1. *Legyen R kommutatív, egységelemes, nullosztómentes gyűrű, $r \in R$ nem nulla és nem egység. Mutassuk meg, hogy ha r prímtulajdonságú elem, akkor r felbontathatatlan, azaz minden $r = ab$ R-beli felbontás esetén a vagy b egység, azaz $a|1$ vagy $b|1$.*

Megoldás: $r \mid r \cdot 1 = ab \Rightarrow r \mid a$ vagy $r \mid b$. Tegyük fel, hogy $r \mid a$. Ekkor van olyan $x \in R$, amelyre $a = rx$, így $a = rx = abx \Rightarrow a(1 - bx) = 0$. De $a \neq 0$, mert $r \neq 0$, tehát az R nullosztómentessége miatt $1 - bx = 0$, azaz $b \mid 1$.

2. *Mutassuk meg, hogy egy racionális együtthatós, $\mathbb{Q}$ felett irreducibilis polinomnak nem lehet $\mathbb{C}$-ben többszörös gyöke.*

Megoldás: Legyen $f(x) \in \mathbb{Q}[x]$, ahol $\deg f \geq 1$. Ha f-nek van többszörös gyöke $\mathbb{C}$-ben, akkor $d(x) = (f(x), f'(x))$ nem konstans. De akkor $d(x) \mid f(x)$, tehát $f(x)$ felbonthatatlansága miatt $d(x) = cf(x)$ valamely $c \neq 0$ konstansra. Viszont $\deg d(x) \leq \deg f'(x) = \deg f(x) - 1$, ami ellentmondás.

3. *Legyenek $f_1(x), f_2(x) \in \mathbb{Z}[x]$ polinomok. Mutassuk meg mod p átmenettel, hogy ha egy p prímszám osztja $f(x) = f_1(x)f_2(x)$ minden együtthatóját, akkor vagy $f_1(x)$, vagy $f_2(x)$ minden együtthatóját osztja, azaz p $\mathbb{Z}[x]$-ben prímtulajdonságú.*

Megoldás: Legyenek $\tilde{f}(x), \tilde{f}_1(x), \tilde{f}_2(x) \in \mathbb{Z}_p[x]$ azok a polinomok, amiket f, f_1, f_2-ből kapunk, ha az együtthatóikat $\bmod p$ tekintjük. Ezekre is igaz, hogy $\tilde{f} = \tilde{f}_1\tilde{f}_2$. Tudjuk, hogy minden test fölötti polinomgyűrű nullosztómentes, tehát ha $\tilde{f}_1\tilde{f}_2 = \tilde{f} = 0$, akkor $\tilde{f}_1$ vagy $\tilde{f}_2$ nulla, ami bizonyítja az állítást.

4. *a) Bizonyítsuk be a Schönemann-Eisenstein-kritériumot mod p átmenettel.*
b) Bizonyítsuk be a fordított Schönemann-Eisenstein kritériumot mod p átmenettel.
c) Mutassuk meg, hogy ha $p(x) \in \mathbb{Z}[x]$ polinom, és $c \in \mathbb{Z}$, akkor $p(x)$ pontosan akkor irreducibilis $\mathbb{Z}$ felett, ha $p(x + c)$ az.

Megoldás: a) Schönemann–Eisentein-kritérium: Ha $f(x) = a_nx^n + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$, és valamely p prímre $p \nmid a_n$, $p \mid a_i \forall i < n$ és $p^2 \nmid a_0$, akkor $f(x)$ irreducibilis $\mathbb{Q}[x]$-ben.
Biz.: Tegyük fel, hogy f-nek van kisebb fokúak szorzatára bontása $\mathbb{Q}$ fölött. Ekkor a megfelelő konstansszorosuk $g(x), h(x) \in \mathbb{Z}[x]$, amelyre $f(x) = g(x)h(x)$. Tekintsük f, g, h-t $\mathbb{Z}_p$ fölötti polinomoknak (vegyük az együtthatókat modulo p): $\tilde{f}, \tilde{g}, \tilde{h} \in \mathbb{Z}_p[x]$ Az együtthatókra vonatkozó feltevések miatt $\tilde{f}(x) = cx^n$ alakú ($0 \neq c \in \mathbb{Z}_p$), ezért a $\mathbb{Z}_p$ test fölötti egyértelmű irreducibilisekre bontás miatt $\tilde{g}$ és $\tilde{h}$ irreducibilis faktorai is csak az x-ek lehetnek, tehát $\tilde{g}(x) = c'x^k$ és $\tilde{h}(x) = c''x^\ell$ valamely $c', c'' \in \mathbb{Z}_p \setminus \{0\}$-ra és $k, \ell > 0$-ra. Ez azt jelenti, hogy g-nek és h-nak a főegyütthatón kívül minden együtthatója osztható p-vel. De akkor f konstans tagja p^2-tel is osztható lenne, ami ellentmond a feltételeknek.

