Midsemestral

Algebraic Number Theory

Instructor: Ramdin Mawia Marks: **30** **Time:** February 20, 2025; 10:00–13:00.

Attempt FOUR problems. The maximum you can score is 30. 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. Prove that the polynomial $f(X) = X^3 + 5X + 9 \in \mathbb{Z}[X]$ is irreducible. Let $\alpha \in \mathbb{C}$ be a root of $f(X)$ and let $K = \mathbb{Q}[\alpha]$. Prove that the ring of integers in K is $\mathbb{Z}[\alpha]$ and find the factorisations (into prime ideals) of $2, 3$ and 5 in $\mathbb{Z}[\alpha]$. **8**

2. Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic field, with $d \in \mathbb{Z}$ squarefree. Find the ring of integers $\mathcal{O}_K$ in K and prove that an odd prime $p \nmid d$ is inert in $\mathcal{O}_K$ if and only if d is not a square mod p. **8**

OR

2′. Let $K \subset \mathbb{C}$ be a cubic field, i.e., $[K : \mathbb{Q}] = 3$. Prove that $K = \mathbb{Q}[\alpha]$ for some $\alpha \in \mathbb{C}$ with minimal polynomial $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$. Suppose there is a prime p such that K is contained in $\mathbb{Q}[\omega]$ for some primitive pth root ω of unity. Show that all roots of $f(X)$ must be real.

3. Let A be a DVR with field of fractions F. Let K be a finite separable extension of F and B be the integral closure of A in K. Prove that B is a PID. **8**

4. Prove that every ideal in a Dedekind domain is generated by at most two elements. **8**

5. State whether the following statements are true or false, with complete justifications: **8**

   i. Let p be an odd prime and $\omega \in \mathbb{C}$ be a primitive pth root of 1. Then the field $\mathbb{Q}[\sqrt{\varepsilon_p p}]$ with $\varepsilon_p = (-1)^{(p-1)/2}$ is the unique quadratic field contained in $\mathbb{Q}[\omega]$.

   ii. The polynomial $p(X) = X^3 + 2X + 7 \in \mathbb{Z}[X]$ is irreducible and for any root $\alpha \in \mathbb{C}$ of $p(X)$, the ring of integers in $\mathbb{Q}[\alpha]$ is $\mathbb{Z}[\alpha]$.

6. Let K/F be a finite Galois extension of number fields with $A = \mathcal{O}_F, B = \mathcal{O}_K$. Given a prime $\mathfrak{p}$ of A, prove that $\mathrm{Gal}(K/F)$ acts transitively on the primes of B lying above $\mathfrak{p}$. Derive that the fundamental identity then takes the form $efg = [K : F]$. **8**

7.[¶] Let $A \subset B$ be integral domains such that B is integral over A. For any prime ideal $\mathfrak{p}$ of A, prove that $\mathfrak{p}B \neq B$ and that there is at least one prime ideal $\mathfrak{P}$ of B such that $\mathfrak{P} \cap A = \mathfrak{p}$. Also prove that in this situation, $\mathfrak{p}$ is maximal if and only if $\mathfrak{P}$ is. **10**

[¶] This has an extra 2 marks as bonus.