D 93265-A

(Pages : 4)

Name.......................................

Reg. No...................................

FIRST SEMESTER M.Sc. (CCSS) DEGREE EXAMINATION, JUNE 2016

Mathematics

MAT 1C 05—NUMBER THEORY

Time : Three Hours

Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 Find all integers n such that $\phi(n) = \frac{n}{2}$.

2 If f is multiplicative, prove that :

$$\sum_{d/n} \mu(d) f(d) = \prod_{p/n} (1 - f(p)).$$

3 If $x \geq 1$, prove that :

$$\sum_{n \leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O\left(x^{\alpha}\right), \text{ if } \alpha \geq 0.$$

4 If $0 < a < b$, prove that there eixsts an x_o such that :

$\pi(ax) < \pi(bx)$ if $x \geq x_o$.

5 For $x \geq 2$, prove that :

$$\pi(x) = \frac{I(x)}{\log x} + \int_2^x \frac{I(t)}{t^2 \log^2 t}\, dt.$$

6 Prove that $\lim_{x \to \infty} \left(\frac{M(x)}{x} - \frac{H(x)}{x \log x} \right) = 0.$

Turn over

7 Evaluate the Legendre symbol (1801/8191) using the reciprocity law for the Jacobi symbl.

8 Let p be an odd prime. Prove that every reduced residue system mod p contains exactly $(p-1)/2$ quadratic residues mod p.

9 Let P be an odd positive integer. Prove that :

$(a^2n/p) = (n/p)$

whenever $(a, p) = 1$.

10 In the 27-letter alphabet (with blank = 26), use the affine enciphering transformation with key $a = 13$, $b = 9$ to encipher the message "HELP ME".

11 Write a brief note on enciphering matrices.

12 What is meant by hash functions. Explain with an example.

(12 × 4 = 48 marks)

Part B

Answer **either** *(A)* **or** *(B) of each question.*
Each question carries 8 marks.

II. (A) (a) For $n \geq 1$, prove that :

$$\phi(n) = n \prod_{p/n} \left(1 - \frac{1}{p}\right).$$

(b) Let f be multiplicative. Prove that f is completely multiplicative if and only if :

$$f^{-1}(n) = \mu(n) \cdot f(n).$$

(B) (a) State and prove Euler's summation formula.

(b) For $x \geq 1$, prove that :

$$\sum_{n \leq x} \wedge(n) \left[\frac{x}{n}\right] = \log [x]!$$

(c) For $x \geq 2$, prove that :

$$\log [x]! = x \log x - x + O(\log x).$$

III. (A) (a) Prove that the following relations are logically equivalent :

(i) $\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$

(ii) $\lim_{x \to \infty} \frac{I(x)}{x} = 1.$

(iii) $\lim_{x \to \infty} \frac{\psi(x)}{x} = 1.$

(b) For $n \geq 1$, prove that the n^{th} prime p_n satisfy the inequality :

$$p_n < 12\left(n \log n + n \log \frac{12}{e}\right).$$

(B) Prove that the prime number theorem implies :

$$\lim_{x \to \infty} \frac{M(x)}{x} = 0.$$

IV. (A) (a) State and prove Gauss lemma.

(b) Prove that 5 is a quadratic residue of an odd prime p if $p \equiv \pm 1 \pmod{10}$ and that 5 is a non-residue if $p \equiv \pm 3 \pmod{10}$.

(B) (a) State and prove the quadratic reciprocity law.

(b) Prove that the Diophantine equation $y^2 = x^3 + k$ has no solutions if k has the form $k = (4n - 1)^3 - 4m^2$ where m and n are integers such that no prime $p \equiv -1 \pmod{4}$ divides m.

V. (A) (a) Find a formula for the number of different affine enciphering transformations there are with an N-letter alphabet.

