ABSZTRAKT ALGEBRA II.
GYŰRŰ- ÉS TESTELMÉLET

Dr. Tóth László egyetemi docens

Pécsi Tudományegyetem, 2005

Bevezetés

Ez az anyag tartalmazza az "Algebra és számelmélet" című tárgy 5. féléves részének kötelező elméleti anyagát és a feldolgozandó feladatoknak nagy részét. Tartalmaz továbbá olyan kiegészítő részeket is, amelyek nem kötelezőek, ezek "★ ★" jelek között szerepelnek. A feladatok előtt ▼ jel áll. A nehezebb feladatokat ▼▼ jelöli.

A tételek, állítások és bizonyítások végét a □ jel mutatja.

Ez a jegyzet az Absztrakt algebra I. jegyzet folytatása, a fejezetek számozása folytatólagos és gyakran hivatkozunk az I. részben található csoportelméleti fogalmakra és tulajdonságokra.

Ezúttal is felhívom a figyelmet

– a definíciók pontos ismeretére (a fogalmak nevei **kövér betűkkel** szedettek),

– az egyes fogalmakra adott példákra (ezek általában • jel után szerepelnek); adjanak, keressenek további példákat az anyag jobb megértése érdekében,

– a Tételek pontos megfogalmazására és a bizonyításokra,

– a kitűzött feladatok megoldására.

További irodalom

1. Szendrei János, Algebra és számelmélet, Nemzeti Tankönyvkiadó, Budapest, 1996.

2. Szendrei Ágnes, Diszkrét matematika, Polygon, Szeged, 2000.

3. Fried Ervin, Általános algebra, Tankönyvkiadó, Budapest, 1981.

4. Fuchs László, Algebra, Tankönyvkiadó, Budapest, 1980.

5. Környei Imre, Algebra (Turán Pál előadásai alapján), Tankönyvkiadó, Budapest, 1974.

Feladatgyűjtemények

1. Varga Árpád, Absztrakt algebra feladatgyűjtemény, Tankönyvkiadó, Budapest, 1983.

2. Varga Árpád, Elemi matematika II. (feladatgyűjtemény), Algebrai struktúrák, PTE, 2000.

3. Bálintné Szendrei Mária, Czédli Gábor, Szendrei Ágnes, Absztrakt algebrai feladatok, Tankönyvkiadó, Budapest, 1988.

10. Gyűrűk és testek

10.A. A gyűrű fogalma, példák

A következőkben kétműveletes struktúrákat vizsgálunk.

Az $(R,+,\cdot)$ algebrai struktúrát **gyűrű**nek nevezzük, ha teljesül a következő három tulajdonság:

1. $(R,+)$ Abel-csoport (ez a gyűrű additív csoportja),

2. $(R,\cdot)$ félcsoport (azaz "$\cdot$" asszociatív),

3. "$\cdot$" **disztributív** a "+"-ra nézve, azaz $\forall a,b,c \in R$ esetén $a(b+c)=ab+ac$ és $(b+c)a=ba+ca$ (bal oldali és jobb oldali disztributivitás).

Megjegyzés. Itt az R jelölés az angol **ring** szó (jelentése: gyűrű) kezdőbetűjéből származik, és nem összetévesztendő az $\mathbb{R}$-rel (valós számhalmaz). Hasonlóan a csoport jelölése általában G (group = csoport), a véges test jelölése F (field = test).

Legyen $(R,+,\cdot)$ egy gyűrű. Az $(R,+)$ csoport semleges elemét a gyűrű **zéruselem**ének nevezzük, jelölés: 0. Azt mondjuk, hogy $(R,+,\cdot)$ **kommutatív gyűrű**, ha $(R,\cdot)$ kommutatív félcsoport. $(R,+,\cdot)$ **egységelemes gyűrű**, ha létezik egységelem a " $\cdot$ " műveletre nézve: $\exists 1 \in R : 1a = a1 = a, \forall a \in R$.

10.A.1. Példák. • $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ kommutatív, egységelemes gyűrűk, az egységelem az 1 szám, a zéruselem pedig a 0 szám.

• Ha $n \in \mathbb{N}, n \geq 2$, akkor $\mathbb{Z}_n = \{\widehat{0},\widehat{1},...,\widehat{n-1}\}$ gyűrű a maradékosztályok összeadására és szorzására nézve: pontosabban $(\mathbb{Z}_n,+,\cdot)$ kommutatív, egységelemes gyűrű, az egységelem az $\widehat{1}$, a zéruselem pedig a $\widehat{0}$ maradékosztály. Ez a **maradékosztályok gyűrűje** (mod n).

• (Függvények gyűrűje) Legyen $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R} | f \text{ függvény}\}$. Az $f,g \in \mathcal{F}$ függvények $f+g$ összegét és fg szorzatát így értelmezzük: $(f+g)(x) = f(x)+g(x)$ és $(fg)(x) = f(x)g(x)$ minden $x \in \mathbb{R}$-re. Ekkor $(\mathcal{F},+,\cdot)$ egy kommutatív és egységelemes gyűrű.

Általánosabban, ha $M \neq \emptyset$ egy halmaz és R egy gyűrű, legyen $R^M = \{f : M \to R | f \text{ függvény}\}$. Akkor $(R^M,+,\cdot)$ gyűrű az $f,g \in R^M$ függvények $f+g$ összegére és fg szorzatára nézve, ahol $(f+g)(x) = f(x)+g(x)$ és $(fg)(x) = f(x)g(x)$, $\forall x \in M$.

• (Mátrixgyűrűk) Legyen R egy gyűrű és $m,n \in \mathbb{N}^*$. Egy $A : \{1,2,...,m\} \times \{1,2,...,n\} \to R$ függvényt $m \times n$ típusú R feletti **mátrix**nak nevezünk, jelölés: $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \in \mathcal{M}_{m,n}(R)$, $\mathcal{M}_n(R) = \mathcal{M}_{n,n}(R)$. A mátrixok összeadására és szorzására nézve $(\mathcal{M}_n(R),+,\cdot)$ gyűrű, amely egységelemes, ha R egységelemes.

• (Gyűrűk direkt szorzata) Legyen $(R_1,+,\cdot)$ és $(R_2,+,\cdot)$ két gyűrű, nem feltétlenül azonos műveletekkel. Az $R_1 \times R_2$ halmazon definiáljuk a következő műveleteket: $(r_1,r_2)+(s_1,s_2) = (r_1+s_1, r_2+s_2)$, $(r_1,r_2)(s_1,s_2) = (r_1s_1, r_2s_2)$. Ekkor $(R_1 \times R_2,+,\cdot)$ gyűrű, az adott gyűrűk ún. **direkt szorzat**a (ellenőrzés !). Ez a konstrukció elvégezhető általánosabban is, ha $(R_i)_{i \in I}$ gyűrűk egy tetszőleges rendszere.

Ha R-nek csak egy eleme van: $R = \{0\}$, akkor a $0+0=0, 0 \cdot 0 = 0$ műveletekkel ez egy gyűrű, az ún. **zérógyűrű**, amely kommutatív és egységelemes: $1 = 0$.

A továbbiakban, ha R egységelemes gyűrű, mindig feltételezzük, hogy $|R| \geq 2$. Ekkor $1 \neq 0$. Valóban, ha $1 = 0$ lenne, akkor $\forall a \in R : a0 = a(0+0) = a0+a0$ (disztributivitás) miatt $a0 = 0$ és így $a = a1 = a0 = 0$, azaz $R = \{0\}$ 1 elemű, ellentmondás.

10.B. Számítási szabályok, zérusosztók

10.B.1. Tétel. (Számítási szabályok gyűrűben) Ha $(R,+,\cdot)$ egy gyűrű és $a,b,c,a_i,b_j \in R$, akkor

1) $a0 = 0a = 0$,

2) $a(b-c)=ab-ac$, $\quad(b-c)a=ba-ca$,

3) $a(-b)=(-a)b=-ab$, $\quad(-a)(-b)=ab$,

4) $(a_1+a_2+\cdots+a_n)(b_1+b_2+\cdots+b_m)=a_1b_1+a_1b_2+\cdots+a_nb_m$,

5) Ha R kommutatív és $n\in\mathbb{N}^*$, akkor $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$.

Bizonyítás. 1) $a0=a(0+0)=a0+a0$ (disztributivitás), ahonnan $a0=0$ és $0a=(0+0)a=0a+0a$ miatt $0a=0$.

2) $ab=a((b-c)+c)=a(b-c)+ac$, ahonnan $a(b-c)=ab-ac$. Hasonlóan a másik.

3) $a(-b)=a(0-b)=a0-ab=0-ab=-ab$ az 1) és 2) szerint.

4) A disztributivitás következménye.

5) $(a+b)^2=(a+b)(a+b)=a^2+ab+ba+b^2=a^2+2ab+b^2$ a kommutativitás miatt, stb. □

Megjegyzés. Egységelemes gyűrű esetén a "+" kommutativitása következménye a gyűrű többi axiómájának.

Valóban, $\forall a,b\in R$ esetén $(a+b)(1+1)=a(1+1)+b(1+1)=a+a+b+b$, ugyanakkor $(a+b)(1+1)=(a+b)1+(a+b)1=a+b+a+b$, ahonnan $a+a+b+b=a+b+a+b$ és $a+b=b+a$.

Ha $(R,+,\cdot)$ egy egységelemes gyűrű, akkor a (szorzásra nézve) invertálható elemek $U(R)$ halmaza csoport: $(U(R),\cdot)$, lásd 3.C. szakasz, ez a **gyűrű egységei**nek csoportja (angolul: unit = egység). Az egységek nem összetévesztendők az egységelemmel.

10.B.2. Példa. • A $(\mathbb{Z}_n,+,\cdot)$ gyűrű egységei: $U(\mathbb{Z}_n)=\{\widehat{x}:(x,n)=1\}$, lásd 3.C. szakasz.

Legyen R egy gyűrű és $a,b\in R$. Ha $a,b\neq 0$ és $ab=0$, akkor az a és b elemeket **zérusosztók**nak nevezzük. Az R gyűrű **zérusosztómentes**, ha nincsenek benne zérusosztók, azaz, ha $\forall x,y\in R: xy=0$ esetén következik, hogy $x=0$ vagy $y=0$. Egy kommutatív, egységelemes, zérusosztómentes gyűrűt **integritástartomány**nak nevezünk.

10.B.3. Példák. • $(\mathbb{Z},+,\cdot)$ integritástartomány.

• Az $\mathcal{M}_2(\mathbb{Z})$ mátrixgyűrűben $A=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ és $B=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ zérusosztók, mert $AB=0$ (nullmátrix). Ezért $(\mathcal{M}_2(\mathbb{Z}),+,\cdot)$ nem integritástartomány.

• A $(\mathbb{Z}_6,+,\cdot)$ gyűrűben $\widehat{2}$ és $\widehat{3}$ zérusosztók, mert $\widehat{2}\cdot\widehat{3}=\widehat{0}$.

10.B.4. Tétel. Ha az R gyűrűben $a\in R$ invertálható, akkor a nem zérusosztó.

Bizonyítás. Ha a invertálható és $ab=0$, akkor a^{-1}-nel szorozva: $a^{-1}ab=0$, ahonnan $b=0$. Hasonlóan, ha $ba=0$, akkor $baa^{-1}=0$, ahonnan $b=0$. □

10.C. A test fogalma, példák

Az $(R,+,\cdot)$ gyűrű neve **test**, ha R legalább két elemű egységelemes gyűrű és minden $a\in R, a\neq 0$ elem invertálható, azaz $U(R)=R\setminus\{0\}$. R **kommutatív test**, ha R test és "$\cdot$" kommutatív.

10.C.1. Tétel. 1) Minden test zérusosztómentes.

2) Az $(R,+,\cdot)$, $|R|\geq 2$ egységelemes gyűrű akkor és csak akkor test, ha $(R^*,\cdot)$ csoport, ahol $R^*=R\setminus\{0\}$.

Bizonyítás. 1) Következik az előbbi tételből.

2) Ha R test, akkor $U(R)=R^*$ és a fentiek szerint $(R^*,\cdot)$ csoport. Közvetlenül: az 1) szerint $\forall x,y\neq 0\Rightarrow xy\neq 0$, tehát R^* zárt a szorzásra nézve és $\forall x\in R^*\Rightarrow\exists x^{-1}\in R^*$ (ha $x^{-1}=0$ lenne, akkor $1=xx^{-1}=x\cdot 0=0$, ellentmondás). Így $(R^*,\cdot)$ csoport.

Fordítva, ha R, $|R|\geq 2$ egységelemes gyűrű és ha $(R^*,\cdot)$ csoport, akkor minden $a\in R, a\neq 0$ elem invertálható, tehát R test. □

10.C.2. Példák. • $(\mathbb{Z},+,\cdot)$ kommutatív gyűrű és nem test, mert pl. a 2 nem invertálható ($2^{-1}=\frac{1}{2}\notin\mathbb{Z}$, az invertálható elemek halmaza $U(\mathbb{Z})=\{-1,1\}$, lásd 3. szakasz).

• $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ kommutatív testek.

• A $(\mathbb{Z}_n,+,\cdot)$ gyűrű akkor és csak akkor test, ha n prímszám (miért ?).

• (A kvaterniók teste) Legyen

$$\mathbb{H}=\left\{\begin{pmatrix} z & w\\ -\overline{w} & \overline{z}\end{pmatrix} : z,w\in\mathbb{C}\right\}\subseteq\mathcal{M}_2(\mathbb{C})$$

Akkor $(\mathbb{H},+,\cdot)$ egy nemkommutatív test, lásd Feladat. $\mathbb{H}$-t a kvaterniók testének nevezzük, ennek elemei a kvaterniók.

10.C.3. Tétel. Minden véges R integritástartomány test.

Bizonyítás. Legyen $a\in R, a\neq 0$. A $t_a : R\to R, t_a(x)=ax$ függvény injektív, mert ha $t_a(x)=t_a(y)$, akkor $ax=ay$, $a(x-y)=0$, s mivel R zérusosztómentes, $x-y=0$, $x=y$ következik. De R véges, ezért t_a szürjektív is és emiatt létezik $x\in R$ úgy, hogy $ax=1$, ahonnan $ax=xa=1$, mert R kommutatív, tehát létezik $a^{-1}=x$. □

Megjegyzések. 1. Ha R egy tetszőleges gyűrű, akkor a $t_a : (R,+)\to(R,+)$, $t_a(x)=ax$ és $t'_a : (R,+)\to(R,+)$, $t'_a(x)=xa$ függvények, ahol $a\in R$ rögzített, csoportmorfizmusuk, mert $t_a(x+y)=a(x+y)=ax+ay=t_a(x)+t_a(y), \forall x,y\in R$ (és hasonlóan a másik).

2. Ha az R gyűrűben a nem zérusosztó és $ab=ac$ vagy $ba=ca$, akkor $b=c$.

3. Igazolható, hogy minden véges test kommutatív (Wedderburn tétele).

10.D. Gyűrű és testmorfizmusok

Legyen $(R,+,\cdot)$ és $(S,+,\cdot)$ két gyűrű és $f : R\to S$ egy függvény. Azt mondjuk, hogy f **gyűrűmorfizmus** (**homomorfizmus**), ha

$$f(x+y)=f(x)+f(y),\qquad f(xy)=f(x)f(y),\qquad \forall x,y\in R,$$

azaz, ha bármely két R-beli elem összegének és szorzatának képe egyenlő a képelemek S-beli összegével, illetve szorzatával.

Ha R és S egységelemesek, akkor az f gyűrűmorfizmus **unitér**, ha $f(1_R)=1_S$, ahol 1_R és 1_S a megfelelő egységelemek.

Az f gyűrűmorfizmus neve **gyűrűizomorfizmus** (röviden **izomorfizmus**), ha f bijektív. Ekkor azt mondjuk, hogy a két gyűrű **izomorf** (algebrailag azonos), jelölés: $R\simeq S$.

Ha $(R,+,\cdot)=(S,+,\cdot)$ azonos gyűrűk, akkor f **endomorfizmus**, jelölés $f\in\mathrm{End}(R)$, illetve bijektivitás esetén **automorfizmus**, jelölés $f\in\mathrm{Aut}(R)$.

Ha R és S testek, akkor **testmorfizmus**ról vagy **testizomorfizmus**ról beszélünk.

• $f : (\mathbb{C},+,\cdot)\to(\mathbb{C},+,\cdot)$, $f(z)=\overline{z}$ homomorfizmus, mert $f(z+w)=\overline{z+w}=\overline{z}+\overline{w}=f(z)+f(w)$ és $f(zw)=\overline{zw}=\overline{z}\cdot\overline{w}=f(z)f(w)$, $\forall z,w\in\mathbb{C}$, pontosabban f automorfizmusa a $(\mathbb{C},+,\cdot)$ testnek.

10.D.1. Tétel. (gyűrűmorfizmusok tulajdonságai) Legyen $f : R\to S$ egy gyűrűmorfizmus. Akkor

(i) $f(0_R)=0_S$, ahol 0_R és 0_S a zéruselemeket jelöli, $f(-x)=-f(x)$, $\forall x\in R$,

(ii) Ha R és S egységelemes gyűrűk és f szürjektív, akkor f unitér. Továbbá, ha f unitér és $x\in R$ invertálható, akkor $f(x^{-1})=f(x)^{-1}$,

(iii) ha $f : R\to S$ izomorfizmus, akkor $f^{-1} : S\to R$ is izomorfizmus,

(iv) $(\mathrm{Aut}(R),\circ)$ csoportstruktúra.

Bizonyítás. (i) Ha $f : (R,+,\cdot) \to (S,+,\cdot)$ gyűrűmorfizmus, akkor $f : (R,+) \to (S,+)$ csoportmorfizmus és alkalmazzuk a csoportokra vonatkozó megfelelő tulajdonságokat.

(ii) Legyen $\forall s \in S$. Akkor f szürjektív $\Rightarrow \exists r \in R : s = f(r)$. Legyen $e = f(1_R)$. Következik, hogy $se = f(r)f(1_R) = f(r1_R) = f(r) = s$ és hasonlóan $es = s$, tehát $se = es = s$, azaz $e = 1_S$. Továbbá, ha f unitér és $x \in R$ invertálható, akkor $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_R) = 1_S$ és hasonlóan $f(x^{-1})f(x) = 1_S$, tehát $f(x)$ és $f(x^{-1})$ egymás inverzei S-ben.

(iii) $\forall u, v \in S$: legyen $x = f^{-1}(u), y = f^{-1}(v)$, akkor $f^{-1}(u+v) = f^{-1}(f(x)+f(y)) = f^{-1}(f(x+y)) = x+y = f^{-1}(u) + f^{-1}(v)$ és $f^{-1}(uv) = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(u)f^{-1}(v)$. □

10.E. Feladatok

▼ 1. Az alábbi halmazok közül melyek alkotnak gyűrűt (a szokásos összeadásra és szorzásra):

a) $\{a+b\sqrt{5} : a,b \in \mathbb{Z}\}$, b) $\{a+b\sqrt[3]{5} : a,b \in \mathbb{Z}\}$, c) $\{a+bi : a,b \in \mathbb{Z}, ab = 0\}$,

d) $\{a+bi : a,b \in \mathbb{Z}, b \text{ páros }\}$, e) $\{\widehat{1},\widehat{3},\widehat{5},\widehat{7},\widehat{9}\} \subset \mathbb{Z}_{10}$.

A gyűrűk közül melyik egységelemes, mely elemeknek van inverze ?

▼ 2. Az alábbi halmazok közül melyek alkotnak testet (a komplex számok összeadására és szorzására):

a) $\{a+b\sqrt[4]{2} : a,b \in \mathbb{Q}\}$, b) $\{a+b\sqrt[3]{3}+c\sqrt[3]{9} : a,b,c \in \mathbb{Q}\}$,

c) $\{a+bi\sqrt{5} : a,b \in \mathbb{Z}\}$.

▼ 3. A $\mathbb{Z}\times\mathbb{Z} = \{(x,y) : x,y \in \mathbb{Z}\}$ halmazon értelmezzük a következő műveleteket: minden $(x,y),(x',y') \in \mathbb{Z}\times\mathbb{Z}$ esetén

$$(x,y)+(x',y') = (x+x', y+y')$$
$$(x,y)(x',y') = (xx', xy'+x'y).$$

Igazoljuk, hogy $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ kommutatív, egységelemes gyűrű.

▼ 4. Legyen $d \in \mathbb{Z}$ egy négyzetmentes szám (azaz nem létezik olyan p prímszám, amelyre $p^2|d$). Igazoljuk, hogy

a) $\mathbb{Z}[\sqrt{d}] = \{m+n\sqrt{d} : m,n \in \mathbb{Z}\} \subset \mathbb{C}$ a komplex számok összeadásával és szorzásával kommutatív, egységelemes gyűrű.

b) $R = \left\{ \begin{pmatrix} m & n \\ dn & m \end{pmatrix} : m,n \in \mathbb{Z} \right\} \subset \mathcal{M}_2(\mathbb{C})$ a mátrixok összeadásával és szorzásával kommutatív, egységelemes gyűrű.

c) az előbbi két gyűrű izomorf.

