Testbővítések. Többszörös gyökök és deriválás

1. *Mennyi $\sqrt{2}+\sqrt[4]{2}$ foka $\mathbb{Q}(\sqrt{2})$, illetve $\mathbb{Q}$ fölött?*

Megoldás. Legyen $\alpha=\sqrt{2}+\sqrt[4]{2}$. Először megmutatjuk, hogy $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt[4]{2})$. Az, persze, nyilvánvaló, hogy $\alpha=\sqrt{2}+\sqrt[4]{2}\in\mathbb{Q}(\sqrt[4]{2})$, hiszen $\sqrt[4]{2}$ és $\sqrt{2}=(\sqrt[4]{2})^2$ is benne van $\mathbb{Q}(\sqrt[4]{2})$-ben. Ez azt jelenti, hogy $\mathbb{Q}(\alpha)\subseteq\mathbb{Q}(\sqrt[4]{2})$. Másrészt tekintsük az alábbi átalakítást:

$$\alpha=\sqrt{2}+\sqrt[4]{2}\quad\Longrightarrow\quad\alpha-\sqrt{2}=\sqrt[4]{2}\quad\overset{(\cdot)^2}{\Longrightarrow}\quad\alpha^2-2\alpha\sqrt{2}+2=\sqrt{2}\quad\Longrightarrow\quad\alpha^2-(2\alpha+1)\sqrt{2}+2=0$$

Az utolsó összefüggésből $\sqrt{2}$ kifejezhető α segítségével, vagyis $\sqrt{2}\in\mathbb{Q}(\alpha)$, és akkor nyilván az is teljesül, hogy $\sqrt[4]{2}=\alpha-\sqrt{2}\in\mathbb{Q}(\alpha)$. Vagyis $\mathbb{Q}(\sqrt[4]{2})\subseteq\mathbb{Q}(\alpha)$. Ezzel megmutattuk, hogy α és $\sqrt[4]{2}$ ugyanazt a bővítést generálja $\mathbb{Q}$ fölött. Viszont $\sqrt[4]{2}$ minimálpolinomja $\mathbb{Q}$ fölött $f(x)=x^4-2$ (hiszen gyöke neki, és f irreducibilis $\mathbb{Q}$ fölött pl. a Schönemann–Eisenstein-kritérium miatt). Ez azt jelenti, hogy $\left|\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}\right|=4$, és az előbbiek miatt α **foka $\mathbb{Q}$ fölött szintén** 4. Ugyanakkor a fokszámtétel miatt a $\mathbb{Q}\leq\mathbb{Q}\sqrt{2}\leq\mathbb{Q}(\sqrt[4]{2})=\mathbb{Q}(\alpha)$ bővítéssorozatban mindkét kis bővítés foka 2: az nyilvánvaló, hogy $\sqrt{2}$ foka $\mathbb{Q}$ fölött 2, és akkor $\left|\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})\right|=2$ is teljesül, hiszen $|\mathbb{Q}(\alpha):\mathbb{Q}|=4$. Ezzel megkaptuk, hogy α **foka** $\mathbb{Q}(\sqrt{2})$ **fölött** 2.

2. *Határozzuk meg az $1+\sqrt{2}\,i$ és a $\sqrt{2}+\sqrt{3}\,i$ algebrai számok fokát.*

Megoldás. $\deg(\sqrt{2}\,i)=2$, hiszen nincs benne $\mathbb{Q}$-ban – tehát a foka nagyobb 1-nél –, de gyöke az x^2+2 polionomnak. Ekkor $\mathbb{Q}(1+\sqrt{2}\,i)=\mathbb{Q}(\sqrt{2}\,i)$ miatt $1+\sqrt{2}\,i$ foka is 2 lesz.
Ugyanakkor megmutatjuk, hogy $\sqrt{2}+\sqrt{3}\,i$ foka $\mathbb{Q}$ fölött 4. Az nyilvánvaló, hogy $\mathbb{Q}\leq\mathbb{Q}(\sqrt{2})\leq\mathbb{Q}(\sqrt{2},\sqrt{3}\,i)$, és ez utóbbi negyedfokú bővítése $\mathbb{Q}$-nak, mert két másodfokú bővítés egymásutánjával kaphatjuk meg. (Mindkét generáló elem, azaz $\sqrt{2}$ és $\sqrt{3}\,i$ is másodfokú $\mathbb{Q}$ fölött, és a második közülük nincs benne az elsővel való bővítésben, hiszen az első lépésben valós résztestet kapunk.)
Most már elegendő igazolunk, hogy $\mathbb{Q}(\sqrt{2},\sqrt{3}\,i)=\mathbb{Q}(\sqrt{2}+\sqrt{3}\,i)$, ehhez pedig azt fogjuk belátni, hogy $\sqrt{2},\sqrt{3}\,i\in\mathbb{Q}(\sqrt{2}+\sqrt{3}\,i)$. A már korábban is látott módon, ha $\alpha=\sqrt{2}+\sqrt{3}\,i$, akkor az alábbi levezetést kapjuk:

$$\alpha=\sqrt{2}+\sqrt{3}\,i\quad\Longrightarrow\quad\alpha-\sqrt{2}=\sqrt{3}\,i\quad\overset{(\cdot)^2)}{\Longrightarrow}\quad\alpha^2-2\alpha\sqrt{2}+2=-3\quad\Rightarrow\quad\sqrt{2}=\frac{\alpha^2+5}{2\alpha},$$

vagyis $\sqrt{2}$ kifejezhető α-val (és racionális számokkal), és ekkor természetesen $\sqrt{3}\,i=\alpha-\sqrt{2}\in\mathbb{Q}(\alpha)$ szintén teljesül. – Megmutattuk tehát, hogy α negyedfokú $\mathbb{Q}$ fölött.

3. *Legyenek c és d különböző négyzetmentes számok. Igazoljuk, hogy $\mathbb{Q}(\sqrt{c})\neq\mathbb{Q}(\sqrt{d})$.*

Megoldás. Az nyilvánvaló, hogy tetszőleges, 1-től különböző c négyzetmentes szám négyzetgyöke irracionális, így $\mathbb{Q}$-nak a gyökkel, $\sqrt{c}$-vel való bővítése másodfokú a racionális számtest fölött. Mutassuk meg, hogy az így kapható testek mind különbözők. Érdemes észrevenni, hogy ha c és d közül az egyik pozitív, a másik negatív, akkor a c-vel és d-vel vett bővítések mindenképpen különböznek, mert az egyik csak valós számokat tartalmaz, míg a másik nem. Az egyszerűség kedvvéért föltehetjük tehát, hogy c is és d is pozitívak, és egyik sem egyenlő 1-gyel. A feltétel szerint vagy van olyan p prím, ami osztja c-t, de nem osztja d-t, vagy van olyan q prím, ami osztja d-t, de nem osztja c-t. Tegyük föl, hogy az első eset áll fönn. Elegendő megmutatnunk, hogy $d\notin\mathbb{Q}(\sqrt{c})$. Tegyük föl, hogy $\sqrt{d}=a+b\sqrt{c}$ valamilyen $a,b\in\mathbb{Q}$-ra. Ekkor $b\neq0$, ellenkező esetben $\sqrt{d}\in\mathbb{Q}$ teljesülne. $a=0$ esetén pedig azt kapnánk, hogy $b=\sqrt{d/c}$, és ez ut=bbi nem lehet racionális, hiszen van olyan p prí, amely osztja c-t, de nem osztja d-t. Végezetül, ha $a,b\neq0$, akkor $a^2+2ab\sqrt{c}+b^2c=d$ miatt $\sqrt{c}$ lenne racionális, ami $c\neq1$ és c négyetmentessége miatt nem lehetséges.

4. *Tegyük fel, hogy az a,b,c,d,r számok benne vannak $\mathbb{R}$ valamely K résztestében, és az $y=ax+b$ egyenletű egyenes metszi az $(x-c)^2+(y-d)^2=r^2$ egyenletű kört. Mutassuk meg, hogy a metszéspontok koordinátái benne vannak $\mathbb{R}$ egy olyan résztestében, amely K-nak másodfokú bővítése.*

Megoldás. Egy köeregyenletből és egy lineáris egyenletből (azaz egy egyenes egyenletéből) álló rendszert kell megoldanunk. Ilyenkor a lineáris egyenletből kifejezve az egyik ismeretlent (pl. az y-t, ha lehet), majd behelyettesítve a kör egyenletébe, egy olyan egyenletet kapunk, amely másodfokú, s az együtthatói benne vannak K-ban. A másodfokú egyenlet megoldóképlete szerint az egyenlet gyökei benne vannak a K egy másodfokú bővítésében, s ugyanígy benne lesz ebben a testben az első változóval lineáris kapcsolatban álló második változó értéke is.