(b) The message "!IWGVIEX!ZRADRYD" was intercepted. The message was sent using a linear enciphering transformation of digraph vectors in a 29-letter alphabet, in which A-Z have numerical equivalents 0-25, blank = 26, ? = 27, ! = 28. The last five letters of plain text are the sender's signature "MARIA". Find the deciphering matrix and read the message.

(B) (a) Compare public key cryptosystem with private key cryptosystem.

(b) Explain the RSA cryptosystem, illustrating with an example.

($4 \times 8 = 32$ marks)

D 13482 (Pages : 3) Name..................................

Reg. No................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2016

(CCSS)

Mathematics

MAT 1C 05—NUMBER THEORY

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 Define the Euler totient function $\phi(n)$. Prove that $\phi(mn) = \phi(m)\cdot\phi(n)$ if $(m, n) = 1$.

2 Prove that the Möbius function is multiplicative but not completely multiplicative.

3 If $x \geq 1$, prove that $\sum_{n \leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$.

4 Prove that $[2x] - 2[x]$ is either 0 or 1.

5 For $x > 0$, prove that $0 \leq \frac{\psi(x)}{x} - \frac{g(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x}\log 2}$.

6 If $a > 0$ and $b > 0$, prove that $\frac{\pi(ax)}{\pi(bx)} \sim a/b$ as $x \to \infty$.

7 Prove that the Legendre's symbol (n/p) is a completely multiplicative function of n.

8 Let p be an odd prime and let $p \equiv 1 \pmod 4$. Prove that $\sum_{\substack{r=1 \\ (r/p)=1}}^{p-1} r = \frac{p(p-1)}{4}$.

9 Define the Jacobi symbol (n/p). Prove that $(m/p)(n/p) = (mn/p)$, where p is an odd positive integer.

10 Explain with suitable examples, the terms enciphering transformations and deciphering transformations.

11 How will you authenticate a message in electronic communication ?

12 Find the inverse of the matrix $\begin{pmatrix} 40 & 0 \\ 0 & 21 \end{pmatrix}$ mod 841.

(12 × 4 = 48 marks)

Turn over

Part B

Answer **either** *A* **or** *B of each question.*
Each question carries 8 *marks.*

II. A (a) Let f be multiplicative. Prove that f is completely multiplicative if and only if $f^{-1}(n) = \mu(n) f(n)$ for all $n \geq 1$.

(b) Prove that $\frac{n}{\phi(n)} = \sum_{d/n} \frac{\mu^2(d)}{\phi(d)}$.

B (a) State and prove Euler's summation formula.

(b) For $x \geq 1$, prove that $\sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right] = 1$.

(c) If $x \geq 2$, prove that $\log[x]! = x \log x - x + 0 (\log x)$.

III. A (a) State and prove Abel's identity.

(b) Prove that the following relations are logically equivalent :

(i) $\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1$.

(ii) $\lim_{x \to \infty} \frac{\pi(x) \log \pi(x)}{x} = 1$.

(iii) $\lim_{x \to \infty} \frac{p_n}{n \log n} = 1$.

(Here p_n denotes the n^{th} prime)

B (a) For $n \geq 1$, prove that the nth prime p_n satisfies the inequalities :

$$\frac{1}{6} n \log n < p_n < 12\left(n \log n + n \log \frac{12}{e}\right).$$

(b) For all $x \geq 1$, prove that

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) = x \log x - x + O(\log x)$$

and $\sum_{n \leq x} g\left(\frac{x}{n}\right) = x \log x + O(x)$.

IV. A (a) State and prove Gauss Lemma.

(b) Determine those odd primes p for which $(-3/p) = 1$ and those for which $(-3/p) = -1$.

B (a) If p and q are distinct odd primes, prove that $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

(b) Determine whether 888 is a quadratic residue or non-residue of the prime 1999.