▼ 5. A $K = \mathbb{R}\times\mathbb{R}$ halmazon értelmezzük a következő műveleteket: minden $(x,y),(x',y') \in \mathbb{R}\times\mathbb{R}$ esetén

$$(x,y)+(x',y') = (x+x', y+y')$$
$$(x,y)(x',y') = (xx'-yy', xy'+x'y).$$

Igazoljuk, hogy $(K,+,\cdot)$ egy kommutatív test, amely izomorf a $(\mathbb{C},+,\cdot)$ testtel.

▼ 6. A $K = (0,\infty)$ intervallumon legyen

$$x \oplus y = xy, \qquad x \odot y = x^{\ln y}.$$

Igazoljuk, hogy $(K,\oplus,\odot)$ kommutatív test, amely izomorf az $(\mathbb{R},+,\cdot)$ testtel.

Útmutatás. Vizsgáljuk az $f : K \to \mathbb{R}$, $f(x) = \ln x$ leképezést.

▼ 7. Legyen $d \in \mathbb{Z}$ egy négyzetmentes szám. Igazoljuk, hogy

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

a komplex számok összeadásával és szorzásával kommutatív test (részteste a $(\mathbb{C}, +, \cdot)$ testnek).

▼ 8. Igazoljuk, hogy egy véges (kommutatív) test nemnulla elemeinek a szorzata -1. Vezessük le innen, hogy ha p prímszám, akkor p osztója $((p-1)! + 1)$-nek (Wilson tétel).

Útmutatás. Állítsuk párba a test nemnulla elemeit: mindegyik x elemet párba állítva x^{-1}-nel. Lehet-e $x = x^{-1}$?

▼ 9. Határozzuk meg a $(\mathbb{Z}, +, \cdot)$ gyűrű endomorfizmusait.

Megoldás. $f(x) = 0$ és $f(x) = \mathbf{1}_{\mathbb{Z}}(x) = x$.

▼▼ 10. Határozzuk meg az $(\mathbb{R}, +, \cdot)$ test automorfizmusait.

Megoldás. Egy automorfizmus van: $f(x) = \mathbf{1}_{\mathbb{R}}(x) = x$. Valóban, ha f automorfizmus, akkor

(1) $f(a) = a \; \forall\, a \in \mathbb{Q}$,

(2) minden $x > 0$ esetén $f(x) > 0$, valóban: ha $x > 0$, akkor $\exists y \in \mathbb{R}^* : x = y^2$ és $f(x) = f(y^2) = (f(y))^2 > 0$ (ha $f(y) = 0$, akkor $f(0) = 0$ miatt $y = 0$, ellentmondás),

(3) minden $x, y \in \mathbb{R}, x < y$ esetén $f(x) < f(y)$, azaz f szigorúan növekvő, valóban: $y - x > 0$ miatt $f(y - x) > 0$, lásd (2), innen $f(y) - f(x) > 0$,

(4) igazoljuk, hogy $f(x) = x, \forall\, x \in \mathbb{R}$. Ha nem így lenne, akkor létezne $x_0 \in \mathbb{R}$: $f(x_0) \neq x_0$. I. eset: ha $f(x_0) < x_0$, akkor $\exists a \in \mathbb{Q} : f(x_0) < a < x_0$, innen (3) szerint $f(a) < f(x_0)$, $a < f(x_0)$, ellentmondás. II. eset: ha $f(x_0) > x_0$, akkor hasonlóan ellentmondás.

Tehát $f(x) = \mathbf{1}_{\mathbb{R}}(x) = x$.

★ ▼ 11. Határozzuk meg az $(\mathbb{C}, +, \cdot)$ test mindazon $f : \mathbb{C} \to \mathbb{C}$ automorfizmusait, amelyekre $f(x) = x$, $\forall\, x \in \mathbb{R}$.

Megoldás. A keresett automorfizmusok: $f(z) = \mathbf{1}_{\mathbb{C}}(z) = z$ és $f(z) = \overline{z}$. Valóban, ha $x + iy \in \mathbb{C}$, akkor $f(x + iy) = f(x) + f(i)f(y) = x + f(i)y$, ahol $-1 = f(-1) = f(i^2) = (f(i))^2$, $f(i) = \pm i$ és kapjuk, hogy $f(x + iy) = x \pm iy$, azaz $f(z) = \mathbf{1}_{\mathbb{C}}(z) = z$ és $f(z) = \overline{z}$.

▼▼ 12. Igazoljuk, hogy ha $R \neq \{0\}$ véges, kommutatív gyűrű, akkor minden $a \in R$, $a \neq 0$ elem vagy zérusosztó, vagy invertálható.

Megoldás. Legyen $a \in R$, $a \neq 0$.

I. Ha a zérusosztó, akkor kész.

II. Ha $a \in R, a \neq 0$ nem zérusosztó, akkor tekintsük az $f : R \setminus \{0\} \to R \setminus \{0\}$, $f(x) = ax$ függvényt, amely helyesen értelmezett, mert ha $f(x) = ax = 0$, ahol $a, x \neq 0$, akkor a zérusosztó, ellentmondás. f injektív, mert ha $f(x) = f(y)$, akkor $ax = ay$, $a(x - y) = 0$, s mivel a nem zérusosztó, $x - y = 0$, $x = y$ következik. De R véges, ezért f szürjektív is és emiatt létezik $x^* \in R$ úgy, hogy $f(x^*) = ax^* = 1$, ahonnan $ax^* = x^*a = 1$, mert R kommutatív, tehát létezik $a^{-1} = x^*$. □

Megjegyzések. 1. Ennek következménye az 10.C.3. Tétel, amely szerint minden véges integritástartomány test.

2. Ha R végtelen, akkor nem igaz az állítás, pl. $(\mathbb{Z}, +, \cdot)$-ban 2 nem zérusosztó és nem invertálható.

3. Az $R = \mathbb{Z}_n$, $n \geq 2$ gyűrűre a feladat állításának közvetlen bizonyítása: Tudjuk, hogy $\widehat{a}$ akkor és csak akkor invertálható, ha $(a, n) = 1$, lásd Csoportelmélet. Tegyük fel, hogy $\widehat{a}$ nem invertálható, akkor $(a, n) > 1$, ezért létezik p prím úgy, hogy $p|a, p|n$ és

következik, hogy $\widehat{a}$ zérusosztó, mert $\widehat{a} \cdot \widehat{n/p} = \widehat{a/p} \cdot \widehat{n} = \widehat{0}$. Pl. $n = 24$, $\widehat{a} = \widehat{4}$: $\widehat{4} \cdot \widehat{12} = \widehat{0}$, $\widehat{a} = \widehat{6}$: $\widehat{6} \cdot \widehat{12} = \widehat{0}$.

▼▼ 13. Legyen $\mathcal{F}$ az $f : \mathbb{N}^* \to \mathbb{R}$ függvények (ún. számelméleti függvények) halmaza és tekintsük az $f, g \in \mathcal{F}$ függvények konvolúció-szorzatát, amely így értelmezett:

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d), \quad n \in \mathbb{N}^*,$$

ahol d befutja az n pozitív osztóit.
Igazoljuk, hogy $(\mathcal{F}, +, *)$ integritástartomány és f-nek akkor és csak akkor létezik inverze $*$-ra nézve, ha $f(1) \neq 0$.

▼▼ 14. Az A nemüres halmaz $\mathcal{P}(A) = \{B : B \subseteq A\}$ hatványhalmazán értelmezzük a következő műveleteket:

$$X \oplus Y = (X \setminus Y) \cup (Y \setminus X), \qquad X \odot Y = X \cap Y.$$

Igazoljuk, hogy $(\mathcal{P}(A), \oplus, \odot)$ gyűrű, amelyben $X \odot X = X$ (ún. Boole-gyűrű). Készítsük el ennek összeadótábláját és szorzótábláját, ha $A = \{a, b\}$.

▼▼ 15. Ha $(F, +, \cdot)$ egy kommutatív test, akkor az $(F, +)$ és $(F^*, \cdot)$ csoportok nem izomorfak.

Megoldás. Tegyük fel, hogy $(F, +) \simeq (F^*, \cdot)$. Akkor $f(0) = 1$ és $\exists\, x \in F, x \neq 0 : f(x) = -1$. Következik, hogy $f(-x) = f(x)^{-1} = -1$, és f injektivitása miatt $x = -x$, $x + x = x(1 + 1) = 0$. Innen $1 + 1 = 0$ (testben nincsenek zérusosztók), tehát $\operatorname{char} F = 2$.

Továbbá $1 = f(0) = f(1+1) = f(1)f(1) = f(1)^2$, $f(1)^2 - 2f(1) + 1 = 0$, $((f(1) - 1)^2 = 0$, $f(1) - 1 = 0$, $f(1) = 1$, ahonnan $0 = 1$, ami ellentmondás. ★

11. Részgyűrűk és résztestek, karakterisztika

11.A. Részgyűrűk és résztestek

Legyen $(R,+,\cdot)$ egy gyűrű és $S \subseteq R$. Azt mondjuk, hogy S **részgyűrű**je R-nek, ha S zárt a "+" és a "$\cdot$" műveletekre nézve (azaz $\forall x,y \in S \Rightarrow x+y \in S, xy \in S$) és ha $(S,+,\cdot)$ maga is gyűrű. Jelölés: $(S,+,\cdot) \leq (R,+,\cdot)$ vagy röviden $S \leq R$.

Ha R egységelemes gyűrű és $1 \in S$, akkor S **unitér részgyűrű**.

Hasonlóképpen, ha $(R,+,\cdot)$ egy test és $S \subseteq R$, akkor azt mondjuk, hogy S **részteste** R-nek, ha S zárt a "+" és a "$\cdot$" műveletekre nézve és $(S,+,\cdot)$ maga is test. Jelölés: $(S,+,\cdot) \leq (R,+,\cdot)$ vagy $S \leq R$.

11.A.1. Példák. • $(\mathbb{Z},+,\cdot) \leq (\mathbb{Q},+,\cdot)$ részgyűrű és $(\mathbb{Q},+,\cdot) \leq (\mathbb{R},+,\cdot) \leq (\mathbb{C},+,\cdot)$ résztestek.

• a $(\mathbb{Z},+,\cdot)$ gyűrűnek $(n\mathbb{Z},+,\cdot)$ részgyűrűje, ahol $n \in \mathbb{N}^*$, és minden részgyűrű ilyen alakú (miért ?)

• minden $(R,+,\cdot)$ gyűrűnek részgyűrűje az $S=\{0\}$ zérusgyűrű és az $S=R$, ezeket **triviális részgyűrűk**nek nevezzük.

11.A.2. Tétel. (részgyűrűk és résztestek jellemzése)

a) Ha $(R,+,\cdot)$ egy gyűrű és $S \subseteq R$, akkor egyenértékűek a következő állítások:

1) $S \leq R$, azaz S részgyűrű,

2) $S \neq \emptyset$ és $\forall x,y \in S \Rightarrow x-y \in S, xy \in S$.

b) Ha $(R,+,\cdot)$ egy test és $S \subseteq R$, akkor egyenértékűek a következő állítások:

1) $S \leq R$, azaz S résztest,

2) $|S| \geq 2$ és $\forall x,y \in S, y \neq 0 \Rightarrow x-y \in S, xy^{-1} \in S$.

Bizonyítás. a) "1) $\Rightarrow$ 2)" Ha $(S,+,\cdot) \leq (R,+,\cdot)$, akkor $(S,+) \leq (R,+)$ részcsoport és a részcsoportok jellemzési tétele szerint $x-y \in S$ (itt additív a jelölés !) és $xy \in S$ a definíció szerint.

"2) $\Rightarrow$ 1)" A feltételek alapján $(S,+) \leq (R,+)$ ismét a részcsoportok jellemzési tétele szerint, tehát $(S,+)$ csoport és következik, hogy $(S,+,\cdot)$ gyűrű, mert a többi tulajdonság öröklődik R-ről S-re.

b) "1) $\Rightarrow$ 2)" Ha $S \leq R$ résztest, akkor $|S| \geq 2$ és $(S,+) \leq (R,+)$ részcsoport, ahonnan $0 \in S, x-y \in S, \forall x,y \in S$. Továbbá $(S^*,\cdot)$ csoport és $(S^*,\cdot) \leq (R^*,\cdot)$, innen $xy^{-1} \in S^*, \forall x,y \in S^*$, újra a részcsoportok jellemzési tétele szerint.

"2) $\Rightarrow$ 1)" Kapjuk, hogy $(S,+) \leq (R,+)$ és $S^* \neq \emptyset$. Továbbá $\forall x,y \in S^* \Rightarrow xy^{-1} \in S^*$, mert nemnulla elem inverze nemnulla és testben nincsenek zérusosztók. Innen $(S^*,\cdot) \leq (R^*,\cdot)$. Következik, hogy $S \leq R$ résztest (a disztributivitás öröklődik). □

11.A.3. Példa. • Ha R egy gyűrű (test), akkor ennek $Z(R) = \{r \in R : rx = xr, \forall x \in R\}$ **centrum**a részgyűrűje (részteste) R-nek.

Valóban, ha pl. R gyűrű, akkor $0 \in Z(R) \neq \emptyset$, mert $0x = x0 = 0, \forall x \in R$. Továbbá, $\forall r,s \in Z(R) \Rightarrow r-s \in Z(R)$ és $rs \in Z(R)$, mert $(r-s)x = rx-sx = xr-xs = x(r-s)$ és $(rs)x = r(sx) = r(xs) = (rx)s = (xr)s = x(rs), \forall x \in R$, és alkalmazzuk az előző Tételt.

11.A.4. Tétel. Részgyűrűk (résztestek) tetszőleges $(S_i)_{i\in I}$ rendszerének $\cap_{i\in I} S_i$ metszete is részgyűrű (résztest).

Bizonyítás. Használjuk a részgyűrűk jellemzési tételét: $0 \in S_i$, $\forall i \in I$, ezért $0 \in \cap_{i\in I} S_i \neq \emptyset$. Továbbá $\forall x,y \in \cap_{i\in I} S_i \Rightarrow x,y \in S_i, \forall i \in I \Rightarrow x-y, xy \in S_i, \forall i \in I \Rightarrow x-y, xy \in \cap_{i\in I} S_i$. Írjuk le a bizonyítást résztestek esetén! □

Részgyűrűk (résztestek) uniója részgyűrű-e (résztest-e)? Miért ?

11.B. Generált részgyűrű

Az előbbi Tételt használva a következő definíció adható:

Ha R egy gyűrű és $X \subseteq R$, akkor $\langle X\rangle = \cap\{S : S \leq (R,+,\cdot), X \subseteq S\}$ részgyűrűje R-nek és ezt az X által **generált részgyűrű**nek nevezzük. Ez a legkisebb (legszűkebb) olyan részgyűrű, amely tartalmazza X-et.

Kérdés: X elemei ismeretében hogyan adható meg $\langle X\rangle$? Ha $x_1, x_2, ..., x_n \in X$, akkor $x_1x_2\cdots x_n \in \langle X\rangle$, ha még $y_1, y_2, ..., y_m \in X$, akkor $y_1y_2\cdots y_m \in \langle X\rangle$ és $x_1x_2\cdots x_n \pm y_1y_2\cdots y_m \in \langle X\rangle$. Tehát $\langle X\rangle$ tartalmazza az X elemeiből alkotott szorzatokat és ezek összegeit is. Pontosabban:

11.B.1. Tétel. Ha $(R,+,\cdot)$ egy gyűrű és $\emptyset \neq X \subseteq R$, akkor

$$(*) \qquad \langle X\rangle = \{\sum \pm x_1x_2...x_n : n \in \mathbb{N}^*, x_i \in X, \forall 1 \leq i \leq n\},$$

azaz $\langle X\rangle$ az összes olyan véges sok tagú összegből áll, ahol a tagok véges sok X-beli elemből (tényezőből) álló szorzatok.

Bizonyítás. (Lásd a csoportokra vonatkozó hasonló tulajdonságot) Legyen

$$S = \{\sum \pm x_1x_2...x_n : n \in \mathbb{N}^*, x_i \in X, \forall 1 \leq i \leq n\}.$$

Akkor $\emptyset \neq X \subseteq S$, hiszen minden $x \in R$-re x egytényezős szorzat ($n = 1$). Továbbá $S \leq R$. Valóban, $\forall y = \sum \pm x_1x_2...x_n, z = \sum \pm x'_1x'_2...x'_m \in S$ esetén $y - z$ és yz is egy-egy ilyen véges összeg, tehát $y - z, yz \in S$.

Belátjuk még, hogy S a legkisebb olyan részgyűrű, amely tartalmazza X-et, azaz $\forall S' \leq R, X \subseteq S'$ esetén $S \subseteq S'$. Valóban, $\forall y = \sum \pm x_1x_2...x_n \in S$ esetén $x_i \in X \subseteq S'$ és kapjuk, hogy $y \in S'$, mert S' részgyűrű.

A fentiek szerint $\langle X\rangle = R$. $\square$

11.C. Gyűrű karakterisztikája

Legyen $(R,+,\cdot)$ egy egységelemes gyűrű, amelynek egységeleme $1_R = 1 \neq 0$. Akkor $(R,+)$ Abel-csoport és minden $n \in \mathbb{Z}$ és $r \in R$ esetén értelmezhető nr, lásd 2.F. szakasz: $nr = \underbrace{r + r + ... + r}_{n}$, ha $n > 0$, $0r = 0$ és $nr = -(-n)r = -(\underbrace{r + r + ... + r}_{-n})$, ha $n < 0$.

Figyeljük meg, hogy $\forall\, n, m \in \mathbb{Z}$ esetén $(nm)1 = n(m1) = (n1)(m1)$. Valóban, ha $n, m > 0$, akkor

$$(nm)1 = \underbrace{1 + 1 + ... + 1}_{nm} = \underbrace{(\underbrace{1 + ... + 1}_{m}) + ... + (\underbrace{1 + ... + 1}_{m})}_{n} = n(\underbrace{1 + ... + 1}_{m}) = n(m1),$$

$$(nm)1 = (\underbrace{1 + 1 + ... + 1}_{m})(\underbrace{1 + ... + 1}_{n}) = (m1)(n1).$$

Ha $n < 0, m > 0$, akkor $(nm)1 = -(-nm)1 = -((-n)m)1 = -((-n)(m1)) = -(-n(m1)) = n(m1)$, hasonlóképpen a többi eset.

Tegyük fel, hogy van olyan $n \in \mathbb{N}^*$ szám, amelyre $n1 = \underbrace{1 + 1 + ... + 1}_{n} = 0$. Akkor minden $r \in R$ elemre $nr = 0$. Valóban, $nr = \underbrace{r + r + ... + r}_{n} = r(\underbrace{1 + 1 + ... + 1}_{n}) = r(n1) = 0$. Ekkor a legkisebb ilyen $n \in \mathbb{N}^*$ számot a **gyűrű karakterisztikájá**nak nevezzük, jelölés: $\operatorname{char} R = \min\{k \in \mathbb{N}^* : k1 = 0\} = n$.

Ellenkező esetben (ha nincs ilyen szám) azt mondjuk, hogy R karakterisztikája 0, jelölés: $\operatorname{char} R = 0$.

11.C.1. Példák. • $\mathbb{Z}_n$ karakterisztikája n: $\operatorname{char} \mathbb{Z}_n = n$.

• $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ karakterisztikája 0: $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.

★ Megjegyzés: ha $(R, +, \cdot)$ egy egységelemes gyűrű, akkor az $f : (\mathbb{Z}, +, \cdot) \to (R, +, \cdot)$, $f(k) = k1$ függvény gyűrűhomomorfizmus, mert $f(k + \ell) = (k + \ell)1 = k1 + \ell 1 = f(k) + f(\ell)$ és $f(k\ell) = (k\ell)1 = (k1)(\ell 1) = f(k)f(\ell)$.

A gyűrű nulla karakterisztikájú, ha f injektív, azaz ha $k1 \neq \ell 1, \forall k, \ell \in \mathbb{Z}, k \neq \ell$. Ha f nem injektív, akkor $\exists k, \ell \in \mathbb{Z}, k \neq \ell : k1 = \ell 1$. Feltehető, hogy $k < \ell$, ekkor $m = \ell - k > 0$ és $m1 = (\ell - k)1 = \ell 1 - k1 = 0$, tehát van olyan $m \in \mathbb{N}^*$ szám, hogy $m1 = 0$.

