1. *Melyek főideálgyűrűk az alábbiak közül?*

a) $\mathbb{Z}$ *b)* $\mathbb{R}$ *c)* $\mathbb{Z}[x]$ *d)* $\mathbb{R}[x]$ *e)* $\mathbb{Z}[i]$

Megoldás: $\mathbb{Z}$, $\mathbb{R}[x]$ és $\mathbb{Z}[i]$ igen, mert euklideszi gyűrűk is, $\mathbb{R}$ is, mert test, és így csak a $0 = (0)$ és az $\mathbb{R} = (1)$ az ideáljai. $\mathbb{Z}[x]$ viszont nem főideálgyűrű, például $(2, x)$ nem főideál.

2*. *Bizonyítsuk be, hogy* $K[x_1, \ldots, x_n]$*-ben (ahol* K *test), az* $(x_1, \ldots, x_n)$ *ideál nem generálható* n*-nél kevesebb elemmel.*

Megoldás: Legyen $R = K[x_1, \ldots, x_n]$, $I = (x_1, \ldots, x_n)$, és $J = (x_i x_j \mid 1 \leq i, j \leq n)$. Ekkor I/J-nek reprezentáns rendszerét alkotják az $x_1, \ldots, x_n$ változók lineáris kombinációi. Tehát I/J vektortér az összeadásra és a konstans polinomokkal mint skalárokkal való szorzásra nézve, és ennek bázisa az $\{ x_1, \ldots, x_n \}$ (függetlenek, mert semelyik nemtriviális lineáris kombinációjuk nem lehet I eleme). R/J-nek az I/J-be eső ideáljai éppen a vektortér alterei, ugyanis egy I-beli polinom R-belivel való szorzata a faktorgyűrűben ugyanaz, mintha csak a második polinom konstans tagjával szoroznánk meg (minden más tag J-beli). I/J-nek mint vektortérnek n elemű a minimális generátorrendszere, így I/J-nek mint R/J-beli ideálnak is. De ha I-t kevesebb elemmel lehetne generálni, akkor az annak megfelelő mellékosztályok generálnák I/J-t is, tehát I sem generálható n-nél kevesebb elemmel.

3. *Mik az irreducibilis és a prím elemek a páros egészek gyűrűjében,* $2\mathbb{Z}$*-ben? Határozzuk meg* $2\mathbb{Z}$ *ideáljait és főideáljait.*

Megoldás: Az irreducibilisek a 4-gyel nem osztható páros számok, prímek viszont nincsenek, mert tetszőleges $a \in 2\mathbb{Z}$-re $a \mid 2a$, de $a \nmid 2$, és $a \nmid a$. Ideál minden additív részcsoport, ugyanis az gyűrűelemmel való szorzás ismételt összeadással, illetve kivonással megvalósítható. Így az ideálok megegyeznek $\mathbb{Z}$-nek a $2\mathbb{Z}$-be eső ideáljaival: $m\mathbb{Z}$ páros m-ekre, és ezek főideálok is.

4. *Mutassuk meg:*

a) $\mathbb{Z}[\sqrt{d}]$ *elemei (ahol* $d \in \mathbb{Z}$ *nem négyzetszám) egyértelműen írhatók* $a + b\sqrt{d}$ *alakban, ahol* $a, b \in \mathbb{Z}$*;*

b) az $N(a + b\sqrt{d}) = a^2 - b^2 d$ *norma multiplikatív;*

c) $z, u \in \mathbb{Z}[\sqrt{d}]$*-re* $z \mid u \Rightarrow N(z) \mid N(u)$*;*

d) $\mathbb{Z}[\sqrt{d}]$*-ben* z *egység* $\Leftrightarrow N(z) = \pm 1$*.*

Megoldás: a) Ha $a + b\sqrt{d} = a' + b'\sqrt{d}$, és $b \neq b'$, akkor $d = ((a - a')/(b' - b))^2$ egy racionális szám négyzete, másrészt d egész, tehát akkor d egy egész négyzetszám lenne, ellentmondva a feltételeknek. Így $b = b'$, amiből $a = a'$ is következik. Vegyük észre, hogy az előző bizonyítás akkor is működik, ha a a, b együtthatókat $\mathbb{Q}$-ból vesszük, tehát meg $\mathbb{Q}[\sqrt{d}]$-ben is egyértelmű a fölírás.