b) Fordított Schönemann–Eisenstein-kritérium: Ha $f(x) = a_nx^n + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$, és valamely p prímre $p \nmid a_0$, $p \mid a_i \forall i > 0$ és $p^2 \nmid a_n$, akkor $f(x)$ irreducibilis $\mathbb{Q}[x]$-ben.
Biz.: Ugyanúgy, mint az a) részben vegyük f-nek egy kisebb fokúak szorzatára bontását, és az ennek megfelelő $\tilde{f}(x) = \tilde{g}(x)\tilde{h}(x)$ felbontást $\mathbb{Z}_p[x]$-ben. Az oszthatósági feltételek miatt $\tilde{f} \neq 0$ konstans polinom, így $\tilde{g}$ és $\tilde{h}$ is konstans. Ez azt jelenti, hogy g és h minden nem konstans tagjának az együtthatója, köztük a főegyüttható, osztható p-vel, tehát f főegyütthatója p^2-tel is osztható, ami ellentmond a feltételeknek.

c) Ha $p(x) = g(x)h(x)$ valódi felbontás, akkor $p(x+c) = g(x+c)h(x+c)$ is az, és fordítva, ha $p(x+c) = g(x)h(x)$ valódi felbontás, akkor $p(x) = p((x-c)+c) = g(x-c)h(x-c)$ is az. Ez természetesen nemcsak egész együtthatós polinomokra működik, hanem tetszőleges test fölötti polinomokra is.

5. *Irreducibilis-e $\mathbb{Q}$ felett:*
a) $x^4 + 10x + 5$, $5x^4 + 10x + 1$;
b) $x^n + p$, *ahol* p *prím;*
c) $x^{p-1} + x^{p-2} + \cdots + x + 1$, *ha* p *prím? Mik ennek a polinomnak a gyökei?*
d) $\dfrac{x^5+1}{x+1}$?

Megoldás: a) Az elsőre a Sch.–E.-kritérium teljesül, a másodikra a fordított Sch.–E.-kritérium $p = 5$-tel, tehát irreducibilisek.

b) Ez is irreducibilis a p prímre alkalmazott Sch.–E.-kritérium miatt.

c) $f(x) = x^{p-1}+x^{p-2}+\cdots+x+1 = \dfrac{x^p-1}{x-1} \Rightarrow f(x+1) = \dfrac{(x+1)^p-1}{x} = \displaystyle\sum_{k=1}^{p}\binom{p}{k}x^{k-1}$,
és itt a főegyütthatótól eltekintve minden együttható osztható p-vel ($\binom{p}{k} = \frac{p!}{k!(p-k)!}$ számlálója osztható p-vel, de a nevezője nem, ha $0 < k < p$), a konstans tag pedig $\binom{p}{1} = p$, így a Schönemann–Eisenstein-kritérium miatt $f(x+1)$ irreducibilis, és akkor a 4. feladat c) része szerint $f(x)$ is az.

d) A c) részhez hasonlóan itt az $x-1$ helyettesítésével kapunk Sch.–E.-es polinomot ($p = 5$-tel): $\dfrac{(x-1)^5+1}{x} = x^4 - 5x^3 + 10x^2 - 10x + 5$ irreducibilis, így az eredeti polinom is az. Mellesleg, a megadott polinom a 10. körosztási polinom: a gyökei azok a tizedik egységgyökök, amelyeknek sem az 5., sem a 2. hatványa nem 1.

