[This question paper contains 2 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 5149 **L**

Unique Paper Code : 2354000016

Name of the Paper : Rings and Fields

Name of the Course : **Common Prog Group (Generic Elective)**

Semester : VIII

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **All** questions are compulsory and carry equal marks.
3. Attempt **two** parts from each question.

1. (a) If F is a field, prove that its only ideals are (0) and F itself. Hence prove that any homomorphism of a field is either an isomorphism or maps every element to 0.

(b) Let R be a commutative ring and $a \in R$. Show that $aR = \{ar \mid r \in R\}$ is a two-sided ideal of R. Give an example to show this may fail if R is not commutative.

(c) Let U and V be ideals of a ring R. Define $U + V = \{u + v \mid u \in U, v \in V\}$.

(i) Prove that U + V is an ideal of R.

(ii) Prove that UV is an ideal of R.

(iii) Prove that $UV \subseteq U \cap V$.

2. (a) Prove that a necessary and sufficient condition that an element a in a Euclidean ring be a unit is that d(a) = d(1), where d is the Euclidean valuation function.

(b) Let R be a Euclidean ring. Prove that any two elements a and b in R have a greatest common divisor d. Moreover show that $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

(c) Prove that the ring of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is a Euclidean ring, with $d(a + bi) = a^2 + b^2$.

3. (a) (i) If p is a prime integer of the form $4n + 3$, then prove that p is a prime number in the ring of Gaussian integer $J[i] = \{a + bi \mid a, b \in Z\}$.

(ii) Find the greatest common divisor in the ring of Gaussian integers J[i] of $11 + 7i$ and $18 - i$.

(b) Let F be the field , and $f(x) = a_0 + a_1x + \ldots + a_nx$ be a polynomial in F[x]. Then, an element $b \in F$ is a root of f(x) if and only if (x - b) divides f(x) in F[x]. Verify the polynomial $1 + x + x^3 + x^4$ is not irreducible over any field F.

P.T.O.

(c) Prove that x^2+1 is irreducible over F, the field of integers mod 11 and show that $\frac{F[x]}{(x^2+1)}$ is a field having 121 elements.

4. (a) (I) Let p is a prime number, then prove that the polynomial $1 + x + x^2 + \ldots + x^{p-1}$ is irreducible over the rationals.

(II) The polynomial $x^4-6x^3+24x^2-30x+14$ is irreducible or reducible over the field of rationals. Justify your answer.

(b) If R is a unique factorization domain and if p(x) is a primitive polynomial in R[x] then prove that p(x) can be factored in a unique way as the product of irreducible elements in R[x].

(c) Let F be a field and f(x) a non-constant polynomial in $F[x]$. Then prove that there is an extension field E of F in which $f(x)$ has a zero. Show that $Q(\sqrt{7}, i)$ is the splitting field for $x^4 - 6x^2 - 7$.

5. (a) (i) Draw a subfield lattice of $GF(2^{24})$.

(ii) Define algebraic extension.

(b) (i) Prove that $8x^2 - 6x - 1$ is irreducible.

(ii) Find the basis for $Q[\sqrt{3}, \sqrt{5}]$ over Q.

(c) State and prove characterization of extensions.

6. (a) Let F be a finite field of order 16.

(i) Determine all possible orders of the subfields of F.

(ii) How many subfields does F contain?

(iii) List all the subfields.

(b) (i) Define degree of extension.

(ii) If F is a field of order 125 and $F^* = \langle a \rangle$, show that $a^{62} = -1$.

(c) Let K be a finite extension field of the field E and E be a finite extension field of the field F then K is a finite extension field of F and [K : F] = [K : E][E : F].