Rendezett gyűrűk. Racionális és egész együtthatós polinomok számelmélete

1. *Igazoljuk, hogy ha egy részbenrendezett gyűrűben $a, b \geq 0$ és $a + b = 0$, akkor $a = b = 0$.*

Megoldás. Az $a + b = 0$ feltétel miatt nyilván $a = 0 \iff b = 0$. Tegyük föl indirekt módon, hogy $a \neq 0$. Ez tehát azt is jelenti, hogy $a, b > 0$. Viszont az $a \geq 0$ feltételből következik, hogy $a + b \geq b > 0$, ami ellentmond az $a + b = 0$ föltevésünknek.

2. *Igazoljuk, hogy részbenrendezett gyűrűben egy pozitív és egy negatív szám szorzata mindig negatív, két negatív szám szorzata pedig pozitív. Mutassuk meg azt is, hogy egy egyenlőtlenséget negatív számmal szorozva annak iránya megváltozik.*

Megoldás. $a < 0$ esetén $a + (-a) = 0 < 0 + (-a) = -a$ tehát negatív szám ellentettje pozitív (és a fordított állítás is nzilván igaz, pl. az előző feladat miatt). Ha $a > 0$ és $b > 0$, akkor a részbenrendezett gyűrűk definíciója miatt $ab > 0b = 0$ (a gyűrűkről föltettük hogy nullosztómentesek!). Ha most $a > 0$ és $b < 0$, akkor az első megjegzés alapján $-b > 0$, és ekkor $a(-b) = -ab > 0$. Viszont ismét az előző megjegyzés alapján $ab = -(-ab) < 0$. – Az alaptulajdonságokból következik, hogy $a > b$ azzal ekvivalens, hogy $a - b > b - b = 0$. Ha most ez utóbbit szorozzuk egy $c < 0$ számmal, akkor az előzőek szerint $ac - bc = (a - b)c < 0$. Mindkét oldalhoz bc-t adva azt kapjuk, hogy $ac < bc$, vagyis az egyenlőtlenség iránya megfordul, ha negatív számmal szorzunk.

3. *Egy kommutatív, egységelemes, nullosztómentes R gyűrűnek legyen P olyan részhalmaza, amely nem tartalmazza a nullelemet, de zárt az összeadásra és a szorzásra nézve. Mutassuk meg, hogy R-en megadható olyan részbenrendezés, amelynek P a pozitivitástartománya.*

Megoldás. Definiáljuk a részbenrendezést oly módon, hogy $a > b$ pontosan akkor teljesüljön, ha $a - b \in P$ igaz. Ha ilyen módon egy jó részbenrendezést kapunk, akkor világos, hogy ennek épp P lesz a pozitivitási tartománya, hiszen $a > 0 \iff a = a - 0 \in P$. A következő dolgokat kell ellenőriznünk:

(1) (Irreflexivitás) $a > a$ soha nem teljesül, de ez valóban igaz, hiszen $a - a = 0 \notin P$.
(2) (Antiszimmetria) Ha $a > b$ teljesül, akkor $b < a$ nem lehet igaz. De ha mindkettő teljesülne, akkor $a - b \in P$ és $b - a \in P$ is igaz lenne, amiből P-nek az összeadásra való zártsága miatt $(a - b) + (b - a) = 0 \in P$ következne, ami a fetétel szerint nem lehetséges.
(3) (Tranzitivitás) Ha $a > b$, és $b > c$, akkor $a > c$. Ez ismét abból következik, hogy P zárt az összeadásra, hiszen $a - b \in P$ és $b - c \in P$ esetén $(a - b) + (b - c) = a - c \in P$. A fenti három feltétel azt biztosítja, hogy egy (szigorú) részbenrendezést kaptunk. Azt kell még ellenőriznünk, hogy ez a reláció „kompatibilis" a műveletekkel, vagyis az aábbiakat.
(4) $a > b$ esetén $a + c > b + c$ tetszőleges c-re. De ez világos, hiszen $a - b \in P$ esetén $(a + c) - (b + c) = a - b \in P$.
(5) $a > b$ és $c > 0$ esetén $ac > bc$. Ez viszont abból adódik, hogy $a - b \in P$ és $c > 0$ esetén $ac - bc = (a - b)c > 0$, hiszen P zárt a szorzásra.

Ezzel az állítást beláttuk.

