-1}b \implies (a \mid b \text{ és } b \mid a)$$

□

Asszociáltság

Következmény.

Az egész számok gyűrűjében $a \sim b$ akkor és csak akkor teljesül, ha $a = \pm b$. Két T test feletti polinom pontosan akkor asszociált, ha egymástól csupán egy nemnulla konstans szorzóban különböznek.

Megjegyzés.

Asszociált elemeket nem érdemes (sőt nem is lehet) megkülönböztetni, ha csak az oszthatóságot vizsgáljuk. Ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor már nemcsak reflexív és tranzitív, hanem antiszimmetrikus is lesz, azaz részbenrendezés. A kapott $(R/\sim; |)$ részbenrendezett halmaz legkisebb eleme $1/\sim = R^*$, legnagyobb eleme $0/\sim = \{0\}$.

Az egész számok gyűrűjében minden asszociáltsági osztály $\{a, -a\}$ alakú, tehát minden osztályban van egy (és csak egy) nemnegatív szám. Ha minden asszociáltsági osztályt a nemnegatív elemével reprezentálunk, akkor az $(\mathbb{N}_0; |)$ részbenrendezett halmazt kapjuk, ami lényegében ugyanaz, mint a $(\mathbb{Z}/\sim; |)$ részbenrendezett halmaz.

Oszthatóság, asszociáltság, egységek

Legnagyobb közös osztó

Irreducibilitás és prímtulajdonság

Euklideszi gyűrűk

Gauss-gyűrűk

Legnagyobb közös osztó

Az oszthatóság és a kongruencia fogalmát és alaptulajdonságait szinte szó szerint lehet általánosítani tetszőleges integritástartományra.
A legnagyobb közös osztó nem mindig létezik, de ha létezik, akkor hasonló tulajdonságokkal rendelkezik, mint az egész számok gyűrűjében, noha a bizonyítások kicsit nehezebbek.

Definíció.

A $d \in R$ elemet az a és b elemek *legnagyobb közös osztójának* nevezzük, ha kielégíti a következő két feltételt:

(L1) $d \mid a$ és $d \mid b$;

(L2) $\forall k \in R : (k \mid a \text{ és } k \mid b) \implies k \mid d$.

A $t \in R$ elem *legkisebb közös többszöröse* a-nak és b-nek, ha kielégíti a következő két feltételt:

(T1) $a \mid t$ és $b \mid t$;

(T2) $\forall k \in R : (a \mid k \text{ és } b \mid k) \implies t \mid k$.

Jelölés.

Az a és b elemek legnagyobb közös osztóját $\operatorname{lnko}(a, b)$ vagy (a, b), legkisebb közös többszörösüket pedig $\operatorname{lkkt}(a, b)$ vagy $[a, b]$ jelöli.

Legnagyobb közös osztó

Megjegyzés.

Ha az a elem osztóinak halmazát D_a jelöli, akkor $\mathrm{Inko}\,(a, b)$ asszociáltsági osztálya nem más, mint a $(D_a \cap D_b / \sim; |)$ részbenrendezett halmaz legnagyobb eleme.

Pozitív egészek esetén az $\mathrm{Inko}(a, b)$ definiálható úgy is, mint a $(D_a \cap D_b \cap \mathbb{N}; \leq)$ részbenrendezett halmaz legnagyobb eleme.

Tetszőleges integritástartomány esetén nincs „nagyság szerinti” rendezés, csak az oszthatósági relációra támaszkodhatunk. Itt tehát nincs mód kétféleképpen definiálni a legnagyobb közös osztó fogalmát.

A legnagyobb közös osztó egyértelműsége

Tétel.

A legnagyobb közös osztó asszociáltság erejéig egyértelműen meghatározott. Azaz bármely $a, b, d_1, d_2 \in R$ esetén

(1) ha d_1 és d_2 is legnagyobb közös osztója a-nak és b-nek, akkor $d_1 \sim d_2$;

(2) ha d_1 legnagyobb közös osztója a-nak és b-nek, és $d_1 \sim d_2$, akkor d_2 is legnagyobb közös osztója a-nak és b-nek.

Hasonló állítás érvényes a legkisebb közös többszörösre is.

Megjegyzés.

Az előző tétel szerint a lnko (és a lkkt) nem egyértelmű, ezért általában nem azt írjuk, hogy $d = \text{lnko}\,(a, b)$, hanem azt, hogy $d \sim \text{lnko}\,(a, b)$. (Az egész számok gyűrűjében megállapodtunk abban, hogy mindig a nemnegatív legnagyobb közös osztót vesszük, test feletti polinomgyűrűben pedig mindig választhatunk főpolinomot legnagyobb közös osztónak.)

Definíció.

Azt mondjuk, hogy az $a, b \in R$ elemek *relatív prímek*, ha $\text{lnko}\,(a, b) \sim 1$.

