Klasszikus algebra előadás

Waldhauser Tamás
2014. április 28.

5. Számelmélet integritástartományokban

Oszthatóság

Mostantól R mindig tetszőleges integritástartományt jelöl.

5.1. 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.

5.2. 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

5.2. Tétel (folyt.).

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

(3) $(a \mid b \text{ és } b \mid a) \iff \exists u \in R^* : b = ua$

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

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

(4) $1 \mid a$

Biz: $a = 1 \cdot a$

(5) $a \mid 0$

Biz: $0 = a \cdot 0$

(6) $a \mid 1 \iff a \in R^*$

Biz: $a \mid 1 \iff \exists u \in R : 1 = au \iff a \in R^*$

5.2. Tétel (folyt.).

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

(7) $0 \mid a \iff a = 0$

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

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

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

(9) $a \mid b \implies a \mid bc$

Biz: $b = au \implies bc = a(uc)$

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

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

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

□

Asszociáltság

5.3. Megjegyzés.

Amint az első két tulajdonság mutatja, az oszthatósági reláció reflexív és tranzitív, de a (3) tulajdonság szerint általában nem antiszimmetrikus (így nem is részbenrendezés). Ezen próbálunk segíteni az asszociáltsági reláció bevezetésével.

5.4. 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 $b \mid a$.

5.5. Tétel.

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

5.6. 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.

Asszociáltság

5.7. 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.

Test feletti polinomgyűrű esetén minden asszociáltsági osztály (a nulláét kivéve) pontosan egy főpolinomot tartalmaz, itt tehát asszociáltság erejéig mindig dolgozhatunk főpolinomokkal. Egy tetszőleges integritástartományban azonban általában nincsenek kitüntetett elemek az asszociáltsági osztályokban.

Kongruencia

5.8. Definíció.

Legyen $a, b, m \in R$. Ha $a - b$ osztható m-mel, akkor azt mondjuk, hogy *a kongruens b-vel modulo m*. Az m elemet a kongruencia *modulus*ának nevezzük.

Jelölés.

A kongruenciát ugyanúgy jelöljük, mint az egész számok gyűrűjében:
$a \equiv b \pmod{m} \iff m \mid a - b$.

5.9. Állítás.

A mod m *kongruencia ekvivalenciareláció az R halmazon, továbbá „szabad" kongruenciákat összeadni, kivonni és összeszorozni: tetszőleges $a_1, b_1, a_2, b_2 \in R$ elemekre*

$$\left.\begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array}\right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}, \; a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

Az 5.9. Állítás bizonyítása

reflexivitás: $a \equiv a \pmod m \iff m \mid a - a = 0$

szimmetria: $a \equiv b \pmod m \implies m \mid a - b$

$\implies m \mid (-1) \cdot (a - b) = b - a$

$\implies b \equiv a \pmod m$

tranzitivitás: $a \equiv b$ és $b \equiv c \pmod m \implies m \mid a - b$ és $m \mid b - c$

$\implies m \mid (a - b) + (b - c) = a - c$

$\implies a \equiv c \pmod m$

Tfh. $a_1 \equiv b_1 \pmod m$ és $a_2 \equiv b_2 \pmod m$. Ekkor $m \mid a_1 - b_1$ és $m \mid a_2 - b_2$.

$a_1 \cdot a_2 \overset{?}{\equiv} b_1 \cdot b_2 \pmod m \iff m \overset{?}{\mid} a_1 a_2 - b_1 b_2$

$\iff m \overset{?}{\mid} a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2$

$\iff m \overset{?}{\mid} (a_1 - b_1) \cdot a_2 + b_1 \cdot (a_2 - b_2)$

Az összeadásra és kivonásra vonatkozó állítások hasonlóan igazolhatók (HF). □

Maradékosztály-gyűrű

5.10. Definíció.

A mod m kongruenciához tartozó ekvivalenciaosztályokat modulo m *maradékosztály*oknak nevezzük.

Jelölés.

Az $a \in R$ elemet tartalmazó modulo m maradékosztályt $\overline{a}$ jelöli (ha a modulus világos a szövegkörnyezetből), a maradékosztályok halmazát (vagyis a modulo m kongruenciához tartozó faktorhalmazt) pedig $R/(m)$ jelöli.
Tehát $R/(m) = \{\overline{a} : a \in R\}$.

5.11. Definíció.

A modulo m maradékosztályok halmazán értelmezzük az összeadást, az additív inverz képzését és a szorzást a következőképpen: tetszőleges $a, b \in R$ esetén legyen $\overline{a} + \overline{b} = \overline{a+b}$, $-\overline{b} = \overline{-b}$, $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

5.12. Állítás.

