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

Megoldás: Mindegyiknek van (egyetlen) egységeleme, de $\mathbb{Z}$ additív csoportját generálja az egységelem, R_1 additív csoportjában az egységelem generátuma csak az $\{(m, 0) \,|\, m \in \mathbb{Z}\}$ részcsoport.

2. *Legyen R véges gyűrű, és n az $(R, +)$ véges Abel-csoport elemeinek maximális rendje. Definiáljuk az $R_{(1)}$ gyűrűt mint a $\mathbb{Z}_n \times R$ Descartes-szorzatot az*

$$(i, r) + (j, s) = (i + j,\ r + s), \qquad (i, r)(j, s) = (ij,\ is + jr + rs)$$

műveletekkel. Bizonyítsuk be, hogy $R_{(1)}$ olyan véges, egységelemes gyűrű, amelybe R ideálként beágyazható. Lássuk be, hogy ha R zérógyűrű, amelyre $1 < |R| < \infty$, akkor ez a lehető legkisebb egységelemes bővítése R-nek (még úgy is, ha R-et csak részgyűrűként kell beágyazni).

Megoldás: Vegyük észre, hogy $nr = 0$ minden $r \in R$-re, ugyanis ha az $|R|$ prímosztóira n_p a maximális olyan p-hatvány, amilyen rendű ciklikus csoport szerepel az $(R, +)$ kanonikus felbontásában, akkor n a p^{n_p} hatványok szorzata, ugyanis a csoportnak van $\prod_p C_{p^{n_p}} \cong C_n$ részcsoportja, azaz van n-edrendű eleme, és mivel minden ciklikus komponens rendje osztója n-nek, $nr = 0$ is igaz minden $r \in R$-re.
Tekintsük az R_1 szokásos egységelemes kiterjesztést erre az R gyűrűre. Ebben $I := \{(mn, 0) \,|\, m \in \mathbb{Z}\}$ ideál, ugyanis nem üres, ilyenek összege és különbsége nyilván ilyen, és ha megszorozzuk egy (k, a) elemmel, akkor a szorzat

$$(k, a)(mn, 0) = (kmn,\ k0 + mna + a0) = (kmn, 0) \in I \text{ és}$$

$$(mn, 0)(k, a) = (mnk,\ mna + k0 + 0a)(mkn, 0) \in I,$$

mert R-ben minden elem n-szerese 0. Könnyen látható, hogy R_1/I éppen az itt definiált $R_{(1)}$ gyűrűt adja: I minden mellékosztályában pontosan egy (i, r) alakú elem van, ahol $i \in \{0, \ldots, n-1\}$, és a mellékosztályok közötti műveletek megfelelnek a feladatban definiáltaknak.
Legyen R zérógyűrű, $1 < |R| < \infty$, n az $(R, +)$ elemeinek maximális rendje, és tegyük fel, hogy egy S egységelemes gyűrű tartalmazza R-et. Ekkor $0 < k < n$-re $k1 \notin R$, mert különben $kr = k1 \cdot r = 0$ minden $r \in R$-re, ellentmondva annak, hogy n a maximális elemrend. De akkor a $k1 + r$ $(0 \le k \le n-1,\ r \in R)$ elemek mind különbözők, így $|S| \ge n|R| = |R_{(1)}|$.

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

Megoldás: $2\mathbb{Z} \le \mathbb{Q}$ test, és minden eleme előáll páros egészek hányadosaként, tehát $\mathbb{Q}$ a hányadostest.

4. *Határozzuk meg $K^{n\times n}$ jobb- és balideáljait.*

Megoldás: Vegyük észre először, hogy tetszőleges $V \le K^n$ altérre azok a mátrixok, amelyeknek az oszloptere V-ben van, jobbideált alkotnak (jelöljük az ilyen mátrixok halmazát $\mathcal{O}_V$-vel), ugyanis $0 \in \mathcal{O}_V$, és ha $A, B \in \mathcal{O}_V$ és $C \in K^{n\times n}$ tetszőleges, akkor $\mathcal{O}(A - B) \le \mathcal{O}(A) + \mathcal{O}(B) \le V$, és $\mathcal{O}(AC) \le \mathcal{O}(A) \le V$.
Másrészt beláthatjuk, hogy $K^{n\times n}$ minden jobbideálja ilyen alakú. Legyen ugyanis J jobbideál, és álljon V a J-beli mátrixok első oszlopaiból. Ez altér, mert nem üres, és

$A_{*1} + \lambda B_{*1} = (A + \lambda B)_{*1}$ (M_{*i}-vel jelölve egy M mátrix i. oszlopát).
Minden $A \in J$-re A i. oszlopa $AE_{i1} \in J$ első oszlopa, tehát $\mathcal{O}(A) \leq V$, és így $J \leq \mathcal{O}_V$.
Fordítva, ha $C \in \mathcal{O}_V$, akkor C i. oszlopa előáll valamely $A^{(i)} \in J$ mátrix első oszlopaként minden i-re, tehát $C = \sum_i A^{(i)} E_{1i} \in J$. Ezért a másik irányú $\mathcal{O}_V \leq J$ tartalmazás is igaz, vagyis $K^{n\times n}$ minden jobbideálja $\mathcal{O}_V$ alakú.