A legnagyobb közös osztó tulajdonságai

Tétel.
Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor minden $a, b, c \in R$ esetén teljesülnek az alábbiak:

(1) $\operatorname{Inko}(\operatorname{Inko}(a, b), c) \sim \operatorname{Inko}(a, \operatorname{Inko}(b, c))$

(2) $\operatorname{Inko}(a, b) \sim \operatorname{Inko}(b, a)$

(3) $\operatorname{Inko}(a, b) \sim a \iff a \mid b$

(4) $\operatorname{Inko}(a, a) \sim a$

(5) $\operatorname{Inko}(0, a) \sim a$

(6) $\operatorname{Inko}(1, a) \sim 1$

A legnagyobb közös osztó tulajdonságai

(7) $\mathrm{lnko}\,(a,b)\cdot c \sim \mathrm{lnko}\,(ac,bc)$

Biz: $c \mid ac, bc \overset{\text{(L2)}}{\Longrightarrow} c \mid \mathrm{lnko}(ac,bc) \Longrightarrow \exists d \in R\colon \mathrm{lnko}(ac,bc) \sim dc.$

Azt kell ellenőrizni, hogy $\mathrm{lnko}(a,b) \sim d$. Tfh. $c \neq 0$.

(L1): $dc \sim \mathrm{lnko}(ac,bc) \overset{\text{(L1)}}{\Longrightarrow} dc \mid ac, bc \overset{c\neq 0}{\Longrightarrow} d \mid a, b.$

(L2): $k \mid a, b \Longrightarrow kc \mid ac, bc \overset{\text{(L2)}}{\Longrightarrow} kc \mid dc \overset{c\neq 0}{\Longrightarrow} k \mid d.$

(8) $\mathrm{lnko}\,(a,b) \not\sim 0 \Longrightarrow \frac{a}{\mathrm{lnko}(a,b)} \perp \frac{b}{\mathrm{lnko}(a,b)}$

Biz: Legyen $d \sim \mathrm{lnko}(a,b) \not\sim 0$.

$\mathrm{lnko}\left(\frac{a}{d}, \frac{b}{d}\right)\cdot d \overset{(7)}{\sim} \mathrm{lnko}(a,b) \sim d \Longrightarrow \mathrm{lnko}\left(\frac{a}{d}, \frac{b}{d}\right) \sim 1$

(9) $a \perp b \Longrightarrow \mathrm{lnko}\,(a,bc) \sim \mathrm{lnko}\,(a,c)$

Biz:

A legnagyobb közös osztó tulajdonságai

Következmény.

Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R, a \perp b$ esetén teljesülnek az alábbiak:

(1) $a \mid bc \iff a \mid c$

Biz: $a \mid bc \iff \text{lnko}\,(a, bc) \sim a \iff \text{lnko}\,(a, c) \sim a \iff a \mid c$

(2) ($a \mid c$ és $b \mid c$) $\iff ab \mid c$

Biz: $a \mid b \cdot \frac{c}{b} \implies a \mid \frac{c}{b} \implies ab \mid c$ □

Következmény.

Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R, \text{lnko}\,(a, b) \nsim 0$ esetén

$$a \mid bc \iff \frac{a}{\text{lnko}\,(a, b)} \,\Big|\, c.$$

Bizonyítás.

A $d \sim \text{lnko}(a, b)$ jelölést használva:

$$a \mid bc \iff d \cdot \frac{a}{d} \,\Big|\, d \cdot \frac{b}{d} \cdot c \iff \frac{a}{d} \,\Big|\, \frac{b}{d} \cdot c \iff \frac{a}{d} \,\Big|\, c.$$ □

Legkisebb közös többszörös

Következmény.

Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor bármely két elemnek létezik legkisebb közös többszöröse is, és minden $a, b \in R$ esetén

$$\operatorname{lnko}(a, b) \cdot \operatorname{lkkt}(a, b) \sim ab.$$

Bizonyítás.

Ha $a = b = 0$, akkor $\operatorname{lnko}(a, b) \sim \operatorname{lkkt}(a, b) \sim 0$. Ellenkező esetben $d := \operatorname{lnko}(a, b) \nsim 0$. Megmutatjuk, hogy $t := \frac{ab}{d}$ eleget tesz a legkisebb közös többszörös definíciójának.

