D 13147-A **(Pages : 4)** **Name.....................................**

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

FIRST SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 session for SDE/Private students]

(CBCSS)

Mathematics

MTH 1C 05—NUMBER THEORY

(2019 Admission onwards)

{Covid instructions are not applicable for Pvt/SDE students (November 2020 session)}

(Multiple Choice Questions for SDE Candidates)

Time : 20 Minutes	**Total No. of Questions : 20**	**Maximum : 5 Weightage**

INSTRUCTIONS TO THE CANDIDATE

1. This Question Paper carries Multiple Choice Questions from 1 to 20.
2. The candidate should check that the question paper supplied to him/her contains all the 20 questions in serial order.
3. Each question is provided with choices (A), (B), (C) and (D) having one correct answer. Choose the correct answer and enter it in the main answer-book.
4. The MCQ question paper will be supplied after the completion of the descriptive examination.

MTH 1C 05—NUMBER THEORY

(Multiple Choice Questions for SDE Candidates)

1. The Dirichlet product of two completely multiplicative functions is completely multiplicative :

(A) False. (B) True.

2. The derivative of the function I is :

(A) 1. (B) 0.

(C) $\mu(n)$. (D) -1.

3. For $n \geq 1$, the divisor sum of the λ function is :

(A) $\begin{cases} 1 & \text{if } n \text{ is odd} \\ -1 & \text{otherwise} \end{cases}$. (B) $\begin{cases} -1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise} \end{cases}$.

(C) $\begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise} \end{cases}$. (D) $\begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$.

4. Let $\mathscr{A}$ be the collection of all multiplicative functions. Then $\mathscr{A}$ is a group :

(A) True. (B) False.

5. The statement $\log x = O\left(\sqrt{x}\right)$ is :

(A) True. (B) False.

6. The fractional part of x is :

(A) $[x]$. (B) $x + [x]$.

(C) $x - [x]$. (D) $[x] - x$.

7. The prime number theorem is equivalent to :

(A) $\lim_{x\to\infty} \frac{\vartheta x}{x} = 1$. (B) $\lim_{x\to\infty} \frac{\vartheta x}{x} = 0$.

(C) $\lim_{x\to\infty} \frac{\vartheta x}{\psi x} = 1$. (D) $\lim_{x\to\infty} \frac{\vartheta x}{M(x)} = 1$.

8. The highest power of 10 that divides 1000! is :

(A) 249. (B) 219.

(C) 229. (D) 239.

9. The Legendre's symbol $(n|p)$ is a completely multiplicative function :

(A) False. (B) True.

10. If p is an odd prime the value of $(2|p)$ is :

(A) $(-1)^{(p^2-1)/2}$. (B) $(-1)^{(p-1)/2}$.

(C) $(-1)^{(p+1)/2}$. (D) $(-1)^{(p-1)/3}$.

11. Let P be an odd integer and $(a,\mathrm{P})=1,$ then $(a^2n|\mathrm{P})=$

(A) 0. (B) 1.

(C) $(n|\mathrm{P})$. (D) $(a^2|\mathrm{P})$.

12. Which of the following statement is equivalent to the relation $\mathrm{M}(x)=o(x)$ as $x\to\infty$:

(A) $\psi(x)\sim x$ as $x\to\infty$. (B) $\theta(x)\sim x$ as $x^2\to\infty$.

(C) $\varphi(x)\sim x$ as $x\to\infty$. (D) $\mathrm{M}(x)\sim x$ as $x\to\infty$.

13. The function M(x) is defined as :

(A) $\sum_{n\le x}\lambda(n)$. (B) $\sum_{n\le x}\mu(n)$.

(C) $\sum_{n\le x}\varphi(n)$. (D) $\sum_{n\le x}\mathrm{A}(n)$.

14. Public key encryption is advantageous over Symmetric key Cryptography because of :

(A) Speed. (B) Key exchange.

(C) Space. (D) Key length.

15. The keys used in cryptography are :

(A) All of them. (B) Secret key.

(C) Public key. (D) Private key.

16. The multiplicative Inverse of 550 mod 1769 is :

(A) 224. (B) 434.

(C) 550. (D) Does not exist.

17. Symmetric algorithms use ———— key(s).

(A) 1. (B) 2.

(C) 3. (D) 4.

18. The ———— is the message after transformation.

(A) Secret-text. (B) Plaintext.

(C) Ciphertext. (D) None of the above.

19. A process of studying cryptographic system is known as Cryptanalysis :

(A) True. (B) False.

20. You are supposed to use hill cipher for encryption technique. You are provided with the following matrix :

$$A = \begin{pmatrix} 4 & 2 \\ 2 & 1 \end{pmatrix}$$

(A) No. (B) Yes.

(C) Can't be determined. (D) Data insufficient.

D 13147

(Pages : 3)

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

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

FIRST SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 session for SDE/Private students]

(CBCSS)

Mathematics

MTH 1C 05—NUMBER THEORY

(2019 Admission onwards)

{Covid instructions are not applicable for Pvt/SDE students (November 2020 session)}

Time : Three Hours Maximum : 30 Weightage

General Instructions

1. *In cases where choices are provided, students can attend* **all** *questions in each section.*
2. *The minimum number of questions to be attended from the Section / Part shall remain the same.*
3. *The instruction if any, to attend a minimum number of questions from each sub section / sub part / sub division may be ignored.*
4. *There will be an overall ceiling for each Section / Part that is equivalent to the maximum weightage of the Section / Part.*

Part A

Answer **all** *questions from this part.*
Each question has weightage 1.

1. Prove that if $2^n + 1$ is prime, then n is a power of 2.

2. If f is a multiplicative function , prove that $f^{-1}(n) = \mu(n) f(n)$ for every square free n.

3. State Selberg's identity.

4. For $x > 0$, show that $0 \le \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \le \frac{(\log x)^2}{2\sqrt{x}\log 2}$.

5. For $n \ge 1$, show that $\sum_{n > x} \frac{1}{n^s} = O\left(x^{1-s}\right)$, if $s > 1$.

Turn over

6. Evaluate the Legendre's symbol (7/11).

7. State Euler's criterion for Legendre's symbol.

8. Determine whether -104 is a quadratic residue or non-residue of the prime 997.

(8 × 1 = 8 weightage)

Part B

Answer any **six** *questions by choosing* **two** *questions from each unit.*
Each question carries a weightage of 2.

Unit I

9. If $n \geq 1$, show that $\log n = \sum_{d/n} \wedge(d)$.

10. If f is an arithmetical function with $f(1) \neq 0$, show that there is a unique arithmetical function f^{-1} such that $f * f^{-1} = f^{-1} * f = I$.

11. State and prove Euler's summation formula.

Unit II

12. For every integer $n \geq 2$, show that $\frac{1}{6}\frac{n}{\log n} < \pi(n) = \frac{6n}{\log n}$.

13. For $n \geq 1$, then the n^{th} prime p_n satisfies the inequalities $\frac{1}{6}\log n < p_n < 12\left(n \log n + n \log \frac{12}{e}\right)$.

14. State and prove Abel's identity.

Unit III

15. Let p be an odd prime. Then for all n prove that $(n / p) \equiv n^{\left(\frac{p-1}{2}\right)} (\bmod p)$.

16. If p and q are distinct odd primes, then show that $(p|q)(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

17. Describe briefly about RSA cryptosystems.

(6 × 2 = 12 weightage)

Part C

Answer any **two** *questions.*
Each question carries weightage of 5.

18. Let f be multiplicative. Then f is completely multiplicative if and only if $f^{-1}(n) = \mu(n) f(n), \forall n \geq 1$.

19. Prove that there is a constant A such that $\sum_{p \leq x} \frac{1}{p} = \log(\log x) + A + O\left(\frac{1}{\log x}\right)$.

20. Show 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.

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

(2 × 5 = 10 weightage)

D 13146–A (Pages : 4) Name.....................................

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

FIRST SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 session for SDE/Private Students]

(CBCSS)

Mathematics

MTH 1C 04—DISCRETE MATHEMATICS

(2019 Admission onwards)

(Multiple Choice Questions for SDE Candidates)

{Covid instructions are not applicable for PVT/SDE students (November 2020 session)}

Time : 20 Minutes	**Total No. of Questions : 20**	**Maximum : 5 Weightage**

INSTRUCTIONS TO THE CANDIDATE

1. This Question Paper carries Multiple Choice Questions from 1 to 20.
2. The candidate should check that the question paper supplied to him/her contains all the 20 questions in serial order.
3. Each question is provided with choices (A), (B), (C) and (D) having one correct answer. Choose the correct answer and enter it in the main answer-book.
4. The MCQ question paper will be supplied after the completion of the descriptive examination.

MTH 1C 04—DISCRETE MATHEMATICS

(Multiple Choice Questions for SDE Candidates)

1. For a given graph G having v vertices and e edges which is connected and has no cycles, which of the following statements is true ?

   (A) $v = e$.
   (B) $v = e + 1$.
   (C) $v + 1 = e$.
   (D) $v = e - 1$.

2. A graph is ———— if it has at least one pair of vertices without a path between them.

   (A) Complete.
   (B) Connected.
   (C) Disconnected.
   (D) Trivial.

3. What is the radius of the Petersen graph ?

   (A) 2.
   (B) 3.
   (C) 4.
   (D) None of the above.

