Mat-tanári szak, első évfolyam, második félév

Válaszok a vizsgakérdésekre (1998. május 29.)

2. a) A $\mathbb{G}[x]$ gyűrű invertálható elemeit, azaz egységeit keressük. Tanultuk, hogy a polinomgyűrű egységei az alapgyűrű egységei, mint konstans polinomok. Ezért a kérdéses csoport elemei az $1, -1, i, -i$, és ezek rendjei $1, 2, 4, 4$.

b) A $\mathbb{C}[x]$-ben. Ha $f = gh$, ahol $f, g \in \mathbb{Q}[x]$ és $h \in \mathbb{C}[x]$, akkor osszuk el maradékosan f-et g-vel $\mathbb{Q}[x]$-ben. Az eredmény $f = gq + r$. Mivel ez is és $f = gh + 0$ is $\mathbb{C}[x]$-beli maradékos osztás, az egyértelműség miatt $h = q \in \mathbb{Q}[x]$. (Hasonló gondolatmenet szerepel a körosztási polinomokról szóló jegyzet 6. oldalának tetején.)

c) Az $x^2 + 1$ a kvaterniók fölött, hiszen gyöke i, j és k is.

d) Nem, $\mathbb{Z}_2$ fölött $x^3 + x^2$-nek a nulla kétszeres gyöke, és deriváltjának, ami x^2, szintén. Jó az x^2 is, amelynek a deriváltja nulla, és így nincs is értelme egyszeres gyökéről beszélni.

3. a) Nem, $\mathbb{R}[x]$-ben minden irreducibilis polinom legfeljebb másodfokú.

b) Ha p prím $\mathbb{Z}$-ben, és osztja az $f = gh$ polinomot, akkor $\mathbb{Z}_p[x]$-re áttérve, azaz f-et (együtthatónként) mod p véve $\overline{f} = 0$ adódik. Mivel ez az áttérés szorzattartó (lásd a körosztási jegyzetben a 3.2. Gyakorlatot), azt kapjuk, hogy $\overline{g}\overline{h} = \overline{gh} = 0$. A $\mathbb{Z}_p[x]$ nullosztómentessége miatt $\overline{g} = 0$ (és ekkor $p \mid g$), vagy $\overline{h} = 0$ (és ekkor $p \mid h$). Tehát p prím $\mathbb{Z}[x]$-ben.

c) Van, például $3x^{10} + 6$, ez a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, a $\mathbb{Z}$ fölött azonban $3(x^{10} + 2)$ nemtriviális felbontás, hiszen a 3 nem egység $\mathbb{Z}[x]$-ben.

d) Igen, minden elem nulla vagy egység, ezért az alaptétel állítása üres (hiszen a nem nulla és nem egység számokról szól), és így igaz.

4. a) A 7^{32}-t kár volt kiszámolni, hiszen az Euler-Fermat tétel szerint tudjuk, hogy 1-et kapunk modulo 96 (1 pont). Mindebből nem következik, hogy a 7 rendje 32 mod 96, mert ahhoz az kell, hogy kisebb pozitív kitevőre emelve nem kapunk 1-et mod 96 (1 pont).

b) Csak 1-et. Ugyanis $c^{16}+1 = \Phi_{32}(c)$, és a Dirichlet-tétel $nk+1$ esetének bizonyításánál tanultuk, hogy ha $p \mid \Phi_n(c)$ prím, akkor $p \mid n$, vagy $p \equiv 1 \ (n)$. Az állítás közvetlenül is igazolható a VIII/6. feladat mintájára (a megoldást lásd a körosztási jegyzetben a 13. oldalon), annak megmutatásával, hogy $o_p(c) = 32$.

5. a) Ha p páratlan (pozitív) prím, akkor az $x^2 \equiv -1 \ (p)$ kongruencia akkor és csak akkor oldható meg, ha $p \equiv 1 \ (4)$.

b) Nem, mert osztható $1 + i$-vel, hiszen a normája páros szám. Sőt, azt is tudjuk, hogy Gauss-prím normája csak prímszám, vagy (egy $4k - 1$ alakú) prím négyzete lehet.

c) $36 = 4 \cdot (2 + 1) \cdot (2 + 1)$, mert $25 = (2 + i)^2(2 - i)^2$, és így az alaptétel miatt osztói egyértelműen $\varepsilon(2 + i)^\alpha(2 - i)^\beta$ alakban írhatók, ahol ε egység, és $0 \le \alpha, \beta \le 2$.

d) Nem; láttuk, hogy $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, de $1 + i\sqrt{5}$ nem osztója sem 2-nek, sem 3-nak (ez az osztás közvetlen elvégzésével látható, de következik abból is, ha a normákat nézzük, vagy ha felhasználjuk, hogy 2 és 3 felbonthatatlanok, az egységek pedig csak ± 1).