5. *Van-e többszörös komplex gyöke az $x^6+x^5+5x^4+4x^3+8x^2+4x+4$ polinomnak?*

Megoldás. A válaszhoz ki kell számolni a megadott $f(x)=x^6+x^5+5x^4+4x^3+8x^2+4x+4$ polinomnak és a deriváltjának, $f'(x)=6x^5+5x^4+20x^3+12x^2+16x+4$-nek a legnagyobb közös osztóját. Euklideszi algoritmussal (ismételt maradékos osztásokkal) megállapíthatjuk, hogy a két polinom legnagyobb közös osztója x^2+2, és ez azt jelenti, hogy $f(x)$-nek van többszörös gyöke (és ezek a -2-nek a négyzetgyökei). A számolás maga meglehetősen hosszadalmas és csúnya, de elvileg végigszámolható, ellentétben azzal, mintha a gyököket kellene meghatároznunk. Persze, lehet trükkösen is: kicsit próbálkozva a faktorizálással rá lehet jönni, hogy $f(x)$-ből ki lehet emelni x^2+x+1-et: $f(x)=(x^2+x+1)(x^4+4x^2+4)=(x^2+x+1)(x^2+2)^2$. Ebből adódik, hogy x^2+2 gyökei kétszeresek.– *Megjegyzés:* A kérdést másképpen is lehet értelmezni. Egy másik, lehetséges értelmezés lehetne pl., hogy azt kérdezzük, $f(x)$-nek van-e többszörös **racionális** (esetleg **valós**) gyöke. Az első esetben elegendő lenne a racionális gyöktesztet alkalmazni, majd Horner-elrendezéssel ellenőrizni a racionális gyökök multiplicitását. A deriváltas teszt viszont azt mondja meg, hogy $f(x)$-nek a racionális számtest **semmilyen bővítésében** sincs többszörös gyöke (tehát pl. $\mathbb{C}$-ben sem), és ezt akkor is elárulja a teszt, ha nem tudjuk, konkrétan mik is azok a komplex gyökök.

6. *Az R szokásos gyűrű fölötti $f=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ polinom deriváltja legyen $f'=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\ldots+2a_2x+a_1$.*

a) *Írjuk fel a definíciót a szummás jelölést használva.*

b) *Ellenőrizzük, hogy $(cf)'=cf'$ és $(f\pm g)'=f'\pm g'$.*

c) *Igazoljuk, hogy $(fg)'=fg'+f'g$.*

Megoldás. a) Ha $f(x)=\sum_{i=0}^{n} a_i\cdot x^i$, akkor $f'(x)=\sum_{i=1}^{n} i\cdot a_i\cdot x^{i-1}$.

b) Legyen $f(x)=\sum_{i=0}^{n} a_i\cdot x^i$, és $g(x)=\sum_{i=0}^{n} b_i\cdot x^i$ (itt nem azonos fok esetén 0 együtthatókkal egészítjük ki valamelyik polinomot). Ekkor:

$$(c\cdot f)'(x)=\big(\sum_{i=0}^{n} c\cdot a_i\cdot x^i\big)'=\sum_{i=1}^{n-1} i\cdot c\cdot a_i\cdot x^{i-1}=c\cdot\sum_{i=1}^{n-1} i\cdot a_i\cdot x^{i-1}=c\cdot f'(x)$$

illetve:

$$(f+g)'(x)=\big(\sum_{i=0}^{n} a_i\cdot x^i+\sum_{i=0}^{n} b_i\cdot x^i\big)'=\big(\sum_{i=0}^{n}(a_i+b_i)\cdot x^i\big)'=\sum_{i=1}^{n} i\cdot(a_i+b_i)\cdot x^{i-1}=$$
$$=\sum_{i=1}^{n} i\cdot a_i\cdot x^{i-1}+\sum_{i=1}^{n} i\cdot b_i\cdot x^{i-1}=f'(x)+g'(x)$$

c) Használjuk az előző rész eredményeit konstansszorosra és többtagú összegekre. Ezeket használva azt kapjuk, elegendő a szorzásszabályt (Leibniz-szabályt) csak egytagúak szorzatára alkalmazni, hiszen f-et és g-t is egytagúak összegeként írhatjuk föl. Így tehát:

$$(x^k\cdot x^n)'=(x^{k+n})'=(k+n)\cdot x^{k+n-1},\quad\text{és}\quad (x^k)\cdot(x^n)'+(x^k)'\cdot(x^n)=x^k\cdot n\cdot x^{n-1}+k\cdot x^{k-1}\cdot x^n=(n+k)\cdot x^{k+n-1}$$