b) Ha az $u = a + b\sqrt{d}$-re az $\tilde{u} = a - b\sqrt{d}$ jelölést használjuk, akkor $N(u) = u\tilde{u}$, továbbá $\widetilde{uu'} = \tilde{u}\tilde{u'}$, ugyanis $u = a + b\sqrt{d}$-re és $u' = a' + b'\sqrt{d}$-re $uu' = aa' + bb'd + (ab' + ba')\sqrt{d}$, így $\widetilde{uu'} = aa' + bb'd - (ab' + ba')\sqrt{d} = (a - b\sqrt{d})(a' - b'\sqrt{d}) = \tilde{u}\tilde{u'}$. Így $N(uu') = uu'\widetilde{uu'} = uu'\tilde{u}\tilde{u'} = u\tilde{u}u'\tilde{u'} = N(u)N(u')$.

c) $z \mid u \Rightarrow \exists v : \; u = zv \Rightarrow N(u) = N(z)N(v) \Rightarrow N(z) \mid N(v)$.

d) z egység $\Leftrightarrow$ $z \mid 1$. Ha $z \mid 1$, akkor c) miatt $N(z) \mid N(1) = 1$, így $N(z) = \pm 1$. Ha $N(z) = \pm 1$, akkor $z\tilde{z} = \pm 1$, azaz z inverze $\tilde{z}$, vagy $-\tilde{z}$, tehát z mindenképpen invertálható.

5. *Bontsuk fel prímek szorzatára a* 7, 13 *és* $5 + i$ *számokat* $\mathbb{Z}[i]$*-ben! Hány egymással nem asszociált prím faktora van* $2 + 2i$*-nek?*

Megoldás: A 4. feladat állításaiból következik, hogy ha $N(z)$ prím, akkor z irreducibilis (ui. $N(z)$ minden $N(u)N(v)$ felbontásában az egyik tényező ± 1), ha pedig $N(z) = pq$ valamely p és q nem feltétlenül különböző prímekre, akkor z csak akkor lehet reducibilis, ha p és q vagy $-p$ és $-q$ előállhat normaként. Speciálisan a Gauss-egészek körében $p \in \mathbb{N}$ prímszám Gauss-prím, ha $p \equiv 3 \pmod 4$, mert $N(p) = p^2$, és p nem áll elő két négyzetszám öszegeként, azaz normaként. Tehát 7 Gauss prím, 13-nak pedig az irreducibilisekre való felbontása: $(2 + 3i)(2 - 3i)$ a $13 = 2^2 + 3^2$ előállításból. $N(5 + i) = 26 = 2 \cdot 13$ felbontása miatt az asszociáltság erejéig egyetlen 2 normájú Gauss-egész, $1+i$ kell, hogy osztója legyen $5 + i$-nek, és komplex osztással azt kapjuk, hogy $(5 + i)/(1 + i) = (5 + i)(1 - i)/2 = 3 - 2i$, tehát $5+i = (1+i)(3-2i)$ irreducibilisekre bontás. $2+2i = 2(1+i) = (1+i)(1-i)(1+i) = -i(1 + i)^3$, tehát asszociáltaktól eltekintve egyetlen prím faktora van $2 + 2i$-nek.

6. *Legyen* $R = \mathbb{Z}[\sqrt{-5}]$*. Adjuk meg* 6*-nak két (lényegesen) különböző, irreducibilis elemekre való felbontását* R*-ben.*

Megoldás: $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$. Mindegyik felbontásban irreducibilisek a faktorok, ugyanis sem 2, sem 3 nem áll elő $a^2 + 5b^2$ alakban, és így a szereplő faktorok normái: 6, 4, illetve 9 nem bonthatók fel két nem egység norma szorzatára. (Megjegyzés: Ez példa arra, hogy egy R-ben nem minden irreducibilis elem prím, például a 2 ilyen.)