4. Let G be a simple graph with every pair of vertices is connected. Then G is :

   (A) Trivial.
   (B) Complete.
   (C) Disconnected.
   (D) Self complementary.

5. Let $G = K_n$ where $n \geq 5$. Then number of edges of any induced sub-graph of G with 5 vertices :

   (A) 10.
   (B) 5.
   (C) 6.
   (D) 8.

6. Number of edges incident with the vertex V is called ?

   (A) Degree of a graph.
   (B) Handshaking lemma.
   (C) Degree of a vertex.
   (D) None of the above.

7. A graph with n vertices will definitely have a parallel edge or self loop if the total number of edges are :

   (A) Greater than $n - 1$.
   (B) Less than $n(n - 1)$.
   (C) Greater than $\frac{n(n-1)}{2}$.
   (D) Less than $\frac{n^2}{2}$.

8. The graph in which, there is a closed trail which includes every edge of the graph is known as ?

(A) Hamiltonian graph. (B) Euler graph.

(C) Directed graph. (D) Planar graph.

9. What is the maximum number of possible non-zero values in an adjacency matrix of a simple graph with n vertices ?

(A) n^2. (B) $\frac{n(v-1)}{2}$.

(C) $\frac{n(n+1).}{2}$ (D) n.

10. The degree sequence of a simple graph is the sequence of the degrees of the nodes in the graph in decreasing order. Which of the following sequences can not be the degree sequence of any graph ?

1. 7, 6, 5, 4, 4, 3, 2, 1.
2. 6, 6, 6, 6, 3, 3, 2, 2.
3. 7, 6, 6, 4, 4, 3, 2, 2.
4. 8, 7, 7, 6, 4, 2, 1, 1.

(A) 1 and 2. (B) 3 and 4.

(C) 4 only. (D) 2 and 4.

11. Let G be a simple undirected planar graph on 10 vertices with 15 edges. If G is a connected graph, then the number of bounded faces in any embedding of G on the plane is equal to :

(A) 4. (B) 5.

(C) 6. (D) 7.

12. The minimum degree (δ) of the Petersen graph :

(A) 1. (B) 2.

(C) 3. (D) 4.

13. If a graph G is simple and $\delta \geq \frac{n-1}{n}$, then G is :

(A) Complete. (B) Bipartite.

(C) Connected. (D) Planar.

14. A **dfa** is defined by the quintuple $M = (Q, \Sigma, \delta, q_0, F)$, where δ stands for :

(A) Internal states. (B) Input alphabet.

(C) Transition function. (D) Minimum degree.

15. If Σ is an alphabet, then :

(A) $\Sigma^{+} = \Sigma^{*} - \{\lambda\}$.

(B) $\Sigma^{+} = \Sigma^{*} - \{\theta\}$.

(C) $\Sigma^{+} = \Sigma - L$.

(D) $\Sigma^{+} = L - \Sigma$.

16. If R is a partial order on a set X then which of the following is a strict partial order :

(A) $X - \Delta X$.

(B) $\Delta X - R$.

(C) $R - \Delta X$.

(D) $\Delta X - X$.

17. Let $(X, \leq)$ be a Poset, $A \subset X$ and $x \in X$. Then x is an upper bound if for all $a \in A$, then :

(A) $a < x$.

(B) $a \leq x$.

(C) $a > x$.

(D) $a \geq x$.

18. Let $(X, +, .)$ be a Boolean algebra. Then for all $x, y, z \in X$ such that $x + x.y = x$ is called :

(A) Law of Absorption.

(B) Law of Idempotency.

(C) Law of Complementation.

(D) De Morgan's Law.

19. Let $(X, +, .)$ be a finite Boolean algebra. Then :

I. Every non-zero element of X contains at least one atom.

II. Every two distinct atoms of X are mutually disjoint.

(A) I and II are true.

(B) I and II are false.

(C) I is true and II is false.

(D) I is false and II is true.

20. Let $(X, \leq)$ be a lattice with minimum element 0 and maximal element 1. Then y is a complement of x, if :

(A) $x \vee y = 0, x \wedge y = 0$.

(B) $x \vee y = 0, x \wedge y = 1$.

(C) $x \vee y = 1, x \wedge y = 0$.

(D) $x \vee y = 1, x \wedge y = 1$.

D 13146 (Pages : 3) Name..................................

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

FIRST SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 session for SDE/Private Students]

(CBCSS)

Mathematics

MTH 1C 04—DISCRETE MATHEMATICS

(2019 Admission onwards)

{Covid instructions are not applicable for PVT/SDE students (November 2020 session)}

Time : Three Hours Maximum : 30 Weightage

General Instructions

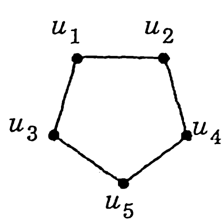
1. *In cases where choices are provided, students can attend* **all** *questions in each section.*
2. *The minimum number of questions to be attended from the Section / Part shall remain the same.*
3. *The instruction if any, to attend a minimum number of questions from each sub section / sub part / sub division may be ignored.*
4. *There will be an overall ceiling for each Section / Part that is equivalent to the maximum weightage of the Section / Part.*

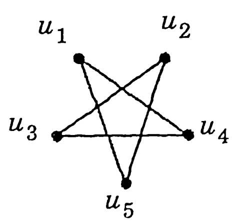
Part A

Answer **all** *questions.*

Each question carries weightage 1.

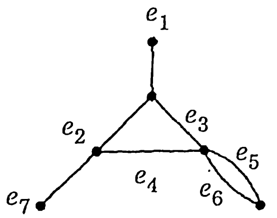
1. Define partial ordering and give an example.
2. What is a chain ? Give an example.
3. Find the maximal elements of the poset X = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} under the partial order $a \mid b$ if a divides b.
4. Define an isomorphism between the following graphs :





Turn over

5. Draw the line graph of the following graph



6. If G is a simple planar graph with at least 3 vertices, prove that $m \leq 3n - 6$, where m and n are the number of edges and vertices of G, respectively.

7. Let $w = a_1 a_2 .. .a_n$ be a string. Find length of w and reverse of w.

8. Define star-closure of a language.

(8 × 1 = 8 weightage)

Part B

Answer any **six** *questions by choosing* **two** *questions from each unit.*
Each question carries a weightage of 2.

Unit I

9. Let (X, ≤) be a poset and A a non-empty finite subset of X. Prove that A has at least one maximal element.

10. Let X be a set and let ≤ be a binary relation defined on X which is reflexive and transitive. Define a binary relation on X by xRy if $x \leq y$ and $y \leq x$. Prove that R is an equivalence relation.

11. Let m be the largest possible number of mutually incomparable elements in a poset X. Prove that X cannot be expressed as a union of less than m chains.

Unit II

12. In any graph G, prove that the number of vertices of odd degree is even.

13. Prove that a vertex v of a connected graph G with at least three vertices is a cut vertex of G if and only if there exist vertices u and w of G distinct from v such that v is in every $u - w$ path in G.

14. Prove that a simple graph is a tree if and only if every pair of vertices is connected by a unique path.

UNIT III

15. Find a grammar that generates the language $L = \{a^n b^{n+1} : n \geq 0\}$.

16. Distinguish between deterministic automata and non-deterministic automata.

17. Let $M = (Q, \Sigma, \delta, q_0, F)$ be a deterministic finite accepter and let G_M be its associate transition graph. Then prove that for every $q_i, q_j \in Q$ and $w \in \Sigma^+, \delta^*(q_i, w) = q_j$ if and only if there is in G_M a walk with label w from q_i to q_j.

(6 × 2 = 12 weightage)

Part C

Answer any **two** *questions.*
Each question carries a weightage of 5.

18. Let A be a chain in a poset X and $|A|$ denotes the length of A. If X = P (B) where B is a set with n elements and the partial order on X is by set inclusion, prove that

(i) For S, T $\in$ X, T covers S iff S $\subset$ T and T – S is singleton set.

(ii) The longest chain in X is of length $n + 1$.

(iii) The number of such chains is n !.

19. (i) Prove that a connected graph G with at least two vertices contains at least two vertices that are not cut vertices.

(ii) Prove that a simple cubic connected graph G has a cut vertex if and only if it has a cut edge.

20. (i) A graph G is planar if and only if each of its blocks is planar.

(ii) Define dual of a planar graph. Draw a planar representation of K_4 and its dual.

21. Find a d.f.a. that :

(i) Recognizes the set of all strings on $\Sigma = \{a, b\}$ starting with prefix ab.

(ii) Accepts all strings on {0,1} except those containing the substring 001.

(2 × 5 = 10 weightage)

D 13145-A **(Pages : 4)** **Name.....................................**

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

FIRST SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 session for SDE/Private students]

(CBCSS)

Mathematics

MTH1C03—REAL ANALYSIS—I

(2019 Admission onwards)

{Covid instructions are not applicable for Pvt/SDE students (November 2020 session)}

(Multiple Choice Questions for SDE Candidates)

Time : 20 Minutes	**Total No. of Questions : 20**	**Maximum : 5 Weightage**

INSTRUCTIONS TO THE CANDIDATE

1. This Question Paper carries Multiple Choice Questions from 1 to 20.
2. The candidate should check that the question paper supplied to him/her contains all the 20 questions in serial order.
3. Each question is provided with choices (A), (B), (C) and (D) having one correct answer. Choose the correct answer and enter it in the main answer-book.
4. The MCQ question paper will be supplied after the completion of the descriptive examination.

