Algebrai Számelmélet

1. feladatsor

beadható 2018. szeptember 19-ig

1. (2 pont) A kvadratikus reciprocitási tétel bizonyításának mintájára a nyolcadik egységgyököket vizsgálva adjunk képletet a $\left(\frac{2}{p}\right)$ Legendre szimbólumra.

---

2. (2+2 pont) Igazoljuk, hogy minden egyértelmű prímfaktorizációs tartomány (pl. $\mathbb{Z}$ és $K[x]$, ahol K test) egészre zárt, de $\mathbb{Z}[\sqrt{5}]$ nem. (Segítség: Gauss-lemma.)

3. (3+3 pont) Határozzuk meg $\mathbb{Z}$ egész lezártját $\mathbb{Q}[x]/(x^3-2)$-ben és $\mathbb{Q}[x]/(x^3-x-4)$-ben.

4. (3 pont) Legyen $A \subseteq B$ integritási tartományok, és legyen $\beta \in B$ egy invertálható elem. Igazoljuk, hogy$A[\beta] \cap A[\beta^{-1}]$ minden eleme egész A felett. (Segítség: Ha $\alpha \in A[\beta] \cap A[\beta^{-1}]$, akkor találjunk egy olyan $M \subseteq B$ végesen generált A-részmodulust B-ben, melyre $\alpha M \subseteq M$.)

5. (1+2+2 pont) Ebben a feladatban azt igazoljuk, hogy ha R egy egészre zárt gyűrű, akkor $R[x]$ is az.

   (a) Először vezessük vissza a feladatot arra, hogy $R[x]$ egészre zárt $K[x]$-ben. ($K[x]$ benne van $R[x]$ hányadostestében és egészre zárt, hiszen főideálgyűrű.)

   (b) Igazoljuk, hogy ha $f, g \in K[x]$ normált polinomok, melyekre $fg \in R[x]$, akkor f és g is $R[x]$-ben van. (Segítség: bontsuk mindkét polinomot gyöktényezők szorzatára egy bővebb testben.)

   (c) Ha egy $f \in K[x]$ gyöke egy $R[x]$ feletti k fokú normált polinomnak, akkor $f + x^N$ is gyöke egy ugyancsak k fokú normált polinomnak. Növeljük N-et és a normált polinom (melynek $f + x^N$ gyöke) konstans tagja felírható két normált polinom szorzataként, melyek közül az egyik épp $f + x^N$.

---

6. (1 pont) Mi $1+\sqrt{2}$ nyoma és normája a $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ bővítésben?

7. (2 pont) Vegyük a $\mathbb{Q}(i)/\mathbb{Q}$ bővítést. Ennek Galois-csoportja Z_2, speciálisan ciklikus. Mi itt egy $a+bi$ alakú szám normája? Mit mond Hilbert 90-es tétele ebben a speciális esetben a Pitagoraszi számhármasokról?

8. (3 pont) Hilbert 90-es tételének felhasználásával adjunk új bizonyítást arra a tételre, hogy ha K tartalmazza az n-edik egységgyököket, és L/K olyan Galois-bővítés, melyre $\mathrm{Gal}(L/K) \cong Z_n$, akkor L egy radikálbővítése K-nak.

9. (3 pont) Legyen $f(x) \in \mathbb{Z}[x]$ egy irreducibilis normált polinom. Tegyük fel, hogy f $\mathbb{Q}$ feletti felbontási testének Galois-csoportja Abel és $f(\alpha) = 0$ valamilyen $\alpha \in \mathbb{C}$, $|\alpha| = 1$ számra. Igazoljuk, hogy f összes többi (komplex) gyöke is 1 abszolútértékű.

10. (4 pont) Igazoljuk, hogy ha α egy olyan algebrai egész szám, melynek az összes Galois-konjugáltja 1 abszolútértékű, akkor α egységgyök.