A (a) The ciphertext message "PWULPZTQAWHF" was intercepted. The message was encrypted using an affine map on digraphs in 26-letter alphabet. A frequency analysis shows that the most frequently occurring digraphs in all that ciphertext are "IX" and "TQ", in that order. It is known that the most common digraphs in the English language are "TH" and "HE" in that order. Find the deciphering key and read the message.

(b) Briefly describe about enciphering matrices.

B (a) Briefly describe about public key cryptosystem.

(b) Working in 26-letter alphabet and using the matrix $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/26Z)$ encipher the plaintext "NOANSWER".

(4 × 8 = 32 marks)

D 13481 (Pages : 3) Name.....................................

Reg. No.................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2016

(CCSS)

Mathematics

MAT 1C 04—DISCRETE MATHEMATICS

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 *marks.*

I. 1 If u and v are the only pendant vertices in a simple graph, does G contain a $u-v$ path. Justify your answer.

2 In any simple graph, prove that $\Gamma(G) = \Gamma(G^c)$.

3 Prove that every connected graph contains a spanning tree.

4 Prove that a simple graph with n vertices, $n \geq 2$, is complete if and only if $\kappa(G) = N - 1$.

5 State the Eulers formula. Does it hold for disconnected graphs. If not, describe such a formula for disconected graphs.

6 Show that the complement of a simple planar graph with 11 vertices is non-planar.

7 Describe a partial order on P (X), the power set of X and exhibit two chains having no maximal element.

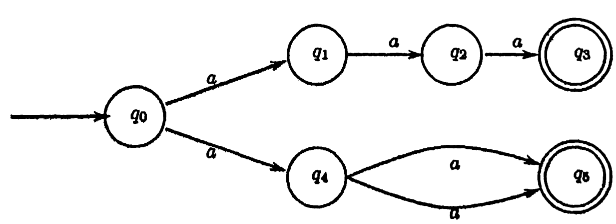
8 If $(X, +, \cdot, ')$ is a Boolean algebra, show that $(a \cdot b)' = a' + b'$, for all $a, b \in X$.

9 Write the conjunctive normal form of :

(i) $xy + x'z$.

(ii) $x_1'x_2(x_1' + x_2 + xx_1x_3)$.

10 Find the complement of the language given by the transition graph :



Turn over

11 Define language accepted by a *nfa* and illustrate it with an example.

12 Find *dfa*'s for the language $L = \{\omega : |\omega| \bmod 3 = 0\}$ on $\Sigma = \{a, b\}$.

(12 × 4 = 48 marks)

Part B

Answer **either** *A* **or** *B of each question.*
Each question carries 8 *marks.*

II. (A) (a) If every vertex of a graph G has degree at least 2, prove that G contains a cycle.

(b) Prove that Eulerian graphs decomposes into cycles.

(c) Explain the Knight's Tour in a chess board.

(B) (a) State and prove the Euler formula for connected graphs.

(b) Let G be a graph with n vertices, $n \geq 1$. Prove that the following are equivalent :

(i) G is connected and has no loops ;

(ii) G has $n - 1$ edges and no cycles ;

(iii) G has no loops and there is exactly one $u - v$ path for every $u, v \in V(G)$.

III. (A) (a) For any simple graph, prove that $\kappa \leq \lambda \leq \delta$.

(b) Prove that K_5 is non-planar.

(c) If G is a plane graph and F be a face of G, prove that there is a plane embedding of G in which F is the exterior face.

(B) (a) If G is a simple planar graph with atleast 3 vertices, prove that $m \leq 3n - 6$.

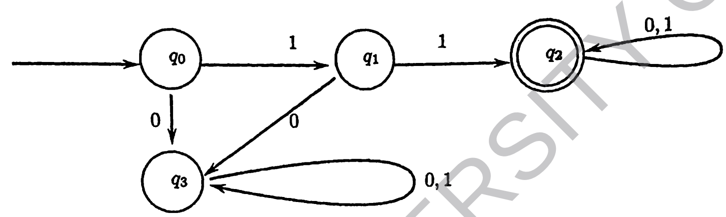
(b) If G is a plane graph, prove that G can be embedded in the plane in such a way that any specified vertex or edge belongs to the unbounded face of the resulting plane graph.

