Mat-tanári gyakorlat, második évfolyam, második félév

Tizenegyedik alkalom — megoldásvázlatok

1. a) Nem, a páros számok gyűrűjének hányadosteste $\mathbb{Q}$-val izomorf, mert minden racionális szám felírható olyan törtként is, aminek számlálója és nevezője is páros. Precízebben, az a megfeleltetés, ami a $(2a, 2b)$ osztályához az a/b törtet rendeli, jóldefiniált, és izomorfizmus ($a, b \in \mathbb{Z}$, $b \neq 0$). Ezt *nagyon jó gyakorlat* kiszámolni. b) Igaz, az $(a+bi, c+di)$ osztályához az $a+bi/c+di$ törtet rendelő megfeleltetés izomorfizmus. c) Hamis, $\mathbb{Z}_6$-ban az 1 additív rendje 6. d) Igaz. Láttuk előadáson, hogy nullosztómentes gyűrűben minden nemnulla elem rendje ugyanaz. Ez a szám nem lehet 6, mert ha a rendje 6, akkor $2a$ rendje 3. *Második megoldás:* ha $6a = 0$, akkor $2a \cdot 3a = a \cdot 6a = 0$, ezért vagy $2a = 0$, vagy $3a = 0$. Azaz a nem lehet hatodrendű. e) Van, például a $\mathbb{Z}_2[x]$ hányadosteste. f) A $\mathbb{Z}_2$ algebrai lezártja jó (mellesleg ez is végtelen). g) Igaz. Láttuk az előadáson, hogy van p^n elemszámú L (kommutatív) test. Tanultuk azt is, hogy minden véges test multiplikatív csoportja ciklikus, legyen g generátora $L^{\times}$-nek. Ha $K \cong \mathbb{Z}_p$ a K prímteste, akkor tehát $L = K(g)$, és így ha m jelöli g minimálpolinomját K felett, akkor m foka éppen $|L : K| = n$, és persze m irreducibilis $K \cong \mathbb{Z}_p$ felett. h) Ha a karakterisztika nem kettő, az állítás igaz, és azon múlik, hogy a másodfokú egyenlet gyökképlete érvényes. Legyen $K \leq L$ egy másodfokú bővítés, és $\alpha \in L$, ami nincs K-ban. Ekkor α minimálpolinomja másodfokú, mondjuk $x^2 + px + q$. Innen $0 = 4\alpha^2 + 4p\alpha + 4q = (2\alpha + p)^2 + 4q - p^2$, és ezért $L = K(\alpha) = K(2\alpha + p) = K(\sqrt{p - 4q})$. Ha a karakterisztika kettő, az állítás nem mindig igaz. Ellenpélda a négyelemű test, amit nem lehet megkapni úgy, hogy a prímtestéhez egy elem négyzetgyökét hozzávesszük, hiszen a prímtest mindkét elemének egyetlen négyzetgyöke van: önmaga. i) Igaz. Legyen K egy p karakterisztikájú test. Vegyük észre először, hogy $(-1)^p = -1$, ami páratlan p-re nyilvánvaló, de igaz $p = 2$-re is, mert akkor $-1 = 1$. Mivel p-karakterisztikában a p-edik hatványra emelés tagonként végezhető, $(a - b)^p = a^p + (-b)^p = a^p - b^p$. Ha tehát $a^p = b^p$, akkor innen $(a - b)^p = 0$, és mivel minden test nullosztómentes, $a = b$. Ezért minden elemnek (tehát az 1-nek is) legfeljebb egy darab p-edik gyöke lehet.