6. *Legyen* $\Phi_n(x) = \prod\limits_{i=1}^{\varphi(n)}(x-\varepsilon_i) \in \mathbb{C}[x]$, *ahol* $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ *a primitív* n*-edik egységgyökök (ez az* n*-edik* **körosztási polinom**). *Bizonyítsuk be teljes indukcióval, hogy* $\Phi_n(x) \in \mathbb{Z}[x]$.

Megoldás: $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Tegyük fel, hogy $k < n$-re tudjuk, hogy $\Phi_k(x) \in \mathbb{Z}[x]$. Vegyük észre, hogy

$$x^n - 1 = \prod_{d|n}\Phi_d(x),$$

ugyanis $x^n - 1$ gyökei éppen az n-edik egységgyökök, és ezek pontosan azok, amelyek primitív d-edik egységgyökök valamely $d \mid n$-re. Ebből megkaphatjuk $\Phi_n(x)$-et mint x^n-1 és a $h(x) = \prod\limits_{d|n,\ d<n}\Phi_d(x)$ hányadosát, ahol $h(x)$ egyrészt 1 főegyütthatós, mert gyöktényezők szorzata, másrészt az indukciós feltevés miatt egész együtthatós is. De a maradékos osztás ugyanazt adja $\mathbb{C}[x]$-ben, mint $\mathbb{Q}[x]$-ben, sőt mivel az osztó 1 főegyütthatós, a hányadosban minden együttható egész lesz, tehát $\Phi_n(x) \in \mathbb{Z}[x]$.

7. *Határozzuk meg az* $x^3 + 6x^2 + 21x + 52$ *polinom gyökeit*
a) a Cardano-formula segítségével,
b) a Rolle-féle gyöktétel segítségével.

Megoldás: a) $y = x+2$ behelyettesítéssel az egyenlet $y^3+9y+26 = 0$. Ennek a megoldása $y = u + v$, ahol u és v az

$$u = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},\ \ v = \frac{-p}{3u}$$

egyik értéke $p = 9$-re és $q = 26$-ra, és ebből a másik két megoldás $\varepsilon u + \varepsilon^2 v$ és $\varepsilon^2 u + \varepsilon v$, ahol $\varepsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ primitív harmadik egységgyök. Tehát $u_1 = -13 + \sqrt{169 + 27} = 1$,

$v_1 = -3$, $y_1 = -2$, továbbá $y_2 = (-\frac{1}{2} + \frac{\sqrt{3}}{2}i) - 3(-\frac{1}{2} - \frac{\sqrt{3}}{2}i) = 1 + 2\sqrt{3}i$, és $y_3 = (-\frac{1}{2} - \frac{\sqrt{3}}{2}i) - 3(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) = 1 - 2\sqrt{3}i$. Ebből az eredeti egyenlet megoldásai:

$$x_1 = -4, \qquad x_{2,3} = -1 \pm 2\sqrt{3}i.$$

b) A lehetséges racionális gyökök $\frac{a}{b}$ alakúak, ahol $a \mid 52$ és $b \mid 1$, tehát ± 1, ± 2, ± 4, ± 13, ± 26 vagy ± 52. Mivel a polinom együtthatói pozitívak, nem lehet pozitív gyöke. Sorra próbálva a többit, azt látjuk, hogy -4 gyöke a polinomnak. Horner-módszerrel kiemelhetjük az $(x+4)$-et: $x^3 + 6x^2 + 21x + 52 = (x+4)(x^2 + 2x + 13)$, a másodfokú tényező gyökei pedig $\dfrac{-2 \pm \sqrt{-48}}{2} = -1 \pm 2\sqrt{3}i$.