D 13143-A (Pages : 4) Name.....................................

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

FIRST SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 session for SDE/Private students]

(CBCSS)

Mathematics

MTH1C01—ALGEBRA—I

(2019 Admission onwards)

{Covid instructions are not applicable for PVT/SDE Students (November 2020 session)}

(Multiple Choice Questions for SDE Candidates)

Time : 20 Minutes	Total No. of Questions : 20	Maximum : 5 Weightage

INSTRUCTIONS TO THE CANDIDATE

1. This Question Paper carries Multiple Choice Questions from 1 to 20.
2. The candidate should check that the question paper supplied to him/her contains all the 20 questions in serial order.
3. Each question is provided with choices (A), (B), (C) and (D) having one correct answer. Choose the correct answer and enter it in the main answer-book.
4. The MCQ question paper will be supplied after the completion of the descriptive examination.

MTH1C01—ALGEBRA—I

(Multiple Choice Questions for SDE Candidates)

1. Which of the following is true ?

   (A) Every abelian group of prime order is cyclic.

   (B) Every abelian group of prime power order is cyclic.

   (C) If a divides the order of a group G, then G has a subgroup of order a.

   (D) None of these.

2. Let G be a non abelian group. Then the order of G could be :

   (A) 35. (B) 37.

   (C) 40. (D) 49.

3. A subgroup H of G is a normal subgroup if and only if :

   (A) $Gh = hG$ for every h in H.

   (B) $gH = Hg$ for every g in G.

   (C) gh = hg for every g $\in$ G and h $\in$ H.

   (D) GH = HG.

4. Which of the following subring of $\mathbb{Z} \times \mathbb{Z}$ is not an ideal

   (A) $\{(n, n) : n \in \mathbb{Z}\}$. (B) $\{(n, 0) : n \in \mathbb{Z}\}$.

   (C) $\{(n, m) : n \in \mathbb{Z}, m \in 2\mathbb{Z}\}$. (D) $\{(n, m) : n \in 2\mathbb{Z}, m \in \mathbb{Z}\}$.

5. Let $f(x) \in \mathbb{Z}[x]$. Then which of the following is true.

   (A) $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

   (B) $f(x)$ is irreducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

   (C) $f(x)$ is reducible over $\mathbb{Z}$, then it is reducible over $\mathbb{Q}$.

   (D) None of these.

6. The number of normal subgroup of the symmetric group S_n, $n \neq 4$ is :

   (A) 1. (B) 2.

   (C) 3. (D) 4.

7. Which of the following is false ?

   (A) Any abelian group of order 27 is cyclic.

   (B) Any abelian group of order 21 is cyclic.

   (C) Any abelian group of order 14 is cyclic.

   (D) Any abelian group of order 30 is cyclic.

8. Which of the following subring of $\mathbb{Z} \times \mathbb{Z}$ is not an ideal.

(A) $\{(n, n) : n \in \mathbb{Z}\}$.

(B) $\{(n, 0) : n \in \mathbb{Z}\}$.

(C) $\{(n, m) : n \in \mathbb{Z}, m \in 2\,\mathbb{Z}\}$.

(D) $\{(n, m) : n \in 2\mathbb{Z}, m \in \mathbb{Z}\}$.

9. Let $f(x) \in \mathbb{Z}[x]$. Then which of the following is true :

(A) $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

(B) $f(x)$ is irreducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

(C) $f(x)$ is reducible over $\mathbb{Z}$, then it is reducible over $\mathbb{Q}$.

(D) None of these.

10. Which of the following is false ?

(A) Every group of order 4 is abelian.

(B) Every group of order 9 is abelian.

(C) Every group of order 16 is abelian.

(D) Every group of order 25 is abelian.

11. Consider the following statements :

(a) Let G be a finite group of even order. Then G contains an element of order 2.

(b) If G is a group and H is a normal sub-group of G such that G/H is cyclic, then G is abelian.

Which of the following is true ?

(A) (a) and (b) are true.

(B) (a) and (b) are false.

(C) (a) is true and (b) is false.

(D) (a) is false and (b) is true.

12. Let G be a group, H be a subgroup of G and N be a normal subgroup of G. Which of the following is true ?

(A) H is a normal subgroup of HN.

(B) HN = G

(C) The order of HN \ N divides the order H.

(D) None of these.

13. What is the order of the factor group $\mathbb{Z}_{12} \times \mathbb{Z}_{18} / < (4, 3) >$?

(A) 12.

(B) 18.

(C) 36.

(D) 72.

14. Let G be a group and $H \subset K \subset G$. Which of the following is true ?

(A) If K is normal in G, then H is normal in G.

(B) If H is normal in G, then H is normal in K.

(C) If H is normal in K, then H is normal in G.

(D) None of these

15. How many different homomorphisms are there of a free group of rank 2 onto $\mathbb{Z}_4$.

(A) 4. (B) 8.

(C) 12. (D) 16.

16. The prime p such that $x + 2$ is a factor of $x^4 + x^3 + x^2 - x + 1$ in $\mathbb{Z}_p[x]$.

(A) 5. (B) 7.

(C) 11. (D) 13.

17. The units in Z $[x]$ are :

(A) 0, 1. (B) 1, – 1.

(C) 1, 0, –1. (D) 0, – 1.

18. If G is a group and H is a sub-group of index 2 in G then which of the following statement is false :

(A) H is a normal subgroup of G. (B) H is not a normal subgroup of G.

(C) G is not simple. (D) None of these.

19. Let $f(x) = x^3 - 9x^2 + 9x + 5$, then :

(A) $f(x)$ is irreducible over $\mathbb{Q}$. (B) $f(x)$ is reducible over $\mathbb{Q}$.

(C) $f(x)$ is reducible over $\mathbb{Z}$. (D) None of these.

20. Which of the following group is indecomposable ?

(A) $\mathbb{Z}_9$. (B) $\mathbb{Z}_6$.

(C) $\mathbb{Z}_2 \times \mathbb{Z}_3$. (D) $\mathbb{Z}_2 \times \mathbb{Z}_2$.

D 13143 (Pages : 3) Name.......................................

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

FIRST SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 session for SDE/Private Students]

(CBCSS)

Mathematics

MTH 1C 01—ALGEBRA—I

(2019 Admission onwards)

{Covid instructions are not applicable for PVT/SDE students (November 2020 session)}

Time : Three Hours Maximum : 30 Weightage

General Instructions

1. *In cases where choices are provided, students can attend* **all** *questions in each section.*
2. *The minimum number of questions to be attended from the Section / Part shall remain the same.*
3. *The instruction if any, to attend a minimum number of questions from each sub section / sub part / sub division may be ignored.*
4. *There will be an overall ceiling for each Section / Part that is equivalent to the maximum weightage of the Section / Part.*

Part A

Answer **all** *questions in this part.*
Each question has weightage 1.

1. Do the rotations about one particular point P, together with the identity map, form a subgroup of the group of plane isometries ? Why or why not ?
2. Find the order of (3, 10, 9) in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$.
3. Find the order of $5 + \langle 4 \rangle$ in the factor group $\mathbb{Z}_{12} / \langle 4 \rangle$.
4. In the group $G = \mathbb{Z}_{36}$ with $H = \langle 9 \rangle$. List the cosets in G/H, showing the elements in each coset.
5. Show that no group of order 20 is simple.
6. How many different homomorphisms are there of a free group of rank 2 onto $\mathbb{Z}_4$?

Turn over

7. Show that $\left(a, b : a^3 = 1, b^2 = 1, ba = a^2 b\right)$ gives a group of order 6 . Show that it is non-abelian.

8. Find all zeros of $x^3 + 2x + 2$ in $\mathbb{Z}_7$.

(8 × 1 = 8 weightage)

Part B

Answer any **six** *questions, choosing* **two** *from each unit.*
Each question has weightage 2.

Unit 1

9. Find all abelian groups, up to isomorphism, of order 360.

10. State and prove the Fundamental Homomorphism Theorem.

11. Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G, then prove that $r \cdot |G| = \sum_{g \in G} |X_g|$.

Unit 2

12. Let H and K be normal subgroups of a group G with $K \leq H$. Show that $G/H \simeq (G/K)/(H/K)$.

13. If G is a finite group and p divides $|G|$, then prove that the number of Sylow p-subgroups is congruent to 1 modulo p and divides $|G|$.

14. If H and K are finite subgroups of a group G, then show that $|HK| = \dfrac{(|H|)(|K|)}{|H \cap K|}$.

Unit 3

15. Compute the evaluation homomorphism $\phi_4\left(3x^{106} + 5x^{99} + 2x^{53}\right), F = E = \mathbb{Z}_7$.

16. Show that $f(x) = x + 3x + 2$ viewed in $\mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5$.

17. Let $G = \{e, a, b\}$ be a cyclic group of order 3 with identity element e. Write the element $(2e + 3a + 0b)(4e + 2a + 3b)$ in the group algebra $\mathbb{Z}_5 G$ in the form $re + sa + tb$ for $r, s, t \in \mathbb{Z}_5$.

(6 × 2 = 12 weightage)

Part C

Answer any **two** *questions.*
Each question has weightage 5.

