1. *Mutassuk meg, hogy minden másodfokú bővítés normális.*

Megoldás: Legyen az $f(x)$ másodfokú polinom, és α az egyik gyöke. Ha kiemeljük az $x-\alpha$ gyöktényezőt $f(x)$-ből, akkor az $f(x)$-et a testbővítésben lineáris faktorokra bontottuk, tehát az α-val való bővítés az $f(x)$ felbontási teste.

2. *Lássuk be, hogy egy K véges test n-edfokú bővítésében minden n-edfokú, $K[x]$-beli irreducibilis polinom lineáris faktorokra bomlik!*

Megoldás: Legyen $|K| = q$, és L a K n-edfokú bővítése. Ekkor $|L| = q^n$, és L elemei éppen az $x^{q^n} - x$ polinom gyökei ($L^\times$ $q^n - 1$-rendű csoport, tehát minden a elemére $a^{q^n-1} = 1$, másrészt az $x^{q^n} - x$ polinomnak minden gyöke egyszeres, mivel a deriváltja, $q^n x^{q^n-1} - 1 = -1$ relatív prím hozzá, így csak az L elemei a gyökei). Ha f egy K fölött irreducibilis n-edfokú polinom, akkor az annak egy α gyökével való bővítés szintén q^n elemű testet ad, következésképpen az α minimálpolinomja, $f(x)$, osztója $x^{q^n} - x$-nek, tehát $f(x)$ L-ben is lineáris faktorokra bomlik.

3. *Mutassuk meg, hogy ha p prím, akkor $x^{p^n} - x$ az összes olyan $\mathbb{F}_p$ fölötti normált irreducibilis polinom szorzata, amelynek foka n-nek osztója.*

Megoldás: Tudjuk, hogy $x^{p^n} - x$ felbontási teste a p^n elemű test (a felbontási testben ennek a polinomnak a gyökei résztestet alkotnak, tehát ez a résztest maga a felbontási test).

Az előző feladat megoldásában láttuk, hogy minden d-edfokú irreducibilis polinom osztója $x^{p^d} - x$-nek. Ha d osztója n-nek, akkor $p^d - 1$ osztója $p^n - 1$-nek, és így $x^{p^d-1} - 1$ osztója $x^{p^n-1} - 1$-nek, amiből $x^{p^d} - x$ osztója $x^{p^n} - x$-nek.

Fordítva, ha $f(x)$ az $x^{p^n} - x$ egyik irreducibilis faktora, akkor az $x^{p^n} - x$ felbontási testének részteste az $\mathbb{F}_p(\alpha)$, ahol α az $f(x)$ egyik gyöke. Ha $\deg f = d$, akkor ez a résztest p^d elemű, a nagy test elemszáma, p^n pedig ennek hatványa, tehát d osztója n-nek.

Végül, minden normált irreducibilis polinom csak egyszer fordul elő faktorként, mert $x^{p^n} - x$-nek nincs többszörös gyöke.

4. *Az előző feladat alapján számítsuk ki, hány 1 főegyütthatós másod-, harmad- és negyedfokú irreducibilis polinom van $\mathbb{F}_3$ fölött!*

Megoldás: Az elsőfokú normált irreducibilis polinomok $x - a$, ahol $a \in \mathbb{F}_3$, tehát három ilyen van. A másodfokúak az $x^{3^2} - x$ polinom ezektől különböző irreducibilis komponensei, így számuk $(9-3)/2 = 3$. Hasonlóan a harmadfokúak az $x^{27} - x$ polinom irreducibilis faktorai az első- és harmadfokú normált irreducibilis polinomok, tehát a harmadfokúak száma $(27-3)/3 = 8$. Végül a negyedfokúak az $x^{81} - x$ nem első- és másodfokú normált faktorai, és ezek száma $(81 - 3 - 3 \cdot 2)/4 = 72/4 = 18$.

5. *Bizonyítsuk be, hogy minden p prímre és minden n pozitív egész számra létezik n-edfokú irreducibilis polinom $\mathbb{F}_p$ fölött.*

Megoldás: Legyen K egy p^n elemű véges test (az $x^{p^n} - x$ felbontási teste). Egy véges test multiplikatív csoportja ciklikus; legyen $K^\times = \langle\alpha\rangle$. Az α elem $\mathbb{F}_p$ fölötti minimálpolinomja csak n-edfokú lehet, mert $\mathbb{F}_p(\alpha) = K$.

