UPSC CSE Mathematics: Previous Year Questions: Modern Algebra

2025

1) Let H and K be two subgroups of a group G such that $o(H) > \sqrt{o(G)}$ and $o(K) > \sqrt{o(G)}$. Show that $H \cap K \neq \{e\}$, where e is the identity element. Here $o(H)$, $o(K)$ and $o(G)$ denote the order of H, K and G respectively.
2) Let $G = \{e, x, x^2, y, yx, yx^2\}$ be a non-Abelian group with $o(x) = 3$ and $o(y) = 2$.
   Show that $xy = yx^2$ (where e is the identity element of G and $o(x), o(y)$ denote the order of the elements x, y respectively).
3) Show that 3 is an irreducible element in the integral domain $Z[i]$.
4) Examine whether the mapping $\phi: Z[x] \to Z$ defined by $\phi(f(x)) = f(0)$, for $f(x) \in Z[x]$, is a homomorphism. Deduce that the ideal $\langle x \rangle$ is a prime ideal in $Z[x]$, but not a maximal ideal in $Z[x]$.

2024

1) Let G be a finite group of order mn , where m and n are prime numbers with $m > n$. Show that G has at most one subgroup of order m.
2) Show that every homomorphic image of an abelian group is abelian, but the converse is not necessarily true.
3) Consider the polynomial ring Z[x] over the ring Z of integers. Let S be an ideal of Z[x] generated by x . Show that S is prime but not a maximal ideal of Z[x].

2023

1) Let G be a group of order 10 and G' be a group of order 6. Examine whether there exists a homomorphism of G onto G'.
2) Express the ideal 4Z +6Z as a principal ideal in the integral domain Z
3) Prove that a non-commutative group of order $2p$, where p is an odd prime, must have a subgroup of order p.
4) Prove that $x^2 + 1$ is an irreducible polynomial in $Z_3[x]$. Further show that the quotient ring $\frac{Z_3[x]}{\langle x^2+1 \rangle}$ is a field of 9 elements.

2022

1) Show that the multiplicative group $G = \{1, -1, i, -i\}$, where $i = \sqrt{(-1)}$, is isomorphic to the group $G' = \{\{0,1,2,3\}, +_4)$.
2) Prove that every homomorphic image of a group G is isomorphic to some quotient group of G.
3) Let R be a field of real numbers and S, the field of all those polynomials $f(x) \in R[x]$ such that $f(0) = 0 = f(1)$. Prove that S is an ideal of $R[x]$. Is the residue class ring $R[x]/S$ an integral domain? Give justification for your answer.

2021

1) Let $m_1, m_2, \cdots, m_k$ be positive integers and $d > 0$ the greatest common divisor of $m_1, m_2, \cdots, m_k$. Show that there exist integers $x_1, x_2, \cdots, x_k$ such that
$$d = x_1 m_1 + x_2 m_2 + \cdots + x_k m_k$$
2) Let F be a field and $f(x) \in F[x]$ a polynomial of degree > 0 over F. Show that there is a field F' and an imbedding $q: F \to F'$ s.t. the polynomial $f^q \in F'[x]$ has a root in F', where f^q is obtained by replacing each coefficient a of f by $q(a)$.
3) Show that there are infinitely many subgroups of the additive group $\mathbb{Q}$ of rational numbers.

2020

1) Let S_3 and Z_3 be permutation group on 3 symbols and group of residue classes module 3 respectively. Show that there is no homomorphism of S_3 in Z_3 except the trivial homomorphism.
2) Let R be a principal ideal domain. Show that every ideal of a quotient ring of is R principal ideal and $R\,/\,P$ is a principal ideal domain for a prime ideal P of R
3) Let G be a finite cyclic group of order n then prove that G has $\phi(n)$ generators where ϕ is Euler's ϕ function.
4) Let R be a finite field of characteristic $p(\geq 0)$.Show that the mapping $f: R \to R$ defined by $f(a) = a^p, \forall a \in R$ is an isomorphism.