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

Megoldás: Tegyük fel, hogy R véges integritási tartomány, tehát véges, kommutatív, egységelemes, és nullosztómentes. Azt kell csak belátnunk, hogy minden nem nulla elem invertálható. Tetszőleges $0 \neq a \in R$-re a $\rho_a : R \to R$, $\rho_a : r \mapsto ra$ leképezés injektív, ugyanis $ra = sa \Rightarrow (r-s)a = 0$, de R nullosztómentes, és $a \neq 0$, így $r - s = 0$, azaz $r = s$. Mivel R véges, a ρ_a leképezésnek szürjektívnek is kell lennie, így van olyan $a' \in R$, amelyre $aa' = 1$, s mivel R kommutatív, ez azt jelenti, hogy a' inverze a-nak.

6. *Legyen K test, $p(x) \in K[x]$, n-edfokú polinom, és $R = K[x]/I$, ahol $I = (p(x)) \lhd K[x]$. Jelöljük α-val a faktorgyűrű $x + I$ elemét.*

a) Bizonyítsuk be, hogy α gyöke a $p(x)$ polinomnak, és R egyértelműen írhatók α legfeljebb $(n-1)$-edfokú polinomjaiként.

b) Alkalmazzuk az előbbi felírást az $R = K[x]/(p(x))$ faktorgyűrűre is, ahol $K = \mathbb{Z}_2$ és $p(x) = x^3 + x + 1$. Lássuk be, hogy R nyolcelemű test. Keressük meg $x^3 + x^2 + 1$ összes gyökét R-ben.

Megoldás: a) $p(\alpha) = p(x + I) = p(x) + I = I$, ami R nulleleme.
Tudjuk, hogy a legfeljebb $(n-1)$-edfokú polinomok teljes reprezentánsrendszert alkotnak a $K[x]/(p(x))$-ben, így R minden eleme előáll $r(x) + I = r(x + I) = r(\alpha)$ alakban, valamely $r(x) \in K[x]$ legfeljebb $(n-1)$-edfokú polinomra, és ez a felírás egyértelmű, mert egy mellékosztályban csak egy ilyen fokú polinom van.

b) R elemei α-nak legfeljebb másodfokú polinomjai $\mathbb{Z}_2$ fölött. Így $|R| = 2^3 = 8$. Az a) rész szerint $\alpha^3 + \alpha + 1 = 0$, azaz $\alpha^3 = \alpha + 1$. A második, $f(x) = x^3 + x^2 + 1$ polinom gyökeit $A\alpha^2 + B\alpha + C$ alakban kereshetjük, ahol A, B, C mindegyike 0 vagy 1, így a számolás során felhasználhatjuk, hogy mindegyik egyenlő önmaga négyzetével, továbbá az $\alpha^3 = \alpha + 1$ összefüggés alapján α kitevőjét is redukálhatjuk:

$$\alpha^3 = \alpha + 1, \quad \alpha^4 = \alpha^2 + \alpha, \quad \alpha^5 = \alpha^2 + \alpha + 1, \quad \alpha^6 = \alpha^2 + 1$$

$$\begin{aligned} f(A\alpha^2 + B\alpha + C) &= (A\alpha^2 + B\alpha + C)^2(A\alpha^2 + B\alpha + C + 1) + 1 = \\ &= (A\alpha^4 + B\alpha^2 + C)(A\alpha^2 + B\alpha + C + 1) + 1 = \\ &= A\alpha^6 + AB\alpha^5 + (A + AB + AC)\alpha^4 + B\alpha^3 \\ &\quad + (B + BC + AC)\alpha^2 + BC\alpha + 1 \\ &= (B + BC)\alpha^2 + (A + B + AC + BC)\alpha + (AB + A + B + 1) = \\ &= B(C+1)\alpha^2 + (A+B)(C+1)\alpha + (A+1)(B+1), \end{aligned}$$

és itt az együtthatók csak akkor lehetnek 0-k, ha $C = 1$, és A és B közül legalább az egyik 1, vagyis $f(x)$ gyökei

$$\alpha + 1, \quad \alpha^2 + 1 \quad \text{és} \quad \alpha^2 + \alpha + 1.$$

(Észrevehetjük, hogy ezek ciklikusan egymás négyzetei, és ezt a tulajdonságot a gyökök megkeresése nélkül is igazolhatjuk: ha valamely β-ra $\beta^3 + \beta^2 + 1 = 0$, akkor $\beta^6 + \beta^4 + 1 = (\beta^3 + \beta^2 + 1)^2 = 0$.)