6. *Igaz-e, hogy egy $K = \mathbb{F}_p(\alpha)$ ($\alpha \notin \mathbb{F}_p$) testben α szükségképpen generátoreleme a K multiplikatív csoportjának?*

Megoldás: Nem igaz: például $\mathbb{F}_9^\times \cong C_8$-ban egy 4-edrendű α elemre $\alpha \notin \mathbb{F}_3$, tehát $\mathbb{F}_3(\alpha) = \mathbb{F}_9$, de α nem generálja a 8-adrendű ciklikus csoportot.

7. *Igaz-e, hogy normális bővítés normális bővítése normális az eredeti test fölött?*

Megoldás: Nem igaz. Tekintsük a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt[4]{2})$ bővítéssorozatot. Mindkét bővítés másodfokú (x^2-2, illetve $x^2-\sqrt{2}$ a minimálpolinomok), így normális, de $\sqrt[4]{2}$ $\mathbb{Q}$ fölötti minimálpolinomjának, x^4-2-nek nem valós gyökei is vannak, és ezek még a bővebb testben sincsenek benne.

8. *Van-e többszörös gyöke az $f(x) = x^4+2x^3-x^2-2x+1 \in \mathbb{Q}[x]$ polinomnak a felbontási testében? Ha igen, bontsuk föl olyan $\mathbb{Q}[x]$-beli polinomok szorzatára, amelyeknek nincs többszörös gyökük!*

Megoldás: Euklideszi algoritmussal számítsuk ki az $f(x)$ és $f'(x) = 4x^3+6x^2-2x-2$ polinom legnagyobb közös osztóját.

$$f(x) = f'(x)\left(\frac{1}{4}x+\frac{1}{8}\right) + \left(-\frac{5}{4}x^2-\frac{5}{4}x+\frac{5}{4}\right),$$

$$f'(x) = (x^2+x-1)(4x+2)+0,$$

tehát x^2+x-1 a legnagyobb közös osztó. Ebből következik, hogy x^2+x-1 gyökei legalább kétszeres gyökei $f(x)$ polinomnak, azaz $(x^2+x-1)^2$ osztója f-nek, és a fokszám miatt f ennél nagyobb nem is lehet. Valóban, $f(x) = (x^2+x-1)^2$, és x^2+x-1-nek már nincs többszörös gyöke.

9. *Milyen karakterisztikájú test fölött lehet az $f(x) = 3x^7+7x^2+2$ polinomnak többszörös gyöke? Bontsuk föl ott $f(x)$-et irreducibilis faktorokra.*

Megoldás: Számítsuk ki euklideszi algoritmussal az $f(x) = 3x^7+7x^2+2$ és $f'(x) = 21x^6+14x$ polinomok legnagyobb közös osztóját, félretéve azokat az eseteket, amilyen karakterisztika mellett valamelyik osztó főegyütthatója 0. A maradékok sorra $5x^2+2$, $14(x-\frac{12}{125})$ és $\frac{6394}{3125}$. Ha a test karakterisztikája $p \neq 2,3,5,7$, akkor végig tudjuk csinálni az euklideszi algoritmust, és csak akkor lesz többszörös gyöke f-nek, ha $6394 = 2\cdot 23\cdot 139 \equiv 0 \pmod{p}$, azaz ha $p = 23$ vagy $p = 139$. Ezekben az esetekben az utolsó maradék, az elsőfokú polinom a legnagyobb közös osztó, tehát annak gyöke kétszeres gyöke f-nek: -8, ha $p = 23$, és 19, ha $p = 139$. Ebben az esetben $f(x) = (x+8)^2(3x^5-2x^4+x^3-3x^2+7x-5)$, illetve $f(x) = (x-19)^2(3x^5+32x^4-35x^3+50x^2+35x-35)$. Ha $p = 2$, akkor $f(x) = x^7+x^2 = x^2(x^5+1)$, és az ötödfokú polinomnak már nincsenek többszörös gyökei. Ha $p = 3$, akkor $f(x) = x^2-1$ és $f'(x) = -x$ nyilván relatív prímek, így f-nek nincs többszörös gyöke. Ha $p = 5$, az $f(x)$-nek az $f'(x)$-szel való osztásánál a maradék 2, így $(f,f') = 1$, vagyis $f(x)$-nek nincs többszörös gyöke. Ha pedig $p = 7$, akkor $f(x) = 3x^7+2$, és mivel $a^7 = a$ igaz $\mathbb{F}_7$ minden elemére, ez tovább írható $3^7x^7+2^7 = (3x+2)^7$ alakban. Összefoglalva: $p = 2,7,23,139$ esetén van f-nek többszörös gyöke.