18. (a) Prove that the group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime, that is, the gcd of m and n is 1 .

    (b) Let H be a subgroup of a group G. Show that left coset multiplication is well defined by the equation $(a\mathrm{H})(b\mathrm{H}) = (ab)\,\mathrm{H}$ if and only if H is a normal subgroup of G.

19. (a) Let G be the additive group of real numbers. Let the action of $\theta \in \mathrm{G}$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counter clockwise about the origin through θ radians. Let P be a point other than the origin in the plane. Show $\mathbb{R}^2$ is a G-set. Describe geometrically the orbit containing P. Find the group G_p.

    (b) Show that the Converse of the Theorem of Lagrange is false.

20. (a) Prove that every group of prime-power order (that is, every finite p-group) is solvable.

    (b) For a prime number p, prove that every group G of order p^2 is abelian.

21. (a) If F is a field, then prove that every non-constant polynomial $f(x) \in \mathrm{F}[x]$ can be factored in $\mathrm{F}[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit (that is, non-zero constant) factors in F.

    (b) Show that the polynomial $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Q}$ for any prime p.

(2 × 5 = 10 weightage)

D 12926 (Pages : 3) Name.......................................

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

FIRST SEMESTER M.Sc. DEGREE (SUPPLEMENTARY) EXAMINATION NOVEMBER 2021

(CUCSS)

Mathematics

MT 1C 05—DISCRETE MATHEMATICS

(2016 to 2018 Admissions)

Time : Three Hours Maximum : 36 Weightage

Part A

Answer **all** *questions.*
Each question carries weightage 1.

1. Define labeled graph.
2. If G is a simple graph and $\delta \geq k$, then prove that G contains a path of length at least k.
3. Prove that for any simple graph G, $Aut(G) = Aut(G^c)$.
4. Define k-vertex cut.
5. State Euler Formula.
6. If G is a simple planar graph with at least three vertices, then prove that $m \leq 3n - 6$.
7. Define plane triangulation.
8. State True *or* False : There is a 6-connected planar graph.
9. Define partially order.
10. Let $(X, +, \cdot, ')$ be a Boolean algebra. Then prove that for all elements x and y of X,

    $x + x \cdot y = x.$
11. Define Boolean function.
12. Define Lattice.

Turn over

13. Define dfa.

14. Define language accepted by an nfa.

(14 × 1 = 14 weightage)

Part B

Answer any **seven** *questions.*
Each question has weightage 2.

15. Prove that the sum of the degrees of the vertices of a graph is equal to twice the number of its edges.

16. Prove that in any group of n persons $(n \geq 2)$, there are at least two with the same number of friends.

17. If G is simple and $\delta \geq \frac{n-1}{2}$, then prove that G is connected.

18. Prove that an edge $e = xy$ is a cut edge of a connected graph G if and only if there exist vertices u and v such that e belongs to every u-v path in G.

19. Prove that every connected graph contains a spanning tree.

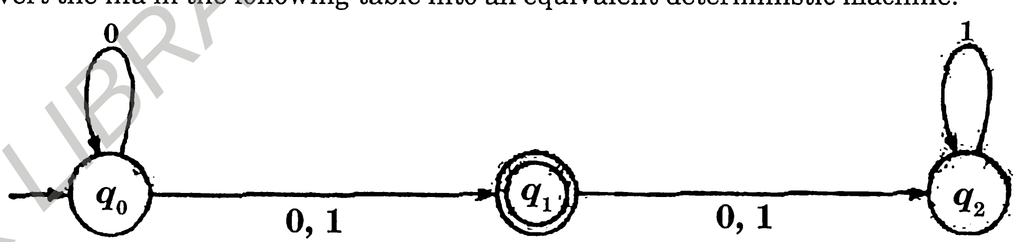
20. Define a chain in a poset. Prove that the intersection of two chains is a chain.

21. Write the following Boolean function in their disjunctive normal form.

$$f(x_1, x_2, x_3) = (x_1 + x_2')\, x_3' + x_2 x_1' (x_2 + x_1' x_3).$$

22. State and prove the law of double complementation in a Boolean algebra.

23. Convert the nfa in the following table into an equivalent deterministic machine.



24. Show that the language

$$L = \{awa : w \in \{a, b\}^*\}$$

is regular.

(7 × 2 = 14 weightage)

Part C

Answer any **two** *questions.*
Each question has weightage 4.

25. Prove that a graph is bipartite if and only if it contains no odd cycles.

26. Prove that the set $Aut(G)$ of all automorphisms of a simple graph G is a group with respect to the composition o of mappings as the group operation.

27. Let X be a finite set and $\leq$ be a partial order on X. Define a binary relation R on X by xRy if and only if y covers x. Then prove that $\leq$ is generated by R.

28. Let $M = (Q, \Sigma, \delta, q_0, F)$ be a deterministic finite accepter, and let G_M be its associated transition graph. Then prove that for every $q_i, q_j \in Q$, and $w \in \Sigma^+$, $\delta^*(q_i, w) = q_j$ if and only if there is in G_M a walk with label w from q_i to q_j.

(2 × 4 = 8 weightage)

D 12925 (Pages : 3) Name.......................................

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

FIRST SEMESTER M.Sc. DEGREE (SUPPLEMENTARY) EXAMINATION NOVEMBER 2021

(CUCSS)

Mathematics

MT 1C 04—NUMBER THEORY

(2016 to 2018 Admissions)

Time : Three Hours Maximum : 36 Weightage

Part A

Answer **all** *questions.*
Each question carries a weightage of 1.

1. Prove that if $2^n + 1$ is prime, then n is a power of 2.

2. If f is a non-zero multiplicative function then prove that $f(1) = 1$.

3. For $n \geq 1$, show that $\log n = \sum_{d|n} \Lambda(d)$.

4. Prove that the power function $N_\alpha(n) = n^\alpha$, where α is a fixed real or complex number is completely multiplicative.

5. For $x \geq 1$, show that $\sum_{n > x} \frac{1}{n^s} = o\left(x^{1-s}\right)$ if $s > 1$.

6. Show that if two lattice points (a, b) and (m, n) are mutually visible if and only if $a - m$ and $b - n$ are relatively prime.

7. Define Chebyshev's function $\psi(x)$ and $\phi(x)$ and show that $\psi(x) = \sum_{m \leq \log_2 x} \vartheta\left(x^{1/m}\right)$.

8. State Abel's identity.

Turn over

9. For $x \geq 2$, show that $\vartheta(x) = \pi(x)\log(x) - \int_x^2 \frac{\pi(t)}{t}\,dt.$

10. State Euler's criterion for Legendre's symbol.

11. Evaluate the Legendre's symbol $\left(\frac{7}{11}\right)$.

12. Determine whether – 104 is a quadratic residue or nonresidue of the prime 997.

13. Describe briefly about RSA cryptosystems.

14. How do classical and public Key cryptosystem differ ?

(14 × 1 = 14 weightage)

Part B

Answer any **seven** *questions.*
Each question carries a weightage of 2.

15. If f is an arithmetical function with $f(1) \neq 0$, show that there is a unique arithmetical function f^{-1} such that $f * f^{-1} = f^{-1} * f = I$.

16. If f and g are multiplicative, then show that their Dirichlet product $f * g$ is also multiplicative.

17. Show that the set of lattice points visible from the origin has density $\frac{6}{\pi^2}$.

18. Let p_n denote then n^{th} prime. Show that the following relations are logically equivalent :

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

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

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

19. For all $x \geq 1$, show that $\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1)$.

20. Let p be an odd prime. Then for all n prove that $(n|p) \equiv n^{\frac{p-1}{2}} \pmod{p}$.

21. Determine whether 888 is a quadratics residue or nonresidue of the prime 1999.

22. State and prove Quadratic Reciprocity Law.

23. Explain enciphering and deciphering transformation.

24. Briefly describe about digraph transformation

(7 × 2 = 14 weightage)

Part C

Answer any **two** *questions.*
Each question carries a weightage of 4.

25. Given f with $f(1) = 1$. Then prove that :

    a) f is multiplicative if and only if $\left(p_1^{a_1} \ldots\ldots p_2^{a_r}\right) = f\left(p_1^{a_1}\right) \ldots\ldots f\left(p_r^{a_r}\right)$ for all primes p_i and all integers $a_i \geq 1$.

    b) If f is multiplicative, then f is completely multiplicative if and only if $f\left(p^a\right) = f(p)^a$ for all primes p and all integers $a \geq 1$.

26. State and prove Euler's summation formula.

27. State and prove Gauss' lemma.

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

(2 × 4 = 8 weightage)

D 12924 (Pages : 4) Name.......................................

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

FIRST SEMESTER M.Sc. DEGREE (SUPPLEMENTARY) EXAMINATION NOVEMBER 2021

(CUCSS)

Mathematics

MT 1C 03—REAL ANALYSIS–I

(2016 to 2018 Admissions)

Time : Three Hours Maximum : 36 Weightage

Part A

Answer **all** *questions.*
Each question carries weightage 1.

1. Prove that balls in a metric space are convex.

2. Examine whether the following subset of $\mathbb{R}^2$ is (i) Closed ; (ii) Open ; (iii) Perfect ; and (iii) Bounded.

   The set of all complex numbers z such that $|z| < 1$.

