KOVÁCS BÉLA,

MATEMATIKA I.

7

A Műszaki Földtudományi Alapszak tananyagainak kifejlesztése a
TÁMOP 4.1.2-08/1/A-2009-0033 pályázat keretében valósult meg.

VII. Gyűrűk

1. Gyűrű

Definíció Egy R gyűrű alatt olyan halmazt értünk, amelyben definiálva van egy összeadás és egy szorzás, amelyek teljesítik a következő axiómákat:

(1) $(R,+)$ egy *Abel csoport*:
$x+y=y+x$ R-nek minden x és y elemére (azaz, az összeadás kommutatív);
$(x+y)+z=x+(y+z)$ R-nek minden x, y és z elemére (azaz, az összeadás *asszociatív*);
létezik R-nek egy 0 eleme (zéró elemként ismert) azzal a tulajdonsággal, hogy $x+0=x$ teljesül R minden elemére;
R-nek egy tetszőleges x eleméhez létezik egy $-x$ elem amelyre $x+(-x)=0$ teljesül;

(2) $(R,\cdot)$ egy *félcsoport* (a szorzás *asszociatív*):
$(xy)z=x(yz)$ R-nek minden x, y és z elemére (azaz, a szorzás *asszociatív*);

(3) a szorzás *disztributív*:
$x(y+z)=xy+xz$ és $(x+y)z=xz+yz$ R-nek minden x, y és z elemére.

Lemma Legyen R *gyűrű*. Ekkor $x0=0$ és $0x=0$ R-nek minden x elemére.

Bizonyítás Az R gyűrűben a 0 nulla elemre teljesül a $0+0=0$ összefüggés. Alkalmazzuk a disztributív törvényt, ekkor $x0+x0=x(0+0)=x0$ és $0x+0x=(0+0)x=0x$. Így, ha hozzáadjuk az $x0+x0=x0$ egyenlet mindkét oldalához a $-(x0)$ tagot, akkor a $x0=0$ eredményre jutunk. Hasonlóan, ha hozzáadjuk az $0x+0x=0x$ egyenlet mindkét oldalához a $-(0x)$ tagot, akkor a pedig $0x=0$ teljesül.

Lemma Legyen R egy *gyűrű*. Ekkor $(-x)y=-(xy)$ és $x(-y)=-(xy)$ teljesülnek R-nek minden x és y elemére.

Bizonyítás A disztributív törvényből következnek az $xy+(-x)y=(x+(-x))y=0y=0$ és az $xy+x(-y)=x(y+(-y))=x0=0$ egyenletek. Ezért $(-x)y=-(xy)$ és $x(-y)=-(xy)$ teljesülnek.

Definíció Egy R gyűrű valamely S részhalmazáról azt mondjuk, hogy **részgyűrűje** R-nek, ha $0\in S, a+b\in S, -a\in S$ és $ab\in S$ teljesülnek minden $a,b\in S$-re.

Definíció Egy R gyűrű *kommutatív*, ha if $xy=yx$ minden $x,y\in R$ esetén.

Definíció Egy R gyűrű **egységelemes**, ha létezik (szükségszerűen pontosan egy) nem nulla *multiplikatív* egységelem, amit 1-el jelölünk, és teljesíti az $1x=x=x1$ egyenletet minden $x\in R$ esetén.

Definíció Egy R egységelemes kommutatív gyűrűről azt mondjuk, hogy **nullosztómentes**, ha R-ben bármely két nem nulla elem szorzata nem lehet nullával egyenlő.

Egy egységelemes gyűrűben az a legcélszerűbb, ha nem ragaszkodunk ahhoz, hogy az egységelem különbözzön a zérus elemtől. Ha történetesen 1 és 0 egybeesnek R-ben, akkor ebből triviálisan következik, hogy R-nek csak egyetlen egy eleme van, ez pedig a zérus elem, és ekkor R-et **zéró gyűrűnek** nevezzük ($R = \{0\}$).

PÉLDA

Az egészek $\mathbb{Z}$ halmaza egyik legalapvetőbb példa kommutatív egységelemes gyűrűre.

Egy F test is kommutatív egységelemes gyűrű, amelyre azonban $F \neq \{0\}$ teljesül, és ezenkívül még

(4) minden $a \neq 0$ F-beli elemhez létezik egy $a^{-1} \in F$ amelyre $a^{-1}a = 1$.

Más szavakkal, $F^{\times} = F - \{0\}$ egy *Abel-csoport* a szorzás műveletére nézve. A csoportokra érvényes egy ismert tétel szerint az inverz egyértelmű.

Gyűrűk izomorfizmusa

Definíció Egy φ leképezést az A gyűrűből egy másik A' gyűrűbe **gyűrű homomorfizmusnak** nevezünk, ha teljesülnek a következő feltételek:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$
$$\varphi(1) = 1$$

minden $a, b \in A$ esetén.

Az első két feltételt *művelettartásnak* szoktuk nevezni.

Ha a $\varphi: A \to A'$ homomorfizmus *injektív*, azaz, $a_1 \neq a_2$ teljesülése esetén $\varphi(a_1) \neq \varphi(a_2)$ is igaz, akkor gyűrű **monomorfizmusról** beszélünk.

Ha pedig a $\varphi: A \to A'$ homomorfizmus *szürjektív*, azaz ha minden $a' \in A'$ esetén létezik olyan $a \in A$ elem amelyre $a' = \varphi(a)$, akkor φ-t gyűrű **epimorfizmusnak** nevezzük.

Ha a $\varphi: A \to A'$ homomorfizmus *bijekció*, azaz egyszerre monomorfizmus is és epimorfizmus is, akkor ezt gyűrű **izomorfizmusnak** nevezzük. Ha létezik egy $\varphi: A \to A'$ izomorfizmus, akkor azt mondjuk, hogy A és A' izomorfak és ezt az $A \cong A'$ módon jelöljük. Ha pedig $A = A'$, akkor φ-t **automorfizmusnak** nevezzük.

2. Egyváltozós polinomok

Nem tekintjük a **polinomokat** függvénynek. A polinomok *formális kifejezések* az algebrában és formálisan végzünk velük műveleteket.