7. *Lássuk be, hogy ha* $\mathbb{Z}[\sqrt{d}]$ *UFD (ahol* d *nem négyzetszám), akkor* 2 *nem irreducibilis* $\mathbb{Z}[\sqrt{d}]$*-ben.*

Megoldás: Ha R UFD, akkor minden irreducibilis elem prím is (a másik irányú következtetés igaz minden integritási tartományban), ugyanis ha p irred., és $p \mid uv = q_1 \cdots q_r$, ahol a $q_1, \ldots, q_r$ irreducibiliseket az u és v felbontásából kaptuk, akkor van olyan w, amellyel $pw = q_1 \cdots q_r$. A felbonthatóság miatt a w elem $p_2 \cdots p_s$ alakban írható, így $pp_2 \cdots p_s = q_1 \cdots q_r$, és ekkor az egyértelműségből következik, hogy p asszociált valamelyik q_i-vel, így osztója u-nak vagy v-nek. Tehát elég bebizonyítani, hogy 2 nem prím. Valóban, ha $2 \nmid d$, akkor $2 \mid 1 - d^2 = (1 + \sqrt{d})(1 - \sqrt{d})$, de $(1 \pm \sqrt{d})/2 = \frac{1}{2} \pm \frac{1}{2}\sqrt{d} \notin \mathbb{Z}[\sqrt{d}]$ a $\mathbb{Q}$ fölötti egyértelmű fölírás miatt, és így $2 \nmid (1 \pm \sqrt{d})$. Hasonlóan látható, hogy $2 \mid d$ esetén $2 \mid 4 + d^2 = (2 + \sqrt{d})(2 - \sqrt{d})$, de $2 \nmid 2 \pm \sqrt{d}$.

8. *Tegyük föl, hogy* $d \in \mathbb{Z}$ *négyzetmentes. Lássuk be, hogy*

a) $d < 0$ *esetén* $\mathbb{Z}[\sqrt{d}]$ *UFD* $\Leftrightarrow$ $d = -1$ *vagy* -2*.*

b) $d \equiv 1 \ (\pmod 4) \Rightarrow \mathbb{Z}[\sqrt{d}]$ *nem UFD.*

Megoldás: a) Ha $d \leq -3$, akkor $N(u) = a^2 + (-d)b^2 \geq 3$ minden olyan esetben, amikor $u \notin \mathbb{Z}$, tehát ilyen elemek normájaként nem állhat elő a 2 (és természetesen -2 sem), a $\mathbb{Z}$-beli számok normája pedig négyzetszám, tehát ± 2 egyáltalán nem lehet norma, és így az 5. feladat megoldásának elején szereplő általános tulajdonság miatt 2 irreducibilis, tehát a 7. feladat állítása miatt $\mathbb{Z}[\sqrt{d}]$ nem lehet UFD. A $d = -1, -2$ esetekben láttuk az előadáson, hogy $\mathbb{Z}[\sqrt{d}]$ euklideszi gyűrű, így UFD is.

b) Ebben az esetben is be tudjuk látni, hogy 2 és -2 nem lehet norma, ugyanis $a^2-b^2d \equiv a^2-b^2 \equiv 0,1$ vagy $-1 \pmod 4$, így nem lehet 2.

9. *Tegyük föl, hogy az S test részgyűrűje az R egységelemes gyűrűnek, és $1 \in S$. Lássuk be, hogy ekkor R vektortér S fölött, és így véges R esetén $|R| = |S|^n$ valamely $n \in \mathbb{N}$-re!*

Megoldás: Minthogy R gyűrű, az összeadásra nézve Abel-csoportot alkot. Az S-beli elemekkel való szorzás értelmezve van az R gyűrűben, és az erre vonatkozó vektortéraxiómák következnek a szorzás asszociativitásából, a disztributivitásból, illetve abból, hogy az S test egységeleme az R gyűrűnek is egységeleme. Ha R véges, akkor van S fölött egy véges bázisa: $\{ b_1, \ldots, b_n \}$, és a koordinátavektorok száma (ami megegyezik a vektortér vektorai számával) éppen $|S|^n$.