4. *Igazoljuk, hogy a racionális számok teste csak egyféleképpen rendezhető.*

Megoldás. Jelölje $\succ$ egy tetszőleges rendezést. Megmutatjuk, hogy $a \succ b$ pontosan akkor igaz, ha $a > b$ a hagyományos rendezéssel. Nevezzük most pozitívnak azokat a racionális számokat, melyekre $a \succ 0$. Korábbiakból tudjuk, hogy pozitív számok szorzata poztív, negatív számok szorzata is pozitív, pozitív és negatív szám szorzata negatív, valamint hogy pozitív szám ellentettje negatív (és megfordítva). Ebből azt kapjuk, hogy:

(1) $1^2 = 1 \succ 0$.
(2) $2 = 1 + 1 \succ 0 + 1 = 1 \succ 0$, és teljes indukcioval, $n + 1 \succ 0 + 1 \succ 0$, tehát minden természetes szám pozitív.
(3) $n \cdot 1/n = 1 \succ 0$ miatt $1/n \succ 0$ minden n természetes számra.
(4) $a \cdot (1/b) = a/b \succ 0$ minden a, b természetes számra.
(5) $0 \succ -(a/b)$ minden a, b természetes számra.

5. **a)** *Legyen p páratlan prímszám. Hány eleme írható fel $\mathbb{Z}_p$-nek x^2 alakban?*
b) *Igazoljuk, hogy $\mathbb{Z}_p$-ben a -1 felírható $x^2 + y^2$ alakban.*

Megoldás. a) A nem nulla elemekre igaz, hogy $a^2 = (-a)^2$ $\mathbb{Z}_p$-ben, tovább', ha $a^2 = b^2$, akkor $a = b$ vagy $a = -b$ (hiszen $a^2 - b^2 = (a - b)(a + b)$ pontosan akkor 0, ha valamelyik tényező nulla (p prím, így $\mathbb{Z}_p$ test, tehát nulosztómentes). Ez p páratlan prím volta miatt azt jelenti, hogy a $\mathbb{Z}_p$ nem nulla elemei párba rendezhetők (összesen $\frac{p-1}{2}$ pár), amelyek ugyanazt a n;egyzetet adják, és ezek a négyzetek mind különbözők (és egyikük sem 0). Mivel $0^2 = 0$ is négyzetszám, ezért összesen $\frac{p+1}{2}$ darab négyzetszámunk van.

b) Az $x^2 + y^2 = -1$ egyenlet ekvivalens az $x^2 + 1 = -y^2$ egyenlettel. az a) rész alapján a bal oldalnak $\frac{p+1}{2}$ lehetséges értéke van, s ugyanez igaz a jobb oldalra is. A skatulyaelv alapján, mivel $\mathbb{Z}_p$-nek csak p darab különböző eleme van, a két halmaznak van közös eleme.

6. *Igazoljuk, hogy a $2x^3+6x^2+24x+120$ polinom irreducibilis $\mathbb{Q}$ fölött. Irreducibilis-e $\mathbb{R}$, illetve $\mathbb{Z}$ fölött?*

Megoldás. A $\mathbb{Q}$ fölötti irreducilitáshoz használhatjuk a Schönemann–Eisenstein-kritériumot: $p=3$ olyan prímszám, ami nem osztja a főegyüttható, osztja az összes többi együtthatót, és $p^2=9$ nem osztja a polinom konstans tagját. (*Megjegyzés:* Mivel a polinom harmadfokú, alkalmazhatnánk a racionális gyöktesztet is: olyan a/b alakú racionális számokat kellene behelyettesíteni a polinomba próbaképpen, amelyekre $a\,|\,120$ és $b\,|\,2$. Igaz, ez jelen esetben kicsit fárasztó, mivel a konstans tag elég nagy, és sok osztója van; egy kicsit segít, hogy csak a negatív a/b értékeket kell kipróbálni, mivel a polinomnak minden együtthatója pozitív.) Azt viszont tudjuk, hogy harmadfokú valós polinomnak mindenképpen van gyöke, tehát a polinom nem lehet irreducibilis $\mathbb{R}[x]$-ben. És nem irreducibilis $\mathbb{Z}[x]$-ben sem, mert az együtthatók mind párosak, tehát $2x^3+6x^2+24x+120=2(x^3+3x^2+212x+60)$, ami $\mathbb{Z}[x]$ ben nem triviális faktorizációnak számít. (Vegyük észre, hogy $\mathbb{Q}[x]$-ben 2 egység, és ezért az előbb fölírt faktorizáció $\mathbb{Q}[x]$-ben triviális.)

7. *Mutassunk példát olyan egész együtthatós polinomra, mely egy alkalmas prímszámmal teljesíti a Schönemann–Eisenstein kritérium feltételeit, de nem irreducibilis $\mathbb{Z}$ fölött.*

Megoldás. Pl. $2x+6$ nem irreducibilis $\mathbb{Z}[x]$-ben (mert $2x+6=2(x+3)$), de $p=3$-mal teljesíti a Schönemann–Eisenstein-kritérium feltételeit.