Tudjuk, hogy $\operatorname{Ker} f \trianglelefteq \mathbb{Z}$. De $(\mathbb{Z}, +, \cdot)$ minden ideálja $n\mathbb{Z}$ alakú, ezért $\operatorname{Ker} f = n\mathbb{Z}$, valamilyen $n \in N$-re. Ha $n \geq 1$, akkor éppen ez az n lesz a gyűrű karakterisztikája. Ha $n = 0$, akkor $\operatorname{Ker} f = \{0\}$, f injektív és a karakterisztika 0. ★

11.C.2. Tétel. a) Minden $R \neq \{0\}$ egységelemes, zérusosztómentes gyűrű karakterisztikája 0 vagy prímszám.

b) Minden test karakterisztikája 0 vagy prímszám.

Bizonyítás. a) Legyen R egy egységelemes, zérusosztómentes gyűrű. Ha $\operatorname{char} R \neq 0$, akkor legyen $\operatorname{char} R = n \geq 1$. Igazoljuk, hogy n prím. Ellenkező esetben $n = pq$ alakba írható, ahol $1 < p, q < n$. De akkor $(p1)(q1) = (pq)1 = n1 = 0$ és következik, hogy $p1$ és $q1$ zérusosztók, ami ellentmondás.

b) Az a) speciális esete, mert minden test zérusosztómentes. □

11.C.3. Tétel. Legyen K egy kommutatív test, amelynek karakterisztikája $\operatorname{char} K = p$. Akkor

1) $(xy)^p = x^p y^p, \qquad \forall\, x, y \in K,$

2) $(x \pm y)^p = x^p \pm y^p, \qquad \forall\, x, y \in K,$

3) (Frobenius) $\varphi : K \to K$, $\varphi(x) = x^p$ testmorfizmus.

Bizonyítás. 1) Azonnali a kommutativitás miatt.

2) Alkalmazható a Newton-féle binomiális képlet:

$$(x \pm y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k (\pm y)^{p-k},$$

ahol a $\binom{p}{k}$, $1 \leq k \leq p - 1$ binomiális együtthatók oszthatók p-vel (p prímszám). Mivel $\operatorname{char} F = p$, kapjuk, hogy $(x \pm y)^p = x^p + (\pm 1)^p y^p$. Ha $p > 2$, akkor p páratlan és $(x \pm y)^p = x^p \pm y^p$. Ha $p = 2$, akkor $(x \pm y)^2 = x^2 + y^2 = x^2 - y^2$, mert $y^2 = -y^2$ igaz $2y^2 = 0$ miatt.

3) Az 1) és 2) alapján. □

11.D. Feladatok

▼ 1. Lássuk be hogy gyűrű homomorf képe gyűrű, pontosabban : Legyenek $(R, +, \cdot)$ és $(S, +, \cdot)$ gyűrűk. Ha $S' \subseteq S$ és ha azt akarjuk igazolni, hogy $(S', +, \cdot)$ gyűrű, akkor elegendő megadnunk egy olyan $f : R \to S$ gyűrűmorfizmust, amelyre $f(R) = S'$ (lásd pl. 10.E.4. és 6. Feladatok).

▼ 2. Legyenek $(R, +, \cdot)$ és $(S, +, \cdot)$ gyűrűk és $f : R \to S$ egy gyűrűhomomorfizmus. Igazoljuk, hogy

i) ha $(R', +, \cdot) \leq (R, +, \cdot)$, akkor $(f(R'), +, \cdot) \leq (S, +, \cdot)$ (részgyűrű homomorf képe részgyűrű);

ii) ha $(S', +, \cdot) \leq (S, +, \cdot)$, akkor $(f^{-1}(S'), +, \cdot) \leq (R, +, \cdot)$;

iii) ha $(S', +, \cdot) \trianglelefteq (S, +, \cdot)$, akkor $(f^{-1}(S'), +, \cdot) \trianglelefteq (R, +, \cdot)$;
iv) vizsgáljuk meg az $R' = R$ és $S' = \{0\}$ eseteket.

▼ 3. (A kvaterniók teste) Legyen

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, w \in \mathbb{C} \right\} \subseteq \mathcal{M}_2(\mathbb{C}).$$

Akkor $(\mathbb{H}, +, \cdot)$ egy nemkommutatív test.

Megoldás. Először megmutatjuk, hogy $\mathbb{H}$ részgyűrűje $\mathcal{M}_2(\mathbb{C})$-nek:

$$\begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix} - \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} = \begin{pmatrix} z_1 - z_2 & w_1 - w_2 \\ -\overline{(w_1 - w_2)} & \overline{z_1 - z_2} \end{pmatrix} \in \mathbb{H},$$

$$\begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix} \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \overline{w_2} & z_1 w_2 + w_1 \overline{z_2} \\ -\overline{w_1} z_2 - \overline{z_1} w_2 & -\overline{w_1} w_2 + \overline{z_1} z_2 \end{pmatrix} =$$

$$\begin{pmatrix} z_1 z_2 - w_1 \overline{w_2} & z_1 w_2 + w_1 \overline{z_2} \\ -\overline{(z_1 w_2 + w_1 \overline{z_2})} & \overline{z_1 z_2 - w_1 \overline{w_2}} \end{pmatrix} \in \mathbb{H},$$

$\forall \begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix}, \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} \in \mathbb{H}.$

Továbbá $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}$ egységelem és minden $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ mátrixnak van inverze, nevezetesen

$$\begin{pmatrix} \frac{\overline{z}}{\Delta} & -\frac{w}{\Delta} \\ \frac{\overline{w}}{\Delta} & \frac{z}{\Delta} \end{pmatrix} \in \mathbb{H},$$

ahol $\Delta = |z|^2 + |w|^2 \neq 0$.

A $\phi : \mathbb{R} \to \mathbb{H}$, $\phi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ leképezés, egy testmorfizmus. Ez lehetővé teszi, hogy az a valós számot azonosítsuk az $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ kvaternióval.

Jelölje még $\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathbb{H}$, akkor $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$, következik, hogy $\mathbb{H}$ nem kommutatív.

Ha $z = a_0 + a_1 i$, $w = b_0 + b_1 i$, akkor

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = \begin{pmatrix} a_0 + a_1 i & b_0 + b_1 i \\ -b_0 + b_1 i & a_0 - a_1 i \end{pmatrix} =$$

$$= \begin{pmatrix} a_0 & 0 \\ 0 & a_0 \end{pmatrix} + \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \begin{pmatrix} b_0 & 0 \\ 0 & b_0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \begin{pmatrix} b_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} =$$

$$= a_0 + a_1 \mathbf{i} + b_0 \mathbf{j} + b_1 \mathbf{k}.$$

Tehát minden kvaternió egyértelműen felírható $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ alakban, ahol $a, b, c, d \in \mathbb{R}$.

Megyjegyzés. Figyeljük meg, hogy $\mathbf{i}, \mathbf{j}, \mathbf{k}$ gyökei az $X^2 + \mathbf{1} = 0$ egyenletnek, tehát egy olyan egyenletnek, amelynek együtthatói egy nemkommutatív testből vannak, lehet több gyöke, mint amennyi a fokszáma.

Kommutatív testek esetén ez nem lehetséges. Ha F egy kommutatív test, akkor minden n-edfokú egyenletnek, $n \geq 1$, amelynek együtthatói F-ből vannak, legfeljebb n gyöke van.

▼ 4. a) Legyen K egy kommutatív test, amelyre $1+1 \neq 0$ (azaz amelynek karakterisztikája $\neq 2$) és tekintsük az $ax^2 + bx + c = 0$, $a, b, c \in K$, $a \neq 0$ másodfokú egyenletet. Igazoljuk, hogy ennek akkor és csak akkor van $x \in K$ megoldása, ha létezik $u \in K$ úgy, hogy $b^2 - 4ac = u^2$ és ekkor a megoldások: $x_{1,2} = (-b \pm u)(2a)^{-1}$.

b) Oldjuk meg a $3x^2 - 4x + 1 = 0$ egyenletet a $\mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{13}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$ testekben.

c) Oldjuk meg az $x^2 - x + 5 = 0$ egyenletet a $\mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$ testekben.

Megoldás. b)$\mathbb{Z}_5$-ben: $x_1 = \widehat{1}, x_2 = \widehat{2}$, $\mathbb{Z}_7$-ben: $x_1 = \widehat{1}, x_2 = \widehat{5}$, $\mathbb{Z}_{19}$-ben: $x_1 = \widehat{1}, x_2 = \widehat{13}$.

c)$\mathbb{Z}_7$-ben: $x_1 = \widehat{2}, x_2 = \widehat{6}$, $\mathbb{Z}_{11}$-ben: $x_1 = \widehat{3}, x_2 = \widehat{9}$, $\mathbb{Z}_{19}$-ben: $x_1 = x_2 = \widehat{10}$.

▼ 5. Legyen p egy prímszám és $\mathbb{Q}(\sqrt[3]{p}) = \{a + b\sqrt[3]{p} + c\sqrt[3]{p^2} : a, b, c \in \mathbb{Q}\}$. Igazoljuk, hogy (lásd 10.E.2. Feladat/b):

i) $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0$ akkor és csak akkor, ha $a = b = c = 0$,

ii) $\mathbb{Q}(\sqrt[3]{p})$ részteste $\mathbb{R}$-nek,

iii) $\{a + b\sqrt[3]{p} : a, b \in \mathbb{Q}\}$ nem résztest.

▼ 6. Az $(R, +, \cdot)$ egységelemes gyűrűt Boole-gyűrűnek nevezzük, ha $x^2 = x$ minden $x \in R$ esetén. Igazoljuk, hogy ha $(R, +, \cdot)$ Boole-gyűrű, akkor

i) $1 + 1 = 0$, azaz $\operatorname{char} R = 2$.

ii) R kommutatív.

Megoldás. 1) $1 + 1 = (1 + 1)^2 = 1 + 1 + 1 + 1$, tehát $1 + 1 = 0$.

ii) Ha $x, y \in R$, akkor $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx$, tehát $xy = -yx$; mivel $1 = -1$, következik, hogy $xy = yx$.

▼ 7. A Gauss-egészek $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ gyűrűjében legyen $X_1 = \{1\}$, $X_2 = \{i\}$, $X_3 = \{1, 1 + i\}$. Adjuk meg az X_1, X_2, X_3 által generált részgyűrűket.

★ ▼▼ 8. Legyen R egy gyűrű. A $\mathbb{Z} \times R = \{(m, r) : m \in \mathbb{Z}, r \in R\}$ halmazon értelmezzük a következő műveleteket: minden $(m, r), (n, s) \in \mathbb{Z} \times R$ esetén

$$(m, r) + (n, s) = (m + n, r + s)$$
$$(m, r)(n, s) = (mn, ms + nr + rs).$$

Igazoljuk, hogy $(\mathbb{Z} \times R, +, \cdot)$ egységelemes gyűrű és létezik egy $\phi : R \to \mathbb{Z} \times R$ injektív homomorfizmus (tehát minden gyűrű beágyazható egy egységelemes gyűrűbe).

Útmutatás. Az egységelem $(1, 0)$. Legyen $\phi(r) = (k, r)$, kérdés: mennyi a k ? Válasz: $k = 0$.

▼▼ 9. Igazoljuk, hogy ha egy (nemkommutatív) egységelemes gyűrűben az $1 - ab$ elemnek van inverze, akkor az $1 - ba$ elemnek is van.

Útmutatás. Legyen u az $1 - ab$ inverze. Igazoljuk, hogy $v = 1 + bua$ inverze az $1 - ba$-nak. ★

12. Gyűrű ideáljai

12.A. Ideálok, példák

Legyen $(R,+,\cdot)$ egy gyűrű és $\emptyset \neq I \subseteq R$. Azt mondjuk, hogy I **bal oldali** (**jobb oldali**) **ideál**ja R-nek, ha

1) $\forall x,y \in I : x-y \in I$, (azaz $(I,+) \leq (R,+)$),

2) $\forall x \in I, \forall r \in R$: $rx \in I$ (illetve $xr \in I$).

Ha I bal oldali és jobb oldali ideál, akkor I-it **kétoldali ideál**nak, vagy röviden **ideál**nak nevezzük. Jelölések: $I \trianglelefteq_b R$, $I \trianglelefteq_j R$, $I \trianglelefteq R$.

Ha R kommutatív, akkor $I \trianglelefteq R \Leftrightarrow I \trianglelefteq_b R \Leftrightarrow I \trianglelefteq_j R$.

Világos, hogy minden ideál (bal oldali, jobb oldali, kétoldali) részgyűrű. Fordítva nem igaz, pl. $(\mathbb{Q},+,\cdot)$-nak $\mathbb{Z}$ részgyűrűje, de nem ideálja, mert pl. $2 \in \mathbb{Z}$, $\frac{1}{3} \in \mathbb{Q}$ és $2 \cdot \frac{1}{3} = \frac{2}{3} \notin \mathbb{Z}$.

12.A.1. Példák. • $\{0\}$ és R (kétoldali) ideáljai R-nek. Ha $I \trianglelefteq R$, $I \neq \{0\}, R$, akkor I-t **valódi ideál**nak nevezzük.

Ha R-nek nincs valódi ideálja, akkor R-et **egyszerű gyűrű**nek nevezzük.

• Ha I ideálja $(\mathbb{Z},+,\cdot)$-nak, akkor $I \leq (\mathbb{Z},+)$, tehát $I = n\mathbb{Z}$ alakú, ahol $n \in \mathbb{N}$. Fordítva, minden $n\mathbb{Z}$ ideálja $\mathbb{Z}$-nek.

• $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z} \right\} \trianglelefteq_j \mathcal{M}_2(\mathbb{Z})$, $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a,b \in \mathbb{Z} \right\} \trianglelefteq_b \mathcal{M}_2(\mathbb{Z})$.

• Ha $f : R \to S$ egy gyűrűmorfizmus, akkor $\operatorname{Ker} f \trianglelefteq R$, mert $(\operatorname{Ker} f,+) \leq (R,+)$ és $\forall a \in \operatorname{Ker} f, \forall r \in R$: $f(ra) = f(r)f(a) = 0$ és $f(ar) = f(a)f(r) = 0$.

• Ha $(R,+,\cdot)$ egy gyűrű és $a \in R$, akkor $Ra = \{ra : r \in R\} \trianglelefteq_b R$,
$aR = \{ar : r \in R\} \trianglelefteq_j R$ és $RaR = \{\sum_{i=1}^n r_i a s_i : n \in \mathbb{N}, r_i, s_i \in R, 1 \leq i \leq n\} \trianglelefteq R$.

Valóban, pl. $RaR \leq R$, mert $\forall x = \sum_{i=1}^n r_i a s_i, y = \sum_{i=1}^m r_i' a s_i' \in RaR : x-y = \sum_{i=1}^n r_i a s_i - \sum_{i=1}^m r_i' a s_i' = \sum_{i=1}^{n+m} r_i^* a s_i^* \in RaR$, ahol $r_i^* = r_i, s_i^* = s_i, 1 \leq i \leq n$, $r_{n+i}^* = -r_i', s_{n+i}^* = s_i', 1 \leq i \leq m$.

Továbbá, RaR ideál, mert $\forall x = \sum_{i=1}^n r_i a s_i \in RaR, \forall t \in R : tx = \sum_{i=1}^n (tr_i) a s_i \in RaR$, $xt = \sum_{i=1}^n r_i a (s_i t) \in RaR$.

12.A.2. Tétel. 1) Ha R egységelemes gyűrű és $I \trianglelefteq_b R$ vagy $I \trianglelefteq_j R$ és létezik $a \in I$ invertálható elem, akkor $I = R$.

2) Testnek nincs valódi ideálja, azaz minden test egyszerű gyűrű.

Bizonyítás. 1) Ha $I \trianglelefteq_b R$, akkor $1 = a^{-1}a \in I$ (ahol $a^{-1} \in R$, $a \in I$) és így $\forall r \in R : r = r \cdot 1 \in I$, tehát $I = R$.

Ha $I \trianglelefteq_j R$, akkor $1 = aa^{-1} \in I$ (ahol $a \in I$, $a^{-1} \in R$), innen $\forall r \in R : r = 1 \cdot r \in I$, tehát $I = R$.

2) Az 1) azonnali következménye. □

12.A.3. Tétel. Ha $(R,+,\cdot)$ egy gyűrű és I_1 és I_2 két baloldali (jobb oldali ill. kétoldali) ideál, akkor

1) $I_1 \cap I_2 = \{x : x \in I_1 \text{ és } x \in I_2\}$,

2) $I_1 + I_2 = \{x_1 + x_2 : x_1 \in I_1 \text{ és } x_2 \in I_2\}$,

3) $I_1 I_2 = \{\sum_{i=1}^n x_i y_i : n \in \mathbb{N}^*, x_i \in I_1, y_i \in I_2\}$ is egy-egy baloldali (jobb oldali ill. kétoldali) ideál.

Bizonyítás. Legyen I_1 és I_2 két bal oldali ideál (a bizonyítás hasonló a többi esetben is).

1) $0 \in I_1 \cap I_2$, ezért $I_1 \cap I_2 \neq \emptyset$. Ha $x,y \in I_1 \cap I_2$, akkor $x,y \in I_1$ és $x,y \in I_2$, és mivel I_1, I_2 (bal oldali) ideálok, $x-y \in I_1, x-y \in I_2$, tehát $x-y \in I_1 \cap I_2$. Ha $r \in R$

és $x \in I_1 \cap I_2$, akkor $x \in I_1, x \in I_2$ és következik, hogy $rx \in I_1, rx \in I_2$, mert I_1, I_2 bal oldali ideálok, ahonnan $rx \in I_1 \cap I_2$. Tehát $I_1 \cap I_2$ bal oldali ideál.

2) $0 = 0+0 \in I_1 + I_2 \neq \emptyset$ és legyen $u, v \in I_1 + I_2$, akkor $u = x_1 + x_2, v = y_1 + y_2$, ahol $x_1, y_1 \in I_1$ és $x_2, y_2 \in I_2$. Így $u - v = (x_1 - x_2) + (y_1 - y_2) \in I_1 + I_2$, mert I_1, I_2 (bal oldali) ideálok. Ha $r \in R$ és $u = x_1 + x_2 \in I_1 + I_2$, akkor $ru = r(x_1 + x_2) = rx_1 + rx_2 \in I_1 + I_2$, mert I_1, I_2 bal oldali ideálok. Tehát $I_1 + I_2$ bal oldali ideál.

3)$0 = 0 \cdot 0 \in I_1 I_2 \neq \emptyset$. Legyen $w, w' \in I_1 I_2$, ahol $w = \sum_{i=1}^{n} x_i y_i, w' = \sum_{i=1}^{m} x_i' y_i'$, ahol $x_i, x_i' \in I_1, 1 \leq i \leq n$ és $y_i, y_i' \in I_2, 1 \leq i \leq m$. Akkor azonnali, hogy $w - w' \in I_1 I_2$ és ha $r \in R$, akkor $rw = \sum_{i=1}^{n} (rx_i) y_i \in I_1 I_2$. Tehát $I_1 I_2$ bal oldali ideál. □

Az $I_1 + I_2$ és $I_1 I_2$ ideálokat az I_1 és I_2 **ideálok összegé**nek illetve **szorzatá**nak nevezzük.

12.A.4. Példa. • $m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$ és $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$, ahol (m, n) és $[m, n]$ az m, n számok lnko-ja ill. lkkt-je, lásd a csoportok hasonló tulajdonságát, 4.J.6. Feladat.

12.B. Generált ideál

Ideálok (bal oldali, jobb oldali, kétoldali) tetszőleges $(I_i)_{i \in I}$ rendszerének $\cap_{i \in I} I_i$ metszete is (bal oldali, jobb oldali, kétoldali) ideál. Ennek alapján:

Ha R egy gyűrű és $\emptyset \neq X \subseteq R$, akkor $(X) = \cap\{I : I \trianglelefteq (R, +, \cdot), X \subseteq I\}$ ideálja R-nek és ezt az X által **generált ideál**nak nevezzük. Ha $X = \{x\}$, akkor az x elem által **generált főideál**ról beszélünk, jel. (x).

Egy I ideál **végesen generált**, ha létezik olyan X véges halmaz, hogy $I = (X)$.

12.B.1. Tétel. Ha $(R, +, \cdot)$ egy kommutatív egységelemes gyűrű és $\emptyset \neq X \subseteq R$, akkor

$$(X) = RX = \{\sum_{i=1}^{n} r_i x_i : n \in \mathbb{N}^*, r_i \in R, x_i \in X, \forall 1 \leq i \leq n\}.$$

Bizonyítás. $X \subseteq RX$, mert $\forall x \in X : x = 1 \cdot x \in RX$. $RX \trianglelefteq R$, mert $\forall y = \sum_{i=1}^{n} r_i x_i, z = \sum_{i=1}^{m} r_i' x_i' \in RX$ esetén $y - z$ is egy ugyanilyen összeg, tehát $y - z \in RX$, ugyanakkor $\forall t \in R : ty = \sum_{i=1}^{n} (tr_i) x_i \in RX$.

