M.Math. IInd year — II Semestral exam 2005
Algebraic number theory — B.Sury
Answer any six

Q 1. *Let* $[K : Q] = n$ *and* $I \neq 0$ *be an ideal in* $\mathcal{O}_K$. *Prove :*
(a) $I = \sum_{i=1}^{n} Z\alpha_i$ *for some* α_i*'s with* $K = \sum_{i=1}^{n} Q\alpha_i$.
(b) $I \cap Z \neq 0$ *and* $\mathcal{O}_K/I$ *is finite.*

Q 2. *For any Galois extension* L/K *of number fields and prime ideal* P *of* $\mathcal{O}_L$, *show that the decomposition group at* P *surjects onto the Galois group of the residue field extension.*

Q 3. *For a prime* $p \geq 3$, *recall that* $K = Q(\sqrt{\pm p})$ *is contained in* $L = Q(\zeta_p)$. *Prove that a prime* q *splits completely in* $\mathcal{O}_K$ *if, and only if, it splits into an even number of primes in* $\mathcal{O}_L$.

Q 4. *Recall that for a number field* K *of degree* n *over* Q, *elements* $\alpha_1, \cdots, \alpha_n$ *in* $\mathcal{O}_K$ *for which disc*$(\alpha_1, \cdots, \alpha_n)$ *is a nonzero, square-free integer, form an integral basis. Assume this. Let* $K = Q(\alpha)$ *where* $\alpha^3 = \alpha + 1$. *Prove that* $\mathcal{O}_K = Z[\alpha]$.

Q 5. *Solve the equation* $x^2 - 2y^2 = 1$ *in integers. Quote precisely the results you use.*

Q 6. *Show that the radius of convergence of* $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ *is* $p^{-1/(p-1)}$ *in* k *where* $[k : Q_p] < \infty$.

Q 7. *For a modulus* $\mathcal{M}$ *of a number field* K, *define the ray class group mod* $\mathcal{M}$. *Show that* $I_K^{\mathcal{M}}/i(K_{\mathcal{M}}) \cong C_K$, *the class group of* K.

Q 8. *State the Frobenius density theorem and use it to deduce that for an abelian extension* L/K, *the Artin map gives a surjection from* $I_K^{\mathcal{M}}$ *onto Gal*(L/K), *provided* $\mathcal{M}$ *is divisible by all ramified places.*

Q 9. *Let* $G = <\sigma>$ *be a cyclic group of order* n *acting on a free abelian group* $A = \sum_{i=1}^{d} Zv_i$ *of rank* d *dividing* n *in the following manner :*

$$\sigma(v_i) = v_{i+1} \ \forall \ i < d \ ; \ \sigma(v_d) = v_1.$$

Compute the Herbrand quotient $q(A)$.