Legyen R nem zérus *kommutatív gyűrű*, tehát $1 \neq 0$.

Egy **egyváltozós polinom** az x határozatlan hatványainak egy lineáris kombinációja $a_0 + a_1x + \ldots + a_nx^n$, ahol az x *szimbólum* nem pedig változó.

Sajnos a polinomoknak ez a természetes fogalma polinomokat polinomokkal definiál, hiszen polinom polinomok lineáris kombinációja. A polinomok következő formális definíciója nem lesz annyira természetes mint az előző volt. A pontos definíció érdekében eltávolítjuk az x-et a formalizmusból és a polinomot ennek $(a_0, a_1, \ldots, a_n, \ldots)$ együtthatóiból álló sorozatként adjuk meg.

Így egy *egyhatározatlanú polinom* R-beli együtthatókkal, az R elemeiből álló végtelen sorozat, amelyben egy bizonyos ponttól kezdve minden elem a zérus elem. Az indexelés nullával kezdődik, és az x nem más mint a (0,1,0,0,...) *sorozat*. Így a $7x^2 + 2x + 3$ polinom nem más mint a következő sorozat: $(3,2,7,0,0,\ldots)$.

Láttuk eddig, hogy tetszőleges R gyűrű feletti egyváltozós polinomot lehet vizsgálni. Mégis gyakran érdemesebb test feletti polinom gyűrűvel foglalkozni.

Legyen $\mathbb{K}$ vagy a $\mathbb{Q}$ racionális számtest, vagy az $\mathbb{R}$ valós számok teste, vagy pedig a $\mathbb{C}$ komplex számok teste. ($\mathbb{K}$ valójában bármilyen *test* lehet.)

Például, $7x^3-3x^2+11$ a $\mathbb{Z}[x]$ egy eleme, amely benne van a $\mathbb{Q}[x]$-ben is, $\mathbb{R}[x]$-ben is, és a $\mathbb{C}[x]$-ben is, mivel $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$. Vegyük észre, hogy $\frac{7}{11}x^3-3x^2+11$ eleme $\mathbb{Q}[x]$-nek, de nem eleme $\mathbb{Z}[x]$-nek. Figyeljük meg, hogy $7x^3-\sqrt{2}x^2+x-11$ eleme $\mathbb{R}[x]$-nek, de nem eleme $\mathbb{Q}[x]$-nek.

Polinomok összeadása, negáltja

A polinomok **összeadása** és a **negáltjának képzése** koordinátánként történik:

$$(a_0,a_1,a_2,\dots,a_n,0,0,0,\dots)+(b_0,b_1,b_2,\dots,b_n,0,0,0,\dots)=(a_0+b_0,a_1+b_1,a_2+b_2,\dots,a_n+b_n,0,0,0,\dots),$$

$$-(a_0,a_1,a_2,\dots,a_n,0,0,0,\dots)=(-a_0,-a_1,-a_2,\dots,-a_n,0,0,0,\dots),$$

és az $R[x]$ polinomok halmaza ekkor *Abel csoport* az összeadás műveletére nézve. Az x^n egy olyan polinom amelyben az n-dik pozícióban 1-es áll $n\geq 0$ feltétel mellett, és 0 minden más pozicióban.

PÉLDA

Példa

$$(2x^3+4x+5)+(5x^7+9x^3+x^2+2x+8)=5x^7+11x^3+x^2+6x+13.$$

Polinomok szorzása

Polinomok **szorzását** úgy definiáljuk, hogy az $a_nx^n+\dots+a_1x+a_0$ és $b_mx^m+\dots+b_1x+b_0$ polinomoknál minden tagot minden taggal szorozzuk, majd a szorzatot x hatványai szerint csoportosítjuk és az azonos hatványú tagokat összeadjuk.

A pontos definíció a következő:

$$(a_0,a_1,a_2,\dots,a_n,0,0,0,\dots)(b_0,b_1,b_2,\dots,b_n,0,0,0,\dots)=(c_0,c_1,c_2,\dots,c_n,0,0,0,\dots),$$

ahol $c_N=\sum_{k=0}^{N}a_kb_{N-k}$.

PÉLDA

Példa

$$(2x^3+4x+5)(5x^7+9x^3+x^2+2x+8)=$$
$$=10x^{10}+20x^8+25x^7+18x^6+2x^5+40x^4+65x^3+13x^2+42x+40.$$

Polinomok tulajdonságai

A $\mathbb{K}$ testre úgy tekinthetünk mint a $\mathbb{K}[x]$ részhalmazára és a $\mathbb{K}[x]$-beli összeadás és szorzás $\mathbb{K}$-ra is kiterjeszthető, azaz $\mathbb{K}$-ban bármely két elem összege és szorzata ugyanaz mintha $\mathbb{K}[x]$-ben végeznénk el.

Állítás Legyen R egy *kommutatív gyűrű*. Ekkor az $R[x]$ halmaz is kommutatív gyűrű lesz a szokásos összeadással és szorzással.

Ha egy polinom esetén minden pozícióban zérus áll, akkor **zérus polinomról** beszélünk. Minden $P=(a_0,a_1,\dots,a_n,\dots)$ nem nulla polinom P fokát $\deg P$-vel jelöljük, és úgy definiáljuk, hogy a legnagyobb olyan n index amelyre $a_n \neq 0$. Ebben az esetben a_n -t **főegyütthatónak** nevezzük, az $a_n x^n$ tagot **főtagnak**; és ha $a_n = 1$, akkor a polinom neve **monic**.

Megállapodás szerint a 0 polinom fokát vagy nem definiáljuk, vagy pedig a foka: $-\infty$. Fontos, hogy két polinom f, g pontosan akkor egyenlő, ha x^i együtthatói megegyeznek f és g esetén.

Az összeadás és a szorzás művelete teljesítik mindazokat az axiómákat amelyeket a gyűrű definíciója során korábban felsoroltunk.