3. If X is a metric space and $E \subset X$, then prove that $\bar{E}$ is closed.

4. Discuss the continuity/discontinuity behaviour of the function f defined by :

   $$f(x) = \begin{cases} 1 & (x \text{ rational}) \\ 0 & (x \text{ irrational}) \end{cases}.$$

5. Define connected subset of a metric space.

6. Let f be defined on $[a, b]$. If f is differentiable at a point $x \in [a, b]$, then prove that f is continuous at x.

7. If f is a real continuous function on $[a, b]$ which is differentiable in (a, b), then prove that there is a point $x \in (a, b)$ at which

   $$f(b) - f(a) = (b - a) f'(x).$$

Turn over

8. If $f \in \Re(\alpha)$ and $g \in \Re(\alpha)$ on $[a, b]$, then prove that $fg \in \Re(\alpha)$.

9. Define Riemann integrable function.

10. Suppose f is a real differentiable function on $[a, b]$ and suppose $f'(a) < \lambda < f'(b)$. Then prove that there is a point $x \in (a, b)$ such that $f'(x) = \lambda$.

11. For $m = 1, 2, 3 \ldots., n = 1, 2, 3, \ldots\ldots,$ let

$$s_{m,n} = \frac{m}{m+n}.$$

Then find $\lim\limits_{n \to \infty} \lim\limits_{m \to \infty} s_{m,n}$ and $\lim\limits_{m \to \infty} \lim\limits_{n \to \infty} s_{m,n}$.

12. Define uniformly bounded sequence of functions.

13. Define rectifiable curve.

14. Define uniform convergence of sequence of functions.

(14 × 1 = 14 weightage)

Part B

Answer any **seven** *questions.*
Each question has weightage 2.

15. If $\{K_\alpha\}$ is a collection of compact subsets of a metric space X such that the intersection of every finite subcollection of $\{K_\alpha\}$ is non-empty, then prove that $\bigcap K_\alpha$ is nonempty.

16. Construct a bounded set of real numbers having exactly three limit points and justify your answer.

17. Prove that every infinite subset of a countable set A is countable.

18. Prove that if a subset E of the real line $\mathbb{R}^1$ is connected then it satisfies the following property :

If $x \in E$, $y \in E$, and $x < z < y$, then $z \in E$.

19. Suppose X, Y, Z are metric spaces, $E \subset X$, f maps E into Y, g maps the range of f, $f(E)$, into Z, and h is the mapping of E into Z defined by

$$h(x) = g(f(x)) \quad (x \in E).$$

If f is continuous at a point $p \in E$ and if g is continuous at the point $f(p)$, then prove that h is continuous at p.

20. Suppose f and g defined on $[a, b]$ and are differentiable at a point $x \in [a, b]$. Then prove that $\frac{f}{g}$ is differentiable at x, and

$$\left(\frac{f}{g}\right)'(x) = \frac{g(x) f'(x) - g'(x) f(x)}{g^2(x)}, \text{ provided } g(x) \neq 0.$$

21. If P* is a refinement of P, then prove that :

$$L(P, f, \alpha) \leq L(P^*, f, \alpha).$$

22. If $f_1(x) \leq f_2(x)$ on $[a, b]$, then prove that

$$\int_a^b f_1 d\alpha \leq \int_a^b f_2 d\alpha.$$

23. Suppose f is a real differentiable function on $[a, b]$ and suppose $f'(a) < \lambda f'(b)$. Then prove that there is a point $x \in (a, b)$ such that $f'(x) = \lambda$.

24. If K is compact, if $f_n \in C(K)$ for $n = 1, 2, 3, \ldots\ldots$, and $\{f_n\}$ is pointwise bounded and equicontinuous on K, then prove that $\{f_n\}$ is uniformly bounded on K.

(7 × 2 = 14 weightage)

Part C

Answer any **two** *questions.*
Each question has weightage 4.

25. Suppose f and g are real and differentiable in (a, b), and $g'(x) \neq 0$ for all $x \in (a, b)$, where $-\infty \leq a \leq b + \infty$. Suppose

$$\frac{f'(x)}{g'(x)} \to \mathrm{A} \text{ as } x \to a.$$

If

$$f(x) \to 0 \text{ and } g(x) \to 0 \text{ as } x \to a,$$

or if

$$g(x) \to +\infty \text{ as } x \to a,$$

then prove that

$$\frac{f(x)}{g(x)} \to \mathrm{A} \text{ as } x \to a.$$

26. Let $\{\mathrm{E}_n\}$, $n = 1, 2, 3......$, be a sequence of countable sets, and put $\mathrm{S} = \bigcup_{n=1}^{\infty} \mathrm{E}_n$.

Then prove that S is countable.

27. Prove that $f \in \Re(\alpha)$ on $[a, b]$ if and only if for every $\varepsilon > 0$ there exists a partition P such that $\mathrm{U}(\mathrm{P}, f, \alpha) - \mathrm{L}(\mathrm{P}, f, \alpha) < \varepsilon$.

28. Suppose $\{f_n\}$ is a sequence of functions, differentiable on $[a, b]$ and such that $\{f_n(x_0)\}$ converges for some point x_0 on $[a, b]$. If $\{f_n'\}$ converges uniformly on $[a, b]$, then prove that $\{f_n\}$ converges uniformly on $[a, b]$, to a function f, and

$$f'(x) = \lim_{n \to \infty} f_n'(x) \quad (a \leq x \leq b).$$

(2 × 4 = 8 weightage)

D 12923 **(Pages : 4)** **Name.......................................**

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

FIRST SEMESTER M.Sc. DEGREE (SUPPLEMENTARY) EXAMINATION NOVEMBER 2021

(CUCSS)

Mathematics

MT 1C 02—LINEAR ALGEBRA

(2016 to 2018 Admissions)

Time : Three Hours Maximum : 36 Weightage

Part A

Answer **all** *questions.*
Each question carries weightage 1.

1. Give an example of a vector space V with an infinite basis.
2. Give a basis for $\mathbb{R}^3$ which is not the standard basis.
3. Let F be a field and let T be the operator on F^2 defined by $T(x, y) = (x, 0)$. Find $[T]_B$, where B be the standard ordered basis for F^2.
4. Describe explicitly a linear transformation from F^2 to F^2 such that $T(\varepsilon_1) = (a, b)$; $T(\varepsilon_2) = (c, d)$.
5. If T is a linear transformation from V into W, then show that $T(0) = 0$.
6. Define Linear functional on a vector space V. Give an example of a linear functional.
7. Show that similar matrices have the same characteristic polynomial.
8. Let T be any linear operator on V, then show that range of T and the null space of T are invariant under T.
9. Prove or disprove "Every square matrix has its characteristic values in $\mathbb{R}$ ".
10. Let V be a vector space and let V^* be the collection of all linear functionals on V. Show that $\dim V^* = \dim V$.
11. Find two linear operators T and U on $\mathbb{R}^2$ such that $TU = 0$ but $UT \neq 0$.
12. Define a projection E on a vector space V. Let R be the range of E and let N be the null space of E. Show that $V = R \oplus N$.

13. For $\alpha = (x_1, x_2)$ and $\beta = (y_1, y_2) \in \mathbb{R}^2$, define $(\alpha / \beta) = x_1 y_1 - x_2 y_1 - x_1 y_2 + 4 x_2 y_2$. Verify that $(/)$ is an inner product.

14. Let $(/)$ be the standard inner product on $\mathbb{R}^2$. Let $\alpha = (1, 2), \beta = (-1, 1)$. IF γ is a vector such that $(\alpha / \gamma) = 1$ and $(\beta / \gamma) = 3$, find γ.

(14 × 1 = 14 weightage)

Part B

Answer any **seven** *questions.*
Each question carries weightage 2.

15. Let V be a vector space over the field F. Prove that intersection of any collection of subspaces of V is a subspace of V.

16. If W is a subspace of a finite- dimensional vector space V , prove that every linearly independent subset of W is finite dimensional and is part of a basis for W.

17. If dim V = n and T : V $\rightarrow$ V be a linear operator such that Ker T = T (V), prove that n is even.

18. Let V be a finite-dimensional vector space over the field F and let T be a linear operator on V. Then prove that T is triangulable if and only if the minimal polynomial for T is a product of linear polynomials over F.

19. If W_1 and W_2 are subspaces of a finite-dimensional vector space, then prove that $W_1 = W_2$ if and only if $W_1^0 = W_2^0$.

20. Let T be a linear operator on a finite-dimensional space V and let c be a scalar. Prove that the following are equivalent :

    (i) c is a characteristic value of T.

    (ii) The operator $(T - cI)$ is singular.

    (iii) Det $(T - cI) = 0$.

21. Let T be a linear operator on an n-dimensional vector space V. Prove that the characteristic and minimal polynomials for T have the same roots, except for multiplicities.

22. Let T be a linear operator on a finite-dimensional space V. If T is diagonalizable and if $c_1, \ldots, c_k$ are the distinct characteristic values of T, then prove that there exist linear operators $E_1, \ldots, E_k$ on V such that :

(i) $T = c_1 E_1 + \ldots + c_k E_k$.

(ii) $I = E_1 + \ldots + E_k$.

(iii) $E_i E_j = 0, = i \neq j$.

(iv) $E_i^2 = E_i$ (E_i is a projection).