Továbbá: ha $I \trianglelefteq R$, $X \subseteq I$, akkor $RX \subseteq I$. Valóban, ekkor $\forall y = \sum_{i=1}^{n} r_i x_i \in RX$ esetén $x_i \in X \subseteq I \Rightarrow r_i x_i \in I, \forall i \in I$ (mert I ideál), innen $y \in I$. □

12.B.2. Következmény. $(X = \{x\})$ Az $(R, +, \cdot)$ kommutatív egységelemes gyűrűben az x elem által generált főideál:

$$(x) = Rx = \{rx : r \in R\},$$

lásd a fejezet elején levő Példák.

Egy gyűrűt **főideálgyűrű**nek nevezünk, ha integritástartomány és minden ideálja főideál. Ilyen például a $(\mathbb{Z}, +, \cdot)$ gyűrű.

12.C. Prímtest

Legyen $(K, +, \cdot)$ egy test. A K összes résztestének $P(K)$ metszete a K-nak részteste, lásd korábbi Tétel. $P(K)$-t a K **prímrésztest**ének nevezzük. Egy test **prímtest**, ha egyenlő saját prímrésztestével: $K = P(K)$, azaz, ha nincs önmagán kívül más részteste.

12.C.1. Példa. • $\mathbb{Q}$ és $\mathbb{Z}_p$ (p prímszám) pímtestek.

Valóban, legyen K részteste $\mathbb{Q}$-nak. Akkor $1 \in K$ (miért ?), innen $2 = 1 + 1 \in K, 3 = 1 + 1 + 1 \in K, ..., n \in K$, $\forall n \in \mathbb{N}^*$. Mivel $0 \in K$, ezért $-n = 0 - n \in K$, azaz $\mathbb{Z} \subseteq K$. Továbbá, így $\forall \frac{m}{n} \in Q$ esetén $\frac{m}{n} = mn^{-1} \in K$ (lásd résztestek jellemzése). Kapjuk, hogy $\mathbb{Q} \subseteq K$, azaz $Q = K$.

★ Nézzük most a $\mathbb{Z}_p$ testet. Szükségünk van a következőre:

Ha $n \in \mathbb{N}^*$, akkor a $(\mathbb{Z}_n, +, \cdot)$ gyűrű részgyűrűjei és ideáljai egybeesnek és megegyeznek a $(\mathbb{Z}_n, +)$ csoport részcsoportjaival. Ennek igazolása: azt kell belátnunk, hogy $\mathbb{Z}_n$ minden S részgyűrűje ideál (fordítva triviális). Ha $(S, +, \cdot) \leq (\mathbb{Z}_n, +, \cdot)$, akkor $(S, +) \leq (\mathbb{Z}_n, +)$, és mivel $(\mathbb{Z}_n, +)$ ciklikus csoport, következik, hogy $(S, +)$ is ciklikus (lásd csoportelméleti Tétel). Tehát $\exists \widehat{x} \in \mathbb{Z}_n : S = \langle \widehat{x} \rangle = \{k\widehat{x} : k \in \mathbb{Z}\}$, ahol $k\widehat{x} = \underbrace{\widehat{x} + \widehat{x} + ... + \widehat{x}}_{k}$. De mindegyik $\langle \widehat{x} \rangle$ ideál, mert $\forall \widehat{\ell} \in \mathbb{Z}_p$, $\forall k\widehat{x} \in \langle \widehat{x} \rangle \Rightarrow \widehat{\ell} \cdot k\widehat{x} = k\ell\widehat{x} \in \langle \widehat{x} \rangle$.

Például, $\mathbb{Z}_6$-ban $\langle \widehat{1} \rangle = \langle \widehat{5} \rangle = \mathbb{Z}_6$ ($\widehat{1}$ és $\widehat{5}$ invertálhatók, lásd 14. szakasz, első Tétel), $\langle \widehat{0} \rangle = \{\widehat{0}\}$, $\langle \widehat{2} \rangle = \langle \widehat{4} \rangle = \{\widehat{0}, \widehat{2}, \widehat{4}\}$, $\langle \widehat{3} \rangle = \{\widehat{0}, \widehat{3}\}$. Tehát $\mathbb{Z}_6$-nak 4 ideálja van, ezek az összes részgyűrűk is: $\{\widehat{0}\}$, $\{\widehat{0}, \widehat{3}\}$, $\{\widehat{0}, \widehat{2}, \widehat{4}\}$, $\mathbb{Z}_6$.

Legyen most F egy tetszőleges részteste $\mathbb{Z}_p$-nek. Akkor F a $\mathbb{Z}_p$ részgyűrűje, és az előzőek alapján következik, hogy F ideál. De testnek nincs valódi ideálja (Tétel), $F = \{0\}$ nem lehet, ezért $F = \mathbb{Z}_p$, amit igazolni akartunk. ★

12.D. Feladatok

▼ 1. Ideált alkotnak-e a megadott I halmazok a megfelelő gyűrűkben:

a) $R = 2\mathbb{Z}$, $I = 4\mathbb{Z}$, b) $R = \mathbb{Z}[i]$, $I = \mathbb{Z}$, c) $R = \mathbb{Z}[i]$, $I = \{a + bi : a, b \text{ páros }\}$.

▼ 2. Mutassuk meg, hogy egy egységelemes gyűrű valódi ideálja nem tartalmazza az egységelemet.

▼ 3. Igazoljuk, hogy egy egységelemes R gyűrű valamely $I \neq \emptyset$ részhalmaza akkor és csak akkor ideál, ha $\forall\, i_1, i_2 \in I$ és $\forall\, r_1, r_2 \in R$ esetén $r_1 i_1 + r_2 i_2 \in I$.

▼ 4. Legyen $(A, +, \cdot)$ egy kommutatív gyűrű és $r(A) = \{a \in A : \exists\, n \in \mathbb{N}^*, a^n = 0\}$ az A gyűrű nilpotens elemeinek halmaza. Igazoljuk, hogy:

a) $r(A) \trianglelefteq A$,

b) $r(A \times B) = r(A) \times r(B)$, ahol B is kommutatív gyűrű és $A \times B$ a gyűrűk direkt szorzata, lásd 10.A.1.

Megoldás. a) $0 \in r(A) \neq \emptyset$; ha $a, b \in r(A)$, akkor $a - b \in r(A)$, valóban: $\exists n, m \in \mathbb{N} : a^n = b^m = 0$ és

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k (-b)^{n+m-k} = 0,$$

mert az összeg minden tagja nulla: ha $k \geq n$, akkor $a^k = 0$, ha pedig $k < n$, akkor $n+m-k > m$ és $b^{n+m-k} = 0$. Továbbá, ha ha $a \in r(A)$ és $x \in A$, $ax \in r(A), xa \in r(A)$, mert $(ax)^n = a^n x^n = 0$, hasonlóan $(xa)^n = x^n a^n = 0$.

b) Tegyük fel, hogy $(a, b) \in r(A \times B)$, akkor $\exists n \in \mathbb{N} : (a, b)^n = (a^n, b^n) = 0 = (0, 0)$, innen $a^n = 0, b^n = 0$ és következik, hogy $a \in r(A), b \in r(B), (a, b) \in r(A) \times r(B)$.

Fordítva, ha $(a, b) \in r(A) \times r(B)$, akkor $\exists n, m \in \mathbb{N} : a^n = 0, b^m = 0$, innen $(a, b)^t = (a^t, b^t) = (0, 0) = 0$, ahol $t = \max(n, m)$, tehát $(a, b) \in r(A \times B)$.

▼ 5. Adjunk példát olyan gyűrűre és ennek olyan részhalmazára, amely által generált részgyűrű és ideál nem egyenlőek.

Útmutatás. Például a $(\mathbb{Q}, +, \cdot)$ gyűrűben legyen $X = \{1\}$.

▼ 6. Igaz-e, hogy egy gyűrű zérusosztói ideált alkotnak ?

Útmutatás. Nem igaz, vizsgáljuk például a $(\mathbb{Z}_6, +, \cdot)$ gyűrűt.

▼ 7. Igazoljuk, hogy a $(\mathbb{Z}_{p^k}, +, \cdot)$ gyűrűben, ahol p prím és $k \geq 1$, a zérusosztók a $\widehat{0}$-val együtt ideált alkotnak.

Útmutatás. Igazoljuk, hogy a zérusosztók pontosan a $\widehat{p\ell}$, $1 \leq \ell < p^{k-1}$ elemek.

13. Faktorgyűrűk, homomorfizmustétel

13.A. Faktorgyűrűk

Ebben a szakaszban definiáljuk a faktorgyűrű fogalmát, amely hasonló a csoportok esetén tárgyalt faktorcsoport fogalmához, de normálrészcsoportok helyett most ideálokkal történik a konstrukció.

Legyen $(R,+,\cdot)$ egy gyűrű és $I \trianglelefteq R$ egy ideál. Az additív műveletet tekintve: $(I,+) \leq (R,+)$ (részcsoport) és tekintsük a következő relációt:

$$\forall a,b \in I: \qquad a \equiv b \pmod{I} \;\Leftrightarrow a-b \in I,$$

amely nem más, mint a csoportokra definiált részcsoport szerinti kongruenciareláció (itt "+" kommutatív).

Tudjuk, hogy "$\equiv$" ekvivalenciareláció és a megfelelő faktorhalmaz a következő:

$$R/I = \{\widehat{a} : a \in R\},$$

ahol az ekvivalenciaosztályok $\widehat{a} = a + I = \{a + x : x \in I\}$ alakúak. Azt is láttuk, hogy az R/I halmazon az $\widehat{a} + \widehat{b} = \widehat{a+b}$ additív művelet egy Abel-csoportot határoz meg.

Definiáljuk most a következő műveletet:

$$\widehat{a} \cdot \widehat{b} = \widehat{ab}, \qquad \forall\, \widehat{a},\widehat{b} \in R/I.$$

Ez nem függ a választott reprezentánsoktól, ugyanis, ha $\widehat{a} = \widehat{a_1}, \widehat{b} = \widehat{b_1}$, akkor $a - a_1 = x \in I$, $b - b_1 = y \in I$ és kapjuk, hogy $ab = (a_1 + x)(b_1 + y) = a_1b_1 + a_1y + b_1x + xy$, ahol az utolsó három tagra: $a_1y + b_1x + xy \in I$, mert I ideál. Innen $ab - a_1b_1 \in I$, azaz $\widehat{ab} = \widehat{a_1b_1}$.

13.A.1. Tétel. Ha $(R,+,\cdot)$ egy gyűrű és I egy ideál, akkor az R/I faktorhalmaz egy gyűrű az előbbiekben definiált műveletekkel. Továbbá $p_I : R \to R/I$, $p_I(x) = \widehat{x}$ egy gyűrűmorfizmus.

Bizonyítás. Ahogy már megjegyeztük, $(R/I,+)$ Abel-csoport. A szorzás tulajdonságai:

1. $(\widehat{a}\widehat{b})\widehat{c} = \widehat{a}(\widehat{b}\widehat{c})$ (asszociativitás),
2. $\widehat{a}(\widehat{b}+\widehat{c}) = \widehat{a}\widehat{b} + \widehat{a}\widehat{c}$ és $(\widehat{a}+\widehat{b})\widehat{c} = \widehat{a}\widehat{c} + \widehat{b}\widehat{c}$ (disztributivitás).

Ezek igazolása azonnali a R-beli megfelelő tulajdonságok felhasználásával. Például,

$$(\widehat{a}\widehat{b})\widehat{c} = (\widehat{ab})\widehat{c} = \widehat{(ab)c} = \widehat{a(bc)} = \widehat{a}\widehat{bc} = \widehat{a}(\widehat{b}\widehat{c}).$$

$p_I : R \to R/I$ csoportmorfizmus, továbbá $p_I(ab) = \widehat{ab} = \widehat{a}\widehat{b} = p_I(a)p_I(b), \forall a,b \in R$, tehát p_I gyűrűmorfizmus. □

Az R/I gyűrűt az R gyűrűnek az I ideálra vonatkozó **faktorgyűrű**jének nevezzük.

Ha R egységelemes, akkor R/I is egységelemes, az egységelem $\widehat{1}$, amelyre $\widehat{a}\widehat{1} = \widehat{a \cdot 1} = \widehat{a}$ és $\widehat{1}\widehat{a} = \widehat{1 \cdot a} = \widehat{a}$, $\forall \widehat{a} \in R/I$. Ekkor $p_I(1) = \widehat{1}$, tehát p_I unitér morfizmus.

Ha R kommutatív, akkor R/I is kommutatív: $\widehat{a}\widehat{b} = \widehat{ab} = \widehat{ba} = \widehat{b}\widehat{a}$, $\forall\, \widehat{a},\widehat{b} \in R/I$.

13.A.2. Példa. • Ha $I \trianglelefteq (\mathbb{Z},+,\cdot)$, akkor tudjuk, hogy $I = n\mathbb{Z}$ alakú, ahol $n \in \mathbb{N}$. Az $n\mathbb{Z}$ szerinti kongruenciareláció éppen a kongruencia modulo n.

Továbbá, a $\mathbb{Z}/n\mathbb{Z}$ faktorgyűrű a maradékosztályok gyűrűje modulo n, ha $n\mathbb{Z} \neq \{0\}$. Ha $n\mathbb{Z} = \{0\}$, azaz ha $n = 0$, akkor $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$, ha pedig $n = 1$, akkor $\mathbb{Z}/1\mathbb{Z}$ a zérógyűrű, lásd 10.A. szakasz.

13.B. Homomorfizmustétel

Ha $f : R \to S$ egy gyűrűmorfizmus, akkor f **magja** a $\operatorname{Ker} f = \{x \in R : f(x) = 0\}$ halmaz.

★ Ha $I \trianglelefteq R$, akkor a $p_I : R \to R/I$, $p_I(x) = \widehat{x}$ **kanonikus projekció** magja éppen az I: $\operatorname{Ker} p_I = I$. Valóban, $\operatorname{Ker} p_I = \{x \in R : \widehat{x} = \widehat{0}\} = I$. Tehát minden ideál egy gyűrűhomomorfizmus magja. ★

13.B.1. Tétel. (homomorfizmus-tétel) Ha $f : R \to S$ egy gyűrűmorfizmus, akkor az

$$\overline{f} : R/\operatorname{Ker} f \to \operatorname{Im} f, \qquad \overline{f}(\widehat{x}) = f(x)$$

függvény gyűrűizomorfizmus, tehát $R/\operatorname{Ker} f \simeq \operatorname{Im} f$.

Bizonyítás. $f : (R, +) \to (S, +)$ csoportmorfizmus, és a csoportokra vonatkozó homomorfizmustétel szerint $\overline{f} : (R/\operatorname{Ker} f, +) \to (\operatorname{Im} f, +)$, $\overline{f}(\widehat{x}) = f(x)$ csoportizomorfizmus. $\overline{f}$ gyűrűmorfizmus is, mert $\forall \widehat{x}, \widehat{y} \in R/\operatorname{Ker} f \Rightarrow \overline{f}(\widehat{x}\widehat{y}) = \overline{f}(\widehat{xy}) = f(xy) = f(x)f(y) = \overline{f}(\widehat{x})\overline{f}(\widehat{y})$. □

Legyen $(P, +, \cdot)$ egy prímtest, tehát egy olyan test, amelynak nincs önmagán kívül más részteste, lásd 12.C. szakasz. A homomorfizmustétel segítségével igazolható:

13.B.2. Tétel. Ha P egy prímtest, akkor $P \simeq \mathbb{Q}$ vagy $P \simeq \mathbb{Z}_p$, ahol p prímszám.

13.C. Feladat

★ ▼ (Kínai maradéktétel) Legyen $m, n \in \mathbb{N}^*, (m, n) = 1$. Akkor $\overline{f} : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \overline{f}(\tilde{x}) = (\widehat{x}, \overline{x})$ gyűrűizomorfizmus, tehát $(\mathbb{Z}_{mn}, +, \cdot) \simeq (\mathbb{Z}_m \times \mathbb{Z}_n, +, \cdot)$.

Megoldás. Alkalmazzuk a homomorfizmustételt. Legyen $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n, f(x) = (\widehat{x}, \overline{x})$. Ez gyűrűhomomorfizmus, mert $f(x + y) = (\widehat{x + y}, \overline{x + y}) = (\widehat{x} + \widehat{y}, \overline{x} + \overline{y}) = (\widehat{x}, \overline{x}) + (\widehat{y}, \overline{y}) = f(x) + f(y)$ és $f(xy) = (\widehat{x + y}\overline{x + y}) = (\widehat{x}\widehat{y}, \overline{x}\overline{y}) = (\widehat{x}, \overline{x})(\widehat{y}, \overline{y}) = f(x)f(y)$.

Továbbá $\operatorname{Ker} f = \{x \in \mathbb{Z} : f(x) = (\widehat{0}, \overline{0})\} = \{x \in \mathbb{Z} : m|x, n|x\} = mn\mathbb{Z}$, mert $(m, n) = 1$.

Következik, hogy $\overline{f} : \mathbb{Z}_{mn} \to \operatorname{Im} f, \overline{f}(x) = (\widehat{x}, \overline{x})$ gyűrűizomorfizmus. Mivel $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$, ezért $\operatorname{Im} f = \mathbb{Z}_m \times \mathbb{Z}_n$ és kapjuk, hogy $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. ★

14. Integritástartomány hányadosteste

14.A. Hányadostest

Legyen $(R, +, \cdot)$ egy integritástartomány és $R^* = R \setminus \{0\}$. Az

$$R \times R^* = \{(a, b) : a, b \in R, b \neq 0\}$$

Descartes-szorzaton értelmezzük a következő "$\sim$" bináris relációt:

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc.$$

14.A.1. Tétel. A "$\sim$" reláció egy ekvivalenciareláció.

Bizonyítás. Minden $(a, b) \in R \times R^*$ esetén $(a, b) \sim (a, b)$, mert $ab = ba$, tehát "$\sim$" reflexív. Ha $(a, b), (c, d) \in R \times R^*$ úgy, hogy $(a, b) \sim (c, d)$, akkor $ad = bc$ vagy $cb = da$, ahonnan $(c, d) \sim (a, b)$ és következik, hogy "$\sim$" szimmetrikus.

"$\sim$" tranzitív is. Valóban, ha $(a, b), (c, d), (e, f) \in R \times R^*$ úgy, hogy $(a, b) \sim (c, d)$ és $(c, d) \sim (e, f)$, akkor $ad = bc$, $cf = de$. Ezeket összeszorozva: $adcf = bcde$ és dc-vel egyszerűsítve, ahol $dc \neq 0$: $af = be$, ami azt jelenti, hogy $(a, b) \sim (e, f)$. □

Tekintsük az így meghatározott ekvivalenciaosztályokat, amelyeket racionális törteknek nevezünk. Jelölés: (a, b) osztálya $\frac{a}{b}$. Itt $\frac{a}{b} = \frac{c}{d}$ akkor és csak akkor, ha $ad = bc$.

Legyen $F(R) = R \times R^*/\sim$ a megfelelő faktorhalmaz, amelyen a következő műveleteket értelmezzük: ha $\frac{a}{b}, \frac{c}{d}$ racionális törtek, ahol $b, d \neq 0$, akkor $bd \neq 0$ és legyen

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Ezek a műveletek helyesen értelmezettek, azaz nem függenek a választott reprezentánsoktól. Ehhez azt kell belátnunk, hogy ha $\frac{a}{b} = \frac{a'}{b'}$ és $\frac{c}{d} = \frac{c'}{d'}$, akkor

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}, \tag{1}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}. \tag{2}$$

Valóban, (1) azt jelenti, hogy

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'},$$

azaz $adb'd' + bcb'd' = a'd'bd + bdb'c'$ vagy $ad'(ab' - a'b) = bb'(dc' - cd')$, ami igaz, mert a feltétel szerint $ab' = a'b$ és $cd' = dc'$.

Hasonlóképpen, (2) jelentése

$$\frac{ac}{bd} = \frac{a'c'}{b'd'},$$

azaz $acb'd' = bda'c'$, ami az $ab' = a'b$, $cd' = c'd$ egyenlőségek összeszorzásából adódik.

14.A.2. Tétel. 1) $(F(R),+,\cdot)$ egy kommutatív test.

2) A $j : R \to F(R)$, $j(a) = \frac{a}{1}$ leképezés egy injektív gyűrűmorfizmus.