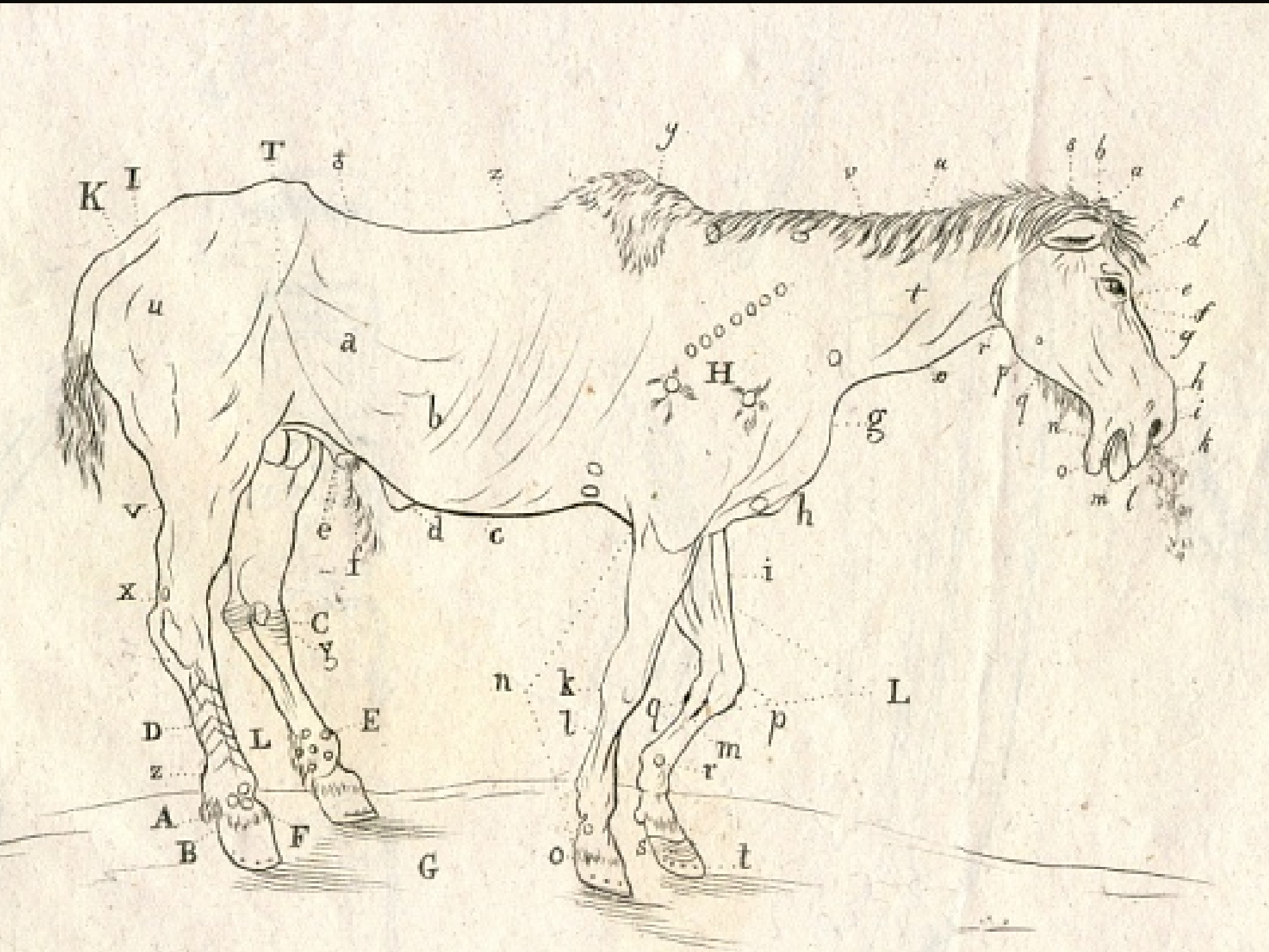
(T1) $a \overset{?}{\mid} t$ és $b \overset{?}{\mid} t$:

Világos, hiszen $t = \frac{a}{d} \cdot b = a \cdot \frac{b}{d}$.

(T2) $\forall k \in R : (a \mid k \text{ és } b \mid k) \overset{?}{\Longrightarrow} t \mid k$:

$$a, b \mid k \implies \tfrac{a}{d}, \tfrac{b}{d} \mid \tfrac{k}{d} \implies \tfrac{a}{d} \cdot \tfrac{b}{d} \mid \tfrac{k}{d} \implies \tfrac{ab}{d} \mid k$$

□


K
I
T
s
y
z
v
u
a
b
c
d
e
f
g
h
i
k
l
m
n
o
p
q
r
t
H
L
C
D
E
F
G
A
B

A legnagyobb közös osztó létezése

Példa.
A $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\right\} = \left\{a + b\sqrt{5}i \colon a, b \in \mathbb{Z}\right\}$ integritástartományban nem létezik bármely két elemnek legnagyobb közös osztója. Legyen $u = 6$ és $v = 2 + 2\sqrt{-5}$.

$$
\begin{aligned}
D_u &= \left\{\pm 1, \pm 2, \pm 3, \pm\left(1 + \sqrt{-5}\right), \pm\left(1 - \sqrt{-5}\right), \pm 6\right\} \\
D_v &= \left\{\pm 1, \pm 2, \pm\left(1 + \sqrt{-5}\right), \pm\left(2 + \sqrt{-5}\right)\right\} \\
D_u \cap D_v &= \left\{\pm 1, \pm 2, \pm\left(1 + \sqrt{-5}\right)\right\}
\end{aligned}
$$

A $\left(D_u \cap D_v / \sim; |\right)$ részbenrendezett halmaznak nincs legnagyobb eleme, ezért $\operatorname{lnko}(u, v)$ nem létezik.

