1. *Legyen R egy legalább kételemű, nem feltétlenül egységelemes gyűrű. Bizonyítsuk be, hogy R-nek akkor és csak akkor nincs a 0-tól és R-től különböző jobbideálja, ha R ferdetest vagy prímrendű zérógyűrű.*

Megoldás: Ha R ferdetest, akkor minden $J \neq 0$ jobbideál csak a teljes R lehet, ugyanis $0 \neq a \in J$-re $1 = aa^{-1} \in J$, és így minden $r \in R$-re $r = 1r \in J$. Ha R prímrendű zérógyűrű, akkor még additív részcsoportból is csak a 0 és a teljes R van.

Most tegyük fel, hogy R-nek nincs 0-tól és R-től különböző jobbideálja. Először belátjuk, hogy ha R nem nullosztómentes, akkor csak prímrendű zérógyűrű lehet.

Tegyük fel, hogy van $0 \neq a, b \in R$, amelyre $ab = 0$. Ekkor az a elem jobb annullátora, $\mathrm{Ann}_r(a) := \{\, r \in R \mid ar = 0 \,\}$ nem nulla jobbideál, ugyanis b benne van, és ha $c, d \in \mathrm{Ann}_r(a)$ és $r \in R$, akkor $a(c-d) = ac - ad = 0 - 0 = 0$, és $acr = 0r = 0$. De akkor a feltétel miatt $\mathrm{Ann}_r(a) = R$, azaz $aR = 0$. R bal annullátora, $\mathrm{Ann}_l(R) = \{\, r \in R \mid rR = 0 \,\}$ szintén jobbideál (sőt ideál is), ugyanis $0 \in \mathrm{Ann}_l(R)$, és ha $c, d \in \mathrm{Ann}_l(R)$ és $r \in R$, akkor $(c-d)R = 0$ és $crR \subseteq cR = 0$. Továbbá $0 \neq a \in \mathrm{Ann}_l(R)$, így $\mathrm{Ann}_l(R) = R$, amiből $RR = 0$ következik, vagyis R zérógyűrű. Ennek pedig minden additív részcsoportja ideál, tehát $(R, +)$ egyszerű Abel-csoport, és így csak prímrendű lehet.

Tekintsük most azt az esetet, amikor R nullosztómentes, és legyen $0 \neq a \in R$. Ekkor $0 \neq a^2 \in aR$, és aR jobbideál $\Rightarrow aR = R \Rightarrow \exists e \in R : ae = a \Rightarrow$ tetszőleges $r \in R$-re $aer = ar \Rightarrow a(er - r) = 0$, de $a \neq 0$, így $er = r$, azaz e bal egységeleme R-nek, tehát $ea = a$ is igaz. Viszont akkor tetszőleges $r \in R$-re $rea = ra \Rightarrow (re - r)a = 0 \Rightarrow re = r$, tehát e jobb egységelem is, vagyis egységeleme R-nek.

Láttuk, hogy tetszőleges $0 \neq a \in R$-re $aR = R$, ezért van olyan a', amelyre $aa' = e$. De akkor $a' \neq 0$, tehát a'-höz is van a'', amelyre $a'a'' = e$. Ebből következik, hogy $a = ae = aa'a'' = ea'' = a''$, így $a'a = e = aa'$, vagyis a-nak van inverze. Ezzel beláttuk, hogy R ferdetest.

2. *Legyen α az $x^2 - x + 1 \in \mathbb{Q}[x]$ polinom egyik gyöke.*

a) Hány dimenziós $\mathbb{Q}(\alpha)$ mint $\mathbb{Q}$ fölötti vektortér?

b) Bizonyítsuk be, hogy α^7 és α lineárisan összefüggnek ebben a vektortérben.