7. *Vezessük le a láncszabályt is: $(f\circ g)'=(f'\circ g)g'$.*

Megoldás. Az előző feladathoz hasonlóan elegendő arra az esetre szorítkozni, amikor $f(x)$ egytagú (és x-hatvány), azaz $f(x)=x^n$, mivel $(f_1+f_2)\circ g=f_1\circ g+f_2\circ g$. Nézzük először azt az esetet, amikor g is egytagú:

$$(x^n\circ(a\cdot x^k))'=(a^n\cdot x^{nk})'=a^n\cdot n\cdot k\cdot x^{nk-1}$$
$$\big((x^n)'\circ(a\cdot x^k)\big)\cdot(a\cdot x^k)'=\big((n\cdot x^{n-1})\circ(a\cdot x^k)\big)\cdot(a\cdot k\cdot x^{k-1})=$$
$$=(n\cdot a^{n-1}\cdot x^{(n-1)k})\cdot a\cdot k\cdot x^{k-1}=n\cdot a^n\cdot x^{nk-k+k-1}$$

Ez mutatja a képlet érvényességét erre a speciális esetre. Most a g-beli egytagúak számára, ℓ-re vonatkozó indukcióval igazoljuk a képletet olyan esetben, amikor g-t két tagnak az összegeként állítjuk elő: $g = g_1 + g_2$, és itt g_1 és g_2 tagjainak a száma kisebb, mint ℓ, tehát ezekre érvényes az indukciós föltevés:

$$\big(x^n \circ (g_1+g_2)\big)' = \left(\sum_{i=0}^{n} \binom{n}{i} g_1^{n-i} \cdot g_2^i\right)' = \sum_{i=0}^{n} \binom{n}{i} \Big(g_1^{n-i} \cdot \big(g_2^i\big)' + \big(g_1^{n-i}\big)' \cdot g_2^i\Big) =$$

$$= \sum_{i=0}^{n} \binom{n}{i} \Big(g_1^{n-i} \cdot i \cdot g_2^{i-1} \cdot g_2' + (n-i) \cdot g_1^{n-i-1} \cdot g_1' \cdot g_2^i\Big)\Big)$$

$$\big((x^n)' \circ (g_1+g_2)\big) \cdot (g_1+g_2)' =$$

Később befejezni!

8. *Legyen $f \in \mathbb{C}[x]$, $k \geq 1$. Igazoljuk, hogy ha α pontosan k-szoros gyöke f-nek, akkor f'-nek pontosan $(k-1)$-szeres gyöke.*

Megoldás. Legyen $k \geq 1$. Ekkor α pontosan k-szoros gyöke f-nek, ha $f = (x-\alpha)^k \cdot g$, ahol $g(\alpha) \neq 0$. Ekkor $f' = k(x-\alpha)^{k-1} \cdot g + (x-\alpha)^k \cdot g' = (x-\alpha)^{k-1}\Big(k \cdot g + (x-\alpha) \cdot g'\Big)$. Itt az utolsó kifejezésben a nagy zárójel első tagjának nem gyöke α, míg a másodiknak igen, tehát az összegnek α nem gyöke. Ez azt jelenti, hogy f-nek az α pontosan $k-1$-szeres gyöke.

