

Algebrai Számelmélet

6. gyakorlat

2015. október 21.

1. (3 pont) Igazoljuk, hogy ha L/K egy olyan Galois-bővítése számtesteknek (K/\mathbb{Q} véges), melynek Galois-csoportja nem ciklikus, akkor legfeljebb véges sok olyan \mathfrak{p} prím van K -ban, melyet csak egyetlen L -beli prím oszt.
 2. (3 pont) Legyen K/\mathbb{Q} egy olyan Galois bővítés, melynek Galois csoportja nem Abel. Igazoljuk, hogy semelyik p prím sem marad prím \mathcal{O}_K -ban.
 3. (5 pont) Legyen K/\mathbb{Q} egy tetszőleges véges bővítés. Igazoljuk, hogy végtelen sok olyan p prím van, ami \mathcal{O}_K -ban teljesen felbomlik.
 4. (3 pont) Legyen L/K egy véges bővítés számtesteknek, és legyen $L \leq F$ az L test normális lezártja. Vezessük be a következő jelöléseket: $G = \text{Gal}(F/K)$, $H = \text{Gal}(F/L)$, $G_P \leq G$ a felbontási részcsoportha egy $\mathfrak{p} \triangleleft \mathcal{O}_K$ feletti $P \triangleleft \mathcal{O}_F$ prímnek. Létesítsünk bijekciót a \mathfrak{p} fölötti L -beli prímekek és a $H \backslash G / G_P$ kettős mellékosztályok között.
 5. (5 pont) Legyen L/K egy – nem feltétlenül Galois – feloldható p -fokú bővítése számtesteknek, ahol p prímszám (tehát L normális lezártjának K feletti Galois-csoportja feloldható). Tegyük fel továbbá, hogy az $\mathfrak{p} \triangleleft \mathcal{O}_K$ prímideál nem ágazik el L -ben, és van legalább kettő darab egy inerciafokú prímosztója L felett. Igazoljuk, hogy \mathfrak{p} teljesen felbomlik L -ben. (Segítség: Felhasználhatjuk Galois tételét, mely szerint ha G egy prímfokú tranzitív feloldható permutációcsoport, akkor G tetszőleges egységtől különböző elemének csak legfeljebb 1 fixpontja van.)
 6. (4 pont) Igazoljuk, hogy minden A Abel-csoportra van olyan L/\mathbb{Q} Galois-bővítés, melyre $\text{Gal}(L/\mathbb{Q}) \cong A$. (A feladat állítása igaz tetszőleges feloldható csoportra (ez Safarevics tétele), de általában véges csoportra megoldatlan.)
 7. (3 pont) Legyen n egy páratlan szám. Jellemezzük \mathbb{Q} azon másodfokú bővítéseit, melyeket $\mathbb{Q}(\zeta_n)$ tartalmazza.
 8. (3 pont) Igazoljuk, hogy minden $d \in \mathbb{Z}$ négyzetmentes számra van olyan n pozitív egész szám, melyre $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_n)$.
 9. (3 pont) Igazoljuk, hogy $q \geq 3$ esetén $\mathbb{Q}(\zeta_{2^q})$ kvadratikus résztesteik éppen $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$.
-

A következő feladatok némileg egymásra épülnek. A cél itt a Fermat-sejtés első esetének igazolása reguláris prímekre.

10. (3 pont) Igazoljuk, hogy a

$$\begin{aligned} \mathcal{O}_n^\times &\rightarrow \mu_n/(\mu_n)^2 \\ u &\mapsto \frac{u}{\bar{u}} \end{aligned}$$

leképezés jóldefiniált és csoporthomomorfizmus, ha \mathcal{O}_n az n -edik körosztási test egészeinek gyűrűjét jelöli. (Az állítás egyébként minden CM-testre igaz, ahol egy F testet CM-testnek nevezünk (CM=complex multiplication), ha F egy teljesen képzetes (azaz $r = 0$) másodfokú bővítése egy teljesen valós (azaz $s = 0$) F^+ testnek.)

11. (3 pont) Legyen p egy páratlan prímszám és jelöljük \mathcal{O}_{p^k} -nak a p^k -edik körosztási testet. Igazoljuk, hogy $\mathcal{O}_{p^k}^\times$ -ben minden u elem felírható $u = \zeta v$ alakban, ahol ζ primitív p^k -edik egységgyök, $v \in \mathbb{Z}[\zeta] \cap \mathbb{R}$ pedig valós.

Tegyük fel, hogy $p \nmid xyz$ olyan egész számok, melyekre $x^p + y^p = z^p$ ($2 < p$ prím).

12. (1+1 pont) Modulo 9 vizsgálódva igazoljuk, hogy $p \neq 3$. Modulo 25 vizsgálódva igazoljuk, hogy $p \neq 5$.

Legyen tehát mostantól $p > 5$ és jelöljük ζ -val egy fix primitív p -edik egységgyököt.

13. (1 pont) Feltehetjük, hogy az x, y, z számok páronként relatív prímelek, továbbá azt is, hogy $p \nmid x - y$.

14. (2 pont) Igazoljuk, hogy az $x + y, x + y\zeta, \dots, x + y\zeta^{p-1}$ számok páronként relatív prímelek \mathcal{O}_p -ben.

15. (2 pont) Igazoljuk, hogy minden $\alpha \in \mathcal{O}_p$ -re $\alpha^p \in \mathbb{Z} + p\mathcal{O}_p$ (azaz van olyan $a \in \mathbb{Z}$, melyre $a - \alpha^p$ osztható p -vel).

16. (2 pont) Legyen $\alpha = a_0 + a_1\zeta + \dots + a_{p-1}\zeta^{p-1}$, ahol $a_i \in \mathbb{Z}$ ($i = 0, \dots, p-1$) és legalább az egyik $a_i = 0$. Igazoljuk, hogy ha $\alpha \in n\mathcal{O}_p$ alkalmas $n \in \mathbb{Z}$ egész számmal, akkor $n \mid a_i$ minden $i = 0, \dots, p-1$ -re.

17. (2 pont) Ha egy számtest osztályszámát nem osztja p és egy ideál p -edik hatványa főideál, akkor az ideál maga is főideál.

18. (3 pont) Tegyük fel, hogy p nem osztja \mathcal{O}_p osztályszámát. Lássuk be, hogy a fenti $x^p + y^p = z^p$ egyenletnek nincs olyan megoldása, amire $p \nmid xyz$. Segítség: alakítsuk az egyenletet $\prod_{j=0}^{p-1} (x + y\zeta^j) = (z)^p$ alakba. Mindkét oldalt bontsuk \mathcal{O}_p -ben prímeállok szorzatára. Vegyük észre, hogy feltételek miatt $x + \zeta^j y = u_j \alpha_j^p$ alakú, ahol $u_j \in \mathcal{O}_p^\times$ egység, $\alpha_j \in \mathcal{O}$. Most α_1 -re alkalmazzuk a 15. Feladatot, u_1 -re pedig a 11. Feladatot, hogy találhassunk egy olyan $r \in \mathbb{Z}$ egész számot, melyre $x + \zeta y = \zeta^r v a$, ahol $v \in \mathbb{R}$, $a \in \mathbb{Z}$. Az előző egyenletet megkonjugálva kapjuk, hogy $p \mid x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y$. A 16. Feladat segítségével jussunk ellentmondásra.