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

23. Let V be a real or complex vector space with an inner product. Prove that :

$\| \alpha + \beta \|^2 + \| \alpha - \beta \|^2 = 2\| \alpha \|^2 + 2\| \beta \|^2$ for every $\alpha, \beta \in V$.

24. State and prove Bessel's inequality.

(7 × 2 = 14 weightage)

Part C

Answer any **two** *questions.*
Each question carries weightage 4.

25. Let V be a finite dimensional vector space over the field F and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an ordered basis for V. Let W be a vector space over the same field F and let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be any set of vectors in W. Then prove that there is precisely one linear transformation T from V into W such that $T\alpha_j = \beta_j, j = 1, 2, \ldots, n$.

26. Let V be a finite-dimensional vector space over the field F, and let $B = \{\alpha_1, \ldots, \alpha_n\}$ and $B' = \{\alpha'_i, \ldots, \alpha'_n\}$ be ordered bases for V. Suppose T is linear operator on V. If $P = [P_1, \ldots, P_n]$ is the $n \times n$ matrix with columns $P_j = [\alpha'_j]_B$, then prove that $[T]B' = P^{-1}[T]_B P$.

27. State and prove Cayley- Hamilton theorem.

28. (a) Let W be a finite-dimensional subspace ofan inner product space V and let E be the orthogonal projection of V on W. Then prove that E is an idempotent linear transformation of V onto $W, W^{\perp}$ is the null space of E, and $V = W \oplus W^{\perp}$.

(b) Under the conditions of the above question prove that I – E is the orthogonal projection of V on $W^{\perp}$.

(2 × 4 = 8 weightage)

D 12922 (Pages : 2) Name.......................................

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

FIRST SEMESTER M.Sc. DEGREE (SUPPLEMENTARY) EXAMINATION NOVEMBER 2021

(CUCSS)

Mathematics

MT 1C 01—ALGEBRA-I

(2016 to 2018 Admissions)

Time : Three Hours Maximum : 36 Weightage

Part A

Answer **all** *questions.*
Each question carries weightage 1.

1. Every isometry of the plane is one of just four types. What are they ?
2. Find the order of (8, 4, 10) in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.
3. Find the order of the factor group $\mathbb{Z}_6 / \langle 3 \rangle$.
4. Define group action on a set.
5. State second isomorphism theorem.
6. Define a solvable group.
7. State second Sylow theorem.
8. Prove or disprove : Every group of order 15 is cyclic.
9. Prove that every group G' is isomorphic image of a free group G.
10. How many polynomials are there of degree ≤ 3 in $\mathbb{Z}_2[x]$.
11. State division algorithm for $F[x]$.
12. Define group rings and group algebras.
13. Define a ring homomorphism.
14. Give two non isomorphic groups of order 10.

(14 × 1 = 14 weightage)

Part B

Answer any **seven** *questions.*
Each question carries weightage 2.

15. If m is a square free integer, then prove that every abelian group of order m is cyclic.
16. Prove that direct product of abelian groups is abelian.
17. How many distinguishable ways can seven people be seated at a round table ?
18. Prove that any two composition series of a group G are isomorphic.
19. Let G be a group of order p^n and let X be a finite G-set. Then prove that $|X| \equiv |X_G| (\bmod p)$.
20. Prove that the polynomial $x^2 - 2$ has no zeros in the set of rational numbers $\mathbb{Q}$.
21. State and prove factor theorem.
22. Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$ and let C be the subring consisting of all the constant functions in F. Is C an ideal in F ? Why ?
23. Show that $(x, y : y^2x = y, yx^2y = x)$ is a presentation of a trivial group of one element.
24. Show that $x^2 + 8x - 2$ is irreducible over the set of rational numbers $\mathbb{Q}$.

(7 × 2 = 14 weightage)

Part C

Answer any **two** *questions.*
Each question carries weightage 4.

25. Prove : $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime.
26. Prove that two subnormal series of a group G have isomorphic refinements.
27. Prove that the set $R[x]$ of all polynomials in an indeterminate x with coefficients in the ring R is a ring under the polynomial addition and multiplication.
28. Determine all groups of order 8 upto isomorphism.

(2 × 4 = 8 weightage)

D 12294 (Pages : 3) Name.......................................

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 05—NUMBER THEORY

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 marks.

1. Prove that the Dirichlet multiplication is associative.
2. Evaluate the Legendre's symbol (73 | 383).
3. If $F(x) = \sum_{n \le x} f(n)$, then prove that $\sum_{n \le x} \sum_{d | n} f(d) = \sum_{n \le x} F\left(\frac{x}{n}\right)$.
4. Define the Chebyshev's functions $\psi(x)$ and $\vartheta(x)$.
5. What is meant by a Cryptosystem ?
6. Describe a method to send a signature in RSA cryptosystem.

(6 × 2 = 12 marks)

Part B

Answer any **five** *questions.*
Each question carries 4 marks.

7. If $n \ge 1$, prove that $\sum_{d | n} \phi(d) = n$.
8. For the Euler totient function, prove that $\phi^{-1}(n) = \prod_{p | n} (1 - p)$.
9. Prove that the Legendre symbol $(n | p)$ is a completely multiplicative function of n.
10. For $x \ge 1$, prove that :

$$\sum_{n > x} \frac{1}{n^s} = O\left(x^{1-s}\right) \text{ if } s > 1.$$

11. If $a > 0$ and $b > 0$, then prove that $\pi(ax)/\pi(bx) \sim a/b$ as $x \to \infty$.

12. For $n \geq 1$, prove that the n^{th} prime p_n satisfies the inequality :

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

13. The ciphertext " OF JDFOHFXOL" was intercepted. The ciphertext was enciphered using an affine transformation of single-letter plaintext units in the 27 letter alphabet (with blank = 26). It is known that the first word is "I". ("I" followed by blank). Determine the enciphering key and read the message.

14. Find the inverse of the matrix $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix} \bmod 5$.

(5 × 4 = 20 marks)

Part C

Answer **either** A **or** B *of each question.*
Each question carries 16 *marks.*

15. A (a) If f and g are multiplicative, prove that their Dirichlet product $f * g$ is also multiplicative.

(b) State and prove the Selberg identity.

B (a) Let p be an odd prime. Prove that $(n \mid p) \equiv n^{(p-1)/2} \pmod{p}$ for all integers n.

(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.

16. A (a) Using Euler's summation formula, prove that, for $x \geq 2$,

$$\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2} \log^2 x + A + O\left(\frac{\log x}{x}\right),$$ where A is a constant.

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

$$\sum_{p \leq x} \left[\frac{x}{p}\right] \log p = x \log x + O(x),$$

where the sum is extended overall primes $\leq x$.

B (a) Prove that the following relations are logically equivalent :

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

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

(b) Prove that there is a constant A such that :

$$\sum_{p \le x} \frac{1}{p} = \log\log x + A + O\left(\frac{1}{\log x}\right) \text{ for all } x \ge 2.$$

17. A (a) Briefly describe about digraph transformation.

(b) The ciphertext message "PWULPZTQAWHF" was intercepted. The message was encrypted using an affine map on digraphs in the 26-letter alphabet where a digraph whose two letters have numerical equivalents x and y corresponds to the integer $26x + y$. An extensive statistical analysis of earlier ciphertexts which had been coded by the same enciphering map shows that the most frequently occurring digraphs in all of that ciphertext are "I X" and " T Q", 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 (a) The message "ZRIXXYVBMNPO" which was resulted from a linear enciphering transformation of digraph-vectors in a 27-letter alphabet,in which A-Z have numerical equivalents 0 – 25, and blank = 26 was intercepted. It was found that the most frequently occurring ciphertext digraphs are "PK" and "RZ", and they correspond to the most frequently occurring plaintext digraphs in the 27-letter alphabet namely "E" (E followed by blank) and "S". Find the deciphering matrix and read the message.

(b) Briefly describe about RSA cryptosystem.

(3 × 16 = 48 marks)

D 12293 (Pages : 3) Name.......................................

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 04—DISCRETE MATHEMATICS

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 marks.

1. Prove that, a simple graph with n vertices is complete if and only if $\kappa(G) = n - 1$.
2. Prove or disprove : A tree with at least two vertices contains at least two pendant vertices.
3. Give an example of a partial order which is not a total order.
4. Describe the difference between the maximum element, and maximal element, in a partially ordered set.
5. Explain the terms : word sentence, complement and reverse of a language. Illustrate with examples.
6. Define a grammar and the language generated by this grammar.

(6 × 2 = 12 marks)

Part B

Answer any **five** *questions.*
Each question carries 4 marks.

7. Show by an example that, the condition $\delta \geq \frac{n-2}{2}$ for a simple graph G need not imply that G is connected.
8. Prove that every connected graph contains a spanning tree.
9. Prove that a graph is planar if and only if it isembeddable on a sphere.

Turn over

10. Let $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be partially ordered sets and define a partial order $\leq$ on $X_1 \times X_2$ by $(x_1, x_2) \leq (y_1, y_2)$ if and only if $x_1 \leq_1 y_1$ and $x_2 \leq_2 y_2$. If $\leq_1$ and $\leq_2$ are total, verify whether $\leq$ is total.

11. Write in disjunctive normal forms :

    (i) $x_1' x_2 (x_1' + x_2 + x_1 x_3)$; and (ii) $a + bc'$.