Bizonyítás. 1) Legyen $0 = \frac{0}{1}$, $1 = \frac{1}{1}$. Figyeljük meg, hogy $0 = \frac{0}{b}$, $1 = \frac{b}{b}$ minden $b \in R^*$ esetén. A definiált összeadás és szorzás a következő tulajdonságokkal rendelkezik: $\forall \frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F(R)$ esetén

(i) $$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f}),$$

(ii) $$\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b},$$

(iii) $$\frac{a}{b} + 0 = \frac{a}{b},$$

(iv) $$\frac{a}{b} + \frac{-a}{b} = 0,$$

(v) $$(\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f} = \frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}),$$

(vi) $$\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b},$$

(vii) $$\frac{a}{b} \cdot 1 = \frac{a}{b},$$

(viii) $$\frac{a}{b}(\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f},$$

(ix) $$\frac{a}{b} \cdot \frac{b}{a} = 1, \quad a, b \neq 0.$$

Ezek közvetlen számolással ellenőrízhetők.

2) Valóban, $\forall a, b \in R$: $j(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = j(a) + j(b)$, $j(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = j(a)j(b)$, továbbá, ha $j(a) = j(b)$, akkor $\frac{a}{1} = \frac{b}{1}$, $a \cdot 1 = b \cdot 1$, azaz $a = b$. □

Az $(F(R),+,\cdot)$ kommutatív testet az R integritástartomány **hányadostest**ének nevezzük.

Következik, hogy j egy izomorfizmust ad az R gyűrű és $F(R)$-nek az $R' = \{\frac{a}{1} : a \in R\}$ részgyűrűje között. Ez az izomorfizmus lehetővé teszi, hogy azonosítsuk R-et R'-tel és az a elemet az $\frac{a}{1}$ racionális törttel, $a = \frac{a}{1}$-et írva. Így, ha $\frac{a}{b} \in F(R)$, akkor írható: $\frac{a}{b} = \frac{a}{1}\frac{1}{b} = \frac{a}{1}(\frac{b}{1})^{-1} = ab^{-1}$.

Ha $R = \mathbb{Z}$, akkor a racionális számok konstrukcióját kapjuk: $F(\mathbb{Z}) = \mathbb{Q}$.

Ha K egy kommutatív test és R részgyűrűje K-nak (következik, hogy R integritástartomány), akkor R hányadosteste a legkisebb olyan részteste K-nak, amely tartalmazza R-et.

14.B. Feladatok

▼ 1. Legyen K egy kommutatív test. Mi lesz ennek hányadosteste ?

▼ 2. Legyen $d \in \mathbb{Z}$ négyzetmentes. Igazoljuk, hogy $\mathbb{Z}[\sqrt{d}]$ hányadosteste $\mathbb{Q}(\sqrt{d})$. Speciálisan, $\mathbb{Z}[i]$ hányadosteste $\mathbb{Q}(i)$.

★ ▼ 3. Legyen p egy prímszám és $\mathbb{Q}_{(p)} = \{\frac{m}{n} : (n,p) = 1\}$. Igazoljuk, hogy $\mathbb{Q}_{(p)}$ részgyűrűje $\mathbb{Q}$-nak és $\mathbb{Q}_{(p)}$ hányadosteste $\mathbb{Q}$. ★

15. Polinomok gyűrűje

15.A. Formális sorok és polinomok gyűrűje

Legyen $(R,+,\cdot)$ egy kommutatív, egységelemes gyűrű. Tekintsük az $R^{\mathbb{N}}=\{f|f:\mathbb{N}\to R\}$ halmazt, amelynek f elemeit R-beli **sorozat**oknak nevezzük, jelölés: $f=(a_0,a_1,a_2,...)$, ahol $a_n=f(n), n\in\mathbb{N}$.

Legyen $f,g\in R^{\mathbb{N}}$, $f=(a_0,a_1,a_2,...)$, $g=(b_0,b_1,b_2,...)$ és definiáljuk a következő műveleteket:

$$(f+g)(n)=f(n)+g(n)=a_n+b_n,$$
$$(f\cdot g)(n)=\sum_{i+j=n}f(i)g(j)=\sum_{i+j=n}a_ib_j.$$

Itt $f\cdot g=(a_0b_0,a_0b_1+a_1b_0,a_0b_2+a_1b_1+a_2b_0,...)$.

Legyen továbbá $\operatorname{supp}(f)=\{n\in\mathbb{N}:a_n\neq 0\}$ az f **tartóhalmaz**a és $R^{(\mathbb{N})}=\{f\in R^{\mathbb{N}}:$ $\operatorname{supp}(f)$ véges halmaz$\}$. Az $R^{(\mathbb{N})}$ elemei azok az $f=(a_0,a_1,a_2,...)$ sorozatok, amelyekre létezik $n\in\mathbb{N}$ úgy, hogy $a_i=0$, ha $i>n$.

15.A.1. Tétel. a) $(R^{\mathbb{N}},+,\cdot)$ kommutatív egységelemes gyűrű. Ha $f=(a_0,a_1,a_2,...)\in R^{\mathbb{N}}$, akkor $f=\sum_{k=0}^{\infty}a_kX^k$, ahol $X=(0,1,0,0,...)$, és ez a felírás egyértelmű.

b) $(R^{(\mathbb{N})},+,\cdot)$ unitér részgyűrűje $R^{\mathbb{N}}$-nek és $i_R:R\to R^{(\mathbb{N})}$, $i_R(a)=(a,0,0,...)$ unitér injektív homomorfizmus. Továbbá, ha $f\in R^{(\mathbb{N})}$, akkor az $X=(0,1,0,0,...)$ jelöléssel, $f=\sum_{k=0}^{n}a_kX^k$, ahol $n=\max\operatorname{supp}(f)$, és ez a felírás egyértelmű.

Bizonyítás. a) Azonnali, hogy $(R^{\mathbb{N}},+)$ Abel-csoport. Vizsgáljuk a "$\cdot$" művelet tulajdonságait:

R kommutatív gyűrű, s emiatt "$\cdot$" kommutatív. Ha $f,g,h\in R^{\mathbb{N}}$ és $n\in\mathbb{N}$, akkor

$$((fg)h)(n)=\sum_{i+j=n}(fg)(i)h(j)=\sum_{i+j=n}(\sum_{k+\ell=i}f(k)g(\ell))h(j)=$$

$$=\sum_{k+m=n}f(k)\sum_{\ell+j=m}g(\ell)h(j)=\sum_{k+m=n}f(k)(gh)(m)=(f(gh))(n),$$

tehát $(fg)h=f(gh)$. Továbbá

$$((f+g)h)(n)=\sum_{i+j=n}(f+g)(i)h(j)=\sum_{i+j=n}(f(i)+g(i))h(j)=$$

$$=\sum_{i+j=n}f(i)h(j)+\sum_{i+j=n}g(i)h(j)=(fh)(n)+(gh)(n)=(fh+gh)(n),$$

tehát $(f+g)h=fh+gh$. Az egységelem $1=(1,0,0,...)$.

Vegyük észre, hogy minden $k\in\mathbb{N}$-re $X^k=(0,0,...,1,0,0,...)$, ahol 1 a k-adik helyen van, tehát $X^k(i)=\delta_{ik}$ (Kronecker-szimbólum). Ha $a=(a,0,0,...)\in R$, akkor $aX^k=(0,...,0,a,0,...)$. Innen $f=(a_0,a_1,a_2,...,a_n,...)=(a_0,0,0,...)+(0,a_1,0,0,...)+...=\sum_{k=0}^{\infty}a_kX^k$ és ez a felírás egyértelmű.

b) $0=(0,0,...)\in R^{(\mathbb{N})}$. Ha $f,g\in R^{(\mathbb{N})}$, akkor létezik $m,n\in\mathbb{N}$ úgy, hogy $f(i)=0$, ha $i>m$ és $g(i)=0$, ha $i>n$. Így $(f-g)(i)=0$, ha $i>\max(m,n)$ és $(fg)(i)=0$, ha $i>m+n$. Tehát $f-g,fg\in R^{(\mathbb{N})}$, azaz $R^{(\mathbb{N})}$ részgyűrűje $R^{\mathbb{N}}$-nek.

Továbbá $\forall a,b \in R$: $i_R(a+b) = (a+b,0,0,...) = (a,0,0,...)+(b,0,0,...) = i_R(a)+i_R(b)$, $i_R(ab) = (ab,0,0,...) = (a,0,0,...)(b,0,0,...) = i_R(a)i_R(b)$, azaz i_R homomorfizmus. Azonnali, hogy i_R unitér és injektív. □

Az $R^{\mathbb{N}}$ gyűrűt az R feletti **formális sorok gyűrűjé**nek nevezzük, jelölés: $R[[X]]$. Az $X = (0,1,0,...)$ formális hatványsor neve X **határozatlan**. Ha $f = (a_0,a_1,a_2,...) \in R^{\mathbb{N}}$, akkor az $f = \sum_{k=0}^{\infty} a_k X^k$ felírást szokás használni. Az a_i elemek, ahol $i \geq 0$, az f **együtthatói**. Azt mondjuk, hogy f egy R feletti **formális sor**.

Az $R^{(\mathbb{N})}$ gyűrű az R feletti **(egyhatározatlanú) polinomok gyűrűje**, jelölés: $R[X]$. Ha $f = (a_0,a_1,a_2,...) \in R^{(\mathbb{N})}$, akkor a továbbiakban az $f = \sum_{k=0}^{n} a_k X^k$ felírást fogjuk használni. Néha az f helyett $f(X)$-et írunk.

Az $a_i, 0 \leq i \leq n$ elemek az f polinom **együtthatói**. Azt mondjuk, hogy f egy R feletti **polinom** (vagy R-beli együtthatós polinom). Az aX^n polinomot **monom**nak nevezzük.

Ha $f \in R[X]$, $f \neq 0$, akkor az f **foka** a $\mathrm{gr}(f) = \max \mathrm{supp}(f) = \max\{n \in \mathbb{N} : a_n \neq 0\}$ természetes szám. Ha $n = \mathrm{gr}(f)$, akkor az a_n együtthatót az f **főegyütthatój**ának nevezzük. Megállapodás szerint $\mathrm{gr}(0) = -\infty$, amelyre érvényesek az alábbiak: $-\infty < n$, $-\infty + n = -\infty$, ahol $n \in \mathbb{N}$, $-\infty + (-\infty) = -\infty$.

15.A.2. Tétel. Legyen $(R,+,\cdot)$ egy gyűrű és $f,g \in R[X]$. Akkor

a) $\mathrm{gr}(f+g) \leq \max\{\mathrm{gr}(f),\mathrm{gr}(g)\}$,

b) $\mathrm{gr}(fg) \leq \mathrm{gr}(f)+\mathrm{gr}(g)$. Továbbá, ha $f,g \neq 0$ és ha vagy az f vagy a g főegyütthatója nem zérusosztó (speciálisan, ha R integritástartomány), akkor $\mathrm{gr}(fg) = \mathrm{gr}(f)+\mathrm{gr}(g)$.

Bizonyítás. a) Legyen $\mathrm{gr}(f) = m, \mathrm{gr}(g) = n$. Ha $f,g \neq 0$, akkor $m,n \geq 0$ és az összeadás és a szorzás definíciója szerint $(f+g)(i) = 0$, ha $i > \max\{m,n\}$ és $(fg)(i) = 0$, ha $i > m+n$.

Ha $f = 0$ vagy $g = 0$, azaz ha $\mathrm{gr}(f) = -\infty$ vagy $\mathrm{gr}(g) = -\infty$, akkor használjuk a $-\infty$ szimbólumra vonatkozó fenti összefüggéseket.

b) Legyen $f = \sum_{i=0}^{m} a_i X^i, a_m \neq 0$, $g = \sum_{j=0}^{n} b_j X^j, b_n \neq 0$. Akkor fg főegyütthatója $a_m b_n \neq 0$. □

Példa • b)-ben az egyenlőtlenség lehet szigorú: $f = 1+\widehat{2}X, g = \widehat{2}X \in \mathbb{Z}_4[X]$, $fg = (1+\widehat{2}X)\widehat{2}X = \widehat{2}X$, $\mathrm{gr}(fg) = 1 < 2 = \mathrm{gr}(f)+\mathrm{gr}(g)$ ($\mathbb{Z}_4[X]$-ben $\widehat{2}$ zérusosztó).

★ **15.A.3. Tétel.** 1) Egy $a \in R$ elem akkor és csak akkor invertálható R-ben, ha invertálható $R[X]$-ben.

2) Ha R integritástartomány, akkor $R[X]$ is integritástartomány és $U(R) = U(R[X])$.

Bizonyítás. 1) Ha $a \in R$ invertálható, akkor $ab = 1$, ahol $b \in R$. Ezt az egyenlőséget $R[X]$-ben tekintve, a és b nulladfokú polinomok és következik, hogy a invertálható $R[X]$-ben. Fordítva, ha a invertálható $R[X]$-ben, akkor létezik $f = a_0+a_1X+...+a_nX^n \in R[X], a_n \neq 0$ úgy, hogy $af = 1$, azaz $aa_0+aa_1X+...+aa_nX^n = 1$. Innen $aa_0 = 1$ és következik, hogy a-nak a_0 az inverze R-ben.

2) Ha R integritástartomány, akkor az előző Tétel szerint $R[X]$ is integritástartomány. Továbbá a jelen Tétel 1) pontja szerint $U(R) \subseteq U(R[X])$. Igazoljuk a fordított irányú bennfoglalást: legyen $f = a_0+a_1X+...+a_mX^n, a_m \neq 0$ egy invertálható polinom $R[X]$-ben. Akkor létezik $g = b_0+b_1X+...+b_nX^n$, $b_n \neq 0$ úgy, hogy $fg = 1$. Innen $\mathrm{gr}(fg) = \mathrm{gr}(1), \mathrm{gr}(f)+\mathrm{gr}(g) = 0, m+n = 0, m = n = 0$. Tehát $f = a_0 \in R, g = b_0 \in R$ é $1 = fg = a_0b_0$, ahonnan $f = a_0 \in U(R)$. □

Példa. • Ha R nem integritástartomány, akkor lehet $U(R) \neq U(R[X])$: pl. $f = 1+\widehat{2}X \in \mathbb{Z}_4[X]$ invertálható, mert $ff = (1+\widehat{2}X)(1+\widehat{2}X) = \widehat{1}$. ★

Legyen R egy kommutatív egységelemes, gyűrű és $f = \sum_{i=0}^{n} a_i X^i \in R[X]$. Ha $x \in R$, akkor az $f(x) = \sum_{i=0}^{n} a_i x^i \in R$ elemet az f x-re vonatkozó **helyettesítési érték**ének

nevezzük.

Definiálható az $\overline{f} : R \to R$, $\overline{f}(x) = \sum_{i=0}^{n} a_i x$ függvény, amelynek neve az f-hez rendelt **polinomfüggvény**.

Ha $f = a \in R$, akkor $\overline{f}$ konstans, $\overline{f}(x) = a$ minden $x \in R$-re. Ezért az R elemeit, polinomokként tekintve, **konstans polinom**oknak nevezzük.

Megjegyezzük, hogy léteznek olyan $\overline{f}$ polinomfüggvények, amelyek konstansok, ugyanakkor $f \notin R$ (pl. $f = X + X^2 \in \mathbb{Z}_2[X]$, amelyre $f(\widehat{0}) = f(\widehat{1}) = \widehat{0}$). De csak az $f = a \in R$ polinomokat nevezzük konstansoknak.

Ha f, g egyenlő polinomok, akkor az $\overline{f}, \overline{g}$ függvények is egyenlőek. Léteznek azonban olyan különböző polinomok is, amelyekhez rendelt függvények egyenlőek, pl. $f = X + \widehat{1}, g = X^2 + \widehat{1} \in \mathbb{Z}_2[X]$. Akkor $\overline{f}, \overline{g} : \mathbb{Z}_2 \to \mathbb{Z}_2$, $\overline{f}(\widehat{0}) = \overline{g}(\widehat{0}) = \widehat{1}$, $\overline{f}(\widehat{1}) = \overline{g}(\widehat{1}) = \widehat{0}$, tehát $\overline{f} = \overline{g}$, de $f \neq g$.

15.A.3. Tétel. Két polinom összegéhez (szorzatához) rendelt polinomfüggvény egyenlő a két polinomhoz rendelt polinomfüggvények összegével (szorzatával):

$$\overline{f+g} = \overline{f} + \overline{g}, \qquad \overline{fg} = \overline{f} \cdot \overline{g},$$

azaz minden $x \in R$ esetén a $\phi : R[X] \to R$, $\phi(f) = f(x)$ leképezés egy gyűrűmorfizmus.

Bizonyítás. Ha $f, g \in R[X]$, $f = a_0 + a_1X + a_2X^2 + ...$, $g = b_0 + b_1X + b_2X^2 + ...$, akkor minden $x \in R$ esetén:

$$\begin{aligned}
&\overline{f}(x) + \overline{g}(x) = f(x) + g(x) = (a_0 + a_1x + a_2x^2 + ...) + (b_0 + b_1x + b_2x^2 + ...) = \\
&= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... = (f+g)(x) = (\overline{f+g})(x), \\
&\overline{f}(x)\overline{g}(x) = f(x)g(x) = (a_0 + a_1x + a_2x^2 + ...)(b_0 + b_1x + b_2x^2 + ...) = \\
&= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ... = (fg)(x) = (\overline{fg})(x). \qquad \square
\end{aligned}$$

15.B. Maradékos osztás, polinomok gyökei

15.B.1. Tétel.(maradékos osztás) Ha R egy integritástartomány és $f = a_0 + a_1X + \cdots + a_nX^n, g = b_0 + b_1X + \cdots + b_mX^m \in R[X]$, adott polinomok úgy, hogy b_m invertálható elem, akkor léteznek az egyértelműen meghatározott $q, r \in R[X]$ polinomok, amelyekre

$$f = gq + r, \qquad \text{ahol} \qquad \operatorname{gr}(r) < \operatorname{gr}(g). \tag{1}$$

Bizonyítás. I. Létezés. Ha $\operatorname{gr}(f) < \operatorname{gr}(g)$, akkor vehető $q = 0$ és $r = f$. Ha $\operatorname{gr}(f) \geq \operatorname{gr}(g)$, akkor $\operatorname{gr}(f) = n$ szerinti indukcióval bizonyítunk. Tegyük fel, hogy minden $h \in R[X]$, $\operatorname{gr}(h) < n$ polinom felírható (1) alakban és legyen $f = a_0 + a_1X + \cdots + a_nX^n$, $\operatorname{gr}(f) = n$, $g = b_0 + b_1X + \cdots + b_mX^m$, $0 \leq \operatorname{gr}(g) = m \leq n$, b_m invertálható. Képezzük a $h = f - a_nb_m^{-1}X^{n-m}g$ polinomot, amelynek foka kisebb mint n és alkalmazva rá az indukciós feltételt kapjuk, hogy léteznek olyan $q_1, r_1 \in R[X]$ polinomok, amelyekre $h = gq_1 + r_1$, ahol $\operatorname{gr}(r_1) < \operatorname{gr}(g)$. Innen $f = g(a_nb_m^{-1}X^{n-m} + q_1) + r_1$, tehát választható $q = a_nb_m^{-1}X^{n-m} + q_1$ és $r = r_1$.

II. Egyértelműség. Tegyük fel, hogy $f = gq + r$, ahol $\operatorname{gr}(r) < \operatorname{gr}(g)$ és $f = gq^* + r^*$, ahol $\operatorname{gr}(r^*) < \operatorname{gr}(g)$. Akkor $f = gq + r = gq^* + r^*$, $g(q - q^*) = r^* - r$, ahol $\operatorname{gr}(r - r^*) < \operatorname{gr}(g)$. Ha $q \neq q^*$, akkor $\operatorname{gr}(g(q - q^*)) \geq \operatorname{gr}(g)$, ami ellentmondás. Ezért következik, hogy $q = q^*$, ahonnan $r = r^*$. $\square$

Megjegyzések. Az előbbi Tételben q az **osztási hányados** és r az **osztási maradék**. Az (1) felírásban vagy $r = 0$, ekkor $\operatorname{gr}(r) = -\infty$ vagy $r \neq 0$ és

$0 \leq \mathrm{gr}(r) < \mathrm{gr}(g)$. Ha R egy kommutatív test, akkor ez a Tétel alkalmazható minden $g \neq 0$ polinomra.

Legyen R egy integritástartomány és $f, g \in R[X]$. Azt mondjuk, hogy f **osztój**a g-nek, jel. $f|g$, ha létezik $h \in R[X]$ úgy, hogy $g = fh$. Ellenkező esetben f nem osztója g-nek, jel. $f \not| g$. Ha $f, g \in R[X]$ és ha g-nek a b_m főegyütthatója invertálható, akkor $f|g$ pontosan akkor teljesül, ha az utóbbi Tételbeli osztási maradék nulla: $r = 0$.

• Ha $f = X - 1, g = X^2 + 3X - 4 \in \mathbb{Z}[X]$, akkor $f|g$.

• Ha $f = X + \widehat{1}, g = \widehat{2}X^2 + X + \widehat{3} \in \mathbb{Z}_4[X]$, akkor $f|g$, mert $g = \widehat{2}X^2 + X + \widehat{3} = (X + \widehat{1})(\widehat{2}X^2 + \widehat{3})$.