11. (2+2 pont) Igazoljuk, hogy ha $K \leq L \leq M$ véges szeparábilis bővítések lánca, akkor $N_{M/K} = N_{L/K} \circ N_{M/L}$. Mi a helyzet, ha a bővítések nem szeparábilisek?

12. (3 pont) Igazoljuk, hogy ha L/K nem szeparábilis bővítés, akkor $Tr_{L/K}$ azonosan 0. (Segítség: a nyom tranzitív, ezért elég egy közbülső bővítésre belátni. Viszont ha L/K nem szeparábilis, akkor $\mathrm{char}(K) = p$ prím és van egy olyan közbülső bővítés, melynél egy adott elem p-edik gyökét adjungáljuk.)

13. (1+2+2+2+2 pont) Legyen L/K egy Galois-bővítés. Ebben a feladatban azt látjuk be, hogy van olyan $\gamma \in L$, melyre $\{\sigma(\gamma) \mid \sigma \in \mathrm{Gal}(L/K)\}$ lineárisan független K felett, azaz L egy bázisát alkotja. Az ilyen bázist normál bázisnak nevezzük.

    (*a*) Legyen $f(x) \in K[x]$ szeparábilis, normált polinom, mely L fölött $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$ gyöktényezők szorzatára bomlik. Legyen $g_i(x) := \frac{f(x)}{f'(\alpha_i)(x-\alpha_i)} \in L[x]$. Igazoljuk, hogy
    (*i*) $\sum_{i=1}^{n} g_i(x) = 1$ („parciális törtekre bontása $1/f(x)$-nek"), és
    (*ii*) $g_i(x)g_j(x) \equiv \begin{cases} 0 \mod (f(x)) & \text{ha } i \neq j \\ g_i(x) \mod (f(x)) & \text{ha } i = j \end{cases}$.

    (*b*) Legyen L/K Galois-bővítés, mint fent, és α olyan, melyre $L = K(\alpha)$, f pedig α minimálpolinomja. Legyen $\mathrm{Gal}(L/K) = \{\mathrm{id} = \sigma_1, \ldots, \sigma_n\}$ és $\alpha_i = \sigma_i(\alpha) \in L$. Képzzük az $A \in L[x]^{n\times n}$ mátrixot a következőképpen: legyen az i-edik sor j-edik eleme $\sigma_i(\sigma_j(g_1(x))) \in L[x]$. Mutassuk meg (az (*a*) rész segítségével), hogy $A^T A \equiv I \mod (f(x))$ (itt I az egységmátrix).

    (*c*) Tegyük fel, hogy K végtelen. A (*b*) részt felhasználva igazoljuk, hogy van olyan $\beta \in K$, melyre $\det(A(\beta)) = \det(\sigma_i\sigma_j(g_1(\beta)))_{i,j} \neq 0$. Speciálisan a $\gamma = g_1(\beta)$ választással a $\{\sigma_1(\gamma), \ldots, \sigma_n(\gamma)\}$ egy bázisa F-nek, mint K feletti vektortérnek.

    (*d*) Legyen most $K = \mathbb{F}_q$ egy véges test és legyen $|L/K| = n$ a fokszám. Határozzuk meg a $\mathrm{Frob}_q\colon L \to L$ K-lineáris leképezés minimálpolinomját. Segítség: Használjuk a Dedekind Lemmát és azt, hogy $\mathrm{Gal}(L/K)$ egy n-edrendű ciklikus csoport, Frob_q-val, mint generátorral.

    (*e*) Tegyük L-et $K[x]$-modulussá úgy, hogy az x-szel való szorzás a Frob_q lineáris leképezés. A főideálgyűrűk feletti végesen generált modulusok alaptételének alkalmazásával (vagy másképp) igazoljuk, hogy ekkor $L \cong K[x]/(x^n - 1)$, tehát ennél az azonosításnál a $\gamma := 1 + (x^n - 1)$ jó választás.