A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (addditív inverze, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel $R/(m)$ kommutatív egységelemes gyűrűt alkot.

Az 5.12. Állítás bizonyítása

A műveletek jóldefiniáltságát az 5.9. Állítás biztosítja. Például (a többi HF):

$$\begin{aligned} \overline{u_1} = \overline{v_1} \text{ és } \overline{u_2} = \overline{v_2} &\implies u_1 \equiv v_1 \text{ és } u_2 \equiv v_2 \pmod{m} \\ &\implies u_1 + u_2 \equiv v_1 + v_2 \pmod{m} \\ &\implies \overline{u_1 + u_2} = \overline{v_1 + v_2} \end{aligned}$$

Az azonosságokat (asszociativitás, kommutativitás, disztributivitás) „örökli” az $R/(m)$ faktorgyűrű az R gyűrűtől. Például (a többi HF):

$$\overline{u} \cdot (\overline{v} + \overline{w}) = \overline{u} \cdot \overline{v + w} = \overline{u \cdot (v + w)} = \overline{u \cdot v + u \cdot w} = \overline{u \cdot v} + \overline{u \cdot w} = \overline{u} \cdot \overline{v} + \overline{u} \cdot \overline{w}$$

additív egységelem: $\overline{0}$

$$\overline{u} + \overline{0} = \overline{u + 0} = \overline{u}$$

$\overline{u}$ additív inverze: $\overline{-u}$

$$\overline{u} + \overline{-u} = \overline{u + (-u)} = \overline{0}$$

multiplikatív egységelem: $\overline{1}$

$$\overline{u} \cdot \overline{1} = \overline{u \cdot 1} = \overline{u}$$

□

Legnagyobb közös osztó

Az oszthatóság és a kongruencia fogalmát és alaptulajdonságait szinte szó szerint lehetett 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.

5.13. Definíció.

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

(1) $d \mid a$ és $d \mid b$;

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

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

(1) $a \mid t$ és $b \mid t$;

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

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

5.14. Megjegyzés.

Ha az a elem osztóinak halmazát D_a jelöli, akkor $\operatorname{lnko}(a, b)$ asszociáltsági osztálya nem más, mint a $(D_a \cap D_b / \sim; |)$ 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 (lásd az 1.14. Megjegyzést a Bevezetés a számelméletbe tárgy előadásvázlatában).

A titkos csodafegyver

Jelölés.

Tetszőleges $a \in R$ esetén legyen $D_a = \{k \in R \colon k \mid a\}$.

Állítás.

Minden $a, b \in R$ *esetén* $a \mid b \iff D_a \subseteq D_b$.

Bizonyítás.

$a \mid b \overset{?}{\Longrightarrow} D_a \subseteq D_b$: Tfh. $a \mid b$, és legyen $k \in D_a$.
Ekkor $k \mid a \mid b$, tehát az oszthatóság tranzitivitása miatt $k \in D_b$.

$D_a \subseteq D_b \overset{?}{\Longrightarrow} a \mid b$: Tfh. $D_a \subseteq D_b$.
Ekkor $a \in D_a$ miatt $a \in D_b$ teljesül, ezért $a \mid b$. □

Következmény.

Minden $a, b \in R$ *esetén* $a \sim b \iff D_a = D_b$.

Bizonyítás.

$a \sim b \iff a \mid b$ és $b \mid a \iff D_a \subseteq D_b$ és $D_b \subseteq D_a \iff D_a = D_b$ □

A titkos csodafegyver

Tétel.

Tetszőleges $a, b, d \in R$ esetén d akkor és csak akkor legnagyobb közös osztója a-nak és b-nek, ha $D_a \cap D_b = D_d$.

Bizonyítás.

Először tegyük fel, hogy d legnagyobb közös osztója a-nak és b-nek.

$D_a \cap D_b \overset{?}{\subseteq} D_d$: Minden $k \in R$ esetén

$$k \in D_a \cap D_b \implies k \mid a, b \overset{(2)}{\implies} k \mid d \implies k \in D_d.$$

$D_d \overset{?}{\subseteq} D_a \cap D_b$: Minden $k \in R$ esetén

$$k \in D_d \implies k \mid d \overset{(1)+\text{tr.}}{\implies} k \mid a, b \implies k \in D_a \cap D_b.$$

Most tegyük fel, hogy $D_a \cap D_b = D_d$.