Mindezek a tulajdonságok könnyen ellenőrizhetők ha felhasználjuk az összeadás és a szorzás definícióját valamint a $\mathbb{K}$ testre vonatkozó műveletek tulajdonságait. Példaként igazoljuk a *disztributív* törvényt:

Legyen
$f(x) = \sum_{i=0}^{l} a_i x^i, g(x) = \sum_{j=0}^{n} b_j x^j$, és $h(x) = \sum_{j=0}^{n} c_j x^j$.

Ekkor

$$f(x)(g(x)+h(x)) = (\sum_{i=0}^{l} a_i x^i)(\sum_{j=0}^{n} b_j x^j + \sum_{j=0}^{n} c_j x^j)$$
$$= \sum_{i=0}^{l} a_i x^i (\sum_{j=0}^{n} (b_j + c_j) x^j)$$
$$= \sum_{i=0}^{l} \sum_{j=0}^{n} a_i (b_j + c_j) x^{i+j}$$
$$= \sum_{i=0}^{l} \sum_{j=0}^{n} (a_i b_j + a_i c_j) x^{i+j}$$
$$= \sum_{i=0}^{l} \sum_{j=0}^{n} (a_i b_j) x^{i+j} + \sum_{i=0}^{l} \sum_{j=0}^{n} (a_i c_j) x^{i+j}$$
$$= (\sum_{i=0}^{l} a_i x^i)(\sum_{j=0}^{n} b_j x^j) + \sum_{i=0}^{l} a_i x^i)(\sum_{j=0}^{n} c_j x^j)$$
$$= f(x)g(x) + f(x)h(x).$$

Az alábbiakban felsorolt tulajdonságok is ugyanilyen egyszerűen ellenőrizhetők:

Állítás

(a) Az összeadás $\mathbb{K}[x]$-ben kommutatív és asszociatív; azaz minden $f, g, h \in \mathbb{K}[x]$ esetén $f + g = g + f$, és $f + (g + h) = (f + g) + h$

(b) 0 polinom zéruselem összeadásra nézve; azaz minden $f \in \mathbb{K}[x]$ esetén $0 + f = f$.

(c) Minden $f \in \mathbb{K}[x]$ elemnek van additív inverze $-f$, amelyre $f + (-f) = 0$.

(d) A szorzás $\mathbb{K}[x]$-ben kommutatív és asszociatív; azaz minden $f, g, h \in \mathbb{K}[x]$ esetén $fg = gf$, és $f(gh) = (fg)h$

(e) 1 a szorzás egységeleme; azaz minden $f \in \mathbb{K}[x]$ esetén $1f = f$.

(f) Teljesül a disztributív törvény: minden $f, g, h \in \mathbb{K}[x]$ esetén: $f(g + h) = fg + fh$.

Megjegyzés Természetesen a fenti tulajdonságok nem csak test feletti polinomokra, hanem bármilyen egységelemes kommutatív gyűrű fölötti polinomokra is teljesülnek. A bizonyítás ugyanúgy történik mint test feletti polinomok esetén.

Lemma Legyen $\mathbb{K}$ egy test és legyen $f \in \mathbb{K}[x]$ egy nem nulla polinom $\mathbb{K}$ -beli együtthatókkal. Ekkor egy adott $h \in \mathbb{K}[x]$ polinom esetén mindig léteznek egyértelműen $q, r \in \mathbb{K}[x]$ polinomok amelyekre $h = fq + r$ és vagy $r = 0$ vagy deg $r <$ deg f.

Bizonyítás Ha deg $h <$ deg f akkor $q = 0$ és $r = h$ esetén kész vagyunk. A q és r létezését a h polinom deg h foka szerinti teljes indukcióval bizonyítjuk. Így tételezzük fel, hogy deg $h \geq$ deg f és minden olyan polinomra amelynek foka kisebb deg h teljesül a tétel állítása, vagyis felírható a kívánt formában. Létezik a $\mathbb{K}$ testnek olyan c eleme, amelyre $h(x)$ és $cf(x)$ legnagyobb kitevőjű tagjainak ugyanaz az együtthatója.

Legyen $h_1(x) = h(x) - cx^m f(x)$, ahol $m = \deg h - \deg f$. Ekkor vagy $h_1 = 0$ vagy deg $h_1 < \deg h$. Az indukciós hipotézis miatt léteznek olyan q_1 és r polinomok amelyekre $h_1 = fq_1 + r$ és vagy $r=0$ vagy deg $r <$ deg f. de ekkor $h=fq+r$ is teljesül, ahol $q(x)= cx^m + q_1(x)$.

Ezután igazoljuk q és r egyértelműségét.

Tételezzük fel, hogy $fq+r= f\bar{q} + \bar{r}$, ahol $\bar{q}, \bar{r} \in \mathbb{K}[x]$ és vagy $\bar{r} = 0$ vagy deg $\bar{r} <$ deg f. Ekkor $(q - \bar{q}) f = r - \bar{r}$.

De $\deg((q-\bar{q})f) \geq$ deg f abban az esetben amikor $q \neq \bar{q}$, és deg $(r - \bar{r}) <$ deg f ha $r \neq \bar{r}$. Ezért a $(q - \bar{q}) f = r - \bar{r}$ egyenlőség nem állhat fenn csak akkor ha $q = \bar{q}$ és $r = \bar{r}$. Ez igazolja q és r egyértelműségét.

Definíció Legyen R kommutatív gyűrű. Az R -nek egy nem üres I részhalmaza ideál a teljesülnek a következő feltételek:

1. $(x, y \in I) \Rightarrow (x + y \in I)$.
2. $(x \in R,\ y \in I) \Rightarrow (xy \in I)$.

Állítás Legyen R kommutatív gyűrű és legyen $f_1, f_2, \ldots, f_n \in R$. Ekkor

$I = \{x \in R : x = g_1 f_1 + g_2 f_2 + \ldots + g_n f_n$ minden $g_i \in R\}$

egy ideálja R -nek. Ezt az ideált gyakran $(f_1, f_2, \ldots, f_n)$ -el jelöljük.

Állítás Legyen $\mathbb{K}[x]$ egy polinom gyűrű az $\mathbb{K}$ test felett.