(c) Prove that $K_{3, 3}$ is non-planar.

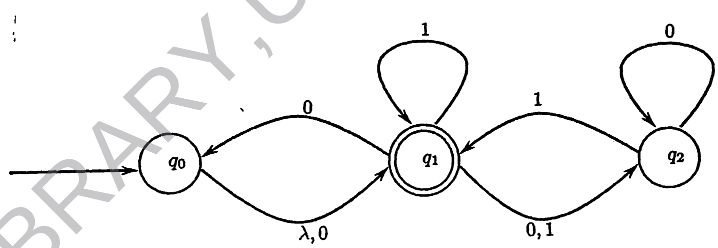
IV. (A) Let $(X, +, \cdot, ')$ be a finite Boolean algebra. Prove that every element of X can be uniquely expressed as the sum of atoms.

(B) Let $(X, \leq)$ be a poset and A be a non-empty, finite subset of X. Prove that A has at least one maximal element. Further show that A has a maximum element if and only if it has a unique maximal element.

V. (a) Find the language accepted by the *dfa* whose transition graph is :



(B) Convert the *nfa* given by the transition graph into an equivalent *dfa* :



(4 × 8 = 32 marks)

D 13480 (Pages : 3)

Name..............................

Reg. No..............................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2016

(CCSS)

Mathematics

MAT 1C 03—LINEAR ALGEBRA

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 Define basis of a vector space V over F. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of V. If $\beta \in V$ and $\beta = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n$, where $a_i \neq 0$, for $i = 1, 2, \ldots, n$ prove that $\{\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \beta\}$ is also a basis of V.

2 Let V be the vector space of all polynomial functions from $\mathbb{R}$ into $\mathbb{R}$ of degree 2. Define $f_1(x) = 1, f_2(x) = x + t, f_3(x) = (x+t)^2$. Prove that $\{f_1, f_2, f_3\}$ is a basis for V. If $f(x) = a_0 + a_1 x + a_2 x^2$ then what are the co-ordinaets of f in the basis $\{f_1, f_2, f_3\}$.

3 If W is a proper subspace of a vector space V and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis for V prove that $\alpha_i \in W$ for some i.

4 Let V and W be vector spaces over F and T : V $\rightarrow$ W be a linear transformation. If T is invertible, prove that T^{-1} is a linear transformation from W into V.

5 Give an example of a non-singular linear transformation which is onto.

6 Let $T \in L(\mathbb{R}^3)$ and $T(x, y, z) = (3x, x - y, 2x + y + z)$. Is T invertible ? If so, find T^{-1}.

7 Find the characteristic polynomial of the identity operator on the finite dimensional vector space $\mathbb{R}^3$.

8 Find a 3 × 3 matrix for which its minimal polynomial is x^2.

9 Let $T \in L(\mathbb{R}^2)$ and $[T] = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ in the standard ordered basis. Computing its characteristic values, find all subspaces of $\mathbb{R}^2$ which are invariant under T.

10 Find a projection T which projects $\mathbb{R}^2$ on $[(1, -1)]$ along $[(1, 2)]$.

11 Let $T \in L(V)$ be such that TP = PT for all projection operator P on V. Determine whether every subspace of V is invariant under T.

Turn over

12 Let T be a linear tranformation on $\mathbf{R}^3$ represented in the standard ordered basis by the matrix $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{bmatrix}$.

Prove that T has no cyclic vectors.

(12 × 4 = 48 marks)

Part B

Answer **either** *A* **or** *B of* **each** *question.*
Each question carries 8 *marks.*

II. A (a) Prove that a non-empty subset W of a vector space V over F is the subspace of V if and only if for each pair of vectors $\alpha, \beta \in V$ and each scalar $c \in F$, the vector $c\alpha + \beta \in W$.

