Mat-alkmat gyakorlat, második évfolyam, első félév

Második alkalom — megoldásvázlatok (2002 ősz)

1. A lineáris kombinációk felírásával, és π transzcendens voltának kihasználásával kapjuk, hogy az első és a harmadik halmaz független. A második nem, mert $\mathbb{C}$ csak másodfokú $\mathbb{R}$ felett.

2. Az ilyen alakú számok a $\mathbb{Q}(\sqrt[3]{2})$ testet alkotják. A $\sqrt[3]{2}$ foka $\mathbb{Q}$ felett három, mert $\mathbb{Q}$ feletti minimálpolinomja x^3-2. Így $|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}|=3$. Tehát e bővítés minden elemének foka osztója háromnak. De a $\sqrt[6]{2}$ foka $\mathbb{Q}$ felett 6, mert a Schönemann-Eisenstein kritérium miatt az x^6-2 polinom irreducibilis $\mathbb{Q}$ felett. Tehát sem ez a szám, sem a másodfokú $\sqrt{2}$ (sem sok harmadfokú szám!) nem írható fel a kívánt alakban.

3. Az eredmény 6, az I/7. vagy a II/4. feladat miatt.

4. Tekintsük a $K \leq K(\alpha) \leq K(\alpha)(\beta) = M$ testláncot. Az első bővítés foka $gr_K(\alpha)$. A második bővítés fokának meghatározásához meg kell vizsgálnunk a β minimálpolinomját $K(\alpha)$ felett. Ha a K feletti minimálpolinomot m jelöli, akkor m foka $gr_K(\beta)$. Az m polinom $K[x]$-beli, és így minden együtthatója benne van a $K(\alpha)$ testben. A $K(\alpha)$ feletti minimálpolinom azonban osztója minden olyan $K(\alpha)[x]$-beli polinomnak, aminek β gyöke, tehát speciálisan m-nek is. Ezért a foka, azaz β foka $K(\alpha)$ felett legfeljebb annyi, mint m foka, azaz $gr_K(\beta)$. Így a fenti testláncból azt kapjuk, hogy $|M:K| \leq gr_K(\alpha)gr_K(\beta)$. Másrészt viszont α és β K feletti foka osztja $|M:K|$-t, és mivel e két szám relatív prím, a szorzatuk is osztja. Vagyis beláttuk, hogy $|M:K| = gr_K(\alpha)gr_K(\beta)$. (A fenti lánc alapján ebből azt is láthatjuk, hogy β foka $K(\alpha)$ felett $gr_K(\beta)$, és ezért a fenti m polinom a $K(\alpha)$ feletti minimálpolinom is egyben, és így irreducibilis $K(\alpha)$ felett.)

5. Tekintsük a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{8}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$ láncot. A nagy bővítés foka 4, a kicsié 2, ezért $|\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{8})| = 2$. Így a keresett fokszám kettő. (Másik megoldásként be lehetne látni, hogy a $\sqrt[4]{2}$ minimálpolinomja $\mathbb{Q}(\sqrt{2})$ felett $x^2-\sqrt{2}$.) A másik kérdéshez tekintsük a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{7}) \leq \mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{2})$ láncot. A 4. feladat miatt itt a nagy bővítés foka 12, és a kicsié 3, ezért az eredmény 4.

6. Legyen ε primitív harmadik egységgyök, melyre $\theta = \varepsilon\sqrt[3]{2}$. Mivel θ minimálpolinomja is x^3-2, a θ foka $\mathbb{Q}$ felett 3. Továbbá ε foka $\varphi(3)=2$ (a minimálpolinom a harmadik körosztási polinom, azaz x^2+x+1). Nyilván $\mathbb{Q}(\sqrt[3]{2}, \varepsilon\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, és így a 4. feladat miatt ez hatodfokú bővítése $\mathbb{Q}$-nak. Ezért θ másodfokú $\mathbb{Q}(\sqrt[3]{2})$ felett (és ez nem osztja a θ fokát $\mathbb{Q}$ felett, tehát a második kérdésre nemleges a válasz). A $\mathbb{Q}(\theta)\cap\mathbb{R}$ test részteste $\mathbb{Q}(\theta)$-nak, és így $\mathbb{Q}$ feletti foka 1 vagy 3. Utóbbi lehetetlen, mert θ nem valós. Ezért a metszet $\mathbb{Q}$.

7. a): Ez a szám primitív 360-adik egységgyök, hiszen 23 és 360 relatív prímek. Ezért foka $\varphi(360)$. b): Legfeljebb hatodfokú, de négyzetre emeléssel kifejezhető a $\sqrt[3]{9}$, ezért az eredmény 6. c): Nyilván 2. d): Négyzetre emeléssel kifejezhető a $\sqrt{2}$, az eredmény 4.

8,9. Ugyanúgy, mint hogy $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ (lásd I/7), majd n szerinti indukció.