1) Legyen $f, g, g_1, g_2 \in \mathbb{K}[x]$ és f nem nulla. Ekkor $(fg = 0 \Rightarrow g = 0)$ és $(fg_1 = fg_2 \Rightarrow g_1 = g_2)$.

2) $f \in \mathbb{K}[x]$ létezik inverze $\mathbb{K}[x]$-ben akkor és csak akkor, ha f nem nulla skalár.

Lemma Legyen $\mathbb{K}$ egy test és legyen I egy ideál a $\mathbb{K}[x]$ polinom gyűrűben. Ekkor létezik egy $f \in \mathbb{K}[x]$ polinom amelyre $I=(f)$, ahol (f) jelöli az f által generált ideált $K[x]$-ben.

Bizonyítás Ha $I = \{0\}$ akkor kész vagyunk hiszen ekkor legyen $f = 0$. Máskülönben legyen $f \in I$ olyan elem, amelyre $f \neq 0$ és f foka nem nagyobb egyetlen nem nulla polinomnál sem I –ben. Ekkor $h=fg+r$ alakban írható ahol vagy $r= 0$ vagy deg $r <$ deg f. (Lásd egy korábbi tételt ▶). De $r \in I$, mivel $r=h - fg$ és h és f az I elemei. Mivel f fokánál r foka nem lehet kisebb, hiszen így választottuk meg f –et, így $r = 0$ és innen $h = qf$. Tehát $I=(f)$.

3. Gyakorlatok

1. Gyakorlat

Hány, egymással nem izomorf gyűrűstruktúra értelmezhető egy kételemű halmazon?

Megoldás

Tudjuk, hogy egy ilyen kételemű gyűrű az összeadásra nézve kommutatív csoportot alkot. Jelölje a zérus elemet 0, a másik elemet pedig a. Tudjuk tehát, hogy $0+0=0$ és $0+a=a+0=a$. Eddig a műveleti tábla egy elemet kivéve ismert:

+	0	a
0	0	a
a	a	?

Hátra van még $a+a$ meghatározása. Elméletileg két lehetőségünk van: az $a+a$ összeg értéke vagy 0 vagy a. Emlékeztetünk arra, hogy a csoportban minden elemnek létezik additív inverze, így $a-$nak is, és ez egyértelműen meghatározott, a szokásos jelölésmódnak megfelelően $-a$-val jelöljük. Tehát $a+(-a)=(-a)+a=0$. Lehet-e az additív inverz a$-a$ nullával egyenlő? Nem lehet, hiszen a műveleti tábla eddig ismert részéből kiolvashatjuk, hogy 0-át a-hoz hozzáadva nem nullát kapunk, hanem a $-$t: $0+a=a+0=a$. Tehát más választásunk nem lévén: a additív inverze csak a lehet: $-a=a$. Tehát: $a+a=0$.

Így az összeadás műveleti táblája:

+	0	a
0	0	a
a	a	0

ami izomorf $(\mathbb{Z}_2$,+)-al.

Tehát az általunk keresett gyűrű additív csoportja izomorf $(\mathbb{Z}_2$,+)-al. Ezután a szorzási műveletek meghatározása történik. Tudjuk, hogy gyűrűben minden x gyűrűelemre igaz, hogy a nulla elemmel való szorzata nulla: $0\bullet x=x\bullet 0=0$. Tehát a szorzás műveleti táblája:

$\bullet$	0	a
0	0	0
a	0	?

A táblázatból látszik, hogy egyedül az $a\bullet a$ értékét kell (lehet) megadni. Két lehetőségünk van: ez az érték vagy nullával vagy pedig a-val egyenlő.

a) eset

$\bullet$	0	a
0	0	0
a	0	0

Ebben az esetben olyan gyűrűt kapunk, amelyben bármelyik két elem szorzata nulla. Ennek neve: zérógyűrű. Könnyű ellenőrizni, hogy ez valóban gyűrű, azaz teljesíti a gyűrű összes axiómáját. A szorzás műveleti táblájából az is leolvasható, hogy ennek a gyűrűnek nincs egységeleme.

b) eset

$\bullet$	0	a
0	0	0
a	0	a

Ekkor a jól ismert $(\mathbb{Z}_2,+,\cdot)$ -vel izomorf gyűrűt kapunk. Könnyű ellenőrizni, hogy ez is valóban gyűrű, azaz teljesíti a gyűrű összes axiómáját. A szorzás műveleti táblájából pedig látható, hogy ez a gyűrű egységelemes, az egységelem természetesen az a. Tehát egységelemes és kommutatív gyűrű. Nyilvánvaló, hogy nemcsak gyűrű hanem test is hiszen a nulla mellett csak egy elem van, az a , ennek pedig az inverze saját maga. A kapott összeadással és szorzással éppen az F_2 testet kaptuk.

2. Gyakorlat

Mutassuk meg, hogy bármely két egységelemes gyűrű izomorf és testet alkot.

Megoldás

Az előző gyakorlat alapján azt állíthatjuk, hogy egy ilyen gyűrű additív csoportja izomorf a $(\mathbb{Z}_2$,+)-al. A gyűrű elemei legyenek ebben az esetben is 0 (itt is 0 jelöli a nulla elemet) és a . A levezetést mellőzve a műveleti tábla ugyanaz mint az előbbi példában:

+	0	a
0	0	a
a	a	0

Ezután a szorzási műveletek meghatározása történik. Tudjuk, hogy gyűrűben minden x gyűrűelemre igaz, hogy a nulla elemmel való szorzata nulla: $0 \bullet x = x \bullet 0 = 0$. Tehát a szorzás műveleti táblája:

$\bullet$	0	a
0	0	0
a	0	?