12. (a) Give a simple description of the language generated by the grammar with productions

    $S \to aA, \quad A \to bS, \quad S \to \lambda.$

    (b) If $\Sigma = \{a, b\}$ and $L = \{aa, bb\}$, using set notation describe $\bar{L}$.

13. For $\Sigma = \{a, b\}$, construct dfa. that accept.

    (i) The set of all strings with exactly one a ;

    (ii) The set of all strings with at least, one a.

14. Find a dfa that recognize the set of all strings $\Sigma = \{a, b\}$ starting with the prolix ab.

(5 × 4 = 20 marks)

Part C

Answer **either** *A* **or** *B of each of the following three questions.*
Each question carries 16 *marks.*

15. (A) For a non-trivial connected graph G prove that the following statements are equivalent.

    (i) G is eulerian,

    (ii) the degree of each vertex of G is an even positive integer.

    (iii) G is an edge disjoint, union of cycles.

Or

(B) (a) Prove that a graph is bipartite if and only if it contains no odd cycles

(b) Show that the complement of a simple graph with 11 vertices is nonplanar.

16. (A) Let $(x \leq)$ be a poset and A be a nonempty finite subset of X. Prove that A has at least one maximal element. Also prove that A has a maximum element if and only if it has a unique maximal element.

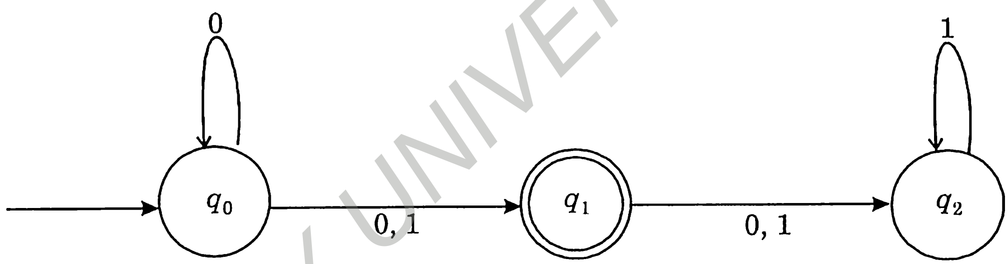
Or

(B) Let $x_1, x_2, \ldots, x_n$ be n mutually independent Boolean variables. Prove that there are 2^{2^n} Boolean functions of these n variables. Also prove that the totality of these Boolean functions constitute a Boolean algebra. Describe the atoms of this Boolean algebra.

17. (A) Let $M = (Q, \Sigma, \delta, q_0, F)$ be a dfa and let G_M be its associated transition graph. For every $q_i, q_j \in Q$ and $w \in \Sigma^+$, prove that $\delta^*(q_i, w) = q_j$ if and only if there is in G_M a walk with label w from q_i to q_j.

Or

(B) Convert the nfa given below into an equivalent deterministic machine.



(3 × 16 = 48 marks)

D 12292 **(Pages : 4)** **Name.......................................**

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 03—REAL ANALYSIS – I

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 *marks.*

1. Prove that every neighborhood is an open set.
2. Let E be a non-empty set of real numbers which is bounded above. If $y = \sup E$, then prove that $y \in \overline{E}$.
3. Identify the discontinuities of the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = [x]$, where $[x]$ denote the largest integer less than or equal to x.
4. Give an example of a continuous real function defined on [–4, 5] which is not differentiable at –1.
5. Let f be a bounded real function and α be a monotonic increasing real function on $[a, b]$. If f is Riemann-Stieltjes integrable with respect to α on $[a, b]$, then prove that $|f|$ is Riemann-Stieltjes integrable with respect to α on $[a, b]$.
6. Let γ be a curve in the complex plane, defined on $[0, 2\pi]$ by $\gamma(t) = e^{2it}$. Prove that γ is rectifiable.
7. Prove that every uniformly convergent sequence of bounded functions is uniformly bounded.
8. Prove that every member of an equicontinuous family is uniformly continuous.

(8 × 2 = 16 marks)

Part B

Answer any **four** *questions.*
Each question carries 4 *marks.*

9. Is arbitrary intersection of open sets in a metric space open ? Justify your answer.
10. Prove that closed subsets of a compact set are compact.

Turn over

11. Let f be a continuous mapping of a compact metric space X into $\mathbb{R}^k$. Prove that f(X) is closed and bounded.

12. Let f be differentiable in (a, b). If $f'(x) \leq 0$ for all $x \in (a,b)$, then prove that f is monotonically decreasing.

13. Let f be a bounded function and α be a monotonic increasing function on $[a, b]$. If f is Riemann-Stieltjes integrable with respect to α on $[a, b]$ and if $a < c < b$, then prove that f is Riemann-Stieltjes integrable with respect to α on $[a, c]$ and on $[c, b]$ and

$$\int_a^c f\, d\alpha + \int_c^b f d\alpha = \int_a^b f\, d\alpha.$$

14. For n = 1, 2, 3, ... and x real, let

$$f_n(x) = \frac{x}{1+nx^2}.$$

Show that $\{f_n\}$ converges uniformly.

(4 × 4 = 16 marks)

Part C

Answer A **or** *B of the following questions.*
Each question carries 12 *marks.*

Unit I

15. A (a) Prove that a subset E of a metric space X is open if and only if its complement E^c is closed.

(b) Let E be a subset of $\mathbb{R}^k$. Prove that the following are equivalent :

(i) E is closed and bounded.

(ii) E is compact.

(iii) Every infinite subset of E has a limit point in E.

B (a) Let $\{G_\alpha\}$ be a collection of open sets in a metric space X. Prove that $\bigcup_\alpha G_\alpha$ is open.

(b) Prove that a subset E of the real line $\mathbb{R}^1$ is connected if and only if E is an interval.

Unit II

16. A (a) Prove 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 E be a non-compact set in $\mathbb{R}^1$. Prove that there exists a continuous function on E which is not bounded.

B (a) Let f be continuous on $[a, b]$ and $f'(x)$ exists at some point $x \in (a,b)$. If g is defined on an interval I which contains the range of f and g is differentiable at the point $f(x)$, then prove that the function h defined on $[a, b]$ by :

$h(t) = g(f(t))$ is differentiable at x and $h'(x) = g'(f(x))f'(x)$.

(b) If f is differentiable on $[a, b]$, then prove that f' cannot have any simple discontinuity on $[a, b]$.

Unit III

17. A (a) Let f be a bounded function and α be a monotonic increasing function on $[a, b]$. If P_1 is a refinement of P, then prove that :

$U(P_1, f, \alpha) \leq U(P, f, \alpha)$.

(b) Let f be a bounded real function and α be a monotonic increasing real function on $[a, b]$. If f is continuous on $[a, b]$, then prove that f is Riemann-Stieltjes integrable with respect to α on $[a, b]$.

B (a) Assume that α increases monotonically and α' is Riemann integrable on $[a,b]$. Let f be a bounded real function on $[a, b]$. Prove that f is Riemann-Stieltjes integrable with respect to α if and only if $f\alpha'$ is Riemann integrable.

(b) If f is Riemann integrable on $[a, b]$ and if there is a differentiable function F on $[a, b]$ such that $F' = f$, then prove that :

$$\int_a^b f\,dx = F(b) - F(a).$$

Unit IV

18. A (a) If $\{ f_n \}$ is a sequence of continuous functions on E and if $f_n \to f$ uniformly on E, then prove that f is continuous on E.

(b) Let (X) denote the set of all complex valued, continuous, bounded functions defined on a metric space X. Prove that (X) is a complete metric space under the metric $d(f,g) = \sup_{x \in X} | f(x) - g(x) |$, where $f, g \in$ (X).

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

(4 × 12 = 48 marks)

D 12291 **(Pages : 4)** **Name.......................................**

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 02—LINEAR ALGEBRA

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *the questions.*
Each question carries 2 marks.

1. Let $S = \{(a_1, a_2, a_3) \varepsilon R^3 : a_1 + 3a_2 = a_3\}$ be the subset of the vector space R^3. Verify whether S is a subspace of R^3.
2. Is there a linear transformation T from R^3 into R^2 such that T (1,–1, 1) = (1, 0) and T (1, 1, 1) = (0, 1) ? Justify your answer.
3. Let T be the linear operator on R^2 defined by $T(x_1, x_2) = (-x_2, x_1)$. What is the matrix of T in the ordered basis $B = \{\alpha_1, \alpha_2\}$, where $\alpha_1 = (1, 2)$ and $\alpha_2 = (1, -1)$.
4. If w_1 and w_2 are subspaces of a finite-dimensional vector space, then $w_1 = w_2$ iff $w_1^0 = w_2^0$.
5. Define minimal polynomial for an $n \times n$ matrix over R. Find a 3 × 3 matrix over R for which the minimal polynomial is x^2.
6. Let T be the linear operator on R^2, the matrix of which in the standard ordered basis is $A = \begin{bmatrix} 1 & -1 \\ 2 & 2 \end{bmatrix}$.

   Determine the subspaces of R^2 invariant under T.
7. Find a projection E which projects R^2 onto the subspace spanned by (1, –1) along the subspace spanned by (1, 2).
8. Describe explicitly all inner products on R.