Oszthatóság, asszociáltság, egységek

Legnagyobb közös osztó

Irreducibilitás és prímtulajdonság

Euklideszi gyűrűk

Gauss-gyűrűk

Irreducibilitás és prímtulajdonság

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

Definíció.

Azt mondjuk, hogy a $p \in R$ elem *irreducibilis* (vagy *felbonthatatlan*), 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 faktorizációról* beszélünk.) Formálisan:

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

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:

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

Irreducibilitás vs. prímtulajdonság

Tétel.

Minden integritástartományban a prímelemek irreducibilisek.

Bizonyítás.

Legyen R egy tetszőleges integritástartomány és $p \in R$ egy prímelem. Ekkor $p \not\sim 0, 1$, 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. $\square$

Irreducibilitás vs. prímtulajdonság

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

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 $p \mid a$. $\square$

Példa.

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

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

Oszthatóság, asszociáltság, egységek

Legnagyobb közös osztó

Irreducibilitás és prímtulajdonság

Euklideszi gyűrűk

Gauss-gyűrűk

Euklideszi gyűrűk

A következőkben speciális integritástartományokat vizsgálunk, amelyekben létezik bármely két elemnek legnagyobb közös osztója. Az egész számok körében a maradékos osztás, illetve az arra épülő euklideszi algoritmus garantálta a legnagyobb közös osztó létezését. Az euklideszi gyűrű fogalma ezt a tulajdonságot általánosítja.

Definíció.

Az R integritástartományt *euklideszi gyűrűnek* nevezzük, ha létezik olyan $\|\cdot\| : R \to \mathbb{N}_0$, $a \mapsto \|a\|$ leképezés (úgynevezett *euklideszi norma*), amire teljesülnek az alábbiak tetszőleges $a \in R$ és $b \in R \setminus \{0\}$ esetén:

(1) $\|a\| = 0 \iff a = 0$;

(2) $a \mid b \implies \|a\| \leq \|b\|$;

(3) $\exists q, r \in R : a = bq + r$ és $\|r\| < \|b\|$.

Megjegyzés.

A fenti $a = bq + r$ előállítást itt is *maradékos osztásnak* nevezzük (q a *hányados*, r a *maradék*). A maradékos osztás lehetővé teszi az *euklideszi algoritmus* elvégzését.

Nevezetes euklideszi gyűrűk

Tétel.

Az egész számok gyűrűjén $\|a\| = |a|$, test feletti polinomgyűrűn $\|f\| = 2^{\deg f}$ (a $2^{-\infty} = 0$ megállapodással), a Gauss-egészek gyűrűjén pedig $\|z\| = |z|^2$ euklideszi normát definiál. Ezek tehát mind euklideszi gyűrűk.

Megjegyzés.

Az előző tételben furcsának tűnhet a test feletti polinomgyűrűkre megadott euklideszi norma. Az exponenciális függvényre csak azért volt szükség, hogy a nulla polinomnak (de csak annak!) nulla legyen a normája. Ugyanezt elérhetjük másképpen is, például legyen

$$\|f\| = \begin{cases} \deg f + 1, & \text{ha } f \neq 0; \\ 0, & \text{ha } f = 0. \end{cases}$$

Euklideszi algoritmus euklideszi gyűrűben

Tétel.

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

Bizonyítás.

Szinte szóról szóra ugyanaz, mint egész számokra. Hajtsuk végre az $a =: r_0 \neq 0$ és $b =: r_1 \neq 0$ 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 $r_{n+1} = 0$. Ekkor $\operatorname{Inko}(a, b) \sim r_n$, és a szokásos visszahelyettesítésekkel kapunk minden i-re olyan $x_i, y_i \in R$ elemeket, amelyekre $ax_i + by_i = r_i$. □

Valódi osztó normája

Lemma.

Legyen R euklideszi gyűrű, $a, b \in R$ és $b \neq 0$. Ha a valódi osztója b-nek, azaz $a \mid b$ és $a \nsim b$, akkor $\|a\| < \|b\|$.

Bizonyítás.

Mivel $b \neq 0$, eloszthatjuk a-t b-vel maradékosan:

$$\exists q, r \in R\colon \ a = bq + r \ \text{ és } \ \|r\| < \|b\|.$$

Meg fogjuk mutatni, hogy

$$\|a\| \leq \|r\| < \|b\|.$$

1. $b \nmid a \implies r \neq 0$
2. $a \mid b \implies a \mid a - bq = r$
3. ($a \mid r$ és $r \neq 0$) $\implies \|a\| \leq \|r\|$ □

A számelmélet alaptétele euklideszi gyűrűkben

Tétel.

Euklideszi gyűrűben minden a nullától és az egységektől különböző elem irreducibilis elemek szorzatára bomlik, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű.

