

**M.Math. IInd year — II Semestral exam 2009**

**Algebraic number theory — B.Sury**

**Answer any FIVE**

**Be brief; quote precisely the results you use.**

**Q 1.**

For any Galois extension  $L/K$  of number fields, show that the decomposition group at almost all prime ideals of  $\mathcal{O}_L$  are cyclic.

**OR**

Prove that for any Galois extension  $K$  of  $\mathbf{Q}$ , the Galois group is generated by the various inertia subgroups of the primes.

**Q 2.**

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

**OR**

Determine with proof the unramified extension of a given degree  $n$  over  $\mathbf{Q}_p$ .

**Q 3.**

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  $K$ .

**OR**

Let  $f \in \mathcal{O}_K[X]$  be monic, and assume that the Galois group of  $f$  over  $K$  fixes at least one root of  $f$ . Then, for every non-zero prime ideal  $P$  of  $\mathcal{O}_K$ , the equation  $f(X) = 0$  has a solution in  $\mathcal{O}_K \bmod P$ .

**Q 4.**

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  $\text{Gal}(L/K)$ , provided  $\mathcal{M}$  is divisible by all ramified places.

**OR**

State the Frobenius density theorem and use it to prove that in a cyclic extension of algebraic number fields, infinitely many primes are inert.

P.T.O.

**Q 5.**

Let  $G = \langle \sigma \rangle$  be a cyclic group of order  $n$  acting on a free abelian group  $A = \sum_{i=1}^d \mathbb{Z}v_i$  of rank  $d$  dividing  $n$  in the following manner :

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

Compute the Herbrand quotient  $q(A)$ .

**OR**

Let  $L/K$  be a cyclic extension of algebraic number fields. For a finite place  $v$  of  $L$ , show that the unit group  $U_v$  of  $L_v$  is a module for the decomposition group at  $v$  and that  $H^1(U_v)$  has order  $e_v$ .

**Q 6.**

Let  $n!(X^n/n! + X^{n-1}/(n-1)! + \dots + X + 1) = f(X)g(X)$  with  $f, g \in \mathbb{Z}[X]$  where  $f$  is irreducible. Prove that any prime  $p$  dividing  $f(0)$  is  $\leq \deg(f)$ .

*Hint:* Work in the field  $K = \mathbb{Q}(\theta)$  where  $\theta$  is a root of  $f$ . Write

$$\theta^n + n\theta^{n-1} + \dots + n!\theta = -n!$$

and consider the  $\mathcal{P}$ -adic valuations of both sides for some  $\mathcal{P}$  lying over  $p$ .

**OR**

Let  $K = \mathbb{Q}(\zeta)$ , where  $\zeta$  is a primitive  $n$ -th root of unity. If  $S$  is the set of prime ideals containing  $(n)$  and  $I_Q(S)$  denotes the group of fractional ideals generated by primes outside  $S$ , find the image and the kernel of the Artin map from  $I_Q(S)$  to  $\text{Gal}(K/Q)$ .