• Minden polinom osztója a nulla polinomnak és a nulla polinom csak önmagának osztója.

Az $f \in R[X]$ polinomnak $x \in R$ **gyök**e, ha $f(x) = 0$.

15.B.2. Tétel. (Bézout) Legyen R egy integritástartomány.

a) $f \in R[X]$ és $a \in R$. Az $a \in R$ elem akkor és csak akkor gyöke az $f \in R[X]$ polinomnak, ha $X - a$ osztója f-nek.

b) Ha $\mathrm{gr}(f) = n \geq 1$, akkor f-nek legfeljebb n különböző gyöke van R-ben.

Bizonyítás. a) Az előző Tétel következménye: $f = (X - a)q + r$, ahol $r = f(a)$, kész.

Más, közvetlen bizonyítás: Legyen $f = a_0 + a_1X + a_2X^2 + ... + a_nX^n$, $a_n \neq 0$ úgy, hogy $f(a) = 0$. Akkor $f = f - 0 = f - f(a) = a_0 + a_1X + a_2X^2 + ... + a_nX^n - (a_0 + a_1a + a_2a^2 + ... + a_na^n) = a_1(X - a) + a_2(X^2 - a^2) + ... + a_n(X^n - a^n)$. De $X - a$ osztója $X^k - a^k$-nak minden $1 \leq k \leq n$ esetén, ezért $X - a$ osztója f-nek. Fordítva, ha $X - a$ osztója f-nek, akkor létezik $h \in R[X]$ úgy, hogy $f = (X - a)h$. Akkor $f(a) = (a - a)h(a) = 0$, tehát a gyöke f-nek.

b) n szerinti indukcióval. Ha $n = 1$, $f = a_0 + a_1X \in R[X]$, akkor f-nek vagy nincs gyöke vagy 1 gyöke van, pl. $f = 3X + 4 \in \mathbb{Z}[X]$-nek nincs gyöke, 2 gyök nem lehet, mert $f(x_1) = a_0 + a_1x_1 = 0$, $f(x_2) = a_0 + a_1x_2 = 0$ alapján $a_1(x_1 - x_2) = 0$, innen $x_1 - x_2 = 0$, $x_1 = x_2$ (R zérusosztómentes).

Tegyük fel, hogy a tulajdonság igaz minden $(n-1)$-edfokú polinomra, legyen $\mathrm{gr}(f) = n$ és a gyöke f-nek. Akkor $f = (X - a)g$, ahol $\mathrm{gr}(g) = n - 1$, tehát g-nek legfeljebb $n - 1$ gyöke van és következik, hogy f-nek legfeljebb n gyöke van. □

Ha R nem integritástartomány, akkor a Tétel b) állítása nem feltétlen igaz.

Példa. • Az $f = X^2 - \widehat{1} \in \mathbb{Z}_{12}$ polinomnak 4 gyöke van $\mathbb{Z}_{12}$-ben: $\widehat{1}, -\widehat{1} = \widehat{11}, \widehat{5}, -\widehat{5} = \widehat{7}$.

• Legyen $R = \mathbb{Z} \times \mathbb{Z}$, amelyben $(0, 1)(1, 0) = (0, 0)$, tehát vannak zérusosztók és ez nem integritástartomány. Tekintsük az $f = (1, 0)X$ polinomot, amelynek foka 1. Minden $(0, n) \in R$ elem gyöke f-nek, mert $f(0, n) = (1, 0)(0, n) = (0, 0)$, tehát f-nek végtelen sok gyöke van.

Azt mondjuk, hogy $a \in R$ k-**ad rendű gyök**e f-nek (k **multiplicitású gyök**), ha $(X - a)^k | f$ és $(X - a)^{k+1} \not| f$.

A Bézout tétel alapján világos, hogy a akkor és csak akkor k-adrendű gyök, ha létezik olyan g polinom, amelyre $f = (X - a)^k g$ és $g(a) \neq 0$.

15.B.3. Tétel. Ha R integritástartomány, $f, g \in R[X]$ és a k-ad rendű gyöke f-nek és ℓ-ed rendű gyöke g-nek, akkor a $k + \ell$-ed rendű gyöke az fg szorzatnak.

Bizonyítás. $f = (X - a)^k f_1$, ahol $f_1(a) \neq 0$ és $g = (X - a)^\ell g_1$, ahol $g_1(a) \neq 0$. Akkor $fg = (X - a)^{k+\ell} f_1 g_1$ és mivel R integritástartomány, $f_1(a)g_1(a) \neq 0$. Tehát a $k + \ell$-ed rendű gyök. □

15.B.4. Tétel. Legyen R integritástartomány és $f \in R[X], f \neq 0$. Ha $a_1, a_2, ..., a_m$ rendre $k_1, k_2, ..., k_m$-ed rendű különböző gyökei f-nek, akkor létezik olyan $g \in R[X]$, hogy

$$f = (X - a_1)^{k_1}(X - a_2)^{k_2} \cdots (X - a_m)^{k_m} g.$$

Bizonyítás. m-szerinti indukcióval bizonyítunk. Ha $m = 1$, akkor az állítás következik a definícióból. Tegyük fel, hogy az állítás igaz $m-1$-re és igazoljuk m-re. Létezik tehát $g_1 \in R[X]$ úgy, hogy

$$f = (X - a_1)^{k_1}(X - a_2)^{k_2} \cdots (X - a_{m-1})^{k_{m-1}} g_1.$$

Akkor $0 = f(a_m) = (a_m - a_1)^{k_1}(a_m - a_2)^{k_2} \cdots (a_m - a_{m-1})^{k_{m-1}} g_1(a_m)$, s mivel $a_m \neq a_i, 1 \leq i \leq m-1$, következik, hogy $g_1(a_m) = 0$, sőt a_m k_m-ed rendű gyöke g_1-nek. Kapjuk, hogy $g_1 = (X - a_m)^{k_m} g$ és ezt visszahelyettesítve készen vagyunk. □

Ha $f \in R[X]$ különböző gyökei $a_1, a_2, ..., a_m \in R$ és ezek rendre $k_1, k_2, ..., k_m$-ed rendű gyökök, akkor azt mondjuk, hogy f gyökeinek száma multiplicitással számolva $k_1 + k_2 + ... + k_m$. Ha f gyökeit tekintjük és nem kötjük ki, hogy ezek különbözőek, akkor mindegyik gyököt annyiszor vesszük, amennyi a multiplicitása.

Következmény. Ha R integritástartomány és $f \in R[X]$, $\mathrm{gr}(f) = n \geq 1$, akkor f-nek legfeljebb n gyöke van multiplicitással számolva.

15.B.5. Tétel. (Viéte-képletek) Legyen R integritástartomány és $f = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$, $a_n \neq 0$ egy nemnulla polinom $R[X]$-ben. Ha f-nek n gyöke van R-ben, multiplicitással számolva, és ezek: $x_1, x_2, ..., x_n$, akkor

$$f = a_n(X - x_1)(X - x_2) \cdots (X - x_n),$$

továbbá

$$\begin{aligned}
&x_1 + x_2 + ... + x_n = -a_{n-1}a_n^{-1},\\
&x_1x_2 + x_1x_3 + ...x_1x_n + ... + x_{n-1}x_n = a_{n-2}a_n^{-1},\\
&.....\\
&x_1x_2 \cdots x_k + x_1x_2 \cdots x_{k-1}x_{k+1} + ... + x_{n-k+1}x_{n-k+2} \cdots x_n = (-1)^k a_k a_n^{-1},\\
&.....\\
&x_1x_2 \cdots x_n = (-1)^n a_0 a_n^{-1}.
\end{aligned}$$

Bizonyítás. Az előző Tétel szerint $f = (X - x_1)(X - x_2) \cdots (X - x_n)g$, ahol $g \in R[X]$. Azonosítva X^n együtthatóit a két oldalon: $g = a_n$. Tehát $f = a_n(X - x_1)(X - x_2) \cdots (X - x_n) = a_n X^n - a_n(x_1 + x_2 + ... + x_n)X^{n-1} + a_n(x_1x_2 + x_1x_3 + ...x_1x_n + ... + x_{n-1}x_n)X^{n-2} + ... + (-1)^k a_n(x_1x_2 \cdots x_k + x_1x_2 \cdots x_{k-1}x_{k+1} + ... + x_{n-k+1}x_{n-k+2} \cdots x_n)X^{n-k} + ... + (-1)^n a_n x_1x_2 \cdots x_n$, ahonnan, azonosítva az együtthatókat az adott egyenlőségeket kapjuk. □

Következmény. (Wilson tétel) Ha $p \geq 2$ prímszám, akkor

$$(p-1)! + 1 \equiv 0 (\mathrm{mod}\ p).$$

Bizonyítás. Tekintsük a $\mathbb{Z}_p$ testet és ebben az $f = X^{p-1} - \widehat{1}$ polinomot. Tudjuk, hogy $\widehat{a}^{p-1} = \widehat{1}$ minden $1 \leq a \leq p-1$ esetén (kis Fermat tétel), tehát f gyökei $\widehat{1}, \widehat{2}, ..., \widehat{p-1}$. Az utolsó Viéte képletből:

$$\widehat{1}\widehat{2} \cdots \widehat{p-1} = (-1)^{p-1}(-\widehat{1}).$$

Ha $p \geq 3$, akkor p páratlan és $(-1)^{p-1} = 1$, ha pedig $p = 2$, akkor $(-1)^{p-1}(-\widehat{1}) = (-1)(-\widehat{1}) = \widehat{1} = -\widehat{1}$. Tehát $\widehat{(p-1)!} = -\widehat{1}$, $\widehat{(p-1)!} + \widehat{1} = \widehat{0}$, azaz $(p-1)! + \widehat{1} \equiv 0 \pmod{p}$. □

15.C. Polinomok formális deriváltjai

Legyen a továbbiakban K egy kommutatív test és definiáljuk a következő leképezést: $d : K[X] \to K[X]$, $d(a) = 0$ és ha $f = \sum_{i=0}^{n} a_i X^i$, $n \geq 1$, akkor

$$d(f) = \sum_{i=0}^{n} i a_i X^{i-1}.$$

$d(f)$-et az f **(formális) deriváltj**ának nevezzük, jelölés $d(f) = f' = f^{(1)}$. A **többszörös deriváltak**at így értelemezzük: $f^{(n)} = d^n(f) = d(d^{n-1}(f))$, ahol $n \geq 1$ és $f^{(0)} = d^0(f) = f$.

15.C.1. Tétel. Ha $f, g \in K[X]$ és $a \in K$, akkor

1) $d(f+g) = d(f) + d(g)$,

2) $d(af) = ad(f)$,

3) $d(fg) = fd(g) + d(f)g$,

4) $d(f^n) = nf^{n-1}f'$, ahol $n \in \mathbb{N}^*$,

Bizonyítás. 1) és 2) azonnali a definíció alapján: ha $f = a_0 + a_1X + a_2X^2 + ...$, $g = b_0 + b_1X + b_2X^2 + ...$, akkor $d(f+g) =$

$$= d((a_0+b_0)+(a_1+b_1)X+(a_2+b_2)X^2+...) = (a_1+b_1)+2(a_2+b_2)X+3(a_3+b_3)X^2+... =$$

$$= (a_1 + 2a_2X + 3a_3X^2 + ...) + (b_1 + 2b_2X + 3b_3X^2 + ...) = d(f) + d(g),$$

$$d(af) = d(aa_0 + aa_1X + aa_2X^2 + ...) =$$

$$= aa_1 + 2aa_2X + 3aa_3X^2 = a(a_1 + 2a_2X + 3a_3X^2 + ...) = ad(f).$$

3) bizonyításához figyeljük meg, hogy definíció szerint $d(X^i) = iX^{i-1}$, $i \geq 1$ és $d(X^{i+j}) = (i+j)X^{i+j-1} = X^i(jX^{j-1}) + (iX^{i-1})X^j = X^i d(X^j) + d(X^i)X^j$. Ennek alapján

$$d(fg) = d(\sum_i a_i X^i \sum_j b_j X^j) = d(\sum_{i,j} a_i b_j X^{i+j}) =$$

$$= \sum_{i,j} a_i b_j d(X^{i+j}) = \sum_{i,j} a_i b_j (X^i d(X^j) + d(X^i)X^j) =$$

$$= \sum_i a_i X^i \sum_j b_j d(X^j) + \sum_i a_i d(X^i) \sum_j b_j X^j =$$

$$= fd(g) + d(f)g.$$

4) n szerinti indukcióval. □

15.C.2. Tétel. (polinomok Taylor-képlete) Legyen K egy kommutatív test, $f \in K[X]$, $\mathrm{gr}(f) = n$ egy nemnulla polinom és $a \in K$. Akkor f felírható

$$f = \sum_{i=0}^{n} b_i (X-a)^i$$

alakban, ahol $b_i \in K$, $0 \leq i \leq n$.

Ha $\operatorname{char} K = 0$, akkor ez a felírás egyértelmű és

$$b_i = \frac{f^{(i)}(a)}{i!}, \qquad 0 \le i \le n.$$

Bizonyítás. A felírás létezését $n = \operatorname{gr}(f)$ szerinti indukcióval igazoljuk. Ha $n = 1$, legyen $f = a_0 + a_1X$, $a_1 \neq 0$. Akkor $f = (a_0 + a_1a) + a_1(X - a)$, legyen tehát $b_0 = a_0 + a_1a \in K$ és $b_1 = a_1 \in K$.

Tegyük fel, hogy tulajdonság igaz minden $n-1$-edfokú polinomra és igazoljuk az n-edfokú f polinomra. Legyen $f = (X - a)g + f(a)$. Itt $\operatorname{gr}(g) = n - 1$ és az indukciós feltétel szerint

$$g = \sum_{j=0}^{n-1} c_j(X - a)^j,$$

és ezt használva

$$f = (X - a)\sum_{j=0}^{n-1} c_j(X - a)^j + f(a) = f(a) + \sum_{j=0}^{n-1} c_j(X - a)^{j+1}.$$

Legyen $j + 1 = i$, $c_j = b_{i+1}$ és kapjuk, hogy

$$f = b_0 + \sum_{i=1}^{n} b_i(X - a)^i = \sum_{i=0}^{n} b_i(X - a)^i.$$

Az f felírását adó képletet tagonként deriválva: $f^{(i)}(a) = i!b_i$, $\qquad 0 \le i \le n$.

Ha $\operatorname{char} K = 0$, akkor következik, hogy a b_i, $0 \le i \le n$ együtthatók egyértelműen meghatározottak. Ha $\operatorname{char} K \neq 0$, akkor $i!b_i$ lehet 0 és b_i nem egyértelmű (pl. $K = \mathbb{Z}_p$-re, ahol p prím, $\operatorname{char} K = p$ és $i!b_i = 0$ minden $i \ge p$-re). □

A következő eredmény jól használható a kommutatív testek felett értelmezett polinomok többszörös gyökeinek vizsgálatára.

15.C.3. Tétel. Legyen K egy kommutatív test, $\operatorname{char} K = 0$, $f \in K[X]$ egy nemnulla polinom, $k \in \mathbb{N}^*$ és $a \in K$.

1) Ha a az f-nek k-adrendű gyöke, akkor a $(k-1)$-edrendű gyöke az f deriváltjának (f'-nek) és $f(a) = f'(a) = ... = f^{(k-1)}(a) = 0$, továbbá $f^{(k)}(a) \neq 0$.

2) Ha $f(a) = f'(a) = ... = f^{(k-1)}(a) = 0$ és $f^{(k)}(a) \neq 0$, akkor f-nek az a k-adrendű gyöke.

Bizonyítás. 1) Ha a k-szoros gyöke f-nek, akkor definíció szerint $f = (X-a)^k g$, ahol $g(a) \neq 0$. Deriválva: $d(f) = k(X-a)^{k-1}g+(X-a)^k d(f) = (X-a)^{k-1}(kg+(X-a)d(f))$. Tehát $d(f) = (X - a)^{k-1}g_1$, ahol $g_1 = kg + (X - a)d(f)$. Innen $(X - a)^{k-1}|d(f)$ és $g_1(a) = kg(a) \neq 0$ (mert $\operatorname{char} K = 0$), azaz a $(k-1)$-szeres gyöke f'-nek.

Indukcióval igazolható, hogy a $(k-i)$-szeres gyöke $f^{(i)}$-nek, ahol $1 \le i \le k$, tehát a 1-szeres gyöke $f^{(k-1)}$-nek és a 0-szoros gyöke $f^{(k)}$-nak, azaz $f^{(k)}(a) \neq 0$.

2) Ha $\operatorname{gr}(f) = n$, akkor az előző Tétel szerint f felírható a következő alakban

$$(**) \qquad f = \sum_{i=0}^{n} b_i(X - x)^i.$$

Mivel $f^{(i)}(a) = 0$, $0 \le i \le k-1$, ezért következik, hogy $b_i = 0$, $0 \le i \le k-1$. Innen $(X - a)^k|f$ és mivel $f^{(k)}(a) \neq 0$, kapjuk, hogy $(X - x)^{k+1}$ nem osztója f-nek. Tehát a az f-nek k-ad rendű gyöke. □

Példa. • A 2) állítás nem feltétlenül igaz nem nemnulla karakterisztikájú testre. Legyen $K = \mathbb{Z}_p$, $\operatorname{char}\mathbb{Z}_p = p$ és $f = X^p$. Akkor $\widehat{0}$ f-nek p multiplicitású gyöke, de $f^{(n)}(\widehat{0}) = \widehat{0}$ minden $n \geq 0$ esetén.

15.D. Feladatok

▼ 1. Adottak $f, g \in \mathbb{Q}[X]$, $f = 2X^4 - 3X^2 + aX + b$, $g = X^2 - 2X + 3$. Határozzuk meg a-t és b-t úgy, hogy $g|f$.

▼ 2. (Rolle-tétel) Legyen $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}[X]$, $\operatorname{gr}(f) = n \geq 1$. Igazoljuk, hogy ha $x = \frac{k}{\ell} \in \mathbb{Q}$, $(k, \ell) = 1$ gyöke f-nek, akkor $k|a_0$ és $\ell|a_n$.

▼ 3. Határozzuk meg a következő polinomok gyökeit:

i) $f = 4X^3 - 2X^2 + 3X - 5$, ii) $f = 2X^3 - 3X^2 - 3X - 5$, iii) $f = \widehat{3}X^2 + \widehat{3}X \in \mathbb{Z}_6[X]$.

▼ 4. Határozzuk meg a következő gyökök multiplicitását:

i) $x = 1$, $f = x^3 - 3X + 2$, ii) $x = 2$, $f = X^5 - 5X^4 + 7X^3 - 2X^2 + 4X - 8$,

iii) $x = -2$, $f = X^5 + 7X^4 + 16X^3 + 8X^2 - 16X - 16$,

▼ 5. Adott $f = 3X^3 - 4X^2 + 2X + 1 \in \mathbb{Q}[X]$. Írjuk fel f-et $f = \sum_{i=0}^{3} b_i(X-1)^i$ alakban.

▼ 6. Legyen K egy kommutatív test, $f \in K[X]$, $a \in K$. Igazoljuk, hogy az f polinom $(X - a)$-val való osztási maradéka $f(a)$.

▼ 7. Legyen $f = X^3 + \widehat{3}X + \widehat{4} \in \mathbb{Z}_5[X]$. Határozzuk meg f-nek $(X + \widehat{3})$-mal való osztási hányadosát és maradékát.

Eredmény: $q = X^2 + \widehat{2}X + \widehat{2}$, $r = \widehat{3}$.

▼ 8. Adottak $f, g \in \mathbb{Z}_5[X]$, $f = \widehat{3}X^5 + X^3 + \widehat{2}X + \widehat{4}$, $g = \widehat{2}X^3 + \widehat{3}X^2 + \widehat{1}$. Határozzuk meg f-nek g-vel való osztási hányadosát és maradékát.

▼ 9. Legyen K egy kommutatív test, $f \in K[X]$ és $a, b \in K$, $a \neq b$. Igazoljuk, hogy

i) az f polinom $(X - a)(X - b)$-vel való osztási maradéka $\frac{f(a)-f(b)}{a-b}X + \frac{af(b)-bf(a)}{a-b}$.

ii) Ha $X - a|f$, $X - b|f$, akkor $(X - a)(X - b)|f$.

▼ 10. Legyen $f \in \mathbb{Z}[X]$, $f = a_0 + a_1X + a_2X^2 + a_3X^3$. Határozzuk meg az együtthatókat tudva, hogy $f(1) + f(2) + \cdots + f(n) = n^4$ minden $n \geq 1$-re.

▼ 11. Határozzuk meg az elsőfokú $f, g \in \mathbb{Z}[X]$ polinomokat úgy, hogy $(X^2 + 2X + 2)f + (X^2 + 3X + 3)g = 1$ legyen.