Formálisan: ha R euklideszi gyűrű és $a \in R$, $a \neq 0, a \nsim 1$, akkor 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 $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

Bizonyítás.

Egzisztencia: Ha $a \nsim 0, 1$ és a nem irreducibilis, akkor van nemtriviális felbontása. A tényezőket megint felbontjuk, ha lehet, és így folytatjuk a felbontogatást, amíg minden tényező irreducibilis lesz.
Ha ez az eljárás nem érne véget véges sok lépésben, akkor kapnánk egy végtelen osztósorozatot: $\cdots \mid a_3 \mid a_2 \mid a_1 \mid a$, ahol minden oszthatóság valódi.
Az előző lemma szerint ekkor $\|a\| > \|a_1\| > \|a_2\| > \|a_3\| > \cdots$, ez pedig nem lehetséges, mert a normák mind nemnegatív egész számok.

A számelmélet alaptétele euklideszi gyűrűkben

Tétel.

Ha R euklideszi gyűrű és $a \in R$, $a \neq 0, a \nsim 1$, akkor 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 $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

Bizonyítás.

Unicitás: Tfh. $a \sim p_1 \cdot \ldots \cdot p_n \sim q_1 \cdot \ldots \cdot q_m$ két irreducibilis faktorizáció. Mivel p_1 osztója a bal oldalnak, osztója a jobb oldalnak is, és így p_1 prímtulajdonsága miatt $p_1 \mid q_i$ valamely i-re. Ez csak úgy lehet, hogy $p_1 \sim q_i$, mert q_i irreducibilis.

Így tehát p_1-gyel (q_i-vel) egyszerűsíthetünk. Ezt folytatjuk addig, amíg el nem fogynak a tényezők. Végül kapunk egy párbaállítást a $p_1, \ldots, p_n$ elemek és a $q_1, \ldots, q_m$ elemek között úgy, hogy az egy párba tartozó elemek asszociáltak. Tehát $n = m$ és a két felbontás lényegében (sorrend és asszociáltság erejéig) megegyezik. $\square$

Gauss-egészek normája

Definíció.
Az $\alpha = a + bi \in \mathbb{Z}[i]$ Gauss-egész normája: $\|\alpha\| = |\alpha|^2 = \alpha\overline{\alpha} = a^2 + b^2$.

Tétel.
Tetszőleges $\alpha, \beta \in \mathbb{Z}[i]$ Gauss-egészek esetén teljesülnek az alábbiak:

(1) $\|\alpha \cdot \beta\| = \|\alpha\| \cdot \|\beta\|$

Biz: $\|\alpha \cdot \beta\| = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = \|\alpha\| \cdot \|\beta\|$

(2) $\alpha \mid \beta \implies \|\alpha\| \,\Big|\, \|\beta\|$

Biz: $\alpha \mid \beta \implies \exists \gamma \in \mathbb{Z}[i] \colon \beta = \alpha \cdot \gamma$
$\implies \|\beta\| = \|\alpha\| \cdot \|\gamma\| \implies \|\alpha\| \,\Big|\, \|\beta\|$

(3) $\alpha \mid 1 \iff \|\alpha\| = 1$

Biz: $\implies$: következik (2)-ből.
$\impliedby$: következik abból, hogy $\alpha \,\Big|\, \|\alpha\| = \alpha\overline{\alpha}$.

Gauss-egészek normája

Következmény.

A Gauss-egészek gyűrűjének egységcsoportja: $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

Bizonyítás.

$\alpha = a + bi \in \mathbb{Z}[i]^* \iff \|\alpha\| = 1 \iff a^2 + b^2 = 1$ □

Tétel.

Tetszőleges $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ esetén léteznek olyan ϑ, ρ Gauss-egészek, amelyekre $\alpha = \beta \cdot \vartheta + \rho$ és $\|\rho\| < \|\beta\|$.

Bizonyítás.

Tetszőleges ϑ esetén a $\rho := \alpha - \beta \cdot \vartheta$ választással teljesülni fog az $\alpha = \beta \cdot \vartheta + \rho$ egyenlőség. A „kunszt" az, hogy olyan ϑ Gauss egészet találjunk, amelyre $\|\rho\| = \|\alpha - \beta \cdot \vartheta\| < \|\beta\|$. Ez ekvivalens azzal, hogy

$$\left| \frac{\alpha}{\beta} - \vartheta \right| < 1.$$

Ha ϑ az $\frac{\alpha}{\beta}$ komplex számhoz legközelebb eső Gauss-egész a komplex számsíkon, akkor ez teljesülni fog. □

A Gauss-egészek gyűrűje euklideszi

Következmény.

A Gauss-egészek gyűrűje euklideszi gyűrű az $\|\alpha\| = |\alpha|^2$ euklideszi normával.

Következmény.

A Gauss-egészek gyűrűjében érvényes a számelmélet alaptétele: minden $\alpha \in \mathbb{Z}[i] \setminus \{0, 1, -1, i, -i\}$ Gauss-egész felbomlik Gauss-prímek szorzatára, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű.

