Semestral

Algebraic Number Theory

Instructor: Ramdin Mawia **Time:** November 28, 2022; 10:00–13:00.

INSTRUCTIONS

i. Attempt FOUR problems, including problem n° 2. Each question carries 15 marks. The maximum you can score is **50**.

ii. MMath students should attempt at least one problem from each of Group I and Group II.

iii. BMath students can choose any of the problems besides problem n° 2.

iv. You may use any of the results proved in class, unless you are asked to prove or justify the result itself. You may also use results from other problems in this question paper, provided you attempt and correctly solve the problem.

Group I

1. Prove that if L/K is a Galois extension of number fields such that $\mathrm{Gal}(L/K)$ is not cyclic, then no prime of K remains inert in L.

2. Let $p \equiv 3 \pmod 4$ be a prime and let $L = \mathbb{Q}[\omega]$ with $\omega = e^{2\pi i/p}$.

   (a) Show that L contains a unique quadratic extension K of $\mathbb{Q}$.

   (b) Prove that if $n = \mathrm{N}_{L/\mathbb{Q}}x \in \mathbb{Z}$ for some $x \in \mathbb{Z}[\omega]$, then $n = z\bar{z}$ for some $z \in \mathbb{Z}[(1+\sqrt{-p})/2]$. [*Hint*: Use transitivity of the norm on the tower $\mathbb{Q} \subset K \subset L$.]

   (c) Let $q \equiv 1 \pmod p$ be another prime. Prove that $\Psi_p(X) := 1 + X + \cdots + X^{p-1}$ splits in $\mathbb{Z}/q\mathbb{Z}[X]$.

   (d) Conclude that $\mathbb{Z}[\omega]$ contains an ideal $\mathfrak{Q}$ such that $[\mathbb{Z}[\omega] : \mathfrak{Q}] = q$.

   (e) Prove that if $\mathfrak{Q}$ is principal then $q = x^2 + xy + (p+1)y^2/4$ for some integers x, y.

   (f) Deduce that for $p = 23$, the ring $\mathbb{Z}[\omega]$ is not a PID.[1] [*Hint*: Think of the smallest prime $q \equiv 1 \pmod{23}$.]

3. Give the definitions of Dedekind domain and discrete valuation ring as in class. Give a complete proof of the following standard result: A Noetherian integral domain A is a Dedekind domain if and only if $A_{\mathfrak{p}}$ is a discrete valuation ring for every maximal ideal $\mathfrak{p}$ of A. Prove that the integral closure of $\mathbb{Z}$ in $\mathbb{R}$ is not a Dedekind domain. [*Hint*: First prove that in a Noetherian integral domain, every nonzero, nonunit can be written (not necessarily uniquely) as a product of irreducibles.]

4. Define the *absolute discriminant* Δ_K of a number field K and prove that it is congruent to either 0 or 1 mod 4. Use this to find the ring of integers in $\mathbb{Q}[\sqrt{d}]$ for a squarefree integer d.

5. Let A be a Dedekind domain with field of fractions K and let B be the integral closure of A in a finite separable extension L of K. Define the discriminant and norm of a fractional ideal $\mathfrak{b}$ of B, and the different of B over A. Prove that the discriminant of B over A is the norm of the different of B over A, i.e., $\mathrm{N}_K^L \mathfrak{D}_{B/A} = \Delta_{B/A}$.

6. State true or false, with brief but complete justifications (**any five**):

   (a) The splitting field of the polynomial $X^3 + X + 5$ over $\mathbb{Q}$ is a cyclotomic extension of $\mathbb{Q}$.

   (b) If $\mathfrak{a}$ is a nonzero ideal of a Dedekind domain A, then $A/\mathfrak{a}$ is a finite ring.

   (c) 2022 is a square modulo 2023.

   (d) The ring of integers in $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ is $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$.

   (e) The prime 17 is inert in the field $\mathbb{Q}[\alpha]$ where $\alpha^3 + 10\alpha + 1 = 0$.

   (f) The integral closure of $\mathbb{Z}[[X]]$ in $\mathbb{Q}((X))$ is $\mathbb{Z}[[X]]$.

Turn the page please ↪

[1] This result is due to Dedekind.

Group II

7. Let K be a nonarchimedean local field with absolute value $|\cdot|$, and let L/K be a finite extension. Prove that $|\cdot|$ has a unique extension $|\cdot|_L$ to L given by $|y|_L = \left|N_{L/K}y\right|^{1/n}$ where $n = [L : K]$. Prove that L is also a nonarchimedean local field with respect to $|\cdot|_L$.

8. Let $(K, |\cdot|)$ be a local field with valuation ring A and residue cardinality $q = \left|\overline{K}\right| = p^f$ for some prime p and some integer $f \geqslant 1$.

   i. Prove that the polynomial $t(X) = X^q - X$ splits completely in K.

   ii. Let $\mathbb{F}$ be the set of roots of $t(X)$ and let $\mathbb{F}^\times = \mathbb{F}\backslash\{0\}$ be the set of nonzero roots. Prove that $\mathbb{F}^\times$ is a subgroup of $A^\times$ isomorphic to $\overline{K}^\times$.

   iii. If $\mathrm{char}K = p > 0$, show that $\mathbb{F}$ is the unique subfield of K isomorphic to $\overline{K}$.

9. Let L/K be an unramified, finite extension of local fields. Show that the Galois group $\mathrm{Gal}(\overline{L}/\overline{K})$ of the residue extension $\overline{L}/\overline{K}$ is cyclic. Deduce that for a Galois extension of number fields L/K, the decomposition group $G_{\mathfrak{P}}$ is cyclic for almost all primes $\mathfrak{P}$ of L.

10. State true or false, with brief but complete justifications (**any five**):

    (a) The field of Laurent series $\mathbb{Q}((T))$ in one variable T with the T-adic valuation $v_T(T) = 1$ is a local field.

    (b) If $(K, |\cdot|)$ is a nonarchimedean local field then the corresponding valuation is a discrete valuation.

    (c) There is a local field which is countable.

    (d) Any nonarchimedean field is totally disconnected.

    (e) The field of rational numbers $\mathbb{Q}$ is complete with respect to the 7-adic absolute value $|\cdot|_7$.

    (f) Let $(K, |\cdot|)$ be a valued field and let V be a finite-dimesional K-vector space. Then any two norms on V are equivalent.