Megoldás: a) Mivel $x^2 - x + 1$ irreducibilis $\mathbb{Q}[x]$-ben, $x^2 - x + 1$ az α mininmálpolinomja, és így $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = (\mathbb{Q}(\alpha) : \mathbb{Q}) = 2$ (bázisát adja az $\{\, 1, \alpha \,\}$).

b) $\alpha^2 = \alpha - 1 \Rightarrow \alpha^3 = \alpha^2 - \alpha = -1 \Rightarrow \alpha^6 = 1 \Rightarrow \alpha^7 = \alpha$, tehát valóban összefüggők. (*Másképp:* $x^2 - x + 1 = \Phi_6(x) \mid x^6 - 1 \Rightarrow \alpha^6 = 1 \Rightarrow \alpha^7 = \alpha$.)

3. *Bizonyítsuk be, hogy $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[x]/(x^2 - 2x - 1)$.*

Megoldás: $x^2 - 2$ és $x^2 - 2x - 1$ is irreducibilisek, így a velük vett faktorgyűrű megkapható a polinom egy gyökével való testbővítésként.
$x^2 - 1$ gyökei $\pm\sqrt{2}$, $x^2 - 2x - 1$ gyökei pedig $1 \pm \sqrt{2}$. Viszont $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + \sqrt{2})$, mert $\sqrt{2}$ is benne van a másodikban, és $1 + \sqrt{2}$ is benne van az elsőben. Így

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + \sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2x - 1).$$

4. *Adjuk meg* $\cos 20^\circ$ *minimálpolinomját* $\mathbb{Q}$ *fölött.*

Megoldás: Használjuk a $\cos 3x = 4\cos^3 x - 3\cos x$ trigonometrikus formulát $x = \cos 20^\circ$-ra:

$$\frac{1}{2} = \cos 60^\circ = 4\cos^3 20^\circ - 3\cos 20^\circ,$$

vagyis $\cos 20^\circ$ gyöke a $8x^3 - 6x - 1$ polinomnak. Ez a polinom irreducibilis, mert nincs racionális gyöke (a racionális gyökteszt miatt csak a $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ számokat kell belepróbálni, vagy $y = 2x$ helyettesítéssel még ennél is kevesebbet). Tehát $\cos 20^\circ$ minimálpolinomja ennek az 1 főegyüttható skalárszorosa, $x^3 - \frac{3}{4}x - \frac{1}{8}$.

5. *Adjuk meg* $\sqrt{2} + \sqrt{3}$ *minimálpolinomját* $\mathbb{Q}$*, illetve* $\mathbb{Q}(\sqrt{6})$ *fölött!*

Megoldás: Legyen $\alpha = \sqrt{2}+\sqrt{3}$. Ekkor $\alpha^2 = 5+2\sqrt{6} \Rightarrow (\alpha^2-5)^2 = 24 \Rightarrow \alpha^4-10\alpha^2+1 = 0$, tehát α gyöke az x^4-10x^2+1 polinomnak. Ez a polinom irreducibilis, mert egyrészt nincs racionális gyöke (csak ± 1 lehetne, de azok sem gyökök), másrészt két másodfokú, egész együtthatós polinom szorzataként sem állhat elő: ilyen felbontás (ahol feltehető, hogy a főegyütthatók pozitívak) csak $(x^2+ax+1)(x^2+bx+1)$ vagy $(x^2+ax-1)(x^2+bx-1)$ alakú lehetne, de az együtthatókat összehasonlítva ebből azt kapnánk, hogy $a^2 = 12$, illetve $a^2 = 8$, és ilyen a egész szám nincs. Így $\alpha = \sqrt{2}+\sqrt{3}$ minimálpolinomja $\mathbb{Q}$ fölött $x^4 - 10x^2 + 1$.

Viszont menetközben láttuk, hogy $\alpha^2 = 5+2\sqrt{6}$, azaz α gyöke az $x^2-5-2\sqrt{6} \in \mathbb{Q}(\sqrt{6})[x]$ polinomnak. Ennél kisebb fokú, $\mathbb{Q}(\sqrt{6})$ fölötti polinomnak nem lehet gyöke, mert akkor α benne lenne $\mathbb{Q}(\sqrt{6})$-ban, pedig az csak másodfokú (az x^2-6 gyökével való) bővítése $\mathbb{Q}$-nak. Tehát α minimálpolinomja $\mathbb{Q}(\sqrt{6})$ fölött $x^2 - 5 - 2\sqrt{6}$.