2019

1) Let G be a finite group H and K subgroups of G such that $K \subset H$ Show that $(G:K) = (G:K)(H:K)$
2) If G and H are finite groups whose orders are relatively prime then prove that there is only one homomorphism from G to H the trivial one.
3) Write down all quotient groups of the group Z_{12}.
4) Let a be an irreducible element of the Euclidean Ring R then prove that $R/(a)$ is a field

2018

1) Let R be an integral domain with unit element. Show that any unit in $R[x]$ is a unit in R
2) Show that the quotient group of $(\mathbb{R}, +)$ modulo $\mathbb{Z}$ is isomorphic to the multiplicative group of complex numbers on the unit circle in the complex plane. Here $\mathbb{R}$ is the set of real number and $\mathbb{Z}$ is the set of integers.
3) Find all the proper subgroups of the multiplicative group of the field $(\mathbb{Z}_{13}, +_{13}, \times_{13})$, where $+_{13}$ and $\times_{13}$ represent addition modulo 13 and multiplication modulo 13 respectively.

2017

1) Let G be a group of order n. Show that G is isomorphic to a subgroup of the permutation group S_n.
2) Let F be a field and $F[x]$ denote the ring of polynomial over F in a single variable X. For $f(X), g(X) \in F[X]$ with $g(X) \neq 0$, show that there exist $q(X), r(X) \in F[X]$ such that degree $r(X) <$ degree $g(X)$ and $f(X) = q(X) \cdot g(X) + r(X)$.
3) Show that the groups $Z_5 \times Z_7$ and Z_{35} are isomorphic.

2016

1) Let K be a field and $K[X]$ be the ring of polynomials over K in a single variable X for a polynomial $f \in K[X]$ Let (f) denote the ideal in $K[X]$ generated by f. show that (f) is a maximal ideal in $K[X]$ if and only iff is an irreducible polynomial over K.
2) Let p be prime number and Z_p denote the additive group of integers modulo p. show that that every nonzero element Z_p of generates Z_p
3) Let K be an extension of a field F prove that the element of K which are algebraic over F form a subfield of K Further if $F \subset K \subset L$ Fare fields L is algebraic over K and K is algebraic over F then prove that L is algebraic over F.
4) Show that every algebraically closed field is infinite.

2015

1) How many generators are there of the cyclic group G of order 8? Explain.
2) Taking a group $\{e, a, b, c\}$ of order 4 , where e is the identity, construct composition tables showing that one is cyclic while the other is not
3) Give an example of a ring having identity but a subring of this having a different identity
4) If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R', prove that $\phi(1)$ is the unit element of R'
5) Do the following sets form integral domains with respect to ordinary addition and multiplication? Is so, state if they are fields:
   (i) The set of numbers of the form $b\sqrt{2}$ with b rational.

(ii) The set of even integers.

(iii) The set of positive integers.

2014

1) Let G be the set of all real 2×2 matrices $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$, where $xz \neq 0$. Show that G is group under matrix multiplication. Let N denote the subset $\left\{\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in R\right\}$. Is N a normal subgroup of G ? Justify your answer.

2) Show that Z_7 is a field. Then find $([5]+[6])^{-1}$ and $(-[4])^{-1}$ in Z_7

3) Show that the set $\{a + b\omega : \omega^3 = 1\}$, where a and b are real numbers, is a field with respect to usual addition and multiplication.

4) Prove that the set $Q(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in Q\}$ is commutative ring with identity.

2013

1) Show that the set of matrices $S = \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} a, b \in R\right\}$ is a field under the usual binary operations of matrix addition and matrix multiplication. What are the additive and multiplicative identities and what is the inverse of $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$? Consider the map $f: C \to S$ defined by $f(a + ib) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Show that f is an isomorphism. (Here R is the set of real numbers and C is the set of complex numbers)

2) Give an example of an infinite group in which every element has finite order

3) What are the orders of the following permutation in S_{10}? $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 7 & 3 & 10 & 5 & 4 & 2 & 6 & 9 \end{pmatrix}$ and $(1\ 2\ 3\ 4\ 5)(6\ 7)$

4) What is the maximal possible order of an element in S_{10} ? Why? Give an example of such an element. How many elements will there be in S_{10} of that order?

5) Let $J = \{a + ib / a, b \in Z\}$ be the ring of Gaussian integers (subring of C). Which of the following is J : Euclidean domain, principal ideal domain, and unique factorization domain? Justify your answer

6) Let R^C = ring of all real value continuous functions on [0, 1], under the operations $(f+g)x = f(x) + g(x), (fg)x = f(x)g(x)$. Let $M = \left\{f \in R^C / f\left(\frac{1}{2}\right) = 0\right\}$. Is M a maximal ideal of R ? Justify your answer.

