1. *Bizonyítsuk be, hogy ha $R = 2\mathbb{Z}$, és $R_1 = \{(a,m) \mid a \in R,\ m \in \mathbb{Z}\}$ az R egységelemes gyűrűvé való szokásos kiterjesztése, akkor R nem izomorf $\mathbb{Z}$-vel.*

Megoldás: $\mathbb{Z}$ minden valódi faktorgyűrűje véges, viszont R_1-ben $\{(a,0) \mid a \in R\} \cong R$ olyan nem nulla ideál, amelyre $R_1/R \cong \mathbb{Z}$ végtelen.

2. *Mi a páros egészek gyűrűjének, $2\mathbb{Z}$-nek a hányadosteste?*

Megoldás: $\mathbb{Q}$ test, tartalmazza $2\mathbb{Z}$-t, és minden eleme előáll $(2a)/(2b)$ alakban, tehát a hányadostest egyértelműsége miatt csak $\mathbb{Q}$ lehet a hányadostest.

3. *Bizonyítsuk be, hogy minden véges integritási tartomány test.*

Megoldás: Legyen R véges, kommutatív, nullosztómentes gyűrű. Ekkor minden $0 \neq r \in R$-re az $x \mapsto xr$ leképezés injektív ($xr = yr \Rightarrow (x-y)r = 0 \Rightarrow x - y = 0$), tehát R végessége miatt bijektív is. Ebből következik, hogy van olyan e, amelyre $er = r$, és akkor minden s-re $ser = sr$, amiből a nullosztómentesség miatt $se = s$ következik, és a kommutativitás miatt $es = s$ is igaz minden s-re, azaz e egységelem. Továbbá $0 \neq r$-re van olyan x, amelyre $xr = e$, tehát r-nek van multiplikatív (a kommutativitás miatt kétoldali) inverze is.

4. *Határozzuk meg az alábbi integritási tartományok hányadostestét, maximális ideáljait, és azokat a homomorf képeit, amelyek testek!*

a) $\mathbb{Z}$ *b)* $K[x]$*, ahol* K *test* *c)* $\mathbb{Z}[x]$ *d)* $\mathbb{Z}[i]$

Megoldás: A hányadostestek $\mathbb{Q}$, $K(x)$ (a K fölötti racionális törtfüggvények teste), $\mathbb{Q}(x)$ és $\mathbb{Q}(i)$. Ezek nyilván mind testek, és könnyű ellenőrizni, hogy minden elemük előáll a megadott gyűrűbeli elemek hányadosaként. A maximális ideáloknak és ezek faktorainak leírása:

a) $\mathbb{Z}$ főideálgyűrű, tehát minden ideálja valamely $n \in \mathbb{Z}$ szám többszöröseiből áll. Ezek között pedig nyilván azok maximálisak, amelyeket egy prímszám generál. A hányadosgyűrű itt bármely $\mathbb{F}_p$ test lehet.

b) Az előbbihez hasonlóan itt is főideálgyűrűről van szó, és a maximális ideálok azok, amelyeket irreducibilis polinom generál. Hányadosgyűrűként megkapjuk K összes egyszerű, algebrai testbővítését.

c) Nyilvánvaló, hogy $\mathbb{Z}[x]$-nek homomorf képe minden $\mathbb{F}_p[x]$ gyűrű, tehát a b) rész szerint ennek a maximális ideálokkal vett faktorai, azaz a véges testek előállnak $\mathbb{Z}[x]$ maximális ideállal vett faktorgyűrűiként. Belátjuk, hogy más nem is lehet, azaz $\mathbb{Z}[x]$ minden nem triviális ideáljában van $p \in \mathbb{Z}$ prím, és így az ideál $(p, f(x))$ alakú, ahol $f(x)$ irreducibilis mint $\mathbb{F}_p$ fölötti polinom.
Legyen $R = \mathbb{Z}[x]$, és $I \lhd R$ maximális ideál. Ha $I \cap \mathbb{Z} \neq 0$, akkor az R/I test véges karakterisztikájú, tehát a karakterisztikája valamely p prím, és így $p \in I$ is igaz. Most tegyük föl, hogy $I \cap \mathbb{Z} = 0$, és legyen $J = I\mathbb{Q}[x]$ az I által $\mathbb{Q}[x]$-ben generált ideál. Ez az ideál nem lehet a teljes polinomgyűrű, mert akkor lennének olyan $f_i(x) \in I$ és $g_i(x) \in \mathbb{Q}[x]$ polinomok, hogy $\sum f_i(x)g_i(x) = 1$, de akkor alkalmas $n \in \mathbb{Z}$ számra $ng_i(x) \in \mathbb{Z}[x]$ minden i-re, és így $n = \sum f_i(x)(ng_i(x)) \in I$, ellentmondva a feltevésünknek. Viszont $\mathbb{Q}[x]$ főideálgyűrű, így $J = g(x)\mathbb{Q}[x]$ valamely $g(x) \in \mathbb{Q}[x]$-re, sőt föltehető, hogy $g(x) \in \mathbb{Z}[x]$ primitív polinom. $I \subseteq J = g(x)\mathbb{Q}[x]$, tehát minden $f(x)$ polinomra van olyan $h(x) \in \mathbb{Q}[x]$, hogy $f(x) = g(x)h(x)$. Mivel $g(x)$ primitív polinom, ebből következik, hogy $h(x) \in \mathbb{Z}[x]$, vagyis $I = g(x)\mathbb{Z}[x]$ főideál. Valamilyen p prímre $g(x)$-nek van egy $a \in \mathbb{Z}$ gyöke modulo p (elég, ha választunk egy olyan $a \in \mathbb{Z}$ számot,