6. *Bizonyítsuk be, hogy ha* $\alpha, \beta \in \mathbb{C}$*-re* $\alpha+\beta$ *és* $\alpha\beta$ *algebrai* $\mathbb{Q}$ *fölött, akkor* α *és* β *is algebraiak.*

Megoldás: Legyen $c = \alpha+\beta$ és $d = \alpha\beta$. Tudjuk, hogy ekkor α és β gyöke az $x^2 - cx + d \in \mathbb{Q}(c,d)[x]$ polinomnak, tehát $\mathbb{Q}(c,d,\alpha) = \mathbb{Q}(c,d,\beta) = \mathbb{Q}(\alpha,\beta)$ a $\mathbb{Q}(c,d)$ fölött véges fokú. Viszont mivel c algebrai $\mathbb{Q}$ fölött, és d algebrai $\mathbb{Q}$ fölött, és így természetesen $\mathbb{Q}(c)$ fölött is,

$$(\mathbb{Q}(\alpha,\beta) : \mathbb{Q}) = (\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(c,d)) \cdot (\mathbb{Q}(c,d) : \mathbb{Q}(c)) \cdot (\mathbb{Q}(c) : \mathbb{Q})$$

véges, és így $\mathbb{Q}(\alpha,\beta)$ minden eleme, így α és β is, algebrai $\mathbb{Q}$ fölött.

7. *Adjunk példát nem véges fokú algebrai bővítésre!*

Megoldás: Legyen K a $\mathbb{C}$-nek az a legkisebb részteste, amely tartalmazza az összes egységgyököt. K elemei véges sok egységgyök racionális kifejezéseként írhatók, mert az ilyen kifejezések biztosan benne vannak minden olyan résztestben, amely tartalmazza az egységgyököket, másrészt ezek már résztestet alkotnak. Viszont véges sok egységgyök benne van egyetlen egységgyökkel való bővítésben (vegyük a szereplő egységgyökök rendjének legkisebb közös többszörösét), tehát a $\mathbb{Q}$ egy véges fokú bővítésében, így ezek a számok algebraiak $\mathbb{Q}$ fölött.

Viszont egy egységgyökkel való bővítés maga is bármilyen nagy véges fokú lehet: egy n-edik egységgyök minimálpolinomja a $\Phi_n(x)$ körosztási polinom, mert a körosztási polinomok irreducibilisek. Speciálisan $n = p$ prím esetére ezt bizonyítottuk is, és így a p-edik primitív egységgyökkel való bővítés foka $\varphi(p) = p - 1$ is akármilyen nagy lehet. Ebből következik, hogy $(K : \mathbb{Q}) = \infty$.

8. *Legyen α az $x^3-2x^2+x+1\in\mathbb{Q}[x]$ polinom egyik gyöke. Adjuk meg α^2+2 reciprokát α legfőljebb másodfokú polinomjaként!*

Megoldás: Keressük azokat az $A,B,C\in\mathbb{Q}$ racionális együtthatókat, amelyekkel $(A\alpha^2+B\alpha+C)(\alpha^2+2)=1$, azaz

$$A\alpha^4+B\alpha^3+(2A+C)\alpha^2+2B\alpha+2C=1.$$

Használjuk, hogy $\alpha^3-2\alpha^2+\alpha+1=0$, azaz

$$\begin{aligned}\alpha^3=&2\alpha^2-\alpha-1 \text{ és}\\ \alpha^4=&2\alpha^3-\alpha^2-\alpha=2(2\alpha^2-\alpha-1)-\alpha^2-\alpha=\\ =&3\alpha^2-3\alpha-2.\end{aligned}$$

$$(5A+2B+C)\alpha^2+(-3A+B)\alpha+(-2A-B+2C)=1.$$

Az $5A+2B+C=0$, $-3A+B=0$, $-2A-B+2C=1$ lineáris egyenletrendszert megoldva azt kapjuk, hogy $A=-\frac{1}{27}$, $B=-\frac{3}{27}$, $C=\frac{11}{27}$, tehát $\dfrac{1}{\alpha^2+2}=\dfrac{1}{27}(-\alpha^2-3\alpha+11)$.

