Semestral

Algebraic Number Theory

Instructor: Ramdin Mawia | Marks: **50** | **Time:** April 28, 2025; 10:00–13:00.

BMath students can choose any FOUR problems. MMath & JRF students should attempt TWO problems each from Group I and Group II. The maximum you can score is 50. You may use any of the results proved in class, unless you are asked to prove or justify the result itself.

Group I

1. State whether the following statements are true or false, with brief justifications (**any two**): **13**
   i. Let $\omega \in \mathbb{C}$ be a primitive 73rd root of unity. The field $K = \mathbb{Q}[\omega]$ contains an element α such that $\alpha^3 = \alpha + 7$.
   ii. The field $\mathbb{Q}$ has no unramified extensions (except itself).
   iii. Let L/K be a Galois extension of number fields. If there is a prime of K which remains inert in L, then $\mathrm{Gal}(L/K)$ is cyclic.

2. Prove that the class number of $\mathbb{Q}[\sqrt{-37}]$ is 2. Using this or otherwise, show that the Diophantine equation $X^3 - Y^2 = 37$ has no solutions in integers. **13**

OR

2′ Prove that the ring of integers in $\mathbb{Q}[\sqrt{-11}]$ is a Euclidean domain. Use this to show that the only integer solutions to the Diophantine equation $X^3 - Y^2 = 11$ are $(15, \pm 58)$.

3. Let K/F be a finite extension of number fields. Prove that a prime of F splits completely in K if and only if it splits completely in the Galois closure of K/F. **13**

4. Show that the polynomial $f(X) = X^3 + 3X^2 + 5X + 8 \in \mathbb{Z}[X]$ is irreducible. Let $K = \mathbb{Q}[\alpha]$ where $\alpha \in \mathbb{C}$ is a root of $f(X)$. Find the factorisations (into prime ideals) of $2, 3$ and 5 in $\mathcal{O}_K$. **13**

5.[¶] Let $n > 1$ be a squarefree integer.
   i. Show that -1 is a sum of squares in $\mathbb{Z}/n\mathbb{Z}$. [*Hint.* Use the CRT to prove that it is enough to look at primes, for which there is a standard argument.] **2**
   ii. Let $u, v \in \mathbb{Z}$ be such that $u^2 + v^2 + 1 \equiv 0 \pmod{n}$. Prove that **5**
   $$\Gamma := \{(a, b, c, d) \in \mathbb{Z}^4 : c \equiv au + bv \pmod{n} \text{ and } d \equiv av - bu \pmod{n}\}$$
   is a lattice of full rank in $\mathbb{R}^4$, of covolume n^2.
   iii. Let $B_r \subset \mathbb{R}^4$ denote the open ball of radius $\sqrt{r}$ centred at 0. Show that $\Gamma \cap B_{2n} \neq \{0\}$. [*Given:* $\mathrm{vol}(B_r) = \pi^2 r^2/2$.] **3**
   iv. Use the above to prove **Lagrange's Theorem:** Every nonnegative integer is a sum of four squares. **5**

6. Let K be a number field and $\mathfrak{a}$ be a given ideal of $\mathcal{O}_K$. Given an integer $n > 0$, prove that there are at most a finite number of extensions L/K such that $[L : K] = n$ and $\Delta_{L/K} = \mathfrak{a}$. **13**

End of Group I

Turn the page please ↪

[¶] This has extra marks as bonus.

Group II

7. Let p be an odd prime.

   i. Prove that $\mathbb{Q}_p$ does not contain any primitive p^n-th root of unity for any $n \geqslant 1$. [*Hint.* Enough to prove for $n = 1$, to which Eisenstein applies.] **6**

   ii. Let $\mu(\mathbb{Q}_p)$ denote the group of roots of unity in $\mathbb{Q}_p$. Show that $\mu(\mathbb{Q}_p)$ is a cyclic group of order $p-1$. [*Hint.* The "only" natural map $\mu(\mathbb{Q}_p) \to (\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ is an isomorphism, by Hensel and Part i. above.] **7**

---

8. Let $(K, |\cdot|)$ be a nonarchimedean local field of characteristic zero with local ring $(A, \mathfrak{m})$ and residue field $k = A/\mathfrak{m}$. Let U be the group of units in A. Prove the following:

   i. $K^\times \cong U \times \mathbb{Z}$ as topological groups in their usual topologies. **3**

   ii. $1 + \mathfrak{m}^j$ is an open subgroup of U for each $j \geqslant 1$ and **5**

$$U / (1 + \mathfrak{m}) \cong (k^\times, \times)$$
$$(1 + \mathfrak{m}^j) / (1 + \mathfrak{m}^{j+1}) \cong (k, +).$$

   iii. Prove that for any positive integer n, the quotient group $K^\times / (K^\times)^n$ is finite, where $(K^\times)^n$ denotes the subgroup of nth powers in $K^\times$. **5**

   iv. **[Bonus]** Show that $[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^n] = np^{v_p(n)} |\mu_n(\mathbb{Q}_p)|$ where $\mu_n(\mathbb{Q}_p)$ denotes the group of nth roots of unity in $\mathbb{Q}_p$. **5**

---

9. Let E/F be an unramified extension of nonarchimedean local fields of characteristic 0 with respective valuation rings $\mathcal{O}_E$ and $\mathcal{O}_F$. Prove that there is some $x \in \mathcal{O}_E$ such that $\mathcal{O}_E = \mathcal{O}_F[x]$. **13**

---

10. State true or false, with brief but complete justifications (**any two**): **13**

    i. 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.

    ii. There is a square root of p in $\mathbb{Q}_p$.

    iii. The ring of p-adic integers $\mathbb{Z}_p$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

---

11. i. Let K be a local field and V be a Hausdorff topological vector space over K. If V is locally compact, prove that it is of finite dimension over K. **6**

    ii. If K is nonarchimedean and of characteristic 0, prove that it is a finite extension of $\mathbb{Q}_p$ for some prime p. **7**

The End

Note: The **Minkowsky Bound** says that for any fractional ideal $\mathfrak{f}$ of a number field K, there is an integral ideal $\mathfrak{a}$ such that

i. $\mathfrak{a}\mathcal{P}_K = \mathfrak{f}\mathcal{P}_K$;

ii. $\|\mathfrak{a}\| \leqslant \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |\Delta_K|^{1/2}$,

where $[K : \mathbb{Q}] = n = r + 2s$ in the usual notation, Δ_K is the absolute discriminant of K, and $\|\mathfrak{a}\|$ is the numerical norm of $\mathfrak{a}$. Also, $\mathcal{P}_K$ is the group of principal fractional ideals.