10. *Bizonyítsuk be, hogy ha $\operatorname{char} K = p$, és $f(x) = g(x^p) \in K[x]$ irreducibilis, akkor f nem szeparábilis, sőt valamely $k \in \mathbb{N}$-re f-nek a felbontási testében minden gyöke pontosan p^k-szoros.*

Megoldás: Feltehetjük, hogy $f(x)$ 1 főegyüttható polinom. Az állítást a g polinom fokára vonatkozó teljes indukcióval bizonyítjuk. Ha g foka 1, akkor $g(x) = (x - \alpha)$, és α-nak a K alkalmas bővítésében van p-edik gyöke, legyen ez β. Ekkor $f(x) = x^p - \alpha = x^p - \beta^p = (x - \beta)^p$. Most tegyük fel, hogy a megadott f-nél kisebb fokú polinomokra már tudjuk az állítást. Mivel $f(x)$ irreducibilis, $g(x)$ is az. Így g vagy szeparábilis, vagy $g'(x) = 0$, tehát $g(x) = h(x^p)$ valamely $h(x)$ polinomra. Az indukciós feltevést alkalmazhatjuk a g és h polinomokra. Eszerint a $g(x)$ felbontási testében $g(x) = (x - \alpha_1)^{p^k} \cdots (x - \alpha_r)^{p^k}$, ahol $\alpha_1, \ldots, \alpha_r$ mind különbözők (ha g szeparábilis, akkor $k = 0$). Bővítsük a testet úgy, hogy minden α_i-nek egy p-edik gyöke is benne legyen: $\beta_i^p = \alpha_i$. Ekkor $f(x) = g(x^p) = (x^p - \alpha_1)^{p^k} \cdots (x^p - \alpha_r)^{p^k} = (x^p - \beta_1^p)^{p^k} \cdots (x^p - \beta_r^p)^{p^k} = (x - \beta_1)^{p^{k+1}} \cdots (x - \beta_r)^{p^{k+1}}$, és itt a β_i-k mind különbözők, mert a p-edik hatványaik is azok.

11. *Legyen* $\operatorname{char} K = p$*, és* $K(t)$ *a* K *test egyszerű transzcendens bővítése. Bizonyítsuk be, hogy* $K(t)$*-ben az* $x^p - t$ *polinom irreducibilis és nem szeparábilis.*

Megoldás: A $K(t)$ egy alkalmas algebrai bővítésében van olyan α, hogy $\alpha^p = t$, így itt $x^p - t = x^p - \alpha^p = (x - \alpha)^p$, vagyis az $x^p - t$ polinomnak minden gyöke megegyezik. Ha a polinom nem lenne irreducibilis $K(t)$-ben, akkor lenne egy irreducibilis faktora, amely vagy lineáris vagy nem szeparábilis. Az utóbbi eset ellentmond annak a ténynek, hogy irreducibilis szeparábilis polinom x^p-nek polinomja, tehát legalább p-edfokú. Ha viszont elsőfokú irreducibilis faktora van $x^p - t$-nek $K(t)$-ben, akkor vannak olyan $g(x), h(x)$ nem 0 polinomok $K[x]$-ben, amelyekre $t = (g(t)/h(t))^p$, azaz $t(h(t))^p = g(t)^p$. Mivel p karakterisztikájú test fölött tagonként lehet p-edik hatványra emelni, az $xh(x)^p$ polinomban csak a p szerint egy maradékot adó kitevőjű tagok együtthatója lehet nem 0, a $g(x)^p$ polinomban pedig csak a p-vel osztható kitevőjű tagoké, ezért t a nem nulla $xg(x)^p - h(x)^p$ polinomnak lenne a gyöke, ami ellentmond annak, hogy t transzcendens K fölött.

Hf1. *Hányadfokú* $x^4 + 3$ *felbontási teste* $\mathbb{Q}$ *és* $\mathbb{F}_7$ *fölött?*

Hf2. *Bizonyítsuk be, hogy* $\mathbb{Q}(\cos 40^\circ)$ *normális bővítése* $\mathbb{Q}$*-nak!*