amelyre $g(a) \neq 0, \pm 1$, és p $g(a)$-nak egy prímosztója), így $g(x) \in (p) + ((x-a))$, és ez az ideál valódi ideálja $\mathbb{Z}[x]$-nek, ugyanis $\mathbb{F}_p[x]$-ben $((x-a))$ valódi ideál. Tehát I maximalitása miatt $I = (p) + ((x-a))$, de ez ellentmond annak, hogy $I \cap \mathbb{Z} = 0$.

d) $\mathbb{Z}[i]$ a Gauss-egészek gyűrűje, és ez is euklideszi, tehát főideálgyűrű, mint az a) és b) részbeli példák. Következésképpen a Gauss-prímek által generált főideálok lesznek a maximális ideáljai. Ha ez a Gauss-prím $\mathbb{Z}$-beli, $p = 4k+3$ alakú prím, akkor a faktorgyűrű p^2-elemű test (a mellékosztályoknak reprezentánsrendszere az $\{\, x+yi \mid 0 \leq x, y \leq p-1 \,\}$ halmaz). Ha viszont u olyan Gauss-prím, amelynek normája $p = 4k+1$ alakú prím, akkor is benne van az ideálban a $p = u\bar{u}$ szám, de van benne olyan is — például maga u —, amely nem többszöröse p-nek, így a faktorgyűrű olyan p karakterisztikájú test, amely p^2-nél kisebb elemszámú, igy izomorf $\mathbb{F}_p$-vel.

5. *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 a 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.

6. *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 még $\mathbb{Q}[\sqrt{d}]$-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, és így egység.

7. *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.

8. *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.)

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

Megoldás: Ha R UFD (alaptételes), 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 $2 \nmid 2 \pm \sqrt{d}$.

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

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

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

Megoldás: a) Használjuk az $n = -d > 0$ jelölést! Az $n = 1$ és $n = 2$ esetben belátjuk, hogy a gyűrű euklideszi, tehát teljesül rá a számelmélet alaptétele. Ugyanis, ha az $a, b \in R = \mathbb{Z}[\sqrt{-n}]$ számokhoz keresünk olyan $q, r \in R$ számot, amelyre $a = bq + r$, és $N(r) < N(b)$, akkor a b és $bi\sqrt{n}$ vektorok által definiált téglalaprácson kell megkeresni azt a bq rácspontot, amelyik a legközelebb van a-hoz, és ez még akkor is, ha a egy téglalap közepére esik, legföljebb $|b|\sqrt{\frac{1}{4} + \frac{d}{4}} \leq |b|\sqrt{\frac{3}{4}} < |b|$ távolságra van a rácspontoktól, így $|r| < |b|$, azaz $N(r) < N(b)$. Ha viszont $n \geq 3$, akkor a 9. feladat eredményét használhatjuk: 2 csak irreducibilis lehet, mivel 2 nem áll elő $x^2 + y^2 n$ alakban ($x, y \in \mathbb{Z}$-re), tehát az $N(2) = 4$ norma csak $1 \cdot 4$ alakban bontható fel két norma szorzatára. Ebből következik, hogy $\mathbb{Z}[\sqrt{-n}]$ nem alaptételes.

b) A $d < -3$ esethez hasonlóan a $d \equiv 1 \pmod 4$ esetben is azt tudjuk megmutatni, hogy 2 nem áll elő $\mathbb{Z}[\sqrt{d}]$-beli elem normájaként. Ugyanis $N(x + y\sqrt{d}) = x^2 - dy^2 \equiv x^2 - y^2 \not\equiv 1 \pmod 4$. Ebből itt is következik, hogy 2 irreducibilis, és így $\mathbb{Z}[\sqrt{d}]$ nem alaptételes.

Hf1. *Gyökjelekkel felírhatók-e, illetve a komplex számsíkon (a tengelyek és az 1-hez tartozó pont ismeretében) megszerkeszthetők-e az* $f(x) = x^6 - 4x^4 + 6x^2 + 2$ *polinom gyökei?*

Hf2. *Legyen* R *egységelemes kommutatív gyűrű. Bizonyítsuk be, hogy ha* $I, J \triangleleft R$*, és* $I + J = R$*, akkor* $IJ = I \cap J$*.*

Hf3. *Legyen* $R = \mathbb{Z}[x]$*, és* I *a* 2 *és* x^2 *által generált ideál* R*-ben. Bizonyítsuk be, hogy az* R/I *faktorgyűrű* 4 *elemű, és lássuk be, hogy* R/I *multiplikatív félcsoportja izomorf* $\mathbb{Z}_4$ *multiplikatív félcsoportjával.*