Gauss-prímek

Lemma.

Minden $\pi \in \mathbb{Z}[i]$ Gauss-prímhez van olyan $p \in \mathbb{N}$ prím, amelyre $\pi \mid p$.

Bizonyítás.

$\pi \mid \pi \cdot \overline{\pi} = \|\pi\| = p_1 \cdot \ldots \cdot p_n \implies \exists k \colon \pi \mid p_k$ □

Lemma.

Ha a $p \in \mathbb{N}$ prímszám nem Gauss-prím, akkor $\mathbb{Z}[i]$-beli prímfelbontása így fest: $p = \pi \cdot \overline{\pi}$.

Bizonyítás.

Ha p nem Gauss-prím, akkor felbomlik Gauss-prímek szorzatára:

$$p = \pi_1 \cdot \ldots \cdot \pi_n \qquad (n \geq 2).$$

Vegyük mindkét oldal normáját:

$$p^2 = \|p\| = \|\pi_1\| \cdot \ldots \cdot \|\pi_n\|.$$

Ez csak úgy lehetséges, hogy $n = 2$ és $\|\pi_1\| = \|\pi_2\| = p$.

Ekkor $\|\pi_1\| = \pi_1 \cdot \overline{\pi_1} = p$. □

Gauss-prímek

Példa.

- $2 = (1+i)\cdot(1-i) \sim (1+i)^2$
- 3 Gauss-prím
- $5 = (2+i)\cdot(2-i)$

Tétel.

(1) A 2 prímszám felbomlik $\mathbb{Z}[i]$-ben: $2 = (1+i)\cdot(1-i) \sim (1+i)^2$.

(2) Ha a p prímszám $4k+3$ alakú, akkor p a $\mathbb{Z}[i]$ gyűrűben is felbonthatatlan.

(3) Ha a p prímszám $4k+1$ alakú, akkor a $\mathbb{Z}[i]$ gyűrűben két Gauss-prím szorzatára bomlik: $p = (a+bi)\cdot(a-bi) = a^2+b^2$.

A Gauss-egészek gyűrűjének irreducibilis elemei éppen a fenti felbontásokban szereplő elemek (asszociáltság erejéig).

Gauss-prímek

Bizonyítás.

(1) Trivi.

(2) Ha p nem lenne Gauss-prím, akkor

$$p = (a + bi) \cdot (a - bi) = a^2 + b^2.$$

A modulo 4 maradékok vizsgálatával belátható, hogy ez $p \equiv 3 \pmod 4$ esetén nem lehetséges.

(3) Ha $p \equiv 1 \pmod 4$, akkor -1 négyzetes maradék modulop p, azaz $k^2 \equiv -1 \pmod p$ alkalmas k egész számmal. Ekkor

