Back paper

Algebraic Number Theory

Instructor: Ramdin Mawia Marks: **50** **Time:** June 05, 2025; 14:00–17:00.

Attempt THREE problems. The maximum you can score is 45. Be brief but complete; you may use results proved in class or problem sessions, unless you are asked to prove the result itself. Clearly mention the results you use.

1. State whether the following statements are true or false, with brief justifications (**any two**): **15**
   i. Let $\omega \in \mathbb{C}$ be a primitive 23rd root of unity. The field $K = \mathbb{Q}[\omega]$ contains an element α such that $\alpha^3 = \alpha + 2$.
   ii. The ring of integers in $\mathbb{Q}[\sqrt{-19}]$ is $\mathbb{Z}[\sqrt{-19}]$.
   iii. The number fields $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are isomorphic.

2. Prove that the class number of $\mathbb{Q}[\sqrt{-23}]$ is 3. **15**

3. Let $K/F, L/F$ be finite extensions of number fields. Prove that a prime of F splits completely in both K and L if and only if it splits completely in the compositum KL. **15**

4. Show that the polynomial $f(X) = X^3 + X + 3 \in \mathbb{Z}[X]$ 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 $\mathcal{O}_K$. **15**

5. Let $p \equiv 1 \pmod 4$ be a prime. Show that $u^2 \equiv -1 \pmod p$ for some $u \in \mathbb{Z}$. Fix one such u. Define **15**

$$\Gamma = \{(a, b) \in \mathbb{Z}^2 : a \equiv bu \pmod p.\}$$

   i. Prove that Γ is a full lattice in $\mathbb{R}^2$ of covolume p, such that $a^2 + b^2 \equiv 0 \pmod p$ for every $(a, b) \in \Gamma$.
   ii. Let $B_r := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < r\}$. Prove that $\Gamma \cap B_{2p} \neq \{0\}$.
   iii. **[Fermat, Euler]** Use the above to show that there are integers a and b such that $a^2 + b^2 = p$.

6. Let L/K be a Galois extension of number fields. Prove that the decomposition group $G_{\mathfrak{P}}$ is cyclic for almost all primes $\mathfrak{P}$ of L. **15**

–The End–