**Second semester 2014-2015**
**Midsemestral exam**
**Algebraic Number Theory**
**B.Math.(Hons.) IIIrd year**
**Instructor : B.Sury**
**Marks : 8, 8, 8, 10, 12, 14 for Questions 1 to 6 respectively**
**Total marks : 60**

**Q 1.** Let $K$ be an algebraic number field and let $O_K$ denote its ring of integers. Let $P$ be a non-zero prime ideal. Prove that $N(P)^n = N(P^n)$ where $N$ stands for the norm of an ideal.

**OR**

Define a fractional ideal $I$ in an integral domain $A$. If $I$ is a fractional ideal such that there exists a fractional ideal $J$ with $IJ = A$, then prove $J = \{x \in K : xI \subset A\}$ and that $I$ is a finitely generated module.

.

---

**Q 2.** Suppose $f := X^n + aX + b$ is irreducible over $\mathbb{Q}$ for some $a, b \in \mathbb{Q}$. Let $f(\alpha) = 0$. Determine the discriminant of $\{1, \alpha, \cdots, \alpha^{n-1}\}$.

**OR**

If $I$ is a non-zero ideal in $O_K$, where $K$ is an algebraic number field, prove that $N(I)/|disc(O_K)|$ is a perfect square.

.

---

**Q 3.** Let $A$ be a Dedekind domain. Prove that an ideal $I$ divides an ideal $J$ if and only if $I \supset J$.

**OR**

If $K$ is an algebraic number field, show that $K = \mathbb{Q}(\alpha)$ where $\alpha \in O_K$. If the minimal polynomial of $\alpha$ has $r_1$ real roots and $2r_2$ non-real roots, determine, with proof, the value of $\frac{disc(K)}{|disc(K)|}$ in terns of $r_1$ and $r_2$.

**Q 4.** Let $N/K$ be a Galois extension of number fields. If $Q$ is a prime ideal of $O_N$ lying over a prime $P$ of $O_K$, look at the decomposition group $D$ of $Q$ over $P$. If $L = N^D, P_D = Q \cap O_L$, prove that $f(Q/P) = f(Q/P_L)$ and $e(Q/P) = e(Q/P_L)$.

**OR**

Let $L/K$ be a Galois extension of number fields. For a prime ideals $P$ of $O_K$, let $P_1, \cdots, P_g$ be the primes of $O_L$ lying over $P$. Prove that $g$ divides $[L : K]$. Further, show that the decomposition groups $D(P_1/P), \cdots, D(P_g/P)$ are mutually conjugate subgroups.

---

**Q 5.** If $K$ is a number field, and $P$ is a non-zero prime ideal of $O_K$ such that $P^e \supset (P \cap \mathbb{Z})O_K$, then prove that $P^{e-1} \supset Diff(K)$, where $Diff(K)$ is the different ideal of $O_K$.

**OR**

If $L/K$ is an extension of number fields, and $P$ is a non-zero prime ideal of $O_K$, let $PO_L = P_1^{e_1} \cdots P_g^{e_g}$ with $P_i$ prime ideals of $O_L$. Prove that the set of prime ideals $Q$ of $O_L$ lying over $P$ coincides with the set $\{P_1, \cdots, P_g\}$.

.

---

**Q 6.** Let $p$ be an odd prime and $L = \mathbb{Q}(\zeta_{p^2})$ where $\zeta_{p^2}$ is a primitve $p^2$-th root of unity. Consider the unique subfield $K$ of $L$ of degree $p$ over $\mathbb{Q}$. Prove that 2 splits completely in $K$ if and only if $2^{p-1} \equiv 1 \bmod p^2$.

**OR**

Let $p \equiv 1 \bmod 3$ be a prime. Let $K \subset \mathbb{Q}(\zeta_p)$ be the unique subfield whose degree is 3 over $\mathbb{Q}$. Prove that a prime $q \neq p$ splits completely in $O_K$ if and only if $q$ is a cube mod $p$.
Use $q = 2$ and $p = 43$ to give an example of a cubic extension $E$ of $\mathbb{Q}$ for which $O_E$ is not of the form $\mathbb{Z}[\alpha]$.