8. *Adjunk meg olyan n egész számot, amelyre $x^4+nx+12$ irreducibilis $\mathbb{Q}$ fölött, és olyat is, amelyre nem az.*

Megoldás. Az irreducibilitást legkönnyebb – ha lehetséges – a Schönemann–Eisenstein-kritériummal kierőszakolni, ahhoz pedig megfelelő prímet kell keresni. Mivel a konstans tag $12=2^4=3$, ezért csak a 3 jöhet szóba: a 2 nem jó, mert $2^2\,|\,12$, a 3-on kívül másik prím pedig nem működhet, mert a konstans tag nem lenne vele osztható. Így ha $3\,|\,n$, akkor a polinom irreducibilis $\mathbb{Q}$ fölött. – A reducibilitás eléréséhez csábító lehetőség, hogy abban bízzunk az előbbiek alapján, hogy ha $3\nmid n$, akkor a polinom nem irreducibilis. Ilyenkor ugyanis nem alkalmazható az előbbi kritérium. Sajnos, **a Schönemann–Eisenstein-kritérium nem megfordítható!** Ugyanakkor könnyen el tudjuk érni, hogy a polinomnak legyen gyöke: $n=13$-ra az $x=-1$ lesz gyök; $n=14$-re az $x=-2$ lesz gyök stb. (Nagyon sok gyökben ne reménykedjünk a racionális gyökteszt miatt!). Ha viszont van $\alpha\in\mathbb{Q}$ gyöke a polinomnak, akkor az $(x-\alpha)$ gyöktényező kiemelhető a polinomból, azaz a polinomunk nem lesz irreducibilis.

9. **a)** *Írjuk fel a $\frac{2}{3}x^2-\frac{4}{5}x+\frac{8}{15}$ polinomot egy racionális szám és egy primitív polinom szorzataként.*
b) *Igazoljuk, hogy minden nullától különböző racionális együtthatós polinom felírható egy racionális szám és egy primitív polinom szorzataként, valamint ha $r_1g_1=r_2g_2$ két különböző ilyen felírás, akkor $r_2=-r_1$ és $g_2=-g_1$.*

Megoldás. a) $\frac{2}{3}x^2-\frac{4}{5}x+\frac{8}{15}=\frac{10}{15}x^2-\frac{12}{15}x+\frac{8}{15}=\frac{2}{15}\cdot(5x^2-6x+4)$.
b) A fölírhatóság nyilvánvaló: emeljük ki az együtthatókban szereplő nevezők legkisebb közös többszörösének reciprokát, majd az így maradó egész együtthatós polinom együtthatóinak legnagyobb közös osztóját: ami marad, az egy primitív egész együtthatós polinom, az elején szorozva két egész szám hányadosával. Azt kell még igazolnunk, hogy a fölírás lényegében egyértelmű. Ehhez az $r_1g_1=r_2g_2$ egyenlőségben szorozzunk át r_2 reciprokával ($r_2=0$ nyilván nem lehetséges, mivel kikötöttük, hogy a kiinduló polinom nem nulla). Azt kapjuk, hogy $(r_1/r_2)g_1=g_2$, és itt g_2 egész együtthatós. Mivel g_1 primitív, az $(r_1/r_2)g_1$ polinom csak úgy lehet egész együtthatós, ha r_1/r_2 egész szám. Ugyanakkor g_2 primitív is, aminek az együtthatói relatív prímek egymáshoz, tehát r_1/r_2 csak ±1 lehet.

10. **a)** *Az $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ polinomhoz, ahol a_n és a_0 nem nulla, rendeljük hozzá az $f^*(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ polinomot. Igazoljuk, hogy ez a hozzárendelés művelettartó a szorzásra nézve.*
b) *Igazoljuk a Schönemann–Eisenstein kritérium következő 'fordított' változatát. Ha az*

$$f=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Z}[x]$$

polinomhoz létezik olyan p prímszám, hogy p nem osztója a konstans tagnak, p osztója az összes többi együtthatónak, de p^2 nem osztója a főegyütthatónak, akkor f irreducibilis $\mathbb{Q}$ fölött.
c) *Igazoljuk, hogy a $20x^4-30x^2+10x-21$ polinom irreducibilis $\mathbb{Q}$ fölött.*

Megoldás. a) Vegyük észre, hogy $f^*(x)=x^nf(\frac{1}{x})$, ahol n a polinom foka. Ekkor ha $\deg f=n$ és $\deg g=k$, akkor $\deg(fg)=n+k$, továbbá $(fg)^*(x)=x^{n+k}(fg)(\frac{1}{x})=x^nf(\frac{1}{x})\cdot x^kg(\frac{1}{x})=f^*(x)g^*(x)$. (Itt kihasználtuk, hogy a behelyetesítés művelettatartó.)
b) A fordított kritérium azt jelenti, hogy f^*-ra teljesül az eredeti Schönemann–Eisenstein-kritérium, tehát f^* irreducibilis. Ha most létezik egy $f=gh$ fölbontás, ahol g és h nem konstans polinomok, akkor $f^*=g^*h^*$, azaz f^*-nak is lenne egy nem triviális faktorizációja (hiszen $\deg g=\deg g^*$ és $\deg h=\deg h^*$). Ez pedig nem lehetséges.
c) A b) részben szereplő fordított kritériumot alkalmazzuk $p=5$-re.