A táblázatból látszik, hogy egyedül az $a \bullet a$ értékét kell (lehet) megadni. Emlékeztetünk arra, hogy egy gyűrű egységelemes, ha létezik egy (szükségszerűen csak egy és nem több) mondjuk 1-el jelölt elem, amelyre igaz az, hogy $1 \neq 0$ és $1 \bullet x = x = x \bullet 1$ minden $x \neq 0$ elem esetén. Mivel a gyűrű egységelemes az egységelem csak az a lehet, hiszen $0 \bullet 0 = 0$ és $0 \bullet a = 0$, több elem pedig nincs . Tehát $a \bullet a = a$. Így a szorzás műveleti táblája:

$\bullet$	0	a
0	0	0
a	0	a

A kapott összeadással és szorzással éppen az F_2 testet kaptuk mint az előző feladat b) részében. Tehát minden kételemű egységelemes gyűrű egyben test is, és izomorf az F_2 testtel. Az a elem helyett írjunk 1-et, ekkor $F_2 = \{0,1\}$. A műveleti táblák pedig következők:

Az összeadás:

+	0	1
0	0	1
1	1	0

és a szorzás:

•	0	1
0	0	0
1	0	1

3. Gyakorlat

Írjuk le az összes gyűrűt az $(\mathbb{Z},+)$ struktúrán.

Megoldás

A disztributív törvény következtében a $\mathbb{Z}$ halmazon definiálni kívánt $*$ szorzás művelet megadásához elég előírni az $1*1$ értéket. Valóban,

$$n*m = (1+\ldots+1)*(1+\ldots+1) = 1*1+\ldots+1*1 = nm(1*1).$$

Könnyen ellenőrizhető, hogy tetszőleges $k \in \mathbb{Z}$ esetén az $n*m = nmk$ szorzás egy gyűrűt eredményez $\mathbb{Z}$-n. Csak $k=1$ vagy $k=-1$ esetén kapunk egységelemes gyűrűt.

4. Gyakorlat

Legyen M egy tetszőleges halmaz és $\mathbf{P}(M)$ az összes részhalmazaiból álló halmazrendszer. Tekintsük az $+ : \mathbf{P}(M)\times\mathbf{P}(M) \to \mathbf{P}(M)$ műveletet az $X+Y=(X-Y)\bigcup(Y-X)$ képlettel definiált módon. Igazoljuk, hogy $(\mathbf{P}(M),+,\bigcap)$ gyűrű, mégpedig kommutatív és egységelemes. Emellett nullosztókat tartalmaz és minden eleme idempotens.

Megoldás

ϕ és M rendre a zérus elem és az egységelem. Emellett M-nek minden nem üres részhalmaza nullosztó, és $A\bigcap A = A$ alapján nyilvánvaló, hogy minden elem idempotens. Minden gyűrűre vonatkozó tulajdonság könnyen ellenőrizhető.

5. Gyakorlat

Legyen M egy tetszőleges halmaz és $\mathbf{P}(M)$ az összes részhalmazainak halmaza. Tekintsük a $+ : \mathbf{P}(M)\times\mathbf{P}(M) \to \mathbf{P}(M)$ műveletet, amelyet az $X+Y=(X-Y)\bigcup(Y-X)$ összefüggés definiál. Ekkor a $(\mathbf{P}(M),+,\bigcap)$ kommutív egységelemes gyűrű, amelyben nullosztók vannak és minden elem idempotens

Megoldás

Az üres halmaz ϕ és az M a zéruselemnek illetve az egységelemenek felelenek meg. Az M minden nem üres diszjunkt részhalmaza nullosztók és $A\bigcap A = A$, így minden elem idempotens. A gyűrű összes tulajdonsága könnyen ellenőrizhető.

6. Gyakorlat

Az $\mathbb{R}^2$-ben tekintsük az $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ összeadást és két különböző szorzást:

(a) $(x_1, x_2) \circ (y_1, y_2) = (x_1 x_2, x_1 y_2 + x_2 y_1)$ és
(b) $(x_1, x_2) * (y_1, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1)$.

Ellenőrizzük, hogy az $(\mathbb{R}^2,+,\circ)$ és $(\mathbb{R}^2,+,*)$ egységelemes gyűrűk. Keressünk nullosztókat az első esetben, és igazoljuk, hogy a második gyűrű $(\mathbb{C},+,\cdot)$-vel. Izomorf-e egymással a két gyűrű?

Megoldás

A gyűrű azonosságok ellenőrzése egyszerű. Az első gyűrűben $(0,1) \circ (0,1) = (0,0)$ így $(0,1)$ (kétoldalú) nullosztó. Egy $f : (\mathbb{R}^2,+,*) \to (\mathbb{C},+,\cdot)$ leképezést definiáljunk az $f(x, y) = x + iy$ összefüggéssel, erről könnyen belátható, hogy gyűrű izomorfizmus. A fenti két $(\mathbb{R}^2,+,\circ)$ és $(\mathbb{R}^2,+,*)$ egységelemes gyűrűk nem izomorfak. Általában, ha R és R' olyan gyűrűk, hogy R-nak van R'-nek pedig nincs nullosztója, akkor a két gyűrű nem izomorf egymással. Valóban, ha $f : R \to R'$ izomorfizmus lenne (elegendő lenne csak injektív gyűrű homomorfizmust azaz monomorfizmust vizsgálni) akkor $ab = 0, a, b \in R$ és $a \neq 0 \neq b$ esetén $f(a) \cdot f(b) = 0$ és $f(a) \neq 0 \neq f(b)$ lenne, ami ellentmondás.

7. Gyakorlat

Legyen $\mathcal{M}_n(R)$ az $n \times n$-es mátrixok gyűrűje az R gyűrű felett ($n \in \mathbb{Z}^+$).

Mutassuk meg, hogy $\mathcal{M}_n(R)$-nek akkor és csak akkor van egységeleme, ha R-nek van.

Mutassuk meg, hogy $n \geq 2$ esetén $\mathcal{M}_n(R)$ kommutatív akkor és csak akkor, ha $R^2 = \{0\}$ (azaz $\forall a, b \in R : ab = 0$).

Az $\mathcal{M}_n(R)$ centere az összes rI_n alakú diagonális mátrixból áll, ahol $r \in Z(R) = \{r \in R : rx = xr, \forall x \in R\}$ (az R-nek a centere).