(1) $d \overset{?}{\mid} a$ és $d \overset{?}{\mid} b$: $d \in D_d = D_a \cap D_b \implies d \mid a, b$

(2) $\forall k \in R : (k \mid a \text{ és } k \mid b) \overset{?}{\implies} k \mid d$: Minden $k \in R$ esetén

$$k \mid a \text{ és } k \mid b \implies k \in D_a \cap D_b = D_d \implies k \mid d.$$

□

A legnagyobb közös osztó egyértelműsége

5.15. 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.

Bizonyítás.

1. Tfh. d_1 és d_2 is legnagyobb közös osztója a-nak és b-nek.
   Ekkor $D_{d_1} = D_a \cap D_b = D_{d_2} \implies d_1 \sim d_2$.
2. Tfh. d_1 legnagyobb közös osztója a-nak és b-nek, és $d_1 \sim d_2$.
   Ekkor $D_{d_2} = D_{d_1} = D_a \cap D_b \implies d_2$ is lnko-ja a-nak és b-nek. □

5.16. 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.)

A legnagyobb közös osztó tulajdonságai

5.17. Definíció.

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

5.18. Tétel.

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

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

Biz: $D_{(a,b)} \cap D_c = (D_a \cap D_b) \cap D_c = D_a \cap (D_b \cap D_c) = D_a \cap D_{(b,c)}$
$\Longrightarrow ((a, b), c) \sim (a, (b, c))$

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

Biz: $D_{(a,b)} = D_a \cap D_b = D_b \cap D_a = D_{(b,a)} \Longrightarrow (a, b) \sim (b, a)$

(3) $\operatorname{lnko}(a, a) \sim a$

Biz: $D_{(a,a)} = D_a \cap D_a = D_a \Longrightarrow (a, a) \sim a$

(4) $\operatorname{lnko}(0, a) \sim a$

Biz: $D_{(0,a)} = D_0 \cap D_a = R \cap D_a = D_a \Longrightarrow (0, a) \sim a$

A legnagyobb közös osztó tulajdonságai

(5) $\operatorname{lnko}(1, a) \sim 1$

Biz: $D_{(1,a)} = D_1 \cap D_a = R^* \cap D_a = R^* = D_1 \implies (1, a) \sim 1$

(6) $\operatorname{lnko}(a, b) \sim a \iff a \mid b$

Biz: $(a, b) \sim a \iff D_a \cap D_b = D_a \iff D_a \subseteq D_b \iff a \mid b$

(7) $\operatorname{lnko}(a + bc, b) \sim \operatorname{lnko}(a, b)$

Biz: $\forall k \in R : \; k \mid a + bc, b \iff k \mid a, b$

$\implies (a + bc, b) \sim (a, b)$

(8) $\operatorname{lnko}(a, b) \cdot c \sim \operatorname{lnko}(ac, bc)$

Biz: a táblán.

(9) $\operatorname{lnko}(a, b) \nsim 0 \implies \operatorname{lnko}\left(\frac{a}{\operatorname{lnko}(a,b)}, \frac{b}{\operatorname{lnko}(a,b)}\right) \sim 1$

Biz: $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) \cdot (a, b) \sim (a, b) \implies \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) \sim 1$

(10) $\operatorname{lnko}(a, b) \sim 1 \implies \operatorname{lnko}(a, bc) \sim \operatorname{lnko}(a, c)$

Biz: a táblán. □

A legnagyobb közös osztó tulajdonságai

5.19. Következmény.

Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R, \operatorname{lnko}(a, b) \sim 1$ esetén teljesülnek az alábbiak:

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

Biz: $a \mid bc \iff (a, bc) \sim a \iff (a, c) \sim a \iff a \mid c$

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

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

5.20. Következmény.

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

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

Bizonyítás.