(b) Prove that two finite dimensional vector spaces over the same field are isomorphic if and only if they are of the same dimension.

B Let V be the set of all complex valued functions f on the real line such that for all t, $f(-t) = \overline{f(t)}$ and $(cf)(t) = cf(t)$. Prove that V is a vector space under these operations. Also find a function $f \in V$ which is not real valued.

III. A Let $n \in \mathbb{N}$ and F be a field. Let $W = \{(x_1, x_2, \ldots, x_n) \in F^n : x_1 + x_2 + \ldots + x_n = 0\}$. Compute the dual space W*.

B Let $T : V \to W$ be a linear transformation where V and W are vector spaces over the same field F. Let T^t be the transpose of T. Then prove the following :

(i) The null space of T^t is the annihilator of the range of T.

(ii) rank T^t = rank T, if V and W are finite dimensional.

(iii) The range of T^t is the annihilator of the null space of T.

IV. A (a) Let V be a finite dimensional vector space, $T \in L(V)$. Prove that the characteristic polynomial and minimal polynomial for T have the same roots except for multiplicities.

(b) Let $A = \begin{bmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}$ be a 3 × 3 matrix over the field F and $a, b, c \in F$.

Find the characteristic polynomial and minimal polynomial for A.

B Let V be a finite dimensional vector space over the field F and $T \in L(V)$. Let $c_1, c_2, \ldots, c_k$ be the distinct characteristic values of T. Let W_i be the null space of $T - c_i I$. Then prove that T is diagonalizable if and only if $\dim W_1 + \dim W_2 + \ldots \dim W_k = \dim V$.

V. A Let V be a finite dimensional vector space over the field F and $T \in L(V)$. Let $c_1, c_2, \ldots, c_k$ be the distinct characteristic values of T. If T is diagonalizable, prove that there exists linear operators $E_1, E_2, \ldots, E_k$ such that :

(i) $T = c_1E_1 + c_2E_2 + \ldots + c_kE_k$.

(ii) $E_iE_j = 0$ for $i \neq j$ and $E_i^2 = E_i$ for $i = 1, 2, \ldots, k$.

(iii) The range of E_i is the characteristic space for T associated with c_i.

B Let V be a finite dimensional vector space over the field F and $T \in L(V)$. Let $0 \neq \alpha \in V$ and p_α be the T-annihilator of α. Then prove the following :

(i) If $\deg p_\alpha = k$ then $\{\alpha, T\alpha, T^2\alpha, \ldots, T^{k-1}\alpha\}$ form a basis of $Z(\alpha ; T)$.

(ii) If U is the linear operator on $Z(\alpha ; T)$ induced by T, then minimal polynomial for U is p_α.

(4 × 8 = 32 marks)

by

ists

iation

entiable

e on $[a, b]$.

that $f \in$ R

D 13479 (Pages : 3) Name..................................

Reg. No..................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2016

(CCSS)

Mathematics

MAT 1C 02—REAL ANALYSIS—I

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 Let $X = [0, 2\pi)$, the half open interval on the real line and $f : X \to Y$ be the mapping defined by

$$f(t) = (\cos t, \sin t), (0 \leq t < 2\pi),$$

where Y consists of all points at a distance 1 from origin. Does the inverse map exist ? If exists is it continuous ?

2 Prove that every bounded infinite subset of R^k has a limit point in R^k.

3 Give an example of an open cover of the segment (0, 1) which has no finite subcover.

4 If $c_0 + \frac{c_1}{2} + \ldots + \frac{c_{n-1}}{n} + \frac{c_n}{n+1} = 0$, where $c_0, \ldots c_n$ are real constants, prove that the equation $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} + c_n x^n = 0$ has at least one root between 0 and 1.

