Mat-tanári szak, első évfolyam, második félév
Vizsgadolgozat — 1998. május 29.

Minden kérdéscsoportot **külön lapra** írjunk, és minden lapon legyen rajta a szerző és a gyakorlatvezető neve. Aki felírja az *email címét* is, annak a javító igyekszik mihamarabb az eredményét emailben elküldeni. *Eredményhirdetés:* június 2 (kedd), reggel 9, az Algebra Tanszék környékén.

Valamennyi megoldásban **indoklás** (azaz bizonyítás vagy ellenpélda) **szükséges**, a puszta eredményért nem jár pont. A kétpontos kérdésekre a válasz általában mindössze egy-két sor, ami sokszor csak egy hivatkozás egy tételre (ez lehet olyan is, amit az előadáson nem bizonyítottunk) vagy egy definícióra. Ne keressünk hosszú, vagy trükkös megoldásokat. A két pont a teljesen helyes és precíz válaszért jár. Aki hibázik, de a lényeget látja, az egy pontot kap, ha a lényeg hiányzik, nulla pontot.

A vizsgán az átmenés szükséges és elégséges feltétele: Lényegében helyesen (azaz apróbb hibáktól eltekintve) le kell írni az első feladatban a bizonyítást, **ÉS** meg kell szerezni a dolgozat összpontszámának felét. Jeles az összpontszám 80 százalékáért jár (ha megvan a bizonyítás is).

1. *(10 pont)*
Bizonyítsuk be, hogy minden p prímre létezik primitív gyök mod p. Bizonyítás nélkül használhatók az elemrend, valamint a $\mathbb{Z}_p[x]$ polinomjainak alapvető tulajdonságai, a többi segédállítást bizonyítani kell.

2. *(2+2+2+2=8 pont)*

a) *Határozzuk meg a $\mathbb{G}[x]^\times$ csoport elemeit, és ezek rendjeit (itt $\mathbb{G}$ a Gauss-egészek gyűrűjét jelöli).*

b) *Amikor bebizonyítjuk a következő állítást:* „ha egy racionális együtthatós polinom oszt egy racionális együtthatós polinomot $\mathbb{C}[x]$-ben, akkor osztja $\mathbb{Q}[x]$-ben is”, *akkor a maradékos osztás egyértelműségét melyik gyűrűben alkalmazzuk?*

c) *Adjunk példát olyan nullosztómentes gyűrű fölötti polinomra, melynek több gyöke van, mint a foka.*

d) *Igaz-e tetszőleges test fölött, hogy ha egy polinomnak egy elem (pontosan) kétszeres gyöke, akkor a deriváltjának (pontosan) egyszeres gyöke?*

3. *(2+2+2+2=8 pont)*

a) *Irreducibilis-e az $x^6 + 2x + 2$ polinom $\mathbb{R}$ fölött?*

b) *Mondjuk ki azt a Gauss-lemmát, amihez az a tény kapcsolódik, hogy $\mathbb{Z}_p[x]$ nullosztómentes, és magyarázzuk el a kapcsolatot.*

c) *Van-e olyan tizedfokú, egész együtthatós polinom, mely $\mathbb{Q}$ felett felbonthatatlan, de $\mathbb{Z}$ felett nem?*

d) *Alaptételes gyűrű-e a valós számtest?*

4. *(2+2+2=6 pont)*

a) *Pistike kiszámolta 7^{32} értékét, megállapította, hogy az eredmény kongruens 1-gyel modulo 96, és kijelentette, hogy eszerint a 7 rendje 32 modulo 96. Mi volt erre a tanító néni* **két** *megjegyzése?*

b) *Milyen maradékot adhatnak a $c^{16} + 1$ szám páratlan prímosztói 32-vel osztva?*

c) *Mondjuk ki az RSA titkosírási módszer alapját képező lemmát.*

5. *(2+2+2+2=8 pont)*

a) *Mondjuk ki azt a számelméleti (egy kongruencia megoldhatóságáról szóló) tételt, amelynek kulcsszerepe van a Gauss-prímek meghatározásában.*

b) *Gauss-prím-e $1997 + 7991i$?*

c) *Hány osztója van a Gauss-egészek között a 25-nek?*

d) *Prímtulajdonságú-e $1 + i\sqrt{5}$ az $\{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ gyűrűben?*