Megoldás

(a) Ha $1 \in R$ akkor $\mathcal{M}_n(R)$ egységeleme a jól ismert egységmátrix

$$I_n = \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & 1 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & . & 1 \end{bmatrix}.$$

Megfordítva, ha $E = (e_{ij})_{1 \leq i,j \leq n}$ az $\mathcal{M}_n(R)$-nek az egységmátrixa, akkor $a \in R$ esetén, legyen az $A = (a_{ij})$ mátrix olyan, amelynek minden eleme zérus, kivéve $a_{11} = a$-t és így az $EA = AE$, felhasználásával azt kapjuk, hogy e_{11} az R egységeleme.

(b) Ha $R^2 = \{0\}$ akkor $(\mathcal{M}_n(R))^2 = \{0_n\}$ és $\mathcal{M}_n(R)$ nyilvánvalóan kommutatív gyűrű.

Megfordítva, ha $\mathcal{M}_n(R)$ kommutatív és $a, b \in R$, akkor $a \cdot b = 0$ -t kapunk az alábbi összefüggésből:

=

$$\begin{bmatrix} a & 0 & . & . & 0 \\ 0 & 0 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & . & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & . & . & b \\ 0 & 0 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & . & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & . & . & b \\ 0 & 0 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & . & 0 \end{bmatrix} \begin{bmatrix} a & 0 & . & . & 0 \\ 0 & 0 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & . & 0 \end{bmatrix}$$

(c) Ha $r \in Z(R)$ és $A \in \mathbf{M}_n(R)$ akkor $rI_n \cdot A = rA = Ar = A \cdot rI_n$.

Megfordítva, ha $U = (u_{ij}) \in Z(\mathbf{M}_n(R))$ tekintsük az E_{ij} mátrixot (ez az un. egységmátrix) amelyben 1 van az i -dik sor és a j -dik oszlop találkozásában és minden más helyen nulla van. Az $UE_{ij} = E_{ij}U$ egyenletből azt kapjuk, hogy $u_{ii} = u_{jj}$ minden $i, j \in \{1, 2, \ldots, n\}$ és $u_{ij} = 0$ ha $i \neq j$, így U diagonális, azaz felírható a következőképpen: mondjuk $u \cdot I_n$. Ha $r \in R$ következik az $(u \cdot I_n)(rE_{11}) = (rE_{11})(u \cdot I_n)$ egyenletből, akkor $u \in Z(R)$.

4. Polinomosztás és gyöktényezős alak

Emlékeztetünk arra, hogy az

$$f(x) := a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

kifejezést **polinomnak** nevezzük.

Az $a_0, a_1, \ldots, a_n$ számok a polinom **együtthatói**, *x* pedig a **változója** (a polinomot függvénynek fogjuk tekinteni, l. racionális egész függvény). Ha $a_n \neq 0$, akkor $f(x)$ **n-edfokú polinom**, *n* a polinom **fokszáma** (**foka**).

Tetszőleges $f(x)$ és nullától különböző $g(x)$ polinomhoz található olyan *q*(x) és $r(x)$ polinom, melyekre

(1) $$f(x) = q(x)\, g(x) + r(x) \,,$$

és $r(x)$ fokszáma kisebb mint $g(x)$ fokszáma. Az (1) azonosság formálisan felírható

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

alakban is, $g(x)$ az osztás **hányadosa**, $r(x)$ a **maradéka**. Ha $r(x) \equiv 0$, akkor $f(x)$ (maradék nélkül) **osztható** $g(x)$ -szel.

1. TÉTEL. Ha az $f(x)$ polinomot $(x - \alpha)$ -val osztjuk, akkor $r(x) = f(\alpha)$.

Ha $f(\alpha) = 0$, akkor α az $f(x)$ polinom **zérushelye** (**gyöke**). Ekkor α egyúttal az $f(x) = 0$ egyenlet **gyöke**.

2. TÉTEL. **(Az algebra alaptétele).** Bármely, legalább első fokú, (valós vagy) komplex együtthatós polinomnak van zérushelye a komplex számtestben.

Ebből a tételből következik, hogy az *n* -edfokú polinomnak pontosan *n* darab zérushelye van. Legyenek ezek $x_1, x_2, \ldots, x_n$. Ekkor a polinom **gyöktényezős alakja**

(2) $$f(x) = a_n (x - x_1)(x - x_2) \ldots (x - x_n) \,,$$

ahol $x-x_1$, $x-x_2$, ..., $x-x_n$ a **gyöktényezők**.

A zérushelyek között megegyezők is lehetnek. Ha az x_1 zérushely s_1 -szer, az x_2 zérushely s_2 -ször, ..., az x_q pedig s_q -szor fordul elő, akkor a gyöktényezős alak.

(3)

$$f(x)=a_n(x-x_1)^{s_1}(x-x_2)^{s_2}\dots(x-x_q)^{s_q}$$

alakú, ahol $s_1+s_2+\dots+s_q=n$. Az s_k szám az x_k zérushely **multiplicitása** (többszörössége). Szokás azt mondani, hogy x_k a polinom s_k *-szoros zérushelye* $(k=1,2,\dots,q)$.

A gyöktényezős alakból látszik, hogy a polinom osztható bármelyik gyöktényezőjével.

Mindezekből következik, hogy az

(4)

$$a_nx^n+a_{n-1}x^{n-1}+\dots+a_2x^2+a_1x+a_0=0$$

n -edfokú algebrai egyenlet gyöktényezős alakja:

(5)

$$a_n(x-x_1)^{s_1}(x-x_2)^{s_2}\dots(x-x_q)^{s_q}=0$$

ahol $x_1, x_2, \dots, x_q$ az egyenlet gyökei.

A valós együtthatójú egyenletekre vonatkozó néhány megjegyzés:

1. Ha az együtthatók egész számok, akkor a (4) egyenlet minden egész gyöke az állandó tag osztója.
2. az együtthatók egész számok és $a_n=1$, akkor a (4) egyenlet minden racionális gyöke egész szám.
3. az együtthatók valós számok és az $a+ib$ komplex szám az egyenletnek gyöke, akkor az $a-ib$ komplex szám is gyöke annak.
4. Ha az egyenlet együtthatóinak összege nulla, akkor az egyenlet egyik gyöke 1 (ez komplex együtthatók esetén is igaz).