2. megoldás: Kibővített euklideszi algoritmus segítségével állítsuk elő az 1-et $(x^3-2x^2+x+1)a(x)+(x^2+2)b(x)$ alakban.

	x^3-2x^2+x+1	x^2+2
x^3-2x^2+x+1	1	0
x^2+2	0	1
$-x+5$	1	$-x+2$
27	$x+5$	$-x^2-3x+11$

Tehát $1=(x^3-2x^2+x+1)\frac{1}{27}(x+5)+(x^2+2)\frac{1}{27}(-x^2-3x+11)\Rightarrow\alpha$-t behelyettesítve: $1=0+(\alpha^2+2)\frac{1}{27}(-\alpha^2-3\alpha+11)\Rightarrow\dfrac{1}{\alpha^2+2}=\dfrac{1}{27}(-\alpha^2-3\alpha+11)$.

9. *Hányadfokú a $\mathbb{Q}(i\sqrt{3})$, illetve a $\mathbb{Q}(i+\sqrt{3})$ bővítés $\mathbb{Q}$ fölött?*

Megoldás: $i\sqrt{3}$ minimálpolinomja x^2+3, mert ennek gyöke az $i\sqrt{3}$, és nyilván irreducibilis $\mathbb{Q}$ fölött. Így $(\mathbb{Q}(i\sqrt{3}):\mathbb{Q})=2$

Legyen $\alpha=i+\sqrt{3}$. Ekkor $(\alpha-\sqrt{3})^2=-1\Rightarrow\alpha^2-2\sqrt{3}\alpha+4=0\Rightarrow\sqrt{3}=\frac{\alpha^2+4}{2\alpha}\in\mathbb{Q}(\alpha)$, és $i=\alpha-\sqrt{3}\in\mathbb{Q}(\alpha)$, így $\mathbb{Q}(\sqrt{3},i)\le\mathbb{Q}(i+\sqrt{3})\le\mathbb{Q}(\sqrt{3},i)$, vagyis $\mathbb{Q}\le\mathbb{Q}(\sqrt{3})\le\mathbb{Q}(\sqrt{3},i)=\mathbb{Q}(\alpha)$, ahol az első bővítés másodfokú (x^2-3 minimálpolinommal), és a második nem elsőfokú, mert $\mathbb{Q}(\sqrt{3})\le\mathbb{R}$, de $\mathbb{Q}(\alpha)\not\le\mathbb{R}$, viszont i gyöke az $x^2+1\in\mathbb{Q}[x]\le\mathbb{Q}(\sqrt{3})[x]$ polinomnak, így a második bővítés is másodfokú. Tehát a szorzattétel szerint $(\mathbb{Q}(\alpha):\mathbb{Q})=2\cdot2=4$.

10. *Számítsuk ki a következő testbővítések fokait $\mathbb{Q}$ fölött!*

a) $\mathbb{Q}(\sqrt{2})$ *b)* $\mathbb{Q}(\sqrt[3]{2})$ *c)* $\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{4})$ *d)* $\mathbb{Q}(\sqrt[3]{2}+\sqrt{2})$

Megoldás: a) $\sqrt{2}$ minimálpolinomja $x^2-2 \Rightarrow (\mathbb{Q}(\sqrt{2}):\mathbb{Q})=2$.

b) $\sqrt[3]{2}$ gyöke az x^3-2 polinomnak, amely irreducibilis is, például a Sch.–E.-kritérium miatt, tehát ez a $\sqrt[3]{2}$ minimálpolinomja, és emiatt $(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})=3$.