(8 × 2 = 16 marks)

Part B

Answer any **four** *questions.*
18 *Each question carries* 4 *marks.*

9. Show that a non-empty subset W of a vector space V is a subspace of V iff for each pair of vectors α, β in W and each scalar in c in F the vector $c\,\alpha + \beta$ is in W.

10. Let T be the linear operator on R^3 defined by $T(x_1, x_2, x_3) = (3x_1, x_1, -x_2, 2x_1 + x_2 + x_3)$. Is T invertible? If so, find a rule for T^{-1}.

11. Let V be a finite-dimensional vector space over the field F, and let $B = \{\alpha_1, \ldots, \alpha_n\}$ be a basis for V. Show that there is a unique dual basis $B^* = \{f_1, \ldots, f_n\}$ for V^* such that $f_i(\alpha_j) = \delta_{ij}$, where $\delta_{ij} = \begin{Bmatrix} 1 \ \textit{if}\ i = j \\ 0 \ \textit{if}\ i \neq j \end{Bmatrix}$.

12. Let T be a linear operator on an n-dimensional vector space V. Show that the characteristic and minimal polynomials for T have the same roots, except for multiplicities.

13. Let $w_1, w_2, \ldots, w_k$ be subspaces of a vector space V such that $V = w_1 \oplus \ldots \oplus w_k$. Show that there exists k linear operators $E_1, E_2, \ldots, E_k$ on V such that :

    (i) $E_i E_j = \begin{cases} E_i & \text{if } \hat{j} = i \\ 0 & \text{if } j \neq i \end{cases}$.

    (ii) $I = E_1 + E_2 + \ldots + E_k$.

    (iii) the range of E_i is W_i.

14. Apply the Gram–Schmidt process to obtain an orthonormal basis for the subspace spanned by the vectors $\beta_1 = (1, 0, i)$ and $\beta_2 = (2, 1, 1+i)$ in the inner product space C^3, with the standard inner product.

(4 × 4 = 16 marks)

Part C

Answer **either** A **or** B *of each of the following questions.*
Each question carries 12 *marks.*

15. A (a) Is the vector $(3,-1,0,-1)$ in the subspace of R^4 spanned by the vectors $(2,-1,3,2)$, $(-1,1,1,-3)$ and $(1,1,9,-5)$? Justify your answer.

(b) Let V be a vector space which is spanned by a finite set of vectors $\beta_1, \beta_2, \ldots, \beta_m$. Show that any independent set of vectors in V is finite and contains no more than m elements.

B Let V be a finite-dimensional vector space over the field F and let $\{\alpha_1, \ldots, \alpha_n\}$ be an ordered basis for V. Let W be a vector space over the same field F and let $\beta_1, \ldots, \beta_n$ be any vectors in W. Show that there is precisely one linear transformation T from V into W such that $T\alpha_j = \beta_j, j = 1, 2, \ldots n$.

16. A Let V be an n-dimensional vector space over the field F and let W be an m-dimensional vector space over F. Show that the vector space L (V, W) is infinite dimensional and has dimension mn.

B (a) Let $g, f_1, \ldots, f_r$ be linear functionals on a vector space V with respective null spaces $N, N_1, \ldots, N_r$. Show that g is a linear combination of $f_1, \ldots, f_r$ iff N contains the intersection $N_1 \cap \ldots \cap N_r$.

(b) If W is a subspace of a finite dimensional vector space V and if $\{g_1, \ldots, g_r\}$ is any basis for w^0, then $W = \bigcap_{i=1}^{r} N_{g_i}$, where N_{g_i} is the null space of g_i.

17. A Let T be a linear operator on a finite-dimensional vector space V. Let $c_1, \ldots, c_k$ be the distinct characteristic values of T and let w_i be the null space of $(T - c_i I)$. Show that T is diagonalizable iff $\dim w_1 + \ldots + \dim w_k = \dim V$.

B (a) Let V be a finite dimensional vector space over the field F and let T be a linear operator on V. Show that T is triangulable iff the minimal polynomial for T is a product of linear polynomials over F.

(b) Show that every matrix A such that $A^2 = A$ is similar to a diagonal matrix.

Turn over

18. A Let T be a linear operator on a finite-dimensional vector space V. Suppose that there exist k distinct scalars $c_1 c_2, \ldots, c_k$ an k non-zero linear operators $E_1, \ldots, E_k$. such that :

(i) $T = c_1 E_1 + \ldots, c_k E_k$.

(ii) $I = E_1 + \ldots + E_k$.

(iii) $E_i E_j = 0$ if $i \neq j$.

Show that T is diagonalizable and $c_1, \ldots, c_k$ are the distinct characteristic values of T with the characteristic space for T associated with c_i is the range of E_i.

B (a) Let W be a finite-dimensional subspace of an inner product space V and let E be the orthogonal projection of V on W. Show that E is an idempotent linear transformation of V onto $w, w^{\perp}$ is the null space of E and $V = w \oplus w^{\perp}$.

(b) Let S be a subset of a finite-dimensional inner product space V. Show that $\left(S^{\perp}\right)^{\perp}$ is the subspace spanned by S.

(4 × 12 = 48 marks)

D 12290 (Pages : 3) Name..

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 01—ALGEBRA – I

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 marks.

1. Verify whether (1,2) is a generator of the cyclic group $\mathbb{Z}_3 \times \mathbb{Z}_4$.
2. Describe an isometry of the plane that fixes the Y-axis.
3. Let G = S_3 and H be the subgroup generated by (1 2). Define an action of G on G/H and find the isotropy group G_x for x = H.
4. Let $F = \mathbb{Z} \times \mathbb{Z} / \sim$ be the field of quotients of $\mathbb{Z}$ where the notations are the usual ones. Find all elements in $\mathbb{Z} \times \mathbb{Z}$ which are $\sim$ – related to (1,1).
5. Verify whether $x^4 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$.
6. Verify whether the ideal generated by 10 is a maximal ideal in $\mathbb{Z}_{12}$.
7. Verify whether $\frac{\sqrt{3}}{\sqrt{2}}$ is algebraic over $\mathbb{Q}$.
8. Show that $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

(8 × 2 = 16 marks)

Part B

Answer any **four** *questions.*
Each question carries 4 marks.

9. Find the order of (1, 2, 3) in $\mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_6$.
10. Let G = H × K. Show that G has a normal subgroup isomorphic to H.

Turn over

11. Let X be a G-set and $g \in G$. Let $\sigma_g : X \to X$ be defined by $x \mapsto gx$. Show that σ_g is onto.

12. Describe the field of quotients of the integral domain $\mathbb{Z}_5$.

13. Prove that $x^5 + 15x^2 + 9x + 3$ is irreducible in $\mathbb{Q}[x]$.

14. Show that if α and β are constructible by straight edge and compass then so is αβ.

(4 × 4 = 16 marks)

Part C

Answer **either** *part A* **or** *part B of each of the* **four** *questions.*
Each question carries 12 *marks.*

15. A (a) Let G be a group and H be a subgroup of G. Show that coset multiplication given by $(aH)(bH) = (ab)H$ is well defined if and only if H is a normal subgroup of G.

(b) Show that if H is a normal subgroup of G then G / H is a group.

B Let $\phi : G \to G'$ be an onto homomorphism of groups. Show that :

(i) if N is a normal subgroup of G then $\phi(N)$ is a normal subgroup of G'.

(ii) if H is a normalsubgroup of G' then $\phi^{-1}(H)$ is a normal subgroup of G.

(iii) if Ker 0 is a maximal normal subgroup of G then G' is simple.

16. A (a) Let G be a finite group and X be a G-set. Let G_x be the isotropy group at x and G_x be the orbit of x for $x \in X$. Show that :

(i) $|Gx| = |G : G_x|$.

(ii) $|Gx|$ is a divisor of $|G|$.

(b) Describe an action of S_3 on the set {1, 2, 3} and find all orbits in this action.

B (a) Let D be an integral domain. For $(a,b),(c,d) \in D \times D$ define $(a,b) \sim (c,d)$ if $ad = bc$. Show that ~ is an equivalence relation on D × D.

(b) Let $[a, b]$ denote the ~- class containing (a, b). Show that $[a,b] + [c,d] = [ad + bc, bd]$ is a well defined addition in $D \times D / \sim$.

17. A (a) Let F be a field and $f(x) \in F[x]$ be of degree 2 or 3. Show that $f(x)$ is irreducible if and only if $f(x)$ has no zero in F.

(b) Let $f(x) \in \mathbb{Z}[x]$. Show that $f(x)$ factors into a product of two polynomials of degree r and s in $\mathbb{Q}[x]$ if and only if it has a factorization with polynomials of degree r and s in $\mathbb{Z}[x]$.

B (a) Define prime ideal of a ring R.

(b) Let R be a commutative ring and N be a prime ideal of R. Show that R / N is an integral domain.

(c) Find all prime ideals of the ring $\mathbb{Z}$ of integers.

18. A (a) Let E be a finite extension of a field F and K be a finite extension of E. Show that $[K : F] = [K : E][E : F]$.

(b) Let α be algebraic over F and let $\beta \in F(\alpha)$. Show that $\deg(\beta ; F)$ divides deg $(\alpha : F)$.

B (a) Show that for every prime p and every natural number n, there is a field of p^n elements.

(b) Let E and F be finite fields of order p^n. Prove that E is isomorphic to F.

(4 × 12 = 48 marks)