10. Mivel i algebrai, ha a és b algebrai, akkor $a+bi$ is az, hiszen az algebrai számok testet alkotnak. Megfordítva, ha $a+bi$ algebrai, akkor gyöke egy racionális együtthatós nem nulla polinomnak. Ennek $a-bi$ is gyöke (hiszen a polinom valós együtthatós), de a és b kifejezhető $a+bi$-vel, $a-bi$-vel és i-vel.

11. Ha $a=\pi+3$ algebrai lenne, akkor $a-3=\pi$ is az lenne, hiszen az algebrai számok testet alkotnak, ami ellentmondás. Hasonlóan látható, hogy $5\pi+6$ és $\pi+\sqrt{2}$ sem lehet algebrai. Ha $\sqrt{\pi}$ algebrai lenne, akkor négyzete is, ez sem lehet. Végül belátjuk, hogy π semmilyen racionális együtthatós, nem nulla polinomja sem lehet algebrai. Ha ugyanis $g(\pi)$ algebrai lenne, azaz gyöke lenne egy racionális együtthatós $f \neq 0$ polinomnak, akkor $f(g(\pi))=0$, azaz π gyöke lenne a racionális együtthatós, nem nulla $f(g(x))$ polinomnak.

12. Algebrai plusz transzcendens mindig transzcendens. Nem nulla algebraiszor transzcendens is transzcendens. Algebrai szám n-edik hatványa és n-edik gyöke is algebrai, minden n egészre.

13. A $\mathbb{Q}$ minden algebrailag zárt bővítése tartalmazza az n-edfokú $\sqrt[n]{2}$ számot minden n-re, és így foka végtelen. Ha K véges test, és elemei $\{a_1, \ldots, a_n\}$, akkor az $f(x) = (x-a_1)\ldots(x-a_n)+1$ nem-konstans polinomnak nincs gyöke K-ban, ezért K nem lehet algebrailag zárt. A $\mathbb{Z}_p$ test esetében vehetnénk ehelyett az x^2-g polinomot, ahol g kvadratikus nemmaradék.

14. Ha $K \leq L$ és $L \leq M$ algebrai, és $\alpha \in M$, akkor bővítsük K-t az α elem L feletti minimálpolinomjának együtthatóival. A kapott N test véges bővítése K-nak, mert véges sok algebrai elemmel bővítettünk. De α algebrai N felett, ezért $K \leq N(\alpha)$ véges, vagyis α algebrai K felett.

15. Az x^2+1 felbontási teste $\mathbb{Q}(i)$, ennek foka 2. Az x^4-1 felbontási teste is $\mathbb{Q}(i)$. Az $x^4+1=\Phi_8(x)$ gyökei a primitív nyolcadik egységgyökök, ha ε ilyen, akkor a többi ennek hatványa, vagyis a felbontási test $\mathbb{Q}(\varepsilon)$, melynek foka $\mathbb{Q}$ felett $\varphi(8)=4$. Az x^6-1 felbontási teste $\mathbb{Q}(\eta)$, ahol η hatodik primitív egységgyök, foka $\varphi(6)=2$. Az x^6-2 felbontási teste $\mathbb{Q}(\sqrt[6]{2},\eta)$, ahol η hatodik primitív egységgyök. Ennek a bővítésnek a foka 12, hiszen η másodfokú $\mathbb{Q}$ felett, és mivel nem valós, másodfokú $\mathbb{Q}(\sqrt[6]{2})$ felett is. Az $(x^2-2)(x^3-2)$ felbontási teste $\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\varepsilon)$, ahol ε primitív harmadik egységgyök. Ez a test megegyezik az előző polinom esetében vizsgált $\mathbb{Q}(\sqrt[6]{2},\eta)$ testtel. Az $(x^2-2)(x^2-3)$ felbontási teste a $\mathbb{Q}(\sqrt{2},\sqrt{3})$, ennek foka $\mathbb{Q}$ felett 4.

16. Tegyük fel, hogy $K\le L$ és $|L:K|=2$. Legyen $\alpha\in L-K$. Ekkor α másodfokú, és mivel m minimálpolinomjának az egyik gyöke L-ben van, ezért ez a minimálpolinom két elsőfokú tényezőre bomlik L felett. Tehát L a felbontási teste m-nek K felett, és így normális bővítése K-nak. (Sőt, azt sem kell használnunk, hogy minden felbontási test normális, hiszen ha f irreducibilis K felett, és van L-ben egy α gyöke, akkor f az α minimálpolinomjának konstansszorosa, és a fenti gondolatmenet szerint f másik gyöke is L-ben van.)

17. Ha M egy $K[x]$-beli polinom felbontási teste, akkor ugyanennek a polinomnak nyilván a felbontási teste L felett is, és készen vagyunk. Tehát azt célszerű tisztáznunk, hogy minden normális bővítés felbontási test-e.

Ha $K\le M$ egyszerű bővítés, mondjuk $M=K(\alpha)$, akkor legyen m az α minimálpolinomja K felett. A normalitás és m irreducibilitása miatt m „összes” gyöke M-ben van, és mivel már α is generátor, az M a m felbontási teste K felett. Hasonló gondolatmenet működik akkor is, ha $K\le M$ véges bővítés. Ekkor végesen generált, és e véges sok generátorelem minimálpolinomjainak szorzata megfelelő lesz.