8. *Határozzuk meg az alábbi polinomok gyökeit. Bontsuk fel őket irreducibilis tényezők szorzatára $\mathbb{C}[x]$-ben, $\mathbb{R}[x]$-ben, $\mathbb{Q}[x]$-ben és $\mathbb{Z}[x]$-ben. Határozzuk meg a gyökök összegét, szorzatát és négyzetösszegét.*

a) $2x^6 + x^5 - 3x^4 - x^3 - 3x^2 - 2x + 2$

b) $x^6 + 1$

Megoldás: a) A lehetséges $\frac{a}{b}$ racionális gyökök azok, amelyekre $a \mid 2$ és $b \mid 2$, tehát ± 1, ± 2, $\pm \frac{1}{2}$. Horner-módszerrel behelyettesítjük ezeket, amíg nem találunk egy gyököt, aztán a hányadospolinommal folytatjuk.

	2	1	−3	−1	−3	−2	2
−1	2	−1	−2	1	−4	2	0
1/2	2	0	−2	0	−4	0	

Ebből $f(x) = 2x^6 + x^5 - 3x^4 - x^3 - 3x^2 - 2x + 2 = (x+1)(x - \frac{1}{2})(2x^4 - 2x^2 - 4) = (x+1)(2x-1)(x^4 - x^2 - 2) = (x+1)(2x-1)(x^2-2)(x^2+1)$. Ezek a komponensek irreducibilisek $\mathbb{Q}[x]$-ben (a másodfokúaknak nincs racionális gyöke), és $\mathbb{Z}[x]$-ben, ugyanis primitívek is. $\mathbb{R}[x]$-ben $x^2 - 2$ tovább bontható, de $x^2 + 1$ irreducibilis: $f(x) = (x+1)(2x-1)(x-\sqrt{2})(x+\sqrt{2})(x^2+1)$ az $\mathbb{R}[x]$-beli felbontás. Végül $\mathbb{C}[x]$-ben $f(x) = (x+1)(2x-1)(x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$, és a gyökök: $-1, \frac{1}{2}, \pm\sqrt{2}, \pm i$. A gyökök összege $-\frac{1}{2}$, a szorzatuk 1, a négyzetösszegük $\frac{13}{4}$.

Ezeket a gyökök megkeresése nélkül az együtthatókból is kiszámíthatjuk. Ha $f(x) = a_n x^n + \ldots + a_2 x + a_0$, akkor a gyökök összege $-\dfrac{a_{n-1}}{a_n} = -\dfrac{1}{2}$, a szorzatuk $(-1)^n \dfrac{a_0}{a_n} = 1$, és a négyzetösszegük

$$\sum_{i=1}^{n} \alpha_i^2 = \left(\sum_{i=1}^{n} \alpha_i \right)^2 - 2 \left(\sum_{1 \le i < j \le n} \alpha_i \alpha_j \right) = \frac{a_{n-1}^2}{a_n^2} - 2\frac{a_{n-2}}{a_n} = \frac{1}{4} + 3 = \frac{13}{4}.$$

b) Ennek a polinomnak nyilván nincs racionális, sőt valós gyöke sem, mivel $x^6 + 1 \ge 1$, ha $x \in \mathbb{R}$. Viszont a gyököket könnyű megtalálni a -1 komplex hatodik gyökeinek kiszámításával vagy az $x^6 + 1 = \dfrac{x^{12} - 1}{x^6 - 1}$ átalakítás segítségével a komplex 12. egységgyökök közül a megfelelők kiválogatásával: ha $\varepsilon = \cos\frac{\pi}{6} + i \sin\frac{\pi}{6}$ az egyik primitív 12. egységgyök, akkor $x^6 + 1$ gyökei az ε hatványai közül azok, amelyek nem 6. egységgyökök, azaz ε páratlan hatványai: ε, ε^3, ε^5, ε^7, ε^9, ε^{11}, vagy másképpen $\cos\frac{(2k+1)\pi}{6} + i \sin\frac{(2k+1)\pi}{6}$, ahol $k = 0, 1, 2, 3, 4, 5$.

Ebből a $\mathbb{C}[x]$-beli felbontás $\prod_{k=0}^{5} \left(x - \cos\frac{(2k+1)\pi}{6} - i \sin\frac{(2k+1)\pi}{6} \right)$.