9. **a)** *Ismétlés: Legyen $\alpha = \cos x + i \sin x$. Az α^3 komplex számot kétféleképpen felírva vezessük le a $\cos 3x = 4\cos^3 x - 3\cos x$ azonosságot.*

b) *Mutassuk meg, hogy $\cos 20^\circ$ harmadfokú algebrai szám.*

Megoldás. a) A de Moivre-képlet alapján egyrészt $\alpha^3 = \cos 3x + i \sin 3x$ másrészt köbre emelve az összeget (pl. használva a binomiális tételt), azt kapjuk, hogy $\alpha^3 = \cos^3 x + 3i \cos^2 x \sin x - 3 \cos x \sin^2 x - i \sin^3 x$. A valós részeket összehasonlítva az adódik, hogy

$$\cos 3x = \cos^3 x - 3\cos x \sin^2 x = \cos^3 x - 3\cos x(1-\cos^2 x) = 4\cos^3 x - 3\cos x.$$

b) Az a) rész alapján $\cos 20^\circ$-ra igaz az alábbi összefüggés: $\cos 60^\circ = 4\cos^3 20^\circ - 3\cos 20^\circ$. Itt $\cos 60^\circ = \frac{1}{2}$, tehát $8\cos^3 20^\circ - 6\cos 20^\circ - 1 = 0$, vagyis $\cos 20^\circ$ gyöke az $f(x) = 8x^3 - 6x - 1$ irreducibilis polinomnak (alkalmazhatjuk a racionális gyöktesztet, hogy megmutassuk, $f(x)$-nek nincs racionális gyöke, így $f(x)$ irreducibilis), tehát $\cos 20^\circ$ harmadfokú $\mathbb{Q}$ fölött.

10. **a)** *Ismétlés: Igazoljuk, hogy $1 + \cos 72^\circ + \cos 144^\circ + \cos 216^\circ + \cos 288^\circ = 0$.*

b) *Mi lesz $\cos 72^\circ$ foka, illetve minimálpolinomja $\mathbb{Q}$ fölött?*

Megoldás. a) Tekintsük az $\omega = \cos 72^\circ + i \sin 72^\circ$ primitív ötödik egységgyököt. Ekkor a fölírt kifejezésre azt kapjuk, hogy:

$$1 + \cos 72^\circ + \cos 144^\circ + \cos 216^\circ + \cos 288^\circ = \operatorname{Re} 1 + \operatorname{Re}\omega + \operatorname{Re}\omega^2 + \operatorname{Re}\omega^3 + \operatorname{Re}\omega^4 = \operatorname{Re}(1+\omega+\omega^2+\omega^3+\omega^4).$$

De tudjuk, hgy ω gyöke az ötödik körosztási polinomnak, $\Phi_5(x) = 1 + x + x^2 + x^3 + x^4$-nek, tehát a fönti egyenlőség jobb oldalán a 0 valós része szerepel. A keresett összeg így valóban 0. (Mondhattuk volna azt is, hogy az ω-hatványok fönti összege épp az ötödikl egységgyökök összegét adja, ami 0.)

b) Mivel $\cos 72^\circ = \frac{1}{2}(\omega + \bar{\omega}) = \frac{1}{2}(\omega + \omega^4)$, ezért $\cos 72^\circ \in \mathbb{Q}(\omega)$, és mivel az utóbbi bővítés foka 4 (az ötödik körosztási polinom foka), a $\cos 72^\circ$ foka legföljebb 4, sőt, a szorzástétel miatt osztója 4-nek. Persze, ez a fok nem lehet 4, mert $\cos 72^\circ \in \mathbb{R}$, tehát $\mathbb{Q}(\cos 72^\circ) \subseteq \mathbb{R}$, és $\omega \notin \mathbb{R}$, tehát $\mathbb{Q}(\cos 72^\circ) \neq \mathbb{Q}(\omega)$. Ugyanakkor $\alpha = i \sin 72^\circ$ esetén $\alpha^2 = -\sin^2 72^\circ = \cos^2 72^\circ - 1 \in \mathbb{Q}(\cos 72^\circ)$, ezért α foka $\mathbb{Q}(\cos 72^\circ)$ fölött legföljebb 2. De ekkor $\omega = \cos 72^\circ + i \sin 72^\circ \in \mathbb{Q}(\cos 72^\circ)(i \sin 72^\circ) = \mathbb{Q}(\omega)$ miatt azt kapjuk a szorzásétel alapján, hogy $|\mathbb{Q}(\cos 72^\circ) : \mathbb{Q}| = 2$ és $|\mathbb{Q}(\omega) : \mathbb{Q}(\cos 72^\circ)| = 2$. Vagyis, $\cos 72^\circ$ foka $\mathbb{Q}$ fölött 2:

$$\begin{array}{ccccc} \mathbb{Q} & \subseteq & \mathbb{Q}(\cos 72^\circ) & \subseteq & \mathbb{Q}(\omega) \\ & \text{foka} \leq 2 & & \text{foka} \leq 2 & \\ & & \text{foka} = 4 & & \end{array}.$$