10. *Bizonyítsuk be, hogy ha $I, J \lhd R$-re $R = I + J$, akkor $R/(I \cap J) \cong R/I \oplus R/J$.*

Megoldás: 1. változat: $\bar{R} = R/I \cap J$-ben $\bar{I} = I/I \cap J$-re és $\bar{J} = J/I \cap J$-re az 1. izomorfizmustétel szerint $\bar{I} \cong (I+J)/J = R/J$ és $\bar{J} \cong (I+J)/I = R/I$, továbbá $\bar{I} \cap \bar{J} \leq \overline{I \cap J} = 0$ és $\bar{I} + \bar{J} = R$, tehát $\bar{R}$ az $\bar{I}$ és $\bar{j}$ ideáljainak direkt összege, és ez éppen a bizonyítandó összefüggést adja.

2. változat: Definiáljuk a $\varphi : R \to R/I \oplus R/J$ leképezést a $\varphi(r) = (r+I, r+J)$ egyenlőséggel. Ez nyilván művelettartó, és $\operatorname{Ker}\varphi = \{ r \,|\, r+I = I,\ r+J = J \} = \{ r \,|\, r \in I,\ r \in J \} = I \cap J$. Belátjuk, hogy φ szürjektív. Legyen ugyanis $(a+I, b+J)$ tetszőleges elem $R/I \oplus R/J$-ben. Az $R = I + J$ feltétel miatt van olyan $i \in I$ és $j \in J$, hogy $a - b = i + j$. Így $a + I = (a-i) + I = (b+j) + I$, és $b + J = (b+j) + J$, tehát $r = b + j$-re $(a+I, b+J) = (r+I, r+J) = \varphi(r)$. A homomorfizmustételből következik, hogy $R/I \cap J = R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = R/I \oplus R/J$.

11. *Legyen $f(x) \in \mathbb{Q}[x]$, és tegyük fel, hogy f-nek nincs többszörös gyöke $\mathbb{C}$-ben. Bizonyítsuk be, hogy $\mathbb{Q}[x]/(f(x))$ testek direkt összege.*

Megoldás: Az állítást $f(x)$ irreducibilis faktoraira vonatkozó teljes indukcióval bizonyítjuk. Ha $f(x)$ irreducibilis, akkor tudjuk, hogy $\mathbb{Q}[x]/((f(x))$ test. Tegyük fel most, hogy $f(x) = g(x)h(x)$, ahol $g(x)$ és $h(x)$ nem konstans. A $g(x)$ és $f(x)$ polinomok relatív prímek $\mathbb{Q}[x]$-ben, ugyanis ha lenne nem triviális közös osztójuk, akkor annak egy komplex gyöke $g(x)$-nek és $h(x)$-nek is gyöke lenne, így $f(x)$-nek legalább kétszeres gyöke volna. A $g(x)$ és $h(x)$ relatív prím voltából következik, hogy vannak olyan $a(x)$ és $b(x)$ polinomok $\mathbb{Q}[x]$-ben, amelyekkel $a(x)g(x) + b(x)h(x) = 1$, tehát az $I = (g(x))$ és $J = (h(x))$ ideálokra $I + J = \mathbb{Q}[x]$. Másrészt $I \cap J$ a $g(x)$ és $h(x)$ közös többszöröseiből áll, és mivel ezek relatív prímek, $I \cap J$ éppen az $f(x) = g(x)h(x)$ többszöröseit tartalmazza, azaz $I \cap J = (f(x))$. Tehát a 10. feladat szerint $\mathbb{Q}[x]/(f(x)) \cong \mathbb{Q}[x]/(g(x)) \oplus \mathbb{Q}[x]/(h(x))$, és az utóbbi két faktorgyűrű az indukciós feltevés miatt testek direkt összege, tehát $\mathbb{Q}[x]/(f(x))$ is az.

Hf1. *Legyen $R = A \oplus B$, $K \lhd R$, $1 \in R$. Bizonyítsuk be, hogy $K = K \cap A \oplus K \cap B$.*

Hf2. *Lássuk be, hogy egy R egységelemes integritási tartományban $a \in R$ akkor és csak akkor prím tulajdonságú, ha az $R/(a)$ faktorgyűrű nullosztómentes.*

Hf3. *Adjuk meg $\mathbb{Z}[i]$-ben a $2 + 6i$ szám irreducibilis elemekre való fölbontását! Az asszociált prímtényezőket vonjuk össze egy hatványba!*

A házi feladatok beadási határideje: május 9.