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

Legkisebb közös többszörös

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

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

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

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

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

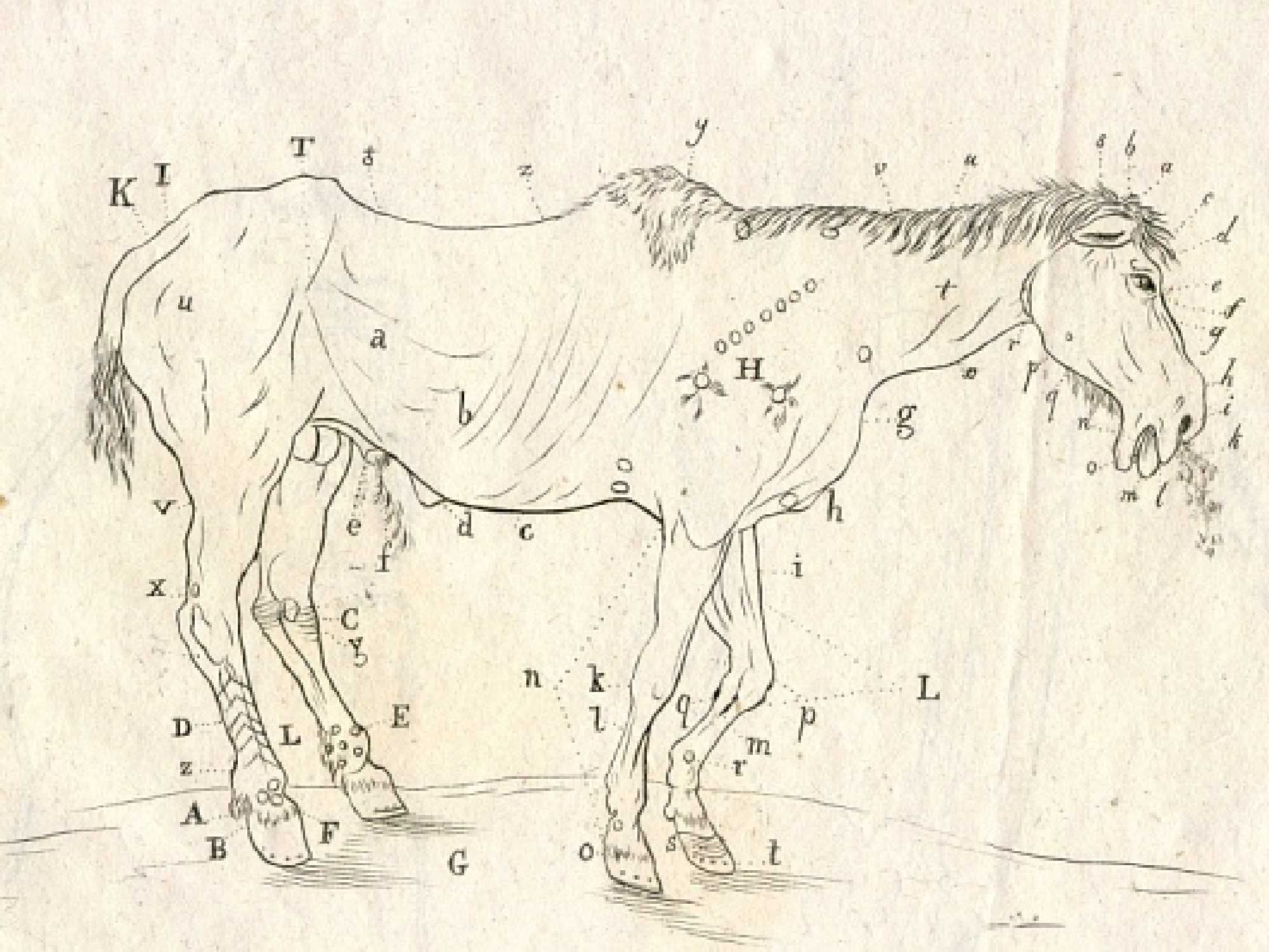
□

A legnagyobb közös osztó létezése

5.22. Megjegyzés.

A legnagyobb közös osztó fenti tulajdonságai közül sokat az egész számok körében ki sem mondtunk, mert a prímtényezős felbontásból triviálisan adódik. Némelyik tulajdonságot még a számelmélet alaptétele előtt láttuk be (hiszen szükségünk volt rájuk az alaptétel bizonyításához), de ezeket is könnyebb volt belátni, mert felhasználhattuk azt, hogy a legnagyobb közös osztó mindig előáll a két elem „lineáris kombinációjaként".

Tetszőleges integritástartományban ez a tulajdonság nem teljesül, és általában egyértelmű prímfelbontás sincs. Sőt, még a legnagyobb közös osztó sem mindig létezik, ezért kezdődik az 5.18 Tétel (és a következményei) úgy, hogy „**Ha** az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, **akkor** . . . ".


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

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 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.

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.

5.23. Definíció.

Az R integritástartományt *euklideszi gyűrű*nek 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 $\|r\| < \|b\|$.

5.24. Megjegyzés.

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

Nevezetes euklideszi gyűrűk

5.25. 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.*

Bizonyítás.

A táblán.

□

5.26. 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

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