5 Let f be defined by $f(x) = x^2 \sin\left(\frac{1}{x}\right)$ if $x \neq 0$ and $f(x) = 0$ if $x = 0$. Show that f is differentiable at all points x but f' is not a continuous function.

6 Let $f_n(x) = \frac{1}{nx+1}$, $0 < x < 1, n = 1, 2, \ldots$. Verify whether $f_n \to 0$ uniformly in (0, 1).

7 If $f(x) = 0$ for all irrational x and $f(x) = 1$ for all rational x. Is f Riemann integrable on $[a, b]$. Justify your answer.

8 Suppose f is a bounded real function on $[a, b]$ and $f^2 \in R$ on $[a, b]$. Does it follow that $f \in R$. Explain, why ?

9 Is it possible that a sequence of bounded functions may converge without being uniformly bounded. Justify your answer by an example.

10 $\{f_n\}$ be a uniformly bounded sequence of continuous functions on a compact set E. Does there always exist a subsequence which converges pointwise on E. Justify your answer.

11 If $\{f_n\}$ be an equicontinuous sequence of functions on a compact set K which converges pointwise on K. Is the convergence uniform on K. Justify your answer.

12 Consider $f(x) = \sum_{n=1}^{\infty} \frac{1}{1+n^2 x}$. On what intervals does it converges uniformly.

(12 × 4 = 48 marks)

Part B

Answer **either** *A* **or** *B of each question.*
Each question carries 8 *marks.*

II. A (a) Is the set of all irrational real numbers countable ? Justify your answer.

(b) Let E be a non-empty set of real numbers which is bounded above and y = supE. Show that $y \in \bar{E}$.

B (a) Show that every k-cell is compact.

(b) Let X be an infinite set. For $p \in X$ and $q \in X$ define

$$d(p,q) = \begin{cases} 1 & \text{if } p \neq q \\ 0 & \text{if } p = q. \end{cases}$$

Prove that this is a metric. Which subsets of the resulting metric space are compact ?

III. A (a) Show that a mapping f of a metric space X into a metric space Y is continuous if and only if f^{-1} (V) is open in X for every open set V in Y.

(b) Let f be differentiable on $[a, b]$ then show that f is continuous on $[a, b]$.

B (a) Suppose f be a real differentiable function on $[a, b]$ and suppose $f'(a) < \lambda < f'(b)$. Show that there exists a point $x \in (a, b)$ such that $f'(x) = \lambda$.

(b) Suppose f is a continuous mapping of $[a, b]$ into R^k and f is differentiable in (a, b). Show that there exists $x \in (a, b)$ such that

$$|f(b) - f(a)| \leq (b-a)|f'(x)|.$$

IV. A (a) Show that if $f_1 \in R(\alpha)$ and $f_2 \in R(\alpha)$ on $[a, b]$ then $f_1 + f_2 \in R(\alpha)$ and $cf \in R(\alpha)$ for every c.

(b) State and prove fundamental theorem of integral calculus.

B (a) If γ' is continuous on $[a, b]$, show that γ is rectifiable and

$$\Lambda(\gamma) = \int_a^b |\gamma'(t)|\, dt.$$

(b) Suppose $\{f_n\}$ be a sequence of equicontinuous of functions on a compact set K and $\{f_n\}$ converges pointwise on K. Prove that $\{f_n\}$ converges uniformly on K.

V. A Let K be a compact set and $\{f_n\}$ be a sequence of continuous functions on K which converges pointwise to a continuous function f on K and $f_n(x) \geq f_{n+1}(x)$ for all $x \in K$. Prove that f_n converges to f uniformly on K. Is this true even if K not necessarily compact.

B If f is a continuous complex function on $[a, b]$, then show that there exists a sequence of polynomials P_n such that $\lim_{n \to \infty} P_n(x) = f(x)$ uniformly on $[a, b]$.

(4 × 8 = 32 marks)

D 13478 (Pages : 2) Name..................................