c) $\alpha := \sqrt[3]{2}+\sqrt[3]{4} = \sqrt[3]{2}+(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$, tehát $\mathbb{Q} \le \mathbb{Q}(\alpha) \le \mathbb{Q}(\sqrt[3]{2})$, és így

$$3 = (\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}) = (\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}(\alpha))\cdot(\mathbb{Q}(\alpha):\mathbb{Q}).$$

De $\sqrt[3]{2}$ gyöke az $x^2+x-\alpha \in \mathbb{Q}(\alpha)[x]$ polinomnak, ezért $(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}(\alpha)) \le 2$, és osztója 3-nak, így csak 1 lehet, és ebből következik, hogy $(\mathbb{Q}(\alpha):\mathbb{Q})=3$.

d) Nyilvánvaló, hogy $\alpha = \sqrt[3]{2}+\sqrt{2}$-re $\mathbb{Q}(\alpha) \le \mathbb{Q}(\sqrt[3]{2},\sqrt{2})$, másrészt $(\alpha-\sqrt{2})^3 = 2 \Rightarrow$ $\alpha^3-3\sqrt{2}\alpha^2+6\alpha-2\sqrt{2}=2 \Rightarrow \sqrt{2}=\dfrac{\alpha^3+6\alpha}{3\alpha^2+2} \in \mathbb{Q}(\alpha)$, és $\sqrt[3]{2}=\alpha-\sqrt{2}\in\mathbb{Q}(\alpha)$, ezért $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$. Az utóbbinak a foka $\mathbb{Q}$ fölött legföljebb $2\cdot 3=6$ a

$$\mathbb{Q} \le \mathbb{Q}(\sqrt{2}) \le \mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\alpha)$$

bővítéssorozat miatt, ahol az első bővítés minimálpolinomja x^2-2, a másodiké legalábbis osztója az x^3-2-nek. Másrészt viszont a

$$\mathbb{Q} \le \mathbb{Q}(\sqrt[3]{2}) \le \mathbb{Q}(\alpha)$$

bővítéssorozatot is figyelembe véve azt látjuk, hogy $(\mathbb{Q}(\alpha):\mathbb{Q})$ osztható 2-vel és 3-mal is, így csak 6 lehet.

11. *Legyen α az x^3+x+1 polinom egyik gyöke $\mathbb{Z}_2$ fölött, és legyen $K=\mathbb{Z}_2(\alpha)$. Irreducibilis-e az $x^2+x+\alpha$ polinom K fölött?*

Megoldás: Azt kell csak ellenőriznünk, hogy $x^2+x+\alpha$-nak van-e gyöke K-ban, azaz van-e α-nak olyan $\mathbb{Z}_2[x]$-beli $A\alpha^2+B\alpha+C$ polinomja, amelyre

$$(A\alpha^2+B\alpha+C)^2+(A\alpha^2+B\alpha+C)+\alpha=0.$$

Ha átalakítjuk az egyenletet, felhasználva, hogy $A,B,C\in\{0,1\}$ miatt $A^2=A$, $B^2=B$ és $C^2=C$, és $\alpha^3=\alpha+1$ és $\alpha^4=\alpha^2+\alpha$, azt kapjuk hogy $A\alpha^4+(A+B)\alpha^2+(B+1)\alpha=0$, azaz $B\alpha^2+(A+B+1)\alpha=0$, tehát $A=1$, $B=0$ és C tetszőleges, vagyis $x^2+x+\alpha$-nak gyöke α^2 és α^2+1, ezért nem irreducibilis.

Hf1. *Határozzuk meg a $\mathbb{Q}(\sqrt{4-\sqrt{2}})$ minimálpolinomját $\mathbb{Q}$ fölött!*

Hf2. *Legyen $K=\mathbb{Z}_2(\alpha)$ a kételemű testnek az $x^4+x+1\in\mathbb{Z}_2[x]$ polinom α gyökével való bővítése. Írjuk fel az $\frac{\alpha^2}{\alpha+1}$ elemet α legföljebb harmadfokú polinomjaként!*