16. Irreducibilis polinomok

Ebben a fejezetben az $f \in K[X]$ polinomok további tulajdonságait vizsgáljuk, ahol K egy kommutatív test. Kitérünk a $K = \mathbb{C}$ és $K = \mathbb{R}$ speciális esetek vizsgálatára.

16.A. Irreducibilis polinomok

Ha K kommutatív test és $f \in K[X]$, akkor a $K[X]$ polimomgyűrűben az f által generált (f) ideál mindazokból a g polinomokból áll, amelyek oszthatók f-fel, azaz $(f) = \{g \in K[X] : f|g\}$, lásd 12.B. szakasz.

16.A.1. Tétel. Ha K kommutatív test és I a $K[X]$ polimomgyűrű egy tetszőleges ideálja, akkor létezik $f \in K[X]$ úgy, hogy $I = (f)$, azaz $K[X]$ főideálgyűrű.

Bizonyítás. Ha $I = \{0\}$, akkor vehető $f = 0$. Ha $I \neq \{0\}$, akkor legyen $f \in I, f \neq 0$ egy minimális fokú polinom, azaz olyan, hogy $\forall h \in I, h \neq 0 \Rightarrow \mathrm{gr}(f) \leq \mathrm{gr}(h)$. Megmutatjuk, hogy $I = (f)$. Valóban, $\forall h \in I \Rightarrow \exists\, q, r \in K[X] : h = fq + r,\ \mathrm{gr}(r) < \mathrm{gr}(f)$. Akkor $r = h - fq \in I$, mert I ideál és $\mathrm{gr}(r) < \mathrm{gr}(f)$ miatt $r = 0$ következik, azaz $h = fq$. □

Azt mondjuk, hogy az $f_1, f_2, ..., f_k \in K[X]$ polinomok **relatív prímek**, ha nem létezik olyan legalább elsőfokú polinom, amely $f_1, f_2, ..., f_k$ mindegyikének osztója (másképp: $\forall d \in K[X], d|f_1, d|f_2, ..., d|f_k \Rightarrow d$ konstans polinom).
Jelölés: $(f_1, f_2, ..., f_k) = 1$.

16.A.2. Tétel. Ha K kommutatív test és $f_1, f_2, ..., f_k \in K[X]$ relatív prímek $(k \geq 2)$, akkor léteznek olyan $u_1, u_2, ..., u_k \in K[X]$ polinomok, amelyekre

$$f_1u_1 + f_2u_2 + \cdots + f_ku_k = 1.$$

Bizonyítás. Legyen $X = \{f_1, f_2, ..., f_k\}$ és tekintsük az X által generált (X) ideált. Az előző Tétel szerint ez főideál, azaz létezik olyan $d \in K[X]$, amelyre $(X) = (d) = \{h \in K[X] : d|h\}$. De $f_1 \in (X)$, ezért $d|f_1$ és hasonlóan $d|f_2$,..., $d|f_k$. Mivel $f_1, f_2, ..., f_k$ relatív prímek, következik, hogy d konstans, ahonnan $(X) = K[X]$. Így a 12.B.1. Tétel szerint minden $f \in K[X]$ polinom felírható $f = f_1u_1 + f_2u_2 + \cdots + f_ku_k$ alakban, ahol $u_1, u_2, ...u_k \in K[X]$ alkalmas polinomok. Speciálisan, ez $f = 1$-re is igaz. □

Azt mondjuk, hogy az $f \in K[X], \mathrm{gr}(f) \geq 1$ polinom **irreducibilis** K felett, ha nem létezik olyan legalább elsőfokú $g \in K[X]$ polinom, amelyre $\mathrm{gr}(g) < \mathrm{gr}(f)$ és amely osztója f-nek (másképp: $\forall g \in K[X], \mathrm{gr}(g) < \mathrm{gr}(f), g|f \Rightarrow g$ konstans polinom). Ellenkező esetben f **reducibilis** polinom, ekkor létezik olyan $g = b_0 + b_1X + \cdots + X^n$, $1 \leq n = \mathrm{gr}(g) < \mathrm{gr}(f)$ **normált polinom** (normált = főegyütthatója 1), amely osztója f-nek.

Példák. • Minden $f \in K[X]$ elsőfokú polinom irreducibilis K felett.

• Az $f = X^2 - 2 \in \mathbb{Q}[X]$ polinom irreducibilis $\mathbb{Q}$ felett. Valóban, ellenkező esetben létezne olyan $g = X - b \in \mathbb{Q}[X]$ elsőfokú polinom, amely osztója f-nek. De akkor a Bézout tétel szerint $b \in \mathbb{Q}$ gyöke f-nek: $b^2 - 2 = 0$. Innen $b = \pm\sqrt{2}$, ami irracionális szám, ellentmondás.

• Az $f = X^2 - 2$ polinom reducibilis $\mathbb{R}$ felett, hiszen $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ és következik, hogy $X - \sqrt{2} \in \mathbb{R}[X]$ osztója f-nek.

16.A.3. Tétel. Ha K kommutatív test, $f, g, h \in K[X]$, f irreducibilis és $f|gh$, akkor $f|g$ vagy $f|h$.

Bizonyítás. Tegyük fel, hogy $f|gh$. Ha $f|g$, akkor készen vagyunk. Ellenkező esetben, azaz ha $f \not| g$, akkor igazoljuk, hogy $f|h$. Valóban, ha $f \not| g$, akkor $(f, g) = 1$, hiszen f irreducibilis volta miatt közös nem konstans osztó csak f lehetne, de ez is kizárt. Az előző Tétel szerint léteznek olyan $u, v \in K[X]$ polinomok, amelyekre $fu + gv = 1$, innen $fhu + ghv = h$ és $f|gh$ miatt következik, hogy $f|h$. □

★ **16.A.4. Tétel.** Ha K egy kommutatív test és $f \in K[X]$ egy irreducibilis polinom K felett, akkor a $K[X]/(f)$ faktorgyűrű test.

Bizonyítás. Itt $(f) = I = \{fh : h \in K[X]\}$ az f által generált ideál és $K[X]/(f) = K[X]/I$ a megfelelő faktorgyűrű, amelynek elemei $\widehat{g} = g + I = \{g + fh : h \in K[X]\}$ alakúak, ahol $g \in K[X]$, és zéruseleme $\widehat{0} = I = \{fh : h \in K[X]\}$. $K[X]$ egységelemes és kommutatív, ezért $K[X]/I$ is egységelemes, az egységelem $\widehat{1} = 1 + I$, és kommutatív.

Megmutatjuk, hogy minden $\widehat{g} \in K[X], \widehat{g} \neq \widehat{0}$ esetén létezik $\widehat{h} \in K[X]$ úgy, hogy $\widehat{g}\widehat{h} = \widehat{1}$. Valóban, f irreducibilis, ezért $(f, g) = 1$ és létezik $u, v \in K[X]$ úgy, hogy $fu + gv = 1$. Innen $\widehat{fu} + \widehat{gv} = \widehat{1}$, $\widehat{gv} = \widehat{0}$, azaz választható $h = v$ és $\widehat{v}$ a $\widehat{g}$ inverze. □★

A következőkben az irreducibilis polinomok tulajdonságait vizsgáljuk és válaszolunk arra a kérdésre, hogy melyek a $\mathbb{C}$ és $\mathbb{R}$ feletti irreducibilis polinomok.

16.A.5. Tétel. Ha K egy kommutatív test, akkor minden $f \in K[X]$ legalább elsőfokú polinomnak létezik irreducibilis (normált) osztója.

Bizonyítás. Tekintsük f legalább elsőfokú osztóit, ilyen például az f. Legyen $g = b_0 + b_1X + \cdots + b_mX^m$ ezek közül egy minimális fokú, $\mathrm{gr}(g) = m$. A g irreducibilis, hiszen ellenkező esetben g-nek létezne $h \in K[X]$, $1 \leq \mathrm{gr}(h) < m$ osztója, amely f-nek is osztója, ellentmondás. Helyettesítve g-t a $g^* = b_m^{-1}g$ polinommal, következik, hogy g^* irreducibilis normált polinom. □

16.A.6. Tétel. Egy K kommutatív test esetén a következő állítások egyenértékűek:

1) Minden olyan $f \in K[X]$ polinom, amely irreducibilis K felett, elsőfokú.

2) Minden $g \in K[X]$ legalább elsőfokú polinomnak van gyöke K-ban.

Bizonyítás. "1) ⇒ 2)" Legyen $g \in K[X], \mathrm{gr}(g) \geq 1$. Akkor az előző Tétel szerint létezik h irreducibilis normált polinom úgy, hogy $h|g$. De 1) miatt $\mathrm{gr}(h) = 1$, azaz $h = X - a|g$, ahol $a \in F$ és Bézout tétele szerint $g(a) = 0$.

"2) ⇒ 1)" Legyen $f \in K[X], \mathrm{gr}(f) \geq 1$ egy irreducibilis polinom. 2) alapján létezik $a \in F$ úgy, hogy $f(a) = 0$. Innen Bézout tétele alapján $X - a|f$. De f irreducibilis és így következik, hogy $\mathrm{gr}(f) = 1$. □

Azt mondjuk, hogy a K test **algebrailag zárt**, ha minden $f \in K[X]$, $\mathrm{gr}(f) \geq 1$ polinomnak van legalább egy gyöke K-ban.

• $\mathbb{Q}$ algebrailag nem zárt, mert láttuk, hogy $X^2 - 2$ irreducibilis $\mathbb{Q}$ felett és másodfokú.

• $\mathbb{R}$ sem zárt algebrailag, mert például az $X^2 + 1 \in \mathbb{R}[X]$ polinomnak nincs gyöke R-ben.

• A $\mathbb{C}$ komplex számtest algebrailag zárt és ez az állítás az **algebra alaptétele**ként ismert (bizonyítás nélkül közöljük):

16.A.7. Tétel. (D'Alembert - Gauss) Minden $f \in \mathbb{C}[X]$, $\mathrm{gr}(f) \geq 1$ polinomnak van legalább egy komplex gyöke.

16.B. Komplex együtthatós és valós együtthatós polinomok

Az algebra alaptételéből azonnali, hogy:

Következmény. Minden $f \in \mathbb{C}[X]$, $\mathbb{C}$ felett irreducibilis polinom elsőfokú.

16.B.1. Tétel. Ha $z \in \mathbb{C}$ gyöke az $f \in \mathbb{R}[X]$ polinomnak, akkor $\overline{z}$ is gyöke f-nek, ahol $\overline{z}$ a z konjugáltja.

Bizonyítás. Legyen $f = a_0 + a_1X + \cdots + a_nX^n$, ahol $a_0, a_1, ..., a_n \in \mathbb{R}$. A feltétel szerint $f(z) = a_0 + a_1z + \cdots + a_nz^n = 0$, ahonnan

$$0 = \overline{0} = \overline{a_0 + a_1z + \cdots + a_nz^n} = \overline{a_0} + \overline{a_1}\,\overline{z} + \cdots + \overline{a_n}\,\overline{z}^n =$$

$$= a_0 + a_1\overline{z} + \cdots + a_n\overline{z}^n = f(\overline{z}),$$

tehát $f(\overline{z}) = 0$. □

Következmény. Minden $f \in \mathbb{R}[X]$, $\mathbb{R}$ felett irreducibilis polinom $f = aX + b$ vagy $f = aX^2 + bX + c$, $b^2 - 4ac < 0$ alakú.

Bizonyítás. Az $f = aX + b \in \mathbb{R}[X]$ elsőfokú polinomok irreducibilisek $\mathbb{R}$ felett.

Legyen most $f \in \mathbb{R}[X]$, $\mathrm{gr}(f) \geq 2$ egy tetszőleges irreducibilis polinom. f-nek nincsenek valós gyökei, mert ha létezne $a \in \mathbb{R}$ úgy, hogy $f(a) = 0$, akkor $X - a | f$ és ez ellentmond annak, hogy f irreducibilis. $f \in \mathbb{R}[X] \Rightarrow f \in \mathbb{C}[X]$ és az algebra alaptétele alapján létezik $z = u + iv \in \mathbb{C}, v \neq 0$ úgy, hogy $f(z) = 0$. Az előző Tétel szerint $f(\overline{z}) = 0$. Továbbá, $X - z | f$, ahonnan $f = (X - z)g$, $g \in \mathbb{C}[X]$ és $f(\overline{z}) = (\overline{z} - z)g(\overline{z}) = 0$. Itt $z \neq \overline{z}$, mert z nem valós és így $g(\overline{z}) = 0$. Így $X - \overline{z} | g$, azaz $g = (X - \overline{z})h$, $h \in \mathbb{C}[X]$ és következik, hogy

$$f = (X - z)(X - \overline{z})h = (X^2 - 2uX + u^2 + v^2)h.$$

Itt $X^2 - 2uX + u^2 + v^2 \in \mathbb{R}[X]$ és ez osztója f-nek, ezért $h \in \mathbb{R}[X]$. Az f irreducibilis voltából következik, hogy $gr(f) = 2$, innen $h = a \in \mathbb{R}, a \neq 0$, $f = aX^2 - 2auX + a(u^2 + v^2)$. Legyen $-2au = b$, $a(u^2 + v^2) = c$, akkor $f = aX^2 + bX + c$ alakú, ahol $b^2 - 4ac = 4a^2u^2 - 4a^2(u^2 + v^2) = -4a^2v^2 < 0$. $\square$

A következő eredmény azt mutatja, hogy $K[X]$-ben érvényes az aritmetika alaptétele.

16.B.2. Tétel. Legyen K egy kommutatív test és $f = a_0 + a_1X + \cdots + a_nX^n$, $gr(f) = n \geq 1$. Akkor léteznek az $f_1, f_2, ..., f_k \in K[X]$ irreducibilis normált polinomok úgy, hogy

$$f = a_n f_1 f_2 \cdots f_k,$$

és ez a felírás a tényezők sorrendjétől eltekintve egyértelmű.

Bizonyítás. Mivel $f = a_n f^*$, ahol f^* normált polinom, feltételezhetjük, hogy f normált.

I. Létezés. $\mathrm{gr}(f) = n$-szerinti indukcióval. Ha $n = 1$, akkor f irreducibilis K felett és $f = f$ egytényezős szorzat. Legyen $n > 1$ és tegyük fel, hogy minden n-nél alacsonyabbfokú polinom felírható véges sok irreducibilis normált polinom szorzataként. Ha f irreducibilis, akkor $f = f$ egytényezős szorzat. Ha f reducibilis, akkor $f = gh$ alakba írható, ahol $1 \leq \mathrm{gr}(g), \mathrm{gr}(h) < n$. Az indukciós feltétel szerint g és h véges sok irreducibilis normált polinom szorzata, tehát $f = gh$ is rendelkezik ezzel a tulajdonsággal.

II. Egyértelműség. Igazoljuk, hogy ha

$$f = f_1 f_2 \cdots f_k = f'_1 f'_2 \cdots f'_{k'} \tag{2}$$

irreducibilis polinomok szorzata, akkor $k = k'$ és a sorrend esetleges megváltoztatásával $f_i = f'_i$, $1 \leq i \leq k$.

Ha $k = 1$, akkor $k' = 1$, mert másképp f_1 reducibilis lenne. Tegyük fel, hogy $k > 1$ és hogy az állítás igaz minden olyan polinomra, amelynek van egy $k - 1$ irreducibilis tényezőkre bontott alakja. (2) alapján $f_1 | f'_1 f'_2 \cdots f'_{k'}$, ahonnan következik, hogy $f_1 | f'_1$ vagy $f_1 | f'_2$ vagy ... vagy $f_1 | f'_{k'}$, lásd korábbi Tétel. Feltételezhetjük, hogy $f_1 | f'_1$ és innen $f_1 = f'_1$, mert mindkettő irreducibilis nomált polinom. (2) alapján

$$f_2 \cdots f_k = f'_2 \cdots f'_{k'},$$

és az indukciós feltétel szerint $k - 1 = k' - 1$, azaz $k = k'$ és eltekintve a tényezők sorrendjétől $f_i = f'_i$, $2 \leq i \leq k$. $\square$

Következmény. Ha $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$, $a_n \neq 0$ egy tetszőleges legalább elsőfokú komplex együtthatós polinom, akkor léteznek az egyértelműen meghatározott $z_1, z_2, ..., z_n \in \mathbb{C}$ számok úgy, hogy

$$f = a_n(X - z_1)(X - z_2)\cdots(X - z_n)$$

(itt $z_1, z_2, ..., z_n \in \mathbb{C}$ az f gyökei).

Következmény. Ha $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{R}[X]$, $a_n \neq 0$ egy tetszőleges legalább elsőfokú valós együtthatós polinom, akkor f a következő alakra hozható:

$$f = a_n(X - \alpha_1)\cdots(X - \alpha_k)(X^2 + \beta_1X + \gamma_1)\cdots(X^2 + \beta_\ell X + \gamma_\ell),$$

ahol $\alpha_i, \beta_j, \gamma_j \in \mathbb{R}, \beta_j^2 - 4\gamma_j < 0$, $1 \leq i \leq k, 1 \leq j \leq \ell, k + 2\ell = n$, és ez a felírás egyértelmű.

16.C. Feladatok

▼ 1. Bontsuk fel az $x^4 + 4$ és $x^6 + 27$ polinomokat irreducibilis tényezők szorzatára $\mathbb{R}$, illetve $\mathbb{C}$ felett.

▼ 2. Bontsuk fel az $f = X^4 + X^3 + \widehat{2}X^2 + X + \widehat{1} \in \mathbb{Z}_5[X]$ polinomot irreducibilis tényezők szorzatára $\mathbb{Z}_5$ felett.

▼ 3. Hány legfeljebb negyedfokú $f \in \mathbb{Z}_2[X]$ polinom van ? Határozzuk meg ezek közül az irreducibilis polinomokat.

▼ 4. Ha K egy kommutatív test és $f \in K[X]$, amelyre $\mathrm{gr}(f) = 2$ vagy $\mathrm{gr}(f) = 3$ és f-nek nincs gyöke K-ben, akkor igazoljuk, hogy f irreducibilis K felett. Ez nem igaz $\mathrm{gr}(f) = 4$ esetén. Adjunk ellenpéldákat.

★ ▼ 5. Alkalmazva a homomorfizmustételt igazoljuk, hogy

i) $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$, ii) $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d)$, iii) $\mathbb{Q}(\sqrt[3]{p}) \simeq \mathbb{Q}[X]/(X^3 - p)$.

Útmutatás. i) Legyen $\phi : \mathbb{R}[X] \to \mathbb{C}$, $\phi(f) = f(i)$. Akkor ϕ szürjektív homomorfizmus és $f = (X^2 + 1)q + aX + b \in \mathrm{Ker}(\phi) \Leftrightarrow a = b = 0 \Leftrightarrow f \in (X^2 + 1)$.

ii) $\phi : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{d}]$, $\phi(f) = f(\sqrt{d})$ és $f \in \mathrm{Ker}(\phi) \Leftrightarrow (x^2 - d)|f$.

iii) $\phi : \mathbb{Q}[X] \to \mathbb{Q}(\sqrt[3]{p})$, $\phi(f) = f(\sqrt[3]{p})$. ★

17. Testbővítések

Legyenek K és L kommutatív testek. Azt mondjuk, hogy L a K **test bővítése**, ha K részteste az L-nek: $K \leq L$.

Példák. • $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

• $\mathbb{Q}(\sqrt{d}) \leq \mathbb{C}$.

Ha $K \leq L$ egy testbővítés és $a \in L$, akkor a következő két logikai eset lehetséges:

1. Létezik olyan $f \in K[X]$ nemnulla polinom, amelynek a gyöke, azaz $f(a) = 0$. Ekkor azt mondjuk, hogy a a K **test feletti algebrai elem**.

2. Nem létezik olyan $f \in K[X]$ nemnulla polinom, amelynek a gyöke. Ekkor a-t a K **test feletti transzcendens elem**nek nevezzük.

Speciálisan, ha $K = \mathbb{Q}$ és $L = \mathbb{C}$, akkor azt mondjuk, hogy $z \in \mathbb{C}$ **algebrai szám**, ha van olyan $f \in \mathbb{Q}[X]$ nemnulla polinom, amelynek z gyöke: $f(z) = 0$. Ellenkező esetben z **transzcendens szám**.

Példák. • $\frac{3}{4}, \sqrt{5}, 1-3i$ algebrai számok, mert ezek gyökei az $f = X - \frac{3}{4}$, $f = X^2 - 5$ illetve $f = X^2 - 2X + 10$ racionális együtthatós polinomoknak. Az $f = X - \frac{3}{4}$ helyett vehető $f = 4X - 3$ is. Minden a algebrai szám esetén van olyan egész együtthatós polinom, amelynek a gyöke (miért ?).

• Minden racionális szám algebrai. Minden $\sqrt{a}$, $a \in \mathbb{Q}, a > 0$ szám algebrai. Minden $a + bi$, $a, b \in Q$ komplex szám algebrai.