Az $\mathbb{R}[x]$-beli felbontást megkapjuk úgy, hogy a gyöktényezők közül a konjugált párokat összevonjuk:
$(x^2 - 2\cos\frac{\pi}{6} + 1)(x^2 - 2\cos\frac{3\pi}{6}x + 1)(x^2 - 2\cos\frac{5\pi}{6}x + 1) =$
$= (x^2 - \sqrt{3}x + 1)(x^2 + 1)(x^2 + \sqrt{3}x + 1)$.
A $\mathbb{Q}$ fölötti felbontásnak az $\mathbb{R}$ fölötti felbontás a finomítása. Mivel a tényezők közül kettő nem racionális együtthatós (és nem is szorozható racionálissá konstans szorzóval, mert 1 főegyütthatós), össze kell vonnunk a két nem eleve racionális együtthatós tényezőt: $x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$, és ezzel megkaptuk a $\mathbb{Q}$ és $\mathbb{Z}$ fölötti irreducibilisekre bontást.
A gyökök összege az együtthatókból kiszámolva 0, a szorzata 1, a négyzetösszege szintén 0.

9. *Adjuk meg azt a legkisebbfokú $p(x)$ polinomot, amelyre $k = 1, 2, 3, 4$ esetén $p(x_k) = y_k$:*

x_k	-1	0	1	2
y_k	-10	-5	0	5

Megoldás: Newton-interpolációval:
Az első ponthoz: $f_1(x) = -10$.
Az első két ponthoz: $f_2(x) = f_1(x) + A(x+1) = -10 + A(x+1)$, ahol $-5 = f_2(0) = -10 + A$ $\Rightarrow A = 5 \Rightarrow f_2(x) = 5x - 5$.
Az első három ponthoz: $f_3(x) = f_2(x) + A(x+1)x = 5x - 5 + A(x+1)x$, ahol $0 = f_3(1) = 2A$ $\Rightarrow A = 0 \Rightarrow f_3(x) = 5x - 5$.
A megadott négy ponthoz: $f_4(x) = f_3(x) + A(x+1)x(x-1) = 5x - 5 + A(x+1)x(x-1)$, ahol $5 = f_4(2) = 5 + 6A \Rightarrow A = 0 \Rightarrow f_4(x) = 5x - 5$.
Tehát a minimális fokú interpoláló polinom $5x - 5$.
Lagrange-interpolációval:
Az alappolinomok:

$$L_1(x) = \frac{x(x-1)(x-2)}{(-1)(-2)(-3)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 - \frac{1}{3}x$$

$$L_2(x) = \frac{(x+1)(x-1)(x-2)}{1(-1)(-2)} = \frac{1}{2}x^3 - x^2 - \frac{1}{2}x + 1$$

$$L_3(x) = \frac{(x+1)x(x-2)}{2 \cdot 1(-1)} = -\frac{1}{2}x^3 + \frac{1}{2}x^2 + x$$

$$L_4(x) = \frac{(x+1)x(x-1)}{3 \cdot 2 \cdot 1} = \frac{1}{6}x^3 - \frac{1}{6}x$$

Ebből az interpoláló polinom:

$$-10L_1 - 5L_2 + 5L_4 = 5x - 5.$$

10. *Fejezzük ki az $x^3 + y^3 + z^3$ polinomot x, y, z elemi szimmetrikus polinomjainak polinomjaként!*
Megoldás: Ha $s_1 = x + y + z$, $s_2 = xy + xz + yz$ és $s_3 = xyz$, akkor

$$\begin{aligned} x^3 + y^3 + z^3 &= (x+y+z)^3 - 3(x^2y + xy^2 + xz^2 + x^2z + y^2z + yz^2) - 6xyz \\ &= (x+y+z)^3 - 3((xy + xz + yz)(x+y+z) - 3xyz) - 6xyz \\ &= s_1^3 - 3(s_2s_1 - 3s_3) - 6s_3 \\ &= s_1^3 - 3s_1s_2 + 3s_3. \end{aligned}$$