2. $x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x - 1)$, tehát a gyökök ötödik hatványa 1. A 27 elemű test multiplikatív csoportjának rendje 26, ez nem osztható 5-tel, ezért az egyetlen ilyen elem az egységelem, ami nem gyöke a fenti polinomnak. Hasonlóan látható (az $x^2 - x + 1 = \Phi_6(x)$ összefüggés miatt), hogy ennek a polinomnak a gyökei pont a hatodrendű elemek, ilyen sincs a Lagrange-tétel miatt. Megjegyezzük, hogy egy 27 elemű test minden eleme harmadfokú a prímtest, azaz $\mathbb{Z}_3$ felett, kivéve a prímtest elemeit, amik elsőfokúak. Tehát egy másodfokú polinomnak csak akkor lehet itt gyöke, ha $\mathbb{Z}_3$-ban is van. Ezzel második megoldást kaptunk az $x^2 - x + 1$ esetére. A másik polinom is elintézhető ezzel az ötlettel (hogyan?).

3. A $\mathbb{Z}_2$ felett $x^4 - 2$ ugyanaz mint x^4, ennek egyetlen gyöke a nulla, tehát felbontási teste $\mathbb{Z}_2$. A $\mathbb{Z}_2$ felett $x^4 - 1 = (x - 1)^4$, tehát ennek is a $\mathbb{Z}_2$ a felbontási teste. Mivel $x^4 - x = x(x - 1)(x^2 + x + 1)$, ezért az eredmény a négyelemű test. Az $x^8 - x$ polinomnak a Lagrange-tétel miatt a nyolcelemű test minden eleme gyöke. Ez az összes gyök, hiszen nyolcadfokú a polinom. Ezért az eredmény a nyolcelemű test (melynek foka 3 a $\mathbb{Z}_2$ felett). Az $x^2 + 1$ polinomnak a $\mathbb{Z}_{17}$-ben gyöke a ± 4, ezért a felbontási test a $\mathbb{Z}_{17}$. Viszont $x^2 - 3$-nak nincs itt gyöke, azaz a felbontási test másodfokú lesz. Végül az $x^{11} - 1$ polinom gyökei az 1 kivételével tizenegyedrendűek. Ezért ha a keresett fokszám n, akkor $11 \mid 2^n - 1$. A legkisebb ilyen n (azaz a 2 rendje modulo 11) a 10. Mivel a 2^{10} elemű test multiplikatív csoportja ciklikus, ebben $x^{11} - 1$ tényleg lineáris tényezőkre bomlik. (Lásd a körosztási jegyzet harmadik fejezetének végén a gyakorlatokat!)

4. A Galois-csoport $\mathbb{Z}_3$, a főtétel igaz, csak a két triviális közbülső test van.

5. $\mathbb{R}[x]$: nullosztómentes, de végtelen dimenziós. $\mathbb{R}^{2\times 2}$: véges dimenziós, de nem nullosztómentes. $\mathbb{Q}(\sqrt{2})$: véges dimenziós, nullosztómentes, de nem $\mathbb{R}$ feletti algebra (hanem $\mathbb{Q}$ feletti).

6. Ezzel az észrevétellel megússzuk annak bizonyítását, hogy a kvaterniók szorzása asszociatív.

7. Kettő. Az egyik a szokásos (amit a valósból kapunk), a másik pedig a következő: $a + b\sqrt{2} \prec c + d\sqrt{2}$ akkor és csak akkor, ha $a - b\sqrt{2} < c - d\sqrt{2}$. Ezek nyilván rendezések. Nincs több, mert minden rendezésnél $\mathbb{Q}$ rendezése nyilván a szokásos (mert az 1 négyetszám), és a fenti két rendezést aszerint kapjuk, hogy $+\sqrt{2}$ pozitív, vagy negatív lesz-e eszerint a rendezés szerint ($+\sqrt{2}$ „előjele” már meghatározza a rendezést).

9. Az első igen, az 1 generálja (ez az egész gyűrű). A második nem, mert $x+4$ irreducibilis $\mathbb{Z}$ fölött (primitív, és elsőfokú), ezért a két polinom kitüntetett közös osztója az 1, de ez nincsen benne az ideálban, hiszen itt minden konstans tag páros.