Reg. No..................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2016

(CCSS)

Mathematics

MAT 1C 01—ALGEBRA—I

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 Verify whether the cyclic group $\mathbb{Z}_{12}$ is isomorphic to a direct product of the groups $\mathbb{Z}_1$ and $\mathbb{Z}_2$.

2 Show that any two abelian groups of order 10 are isomorphic.

3 Find the kernel of the homomorphism $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ defined by $\phi(x, y) = x$.

4 Find the commutator subgroup of the symmetric group S_3.

5 Let $G = S_3$ act on the set $S = \{1, 2, 3\}$ be $g \cdot x = g(x)$ for $g \in G$ and $x \in S$. Find G_x for $x = 1$.

6 Show that the group $\mathbb{Z}$ of integers under addition is a free group.

7 Let G be a group of order 5^3. Show that G is not simple.

8 Find all Sylow 2-subgroups of the symmetric group S_3.

9 Consider the integral domain $D = \mathbb{Z}_5$. Show that the field of quotients of D is isomorphic to D.

10 Show that $4x^5 + 9x^4 - 3x^2 + 6$ is irreducible over the rationals.

11 Show that $3\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

12 Verify whether $I = \{f(x) \in \mathbb{Q}[x] : f(1) = 0\}$ is a maximal ideal in $\mathbb{Q}[x]$.

($12 \times 4 = 48$ marks)

Part B

Answer **either** *A* **or** *B of* **each** *question.*
Each question carries 8 marks.

II. A (a) Let G_1, G_2 be groups and $x \in G_1$ and $y \in G_2$. Prove that if x is of order m and y is of order n then the order of (x, y) in $G_1 \times G_2$ is the lcm of m and n.

(b) Show that if m and n are relatively prime then $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$.

B (a) Describe the quotient group G/H of a group G and a normal subgroup H.

(b) Show that the coset multiplication $(a\text{H})(\text{H}) = ab\text{H}$ is well defined if and only if H is a normal subgroup of G.

Turn over

III. A (a) Give an example of a transitive action.

(b) Let X be a G-set. For $x_1, x_2 \in X$ let $x_1 \sim x_2$ if $x_1 = gx_2$ for some $g \in G$. Show that $\sim$ is an equivalence relation on X.

B (a) Let G be a finite group and X be a G-set. For each $g \in G$ let $X_g = \{x : gx = x\}$. Show that the number of orbits in X is equal to $\frac{1}{|G|} \Sigma_{g \in G} |X_g|$.

(b) For $G = \mathbb{Z}_2$ and $X = \{a, b, c, d\}$ consider the action as follows : $0 . x = x$ for all $x \in X$ and $1.a = b$, $1.b = a$, $1.c = d$, $1.d = c$. Find the number of orbits of X.

IV. A (a) Let G be a finite group and p be a prime such that p divides $|G|$. Show that G has a subgroup of order p.

(b) Define p-group and show that every subgroup of a p-group is a p-group.

B (a) Let F be the field of quotients of an integral domain D. Show that $i : D \to F$ defined by $i(a) = [a, 1]$ is an isomorphism from D into F.

(b) Show that image of i is an integral domain.

V. A (a) Let F be a field and $f(x), g(x) \in F[x]$. Show that there exists $q(x), r(x) \in F[x]$ such that $f(x) = q(x)\, g(x) + r(x)$, where degree of $r(x)$ is less than degree of $g(x)$.

(b) Show that $q(x)$ and $r(x)$ above are unique.

B (a) Let F be a field. Show that every non constant polynomial in F[x] is a product of irreducible polynomials.

(b) Let $p(x)$ be an irreducible polynomial in F[x] and let $p(x)$ divide $r(x) . s(x)$ where $r(x), s(x) \in F[x]$. Show that $p(x)$ divides $r(x)$ on $p(x)$ divides $s(x)$.

(4 × 8 = 32 marks)