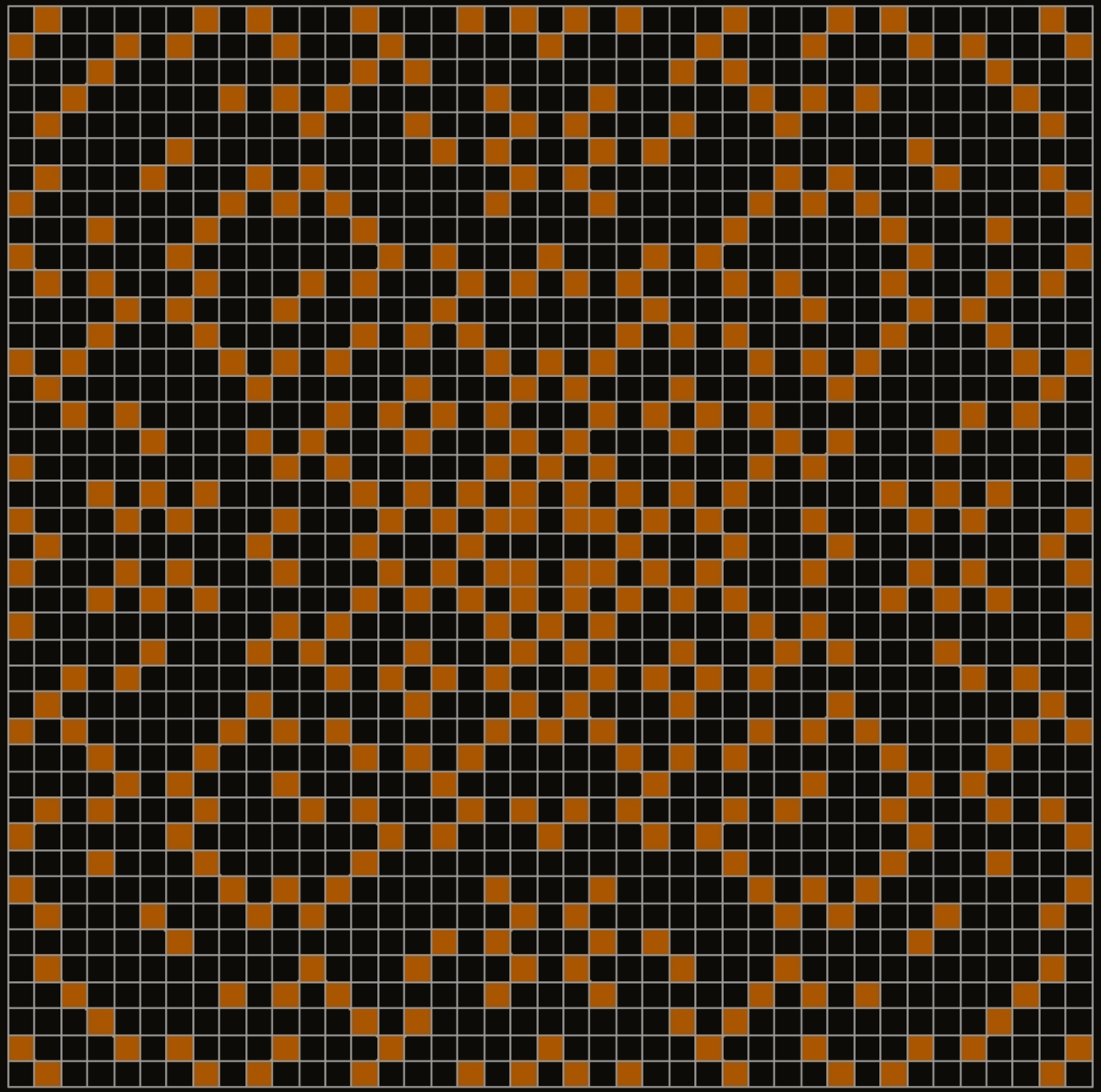
$$p \mid k^2 + 1 = (k + i)(k - i).$$

Ha p Gauss-prím lenne, akkor ebből az következne, hogy

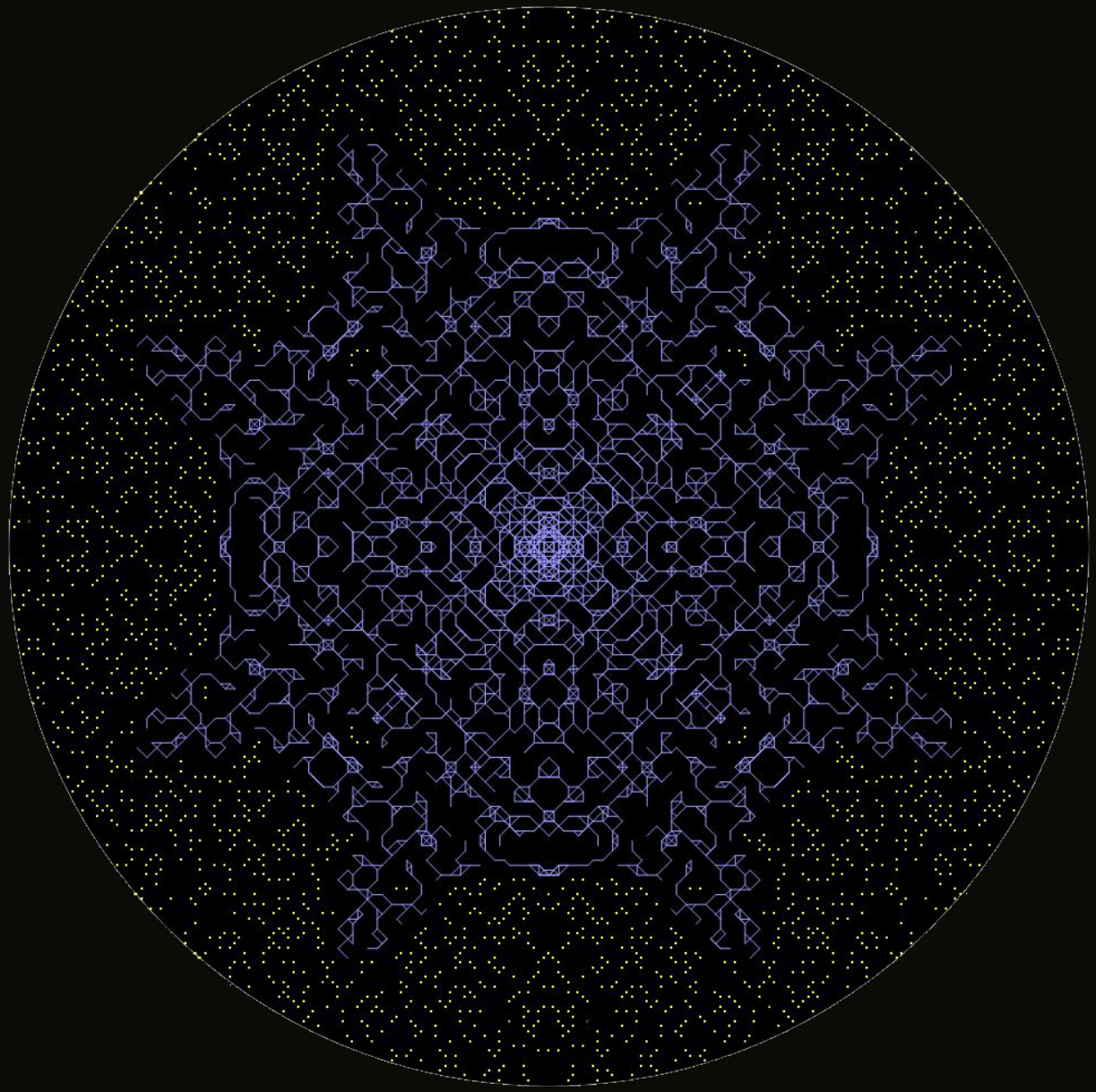
$$p \mid k + i \text{ vagy } p \mid k - i,$$