• e, π transzcendens számok.

Ha $a_1, a_2, ..., a_n \in L$, akkor L-nek azt a legszűkebb résztestét, amely tartalmazza K-t és az $a_1, a_2, ..., a_n$ elemeket, a K **testnek az adott elemekkel való bővítésé**nek nevezzük, jelölés: $K(a_1, a_2, ..., a_n)$. Azt is mondjuk, hogy $K(a_1, a_2, ..., a_n)$ a K testből az adott elemek **adjunkciójá**val jött létre. Ha $n = 1$, $a_1 = a$, akkor az egy elem adjunkciójával létrejövő $K(a)$ testbővítést **egyszerű testbővítés**nek nevezzük.

Ha a algebrai elem a K felett, akkor a $K \leq K(a)$ testbővítést **egyszerű algebrai testbővítés**nek nevezzük. Legyen $f \in K[X]$ az a minimális fokszámú normált polinom, amelyre $f(a) = 0$. Ez az f polinom, neve az a elem **definiáló polinom**ja, egyértelműen meghatározott (lásd az alábbi Tétel bizonyítását) és irreducibilis (ha f reducibilis lenne, akkor $f = f_1 f_2$ alakú lenne, ahol $\mathrm{gr}(f_1), \mathrm{gr}(f_2) < \mathrm{gr}(f)$ és $f_1(a) = 0$ vagy $f_2(a) = 0$, ami ellentmondás).

17.1. Tétel. Legyen $K \leq L$ egy testbővítés és legyen $a \in L$ algebrai elem K felett. Akkor a $K(a)$ egyszerű algebrai testbővítés izomorf a $K[X]/(f)$ testtel, ahol f az a elem definiáló polinomja.

★ **Bizonyítás.** Legyen $g \in K[X]$ egy tetszőleges olyan polinom, amelynek a gyöke. Akkor $f|g$. Valóban, a maradékos osztás tétele szerint: $g = fq + r$, ahol $\mathrm{gr}(r) < \mathrm{gr}(f)$. Ha $r \neq 0$, akkor $0 = g(a) = f(a)q(a) + r(a) = r(a)$ miatt r-nek a gyöke, ami ellentmond annak, hogy f foka minimális. Ezért $r = 0$ és kapjuk, hogy $f|g$.

Innen következik, hogy f egyértelműen meghatározott, mert ha f_1 egy másik ugyanilyen tulajdonságú polinom (minimális fokszámú, normált, amelynek a gyöke), akkor egyrészt $f|f_1$, ugyanakkor $f_1|f$, ahonnan $f = cf_1$. De minkettő normált, ezért $c = 1$ és $f = f_1$.

Tekintsük a $\phi : K[X] \to L$, $\phi(f) = f(a)$ függvényt. Ez homomorfizmus (művelettartó) a $K[X]$ és az L gyűrűkre nézve. Továbbá $\mathrm{Ker}(\phi) = \{g \in K[X] : g(a) = 0\} = \{g \in K[X] : f|g\} = (f)$ és $\mathrm{Im}(\phi) = \{g(a) : g \in K[X]\}$. A gyűrűhomomorfizmustétel alapján következik, hogy $K[X]/(f) \simeq \{g(a) : g \in K[X]\}$.

Igazolnunk kell még, hogy $\{g(a) : g \in K[X]\} = K(a)$. Valóban, f irreducibilis, ezért a $K[X]/(f)$ faktorgyűrű test, lásd 16. fejezet, és izomorf $\{g(a) : g \in K[X]\}$-val,

tehát ez utóbbi is test. Továbbá, a $K(a)$ test tartalmazza a K elemeit és a-t, ezért tartalmaz minden $a_0 + a_1a + a_2a^2 + ... + a_na^n$ elemet is, ahol $a_0, a_1, a_2, ..., a_n \in K$, azaz $K(a) \subseteq \{g(a) : g \in K[X]\}$. De ez már test, ezért $K(a)$, mint a legszűkebb olyan test, amely tartalmazza K-t és a-t, éppen $\{g(a) : g \in K[X]\}$. $\square\bigstar$

Következmény. Ha $K \leq L$ egy testbővítés és $a \in L$ algebrai elem K felett, akkor a $K(a)$ egyszerű algebrai testbővítés minden eleme

$$a_0 + a_1a + a_2a^2 + ... + a_na^n$$

alakban írható, ahol $n \in \mathbb{N}$ és $a_0, a_1, a_2, ..., a_n \in K$.

Példa. $K = \mathbb{R}$, $L = \mathbb{C}$, $a = i$, akkor $\mathbb{R}(i)$ elemei $a_0 + a_1i + a_2i^2 + ... + a_ni^n$ alakúak, ahol $n \in \mathbb{N}$ és $a_0, a_1, a_2, ..., a_n \in \mathbb{R}$. De $i^2 = -1, i^3 = -i, i^4 = 1, ...$, ezért minden elem $a_0 + a_1i$ alakú, tehát $\mathbb{R}(i) = \mathbb{C}$ és $R(i) \simeq \mathbb{R}[X]/(X^2 + 1)$, lásd 16.C.5. Feladat, ahol $f = X^2 + 1$ az i definiáló polinomja.

Ha a transzcendens elem a K felett, akkor igazolható, hogy

17.2. Tétel. Ha $K \leq L$ egy testbővítés és $a \in L$ transzcendens elem K felett, akkor a $K(a)$ egyszerű testbővítés izomorf a $\{\frac{f(a)}{g(a)} : f, g \in K[X]\}$ testtel és $K(a)$ minden eleme felírható

$$\frac{a_0 + a_1a + a_2a^2 + ... + a_na^n}{b_0 + b_1a + b_2a^2 + ... + b_ma^m}$$

alakban, ahol $n, m \in \mathbb{N}$ és $a_0, a_1, a_2, ..., a_n, b_0, b_1, b_2, ..., b_m \in K$.

18. Többhatározatlanú polinomok

18.A. Többhatározatlanú polinomok gyűrűje

A 15. fejezetben definiáltuk az R kommutatív egységelemes gyűrű feletti egyhatározatlanú polinomok $R[X]$ gyűrűjét. Ha R egy ilyen gyűrű, akkor az $X_1, X_2, ..., X_n$ határozatlanú polinomok $R[X_1, X_2, ..., X_n]$ gyűrűjét induktíve értelmezzük: $R[X_1]$ az R feletti X_1 határozatlanú polinomok gyűrűje, $R[X_1, X_2]$ legyen az $R[X_1]$ feletti X_2 határozatlanú polinomok gyűrűje, azaz $R[X_1, X_2] = R[X_1][X_2]$, ..., $R[X_1, X_2, ..., X_n]$ legyen az $R[X_1, X_2, ..., X_{n-1}]$ feletti X_n határozatlanú polinomok gyűrűje, azaz $R[X_1, X_2, ..., X_n] = R[X_1, X_2, ..., X_{n-1}][X_n]$.

Ha $f \in R[X_1, X_2, ..., X_n]$, akkor f egy X_n határozatlanú polinom, amelynek együtthatói $R[X_1, X_2, ..., X_{n-1}]$-ből vannak, azaz

$$f = f_0 + f_1 X_n + ... + f_{k_n} X_n^{k_n},$$

ahol $f_i \in R[X_1, X_2, ..., X_{n-1}], 0 \leq i \leq k_n$. Az f_i-ket beírva és lépésről lépésre haladva f felírható úgy, mint véges sok $\sum a_{i_1 i_2 ... i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ alakú kifejezés összege, ahol $a_{i_1 i_2 ... i_n}$ az f **együtthatói**. Kapjuk, hogy

18.A.1. Tétel. Ha $f \in R[X_1, X_2, ..., X_n]$, akkor f egyértelműen felírható

$$f = \sum_{i_1, i_2, ..., i_n = 0}^{k_1, k_2, ..., k_n} a_{i_1 i_2 ... i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$$

alakban.

Példa. • $f = X_1^2 X_2^3 + 5X_1^3 X_2^2 - 3X_1^7 X_2^2 X_3^2$ egy X_1, X_2, X_3 határozatlanú polinom $\mathbb{Z}$ felett.

Az $aX_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ alakú polinomokat, ahol $a \neq 0$, **monom**oknak nevezzük. A fentiek szerint minden polinom felírható monomok (ezeket a polinom tagjainak nevezzük) összegeként.

Két $X_1, X_2, ..., X_n$ határozatlanú polinomot, f-et és g-t, úgy adunk össze, hogy összeadjuk (öszevonjuk) f és g tagjait és úgy szorozzuk össze, hogy f minden tagját szorozzuk g minden tagjával.

Példa. • Ha $f = 2X_1^2 X_2 + X_1 X_2^3, g = X_1^2 X_2 - X_1^2 X_2^3 \in \mathbb{Z}[X_1, X_2]$, akkor $f + g = 3X_1^2 X_2 + X_1 X_2^3 - X_1^2 X_2^3$, $fg = (2X_1^2 X_2 + X_1 X_2^3)(X_1^2 X_2 - X_1^2 X_2^3) = 2X_1^4 X_2^2 + X_1^3 X_2^4 - 2X_1^4 X_2^4 - X_1^3 X_2^6$.

Ha $f \in R[X_1, X_2, ..., X_n]$, akkor f-nek az X_i **határozatlanra vonatkozó foka** a legnagyobb kitevő, amelyen X_i szerepel f-ben, $1 \leq i \leq n$. Ha X_i nem szerepel f-ben, akkor ez 0. Egy $aX_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ **monomnak a foka** $\mathrm{gr}(aX_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}) = i_1 + i_2 + ... + i_n$.

Ha $f \in R[X_1, X_2, ..., X_n]$, akkor f-nek a **fok**a, jelölés $\mathrm{gr}(f)$, az f tagjai fokainak a maximuma, ha $f \neq 0$. Ha $f = 0$, akkor $\mathrm{gr}(0) = -\infty$.

Ha $f \in R[X_1, X_2, ..., X_n]$ minden tagja egyenlő fokú, akkor f-et **homogén polinom**nak nevezzük.

Példák. • Az $f = 3X_1^2 X_2^4 + 2X_1^3 X_2^2 - X_1 X_2^4 X_3^2$ polinom X_1-re vonatkozó foka 3, X_2-re vonatkozó foka 4, X_3-ra vonatkozó foka pedig 2. A benne szereplő monomok fokai rendre $6, 5, 7$ és f foka $\mathrm{gr}(f) = 7$. Ez nem homogén polinom.

• $f = 2X_1^2 X_2 - X_1 X_2 X_3 + 4X_1 X_3^2$ egy X_1, X_2, X_3 határozatlanú homogén polinom $\mathbb{Z}$ felett, $\mathrm{gr}(f) = 3$.

A többhatározatlanú polinomok tagjait az ún. **lexikografikus rendezés** szerint szokás felírni. Ennek megfelelően az az első tag, amelyben X_1 a legmagasabb hatványon van. Ha több olyan tag is van, amelyekben X_1 azonos hatványon szerepel, akkor az X_2 csökkenő hatványai szerint rendezünk, majd X_3 csökkenő hatványai szerint, stb.

Példa. • $f = X_1^3X_2^2X_3^5 + 2X_1^3X_2^2X_3^2 - 3X_1^3X_2X_3^3 + X_1^2X_2^7X_3^4 + 2X_1^2X_2^2X_3^2 + X_1X_2X_3$.

Ha f és g két homogén polinom, akkor fg egy nemnulla homogén polinom, amelynek foka $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$ vagy $fg = 0$.

Az $f \neq 0$ n-edfokú polinom felírható egyértelműen $f = f_0 + f_1 + ... + f_n$ alakban, ahol f_i egy i-edfokú homogén polinom vagy $f_i = 0$ minden $1 \leq i \leq n$-re.

18.A.2. Tétel. Legyen $(R, +, \cdot)$ egy gyűrű és $f, g \in R[X_1, X_2, ..., X_n]$. Akkor

1) $\mathrm{gr}(f + g) \leq \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$,

2) $\mathrm{gr}(fg) \leq \mathrm{gr}(f) + \mathrm{gr}(g)$.

3) Ha R integritástartomány, akkor $R[X_1, X_2, ..., X_n]$ is integritástartomány és 2)-ben egyenlőség van.

Bizonyítás. 1) és 2) azonnali felhasználva a polinomoknak homogén polinomok összegeként való felírását.

3) n-szerinti indukcióval. Ha $n = 1$, akkor a tulajdonság igaz, lásd korábbi Tétel. Ezt alkalmazva, ha feltételezzük, hogy $R[X_1, X_2, ..., X_{n-1}]$ integritástartomány, akkor következik, hogy $R[X_1, X_2, ..., X_{n-1}][X_n] = R[X_1, X_2, ..., X_n]$ is integritástartomány.

Legyen $f, g \neq 0$, $\mathrm{gr}(f) = p, \mathrm{gr}(g) = q$ és $f = f_0 + f_1 + ... + f_p$, $g = g_0 + g_1 + ... + g_q$, ahol $f_p, g_q \neq 0$ valamint f_i és f_j i-edfokú illetve j-edfokú polinom vagy a nulla polinom. Ekkor $fg = \sum_{k=0}^{p+q} h_k$, ahol $h_k = \sum_{i+j=k} f_i g_j$. $R[X_1, X_2, ..., X_n]$ integritástartomány, ezért $h_{p+q} = f_p g_q \neq 0$, innen $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$. □

Az $R[X_1, X_2, ..., X_n]$ integritástartomány hányadostestét $R(X_1, X_2, ..., X_n)$-nel jelöljük, ennek neve az R feletti $X_1, X_2, ..., X_n$ határozatlanú **racionális törtek teste**.

Ha $f \in R[X_1, X_2, ..., X_n]$,

$$f = \sum_{i_1, i_2, ..., i_n = 0}^{k_1, k_2, ..., k_n} a_{i_1 i_2 ... i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n},$$

és $x_1, x_2, ..., x_n \in R$, akkor az

$$f = \sum_{i_1, i_2, ..., i_n = 0}^{k_1, k_2, ..., k_n} a_{i_1 i_2 ... i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

R-beli elemet az f helyettesítési értékének nevezzük, jelölés $f(x_1, x_2, ..., x_n)$.

18.B. Szimmetrikus polinomok

Legyen R egy kommutatív egységelemes gyűrű és $R[X_1, X_2, ..., X_n]$ az $X_1, X_2, ..., X_n$ határozatlanú polinomok gyűrűje.

Ha $\sigma \in S_n$ egy n-edfokú permutáció, értelmezzük a következő leképezést:
$\sigma^* : R[X_1, X_2, ..., X_n] \to R[X_1, X_2, ..., X_n]$, ahol
$\sigma^*(f(X_1, X_2, ..., X_n)) = f(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma_(n)})$. Tehát, ha

$$f = \sum_{i_1, i_2, ..., i_n = 0}^{k_1, k_2, ..., k_n} a_{i_1 i_2 ... i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n},$$

akkor

$$\sigma^*(f) = \sum_{i_1,i_2,...,i_n=0}^{k_1,k_2,...,k_n} a_{i_1 i_2 ... i_n} X_{\sigma(1)}^{i_1} X_{\sigma(2)}^{i_2} \cdots X_{\sigma(n)}^{i_n}.$$

Példa. • $n = 3$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $f = 2X_1^2X_2X_3^3 + 3X_1^2X_2^3X_3$ esetén $\sigma^*(f) = 2X_3^2X_1X_2^3 + 3X_3^2X_1^3X_2 = 2X_1X_2^3X_3^2 + 3X_1^3X_2X_3^2$.

18.B.1. Tétel. 1) Ha $\sigma, \tau \in S_n$, akkor $(\sigma\tau)^*(f) = \sigma^*(\tau^*(f))$.

2) Ha $e \in S_n$ az identikus permutáció, akkor $e^*(f) = f$.

3) Ha $\sigma \in S_n$, akkor σ^* egy automorfizmusa az $R[X_1, X_2, ..., X_n]$ gyűrűnek, ahol σ^* inverze $(\sigma^{-1})^*$.

Bizonyítás. Következik a permutációk tulajdonságai alapján. 3) azt jelenti, hogy $\sigma^*(f+g) = \sigma^*(f) + \sigma^*(g)$ és $\sigma^*(fg) = \sigma^*(f)\sigma^*(g)$, $\forall\, f, g \in R[X_1, X_2, ..., X_n]$. □

Azt mondjuk, hogy $f \in R[X_1, X_2, ..., X_n]$ **szimmetrikus polinom**, ha minden $\sigma \in S_n$-re $\sigma^*(f) = f$, azaz ha f invariáns a határozatlanok összes permutációjára nézve.

Példák. • $n = 3$ esetén az előbbi $f = 2X_1^2X_2X_3^3 + 3X_1^2X_2^3X_3$ polinom nem szimmetrikus, $g = X_1^2 + X_2^2 + X_3^2 - X_1X_2X_3$ szimmetrikus polinom.

• Az **elemi szimmetrikus polinomok** a következők:

$$\begin{aligned}
&s_1 = X_1 + X_2 + ... + X_n,\\
&s_2 = X_1X_2 + X_1X_3 + ... + X_1X_n + ... + X_{n-1}X_n,\\
&.....\\
&s_k = X_1X_2\cdots X_k + X_1X_2\cdots X_{k-1}X_{k+1} + ... + X_{n-k+1}X_{n-k+2}\cdots X_n,\\
&.....\\
&s_n = X_1X_2\cdots X_n.
\end{aligned}$$

Mivel minden permutáció transzpozíciók szorzata, f szimmetrikus, ha invariáns minden transzpozícióra nézve.

Jelölje $T[X_1, X_2, ..., X_n]$ az $R[X_1, X_2, ..., X_n]$ gyűrű szimmetrikus polinomjainak halmazát.

18.B.2. Tétel. $T[X_1, X_2, ..., X_n]$ gyűrű a polinomok összeadására és szorzására nézve.

Bizonyítás. Megmutatjuk, hogy $T[X_1, X_2, ..., X_n]$ részgyűrűje $R[X_1, X_2, ..., X_n]$-nek. Valóban, minden $f, g \in T[X_1, X_2, ..., X_n]$ és $\sigma \in S_n$ esetén:

$$\sigma^*(f-g) = \sigma^*(f) - \sigma^*(g) = f - g,$$

$$\sigma^*(fg) = \sigma^*(f)\sigma^*(g) = fg,$$

tehát $f - g, fg \in T[X_1, X_2, ..., X_n]$. □

Bizonyítás nélkül adjuk meg a szimmetrikus polinomok alaptételét:

18.B.3. Tétel. Minden szimmetrikus polinom felírható az elemi szimmetrikus polinomok egy polinomjaként, azaz ha $f \in T[X_1, X_2, ..., X_n]$ egy szimmetrikus polinom, akkor létezik (és egyértelműen meghatározott) egy olyan $g \in R[X_1, X_2, ..., X_n]$ polinom, amelyre

$$f = g(s_1, s_2, ..., s_n).$$

Példák. • $n = 2$-re $f = X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2X_1X_2 = s_1^2 - 2s_2$, $f = X_1^3 + X_2^3 = (X_1 + X_2)(X_1^2 - X_1X_2 + X_2^2) = s_1(s_1^2 - 3s_1s_2) = s_1^3 - 3s_1^2s_2$.

• $n = 3$-ra $f = X_1^2+X_2^2+X_3^2 = (X_1+X_2+X_3)^2-2(X_1X_2+X_1X_3+X_2X_3) = s_1^2-2s_2$.

18.C.Feladatok

▼ 1. Adottak $f = 2X_1^3X_2 + X_1X_2^4, g = X_1^3X_2^3 - 3X_1^2X_2^2 \in \mathbb{Z}[X_1, X_2]$.

i) Mennyi f és g X_1 és X_2-re vonatkozó foka? Mennyi $\mathrm{gr}(f)$ és $\mathrm{gr}(g)$?

ii) Homogén ill. szimmetrikus-e az f és g ?

iii) Számítsuk ki: $f + g$, fg, $f^2 + 3g$.

▼ 2. Írjuk fel az elemi szimmetrikus polinomok polinomjaként:

a) $f = X_1^4 + X_2^4, g = X_1^5 + X_2^5, h = 3X_1^3 + 3X_2^3 + 5X_1^2X_2^2 \in \mathbb{Z}[X_1, X_2]$,

b) $f = X_1^3 + X_2^3 + X_3^3, g = X_1^2 + X_2^2 + X_3^2 - 5X_1^2X_2^2X_3^2 \in \mathbb{Z}[X_1, X_2, X_3]$,

c) $f = X_1^2 + X_2^2 + X_3^2 + X_4^2, g = X_1^2X_2^2 + X_1^2X_3^2 + X_1^2X_4^2 + X_2^2X_3^2 + X_3^2X_4^2 \in \mathbb{Z}[X_1, X_2, X_3, X_4]$.

Tartalomjegyzék