Végezetül, hogy a minimálpolinomot megtaláljuk, használjuk ki, hogy az ötödik körosztási polinom ún. reciprok polinom: minden gyökkel együtt annak reciproka is gyöke a polinomnak (pl. ω-val együtt $\omega^{-1}=\omega^4$), azaz $x+(1/x)$ polinomjaként lehet fölírni. Azaz $\alpha=\omega+\omega^{-1}$ jelöléssel:

$$0=1+\omega+\omega^2+\omega^3+\omega^4=1+(\omega+\omega^{-1})+(\omega^2+\omega^{-2})=1+\alpha+\alpha^2-2=\alpha^2+\alpha-1.$$

Nekünk tkp. $\cos 72^\circ=\beta=\alpha/2$-re kellene az összefüggés, tehát:

$$\alpha^2+\alpha-1=(2\beta)^2+2\beta-1=0,$$

vagyis β minimálpolinomja (hogy normált legyen): $m(x)=x^2+\frac{1}{2}x-\frac{1}{4}$.

11. **a)** *Legyen p prímszám. Mutassuk meg, hogy az x^p-x-1 polinomnak nincs gyöke $\mathbb{Z}_p$-ben.*

b) *Bizonyítsuk be, hogy az x^p-x-1 polinom irreducibilis $\mathbb{Z}_p$ fölött. (A megoldáshoz nem szükséges, de felhasználhatjuk, hogy létezik olyan p karakterisztikájú test, amely fölött a polinom gyöktényezők szorzatára bomlik.)*

Megoldás. **a)** $\mathbb{Z}_p$ minden α elemére $\alpha^p=\alpha$ (ez a kis Fermat-tétel), ezért $\alpha^p-\alpha-1=-1$. Tehát x^p-x-1-nek nincs gyóke $\mathbb{Z}_p$-ben.

b) Legyen K az a test, amelyben az $f(x)=x^p-x-1$ polinom gyöktényezők szorzatára bomlik, és tegyük föl hogy $f(x)$ nem irreducibilis $\mathbb{Z}_p[x]$-ben: $f(x)=f_1(x)\cdot f_2(x)\cdots f_k(x)$, és itt $k>1$. Föltehető, hogy f_i-k irreducibilisek $\mathbb{Z}_p[x]$-ben. Mivel K-ban az f gyöktényezőkre bomlik, minden f_i-nek van α_i gyöke K-ban. Az f_i-k irreducibilitása miatt minden i-re α_i foka $\mathbb{Z}_p$ fölött $\deg_i$-vel egyenlő. Ugyanakkor ha α és β gyöke f-nek, akkor $\alpha^p-\alpha-1=0$ és $\beta^p-\beta-1=0$, és a két egyenlőséget kivonva egymásból, valamint használva, hogy p karakterisztikában szabad tagonként hatványozni, azt kapjuk, hogy $(\alpha^p-\beta^p)-(\alpha-\beta)=0$, azaz $(\alpha-\beta)^p-(\alpha-\beta)=0$. Ez azt jelenti, hogy $\alpha-\beta$ gyöke az x^p-x polinomnak, aminek viszont minden gyöke $\mathbb{Z}_p$-beli: $\mathbb{Z}_p$ minden eleme gyöke, és p-nél több gyöke nem is lehet még K-ban sem. Vagyis $\beta\in\mathbb{Z}_p(\alpha)$, minden α,β gyökpárra, hiszen $\beta=\alpha+(\beta-\alpha)$. Ez azt jelenti, hogy f minden gyökének azonos a foka (hiszen bármelyik gyök benne van a másik által generált bővítésben), vagyis f_i-k fokai egyenlők. De ekkor $k\cdot\deg f_1=\deg f=p$, és ez csak úgy lehet, ha $\deg f_i=1$. Ez viszont ellentmondás, mert az a) rész alapján tudjuk, hogy $f(x)$-nek nincs gyöke $\mathbb{Z}_p$-ben.