de egyik sem lehetséges. □

Gauss-prímek



Gauss-prímek



Kétnégyzetszám-tétel

Tétel (Fermat).

Egy pozitív egész akkor és csak akkor bontható két négyzetszám összegére, ha prímhatványtényezős felbontásában a $4k+3$ alakú prímek páros kitevővel szerepelnek.

Bizonyítás.

A két négyzetszám összegeként előálló pozitív egészek pontosan a nemnulla Gauss-egészek normái. Tekintsük egy tetszőleges $0 \neq \zeta$ Gauss-egész prímfelbontását $\mathbb{Z}[i]$-ben:

$$\zeta \sim (1+i)^{\ell} \cdot p_1^{n_1} \cdot \ldots \cdot p_s^{n_s} \cdot \pi_1^{m_1} \cdot \ldots \cdot \pi_r^{m_r}, \text{ ahol}$$

(1) $\ell \in \mathbb{N}_0$,

(2) mindegyik p_j egy $4k+3$ alakú prímszám, $s \in \mathbb{N}_0$, $n_j \in \mathbb{N}$,

(3) mindegyik π_j olyan Gauss-prím, amelynek normája $q_j := \|\pi_j\|$ egy $4k+1$ alakú prímszám, $r \in \mathbb{N}_0$, $m_j \in \mathbb{N}$,

Ekkor ζ normája:

$$\|\zeta\| = 2^{\ell} \cdot p_1^{2n_1} \cdot \ldots \cdot p_s^{2n_s} \cdot q_1^{m_1} \cdot \ldots \cdot q_r^{m_r}. \qquad \square$$

Oszthatóság, asszociáltság, egységek

Legnagyobb közös osztó

Irreducibilitás és prímtulajdonság

Euklideszi gyűrűk

Gauss-gyűrűk

Gauss-gyűrűk

Definíció.
Gauss-gyűrűnek 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 $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

Gauss-gyűrűk

Amikor bebizonyítottuk, hogy minden euklideszi gyűrűben érvényes a számelmélet alaptétele, akkor tulajdonképpen azt láttuk be, hogy minden euklideszi gyűrű Gauss-gyűrű.

(Ennek az állításnak a megfordítása nem igaz, például $\mathbb{Z}[x]$ Gauss-gyűrű, de nem euklideszi.)

A bizonyítás az euklideszi gyűrűk alábbi két tulajdonságon múlt:

($\nexists\searrow$) Az $(R/\sim;|)$ részbenrendezett halmazban nincsen végtelen szigorúan csökkenő sorozat, vagyis ha $\cdots \mid a_3 \mid a_2 \mid a_1$, akkor van olyan $k \in \mathbb{N}$, amelyre $a_k \sim a_{k+1} \sim a_{k+2} \sim \cdots$.

($\exists$ Inko) R-ben bármely két elemnek létezik legmagyobb közös osztója (és így minden irreducubilis elem prím).

Gauss-gyűrűk

Tétel.

Legyen R Gauss-gyűrű, és legyen $a, b \in R$ prímfelbontása

$$a \sim p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \text{ és } b \sim p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}.$$

Ekkor teljesülnek az alábbiak:

(1) $a \mid b \iff \alpha_i \leq \beta_i \ \ (i = 1, \ldots, n)$;

(2) $\text{Inko}\,(a, b) \sim p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$;

(3) $\text{Ikkt}\,(a, b) \sim p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

Bizonyítás.

Ugyanaz mint az egész számok esetén, felhasználva a prímfelbontás létezését és egyértelműségét. □

Következmény.

Egy integritástartomány akkor és csak akkor Gauss-gyűrű, ha teljesíti a $(\nexists \searrow)$ és $(\exists\,\text{Inko})$ feltételeket.

Amikor azt mondják az ötödéves matekosok, hogy a tavaszi absztrakt algebra az őszinek a hatványozott nehezítése...