Általában nem igaz, hogy minden normális bővítés egy polinom felbontási teste, hiszen akkor végesen generált (és így az algebraiság miatt véges) is lenne (márpedig például az algebrai számok teste normális, de nem véges bővítése $\mathbb{Q}$-nak). Azonban minden $K\le M$ normális bővítés egy alkalmas polinom*halmaz* felbontási teste lesz, azaz olyan $K[x]$-beli polinomok összes gyökei generálják K felett, amelyek mindegyike M-ben lineáris tényezőkre bomlik. Az előadáson szerepelt bizonyítás mutatja, hogy polinomhalmaz felbontási teste is mindig normális bővítés. Megfordítva, minden $K\le M$ normális bővítés felbontási test lesz, ha a polinomhalmazba az M összes elemének K feletti minimálpolinomját bevesszük. Ha $K\le L\le M$, akkor ugyanennek a polinomhalmaznak az M az L felett is felbontási teste, tehát $L\le M$ is normális.

18. Segédállításként belátjuk, hogy ha $K\le L$ normális bővítés, melynek Galois-csoportja G, és K tökéletes test, akkor tetszőleges $\gamma_1,\dots,\gamma_k\in L$ elemek esetén az $p(x)=(x-\gamma_1)\dots(x-\gamma_k)$ polinomra pontosan akkor igaz, hogy $K[x]$-beli, és K felett irreducibilis, ha a γ_i számok páronként különbözők, és G egy orbitját alkotják. Valóban, legyen $q(x)=\prod(x-g(\gamma_1))$, ahol g befutja G elemeit. E polinomra G bármely elemét alkalmazva csak a tényezők cserélődnek, a polinom nem változik. Ezért $q\in K[x]$. Ha tehát $p\in K[x]$ irreducibilis, akkor $p\mid q$, vagyis a γ_i számok benne vannak γ_1 orbitjában. Továbbá p invariáns G-re, ezért $g(\gamma_1)$ gyöke p-nek, azaz γ_1 orbitjának elemei a γ_i számok közül valók. Tehát a γ_i számok tényleg orbitot alkotnak. Végül K tökéletes, ezért a γ_i számok (mint a p irreducibilis polinom gyökei) páronként különbözők. Most tegyük fel azt, hogy a γ_i számok páronként különbözők, és orbitot alkotnak. Ekkor $p(x)$ nyilván G-invariáns, és így $K[x]$-beli. Ha m jelöli a γ_1 minimálpolinomját K felett, akkor $m\mid p$. De m-nek gyöke $g(\gamma_1)$ minden G-re, ezért $m=p$ (ugyanazok a gyöktényezőik), vagyis p is irreducibilis.

A feladat megoldására térve belátjuk, hogy az állítás igaz akkor is, ha $\mathbb{Q}$ helyett tetszőleges $K\subseteq\mathbb{C}$ testet veszünk. Legyen α minimálpolinomja K felett f, ennek komplex gyökei $\alpha=\alpha_1,\alpha_2,\dots,\alpha_n$, a β minimálpolinomja g, gyökei pedig $\beta=\beta_1,\dots,\beta_m$. Legyen $h(x)=\prod(x-\alpha_i-\beta_j)$. Elég belátni, hogy ez az nm fokú polinom irreducibilis K felett, mert akkor ez $\alpha+\beta$ minimálpolinomja lesz, és így $\alpha+\beta$ foka tényleg nm. Legyen $N\ge K$ az fg felbontási teste K felett, azaz az α_i és β_j számok, valamint K által generált résztest, és G az $N\ge K$ bővítés Galois-csoportja. A segédállítás miatt α_i és β_j is egy-egy G-orbitot alkotnak, és elég belátni, hogy az $\alpha_i+\beta_j$ számok páronként különbözők, és szintén orbitot alkotnak.

Belátjuk, hogy G tranzitívan hat az (α_i,β_j) párok halmazán. Legyen N az α_1 stabilizátora G-ben (ennek indexe n), és M a β_1 stabilizátora G-ben (ennek indexe m). Ekkor az (α_1,β_1) pár stabilizátora $N\cap M$. Nyilván $N\cap M$ indexe osztható n-nel is és m-mel is, és mivel ezek relatív prímek, nm-mel is. Tehát (α_1,β_1) stabilizátorának indexe legalább nm, vagyis orbitja legalább nm elemű, azaz az összes párt tartalmazza.

Végül elég megmutatni, hogy az $\alpha_i+\beta_j$ számok páronként különbözők, és mivel G tranzitív ezek halmazán, elegendő egy konkrét $\alpha_i+\beta_j$ számról belátni, hogy a többitől különbözik. Ezt a következőképpen választjuk. Tekintsük az α_i-k között azokat, amelyeknek a lehető legkisebb a valós része, és ha több ilyen van, akkor ezek között azt, aminek a lehető legkisebb a képzetes része. Válasszuk β_j-t ugyanígy. Ez nyilván jó lesz.