5. Mintapéldák

Megoldások: ⊙ láthatók ○ nem láthatók

1. Legyen $f(x)=2x^4-5x^3+x+7$, $g(x)=x^2-3$. Állítsuk elő $f(x)$ -et *q*(*x*)*g*(*x*) + *r*(*x*) alakban.

Megoldás. Előbb végezzük el az $f(x)$ / $g(x)$ osztást:

$(2x^4-5x^3+x+7):(x^2-3)=2x^2-5x+6=q(x)$

$\pm 2x^4 \mp 6x^2$

$-5x^3+6x^2+x+7$

$\mp 5x^3 \qquad \pm 15x$

$6x^2-14x+7$

$\pm 6x^2 \qquad \mp 18$

$-14x+25=r(x)$

A hányados $q(x) = 2x^2 - 5x + 6$, a maradék pedig $r(x) = -14x + 25$. Így tehát $f(x) = (2x^2 - 5x + 6)(x^2 - 3) - 14x + 25$. A szorzás és összevonások elvégzése után könnyű meggyőződni az előállítás helyességéről.

Célszerű lehet az *f*(*x*)/*g*(*x*) tört formális felírása. Jelen esetben

$$\frac{f(x)}{g(x)} = \frac{2x^4 - 5x^3 + x + 7}{x^2 - 3} = 2x^2 - 5x + 6 + \frac{-14x + 25}{x^2 - 3}.$$

- **2.** Legyen $f(x) = x^4 + 5x^2 + 1$. Számítsuk ki az osztási maradékot, ha $f(x)$ -et osztjuk $(x - i)$ -vel.

Megoldás. Az 1. tétel alapján $r = f(\alpha) = f(i) = i^4 + 5i^2 + 1 = 1 - 5 + 1 = -3$.

3. Írjuk fel az alábbi polinomok gyöktényezős alakját:

a) $f(x) = x^5 - 4x^3$; **b)** $g(x) = x^4 - 1$; **c)** $h(x) = x^3 - 2x^2 + 5x$.

Megoldás

a) $f(x) = x^5 - 4x^3 = x^3(x^2 - 4) = x^3(x - 2)(x + 2)$. Ebből a gyöktényezős alakból látszik, hogy a zérushelyek: $x_1 = 0$ (háromszoros), $x_2 = 2$ (egyszeres), $x_3 = -2$ (egyszeres).

b) $g(x) = x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x - i)(x + i)$.

A zérushelyek: $x_1 = 1$, $x_2 = -1$, $x_3 = i$, $x_4 = -i$. Nyilván mindegyik egyszeres.

c) $h(x) = x^3 - 2x^2 + 5x = x(x^2 - 2x + 5)$. Az egyik zérushely $x_1 = 0$. A további két zérushely az $x^2 - 2x + 5 = 0$ egyenlet két gyöke:

$$x_{2,3} = \frac{2 \pm \sqrt{4 - 20}}{2} = \frac{2 \pm \sqrt{-16}}{2} = \frac{2 \pm 4\sqrt{-1}}{2} = \frac{2 \pm 4i}{2} = 1 \pm 2i$$

A zérushelyek tehát $x_1 = 0$, $x_2 = 1 + 2i$, $x_3 = 1 - 2i$, így a gyöktényezős alak:

$h(x) = x(x - (1 + 2i))(x - (1 - 2i))$.

- **4.** Legyen $f(x) = 7(x - 2)^3 (x + 5)(x - 2i)(x + 2i)$ egy hatodfokú polinom. Állapítsuk meg a zérushelyeit.

Megoldás. $x_1 = 2$ háromszoros, $x_2 = -5$, $x_3 = 2i$, $x_4 = -2i$ pedig egyszeres zérushelyek. A háromszoros zérushely három zérushelynek számít, így valóban felírtuk mind a hatot. Lehetne így jelölni őket: $x_1 = 2$, $x_2 = 2$, $x_3 = 2$, $x_4 = -5$, $x_5 = 2i$, $x_6 = -2i$.

- **5.** Legyenek egy ötödfokú polinom zérushelyei: $x_1 = 0$, $x_2 = x_3 = 3$, $x_4 = i$, $x_5 = -i$. Írjuk fel a polinomot, ha $a_5 = 1$.

Megoldás. A polinom gyöktényezős alakja:

$f(x) = 1 \cdot x(x - 3)^2 (x - i)(x + i)$.

A szorzásokat és összevonásokat elvégezve:

$$f(x) = x^5 - 6x^4 + 10x^3 - 6x^2 + 9x \cdot$$

6. Írjuk fel az $x^3 - 8 = 0$ egyenlet gyöktényezős alakját.

Megoldás. Először megoldjuk az egyenletet:

$$x^3 - 8 = 0 \Rightarrow x = \sqrt[3]{8} = 2\left(\cos\frac{2k\pi}{3} + i\sin\frac{2k\pi}{3}\right),\ k = 0,1,2.$$

$$k = 0 \Rightarrow x_1 = 2(\cos 0 + i\sin 0) = 2,$$

$$k = 1 \Rightarrow x_2 = 2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right) = -1 + \sqrt{3}i,$$

$$k = 2 \Rightarrow x_3 = 2\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right) = -1 - \sqrt{3}i \cdot$$

Az egyenlet gyöktényezős alakja:

$$(x-2)(x-(-1+\sqrt{3}i))(x-(-1-\sqrt{3}i)) = 0 \cdot$$

- **7.** Oldjuk meg az $x^6 + x^5 + 2x^4 + 4x^3 - 8x^2 = 0$ egyenletet, ha tudjuk, hogy egyik gyöke 2*i*, Írjuk fel az egyenlet gyöktényezős alakját is.

Megoldás

A bal oldalon x^2 -et kiemelve, az egyenlet

$$x^2(x^4 + x^3 + 2x^2 + 4x - 8) = 0$$

alakú lesz. Innen látható, hogy $x = 0$ kétszeres gyök, azaz $x_1 = 0$ és $x_2 = 0$. Az $x^4 + x^3 + 2x^2 + 4x - 8 = 0$ egyik gyöke 2*i*.

Mivel az együtthatók valósak, ezért ennek konjugáltja, azaz $-2i$ is gyök. Tehát $x_3 = 2i$, $x_4 = -2i$. Így a negyedfokú egyenlet bal oldala osztható az

$$(x-2i)(x+2i) = x^2 - 4i^2 = x^2 + 4$$

polinommal.

Végezzük el az osztást:

$$(x^4 + x^3 + 2x^2 + 4x - 8):(x^2 + 4) = x^2 + x - 2$$

$$\pm x^4 \qquad \pm 4x^2$$

$$x^3 - 2x^2 + 4x - 8$$

$$\pm x^3 \qquad \pm 4x$$

$$-2x^2 - 8$$

$$\mp 2x^2 \mp 8$$

$$\varnothing$$

Ennek eredményeként $x^4 + x^3 + 2x^2 + 4x - 8 = (x^2+1)(x^2 + x - 2)$.

Az $x^2 + x - 2 = 0$ másodfokú egyenlet gyökei: 1 és -2. Tehát az eredeti egyenlet hat gyöke: $x_1 = 0$, $x_2 = 0$, $x_3 = 2i$, $x_4 = -2i$, $x_5 = 1$, $x_6 = -2$, így az egyenlet gyöktényezős alakja:

$$x^2(x-2i)(x+2i)(x-1)(x+2) = 0 \cdot$$

Megjegyezzük, hogy az osztás helyett a következőképpen is eljárhatunk: Mivel $g(x) = x^2 + 4$ másodfokú,

$f(x) = x^4 + x^3 + 2x^2 + 4x + 8$ negyedfokú, a maradék pedig nulla, ezért a $q(x)$ hányados másodfokú, azaz $q(x) = Ax^2 + Bx + C$ alakú. Így felírható a következő azonosság:

$$x^4 + x^3 + 2x^2 + 4x - 8 \equiv (Ax^2 + Bx + C)(x^2 + 4) \equiv$$
$$\equiv Ax^4 + 4Ax^2 + Bx^3 + 4Bx + Cx^2 + 4C.$$

Az együtthatókat összehasonlítva azt kapjuk, hogy $A = 1$, $B = 1$, $C = -2$, így $q(x) = x^2 + x - 2$.

8. Oldjuk meg az $(x^2 - 9)^2\,(2x - 1)\,(x^2 + 4) = 0$ egyenletet.

Megoldás. Egy szorzat akkor nulla, ha valamelyik tényezője nulla. Az első tényező akkor nulla, ha $(x^2 - 9)^2 = 0$, azaz ha $x^2 - 9 = 0$. Innen $x = 3$ és $x = -3$. Ezek azonban kétszeres gyökök, mert $(x^2 - 9)^2 = (x - 3)^2\,(x + 3)^2 = 0$. A második tényező akkor nulla, ha $x = \frac{1}{2}$. Végül az $x^2 + 4 = 0$ egyenlet gyökei $2i$ és $-2i$. Tehát az eredeti egyenlet gyökei: $x_1 = x_2 = 3$, $x_3 = x_4 = -3$, $x_5 = \frac{1}{2}$, $x_6 = 2i$, $x_7 = -2i$.

6. FELADATOK

1. Igazolja, hogy az alábbi feladatokban $f(x)$ osztható $g(x)$ -szel, majd írja fel $f(x)$ -et $q(x)g(x)$ alakban:

a) $f(x) = x^2 - 8x + 15$, $g(x) = x - 3$;

b) $f(x) = x^2 - 8x + 15$, $g(x) = 7x - 21$;

c) $f(x) = x^5 + 6x^4 + 13x^3 + 14x^2 + 12x + 8$, $g(x) = x^2 + 1$;

d) $f(x) = x^4 + 1$, $g(x) = x^2 + \sqrt{2}x + 1$.

2. Számítsa ki a maradékot, ha az $f(x)$ polinomot osztjuk $(x - \alpha)$ -val:

a) $f(x) = x^4 + 1$, $\alpha = 1$, $\alpha = 2i$, $\alpha = \frac{\sqrt{2}}{2}(1 + i)$;

b) $f(x) = x^3 + x - 2$, $\alpha = 1$, $\alpha = i$.

3. Szorzattá alakításokkal írja fel az alábbi egyenletek gyöktényezős alakját, majd ebből határozza meg a gyököket:

a) $x^3 - 4x = 0$;

b) $x^3 - x^2 + x - 1 = 0$;

c) $(2x^2 + 1)(2x^2 - 1) = 0$;

d) $x^3 + ix^2 - x - i = 0$;

e) $x^3 + 3x^2 + 3x + 1 = 0$;

f) .

$$x^2(x^2+4x)=0$$

4. Igazolja, hogy az 1 szám kétszeres gyöke a $2x^3-3x^2+1=0$ egyenletnek, azaz kétszeres zérushelye az $f(x) = 2x^3-3x^2+1$ polinomnak.

5. Az $f(x)$ ötödfokú, valós együtthatós polinom egyik gyöke $1-3i$. Tudjuk továbbá, hogy $f(x)$ -et $(x-2)$ -vel, $(x + 5)$ -tel és $(x + 6)$ -tal osztva, a maradék mindhárom esetben nulla. Határozza meg az $f(x) = 0$ egyenlet gyökeit.

6. Igazolja, hogy a 2 szám is és az *i* szám is gyöke az $x^3-2x^2+x-2=0$ egyenletnek. Állapítsa meg a harmadik gyököt.

7. Oldja meg az alábbi egyenleteket:

a) $x^3-4x+3=0$;

b) $x^4-x^3+x^2-3x-6=0$;

c) $x^6-1=0$;

d) $(x^2+9x+25)(x^2+9)=0$.

8. Állapítsa meg az $f(x)=(x^3-2x^2)(x^2-1)(x^2+x)$ polinom zérushelyeit azok többszörösségével együtt, majd írja fel $f(x)$ gyöktényezős alakját.

9. A $3x^4-5x^3+3x^2+4x-2=0$ egyenlet egyik gyöke $1 + i$. Határozza meg a többi gyököt.

10. Az $x^4-2x^3-7x^2+8x+12=0$ egyenlet mindegyik gyöke egész szám. Határozza meg ezeket.