2012

1) How many elements of order 2 are there in the group of order 16 generated by a and b such that the order of a is 8 , the order of b is 2 and $bab^{-1} = a^{-1}$.

2) How many conjugacy classes does the permutation group S_5 of permutation 5 numbers have? Write down one element in each class (preferably in terms of cycles).

3) Is the ideal generated by 2 and X in the polynomial ring $Z[X]$ of polynomials in a single variable X with coefficients in the ring of integers Z, a principal ideal? Justify your answer

4) Describe the maximal ideals in the ring of Gaussian integers $Z[i] = \{a + ib/a, b \in Z\}$.

2011

1) Show that the set $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ of six transformations on the set of Complex numbers defined by $f_1(z) = z,\ f_2(z) = 1 - z,\ f_3(z) = \frac{z}{(1-z)},\ f_4(z) = \frac{1}{z},\ f_5(z) = \frac{1}{(1-z)},\ f_6(z) = \frac{(z-1)}{z}$ is a nonabelian group of order 6 w.r.t. composition of mappings

2) Prove that a group of Prime order is abelian.

3) How many generators are there of the cyclic group $(G,.)\ of\ \ Order 8$?

4) Give an example of a group G in which every proper subgroup is cyclic but the group itself is not cyclic

5) Let F be the set of all real valued continuous functions defined on the closed interval [0, 1]. Prove that $(F, +, .)$ is a Commutative Ring with unity with respect to addition and multiplication of functions defined point wise as below:

$$\left.\begin{array}{l}(f+g)x = f(x) + g(x)\\(fg)x = f(x)g(x)\end{array}\right\} x \in [0,1] \text{ where } f, g \in F$$

6) Let a and b be elements of a group, with $a^2 = e, b^6 = e$ and $ab = b^4 a$. Find the order of ab, and express its inverse in each of the forms $a^m b^n$ and $b^m a^n$

2010

1) Let $G = R - \{-1\}$ be the set of all real numbers omitting -1. Define the binary relation * on G by $a * b = a + b + ab$. Show $(G,*)$ is a group and it is abelian

2) Show that a cyclic group of order 6 is isomorphic to the product of a cyclic group of order 2 and a cyclic group of order 3 . Can you generalize this? Justify.

3) Let $(R^*, .)$ be the multiplicative group of non-zero reals and $(GL(n, R), X)$ be the multiplicative group of $n \times n$ non-singular real matrices. Show that the quotient group $\frac{GL(n,R)}{SL(n,R)}$ and $(R^*, .)$ are isomorphic where $SL(n, R) = \{A \in GL(n, R)/\det\ A = 1\}$. What is the center of $GL(n, R)$

4) Let $C = \{f: I = [0,1] \to R/f$ is continuous $\}$. Show C is a commutative ring with 1 under point wise addition and multiplication. Determine whether C is an integral domain. Explain.

5) Consider the polynomial ring $Q[x]$. Show $p(x) = x^3 - 2$ is irreducible over Q. Let I be the ideal $Q[x]$ in generated by $p(x)$. Then show that $\frac{Q[x]}{I}$ is a field and that each element of it is of the form $a_0 + a_1 t + a_2 t^2$ with a_0, a_1, a_2 in Q and $t = x + I$

6) Show that the quotient ring $\frac{Z[i]}{1+3i}$ is isomorphic to the ring $\frac{Z}{10Z}$ where $Z[i]$ denotes the ring of Gaussian integers.

2009

1) If R is the set of real numbers and $R_+$is the set of positive real numbers, show that R under addition $(R,+)$ and R_+under multiplication $(R_+,.)$are isomorphic. Similarly, if Q is set of rational numbers and $Q_+$is the set of positive rational numbers, are $(Q,+)$ and $(Q_+,.)$isomorphic? Justify your answer.
2) Determine the number of homomorphisms from the additive group Z_{15} to the additive group Z_{10} (Z_n is the cyclic group of order n)
3) How many proper, non-zero ideals, does the ring Z_{12} have? Justify your answer. How many ideals does the ring $Z_{12} \oplus Z_{12}$ have? Why?
4) Show that the alternating group of four letters A_4 has no subgroup of order 6.
5) Show that $Z[X]$ is a unique factorization domain that is not a principal ideal domain (Z is the ring of integers). Is it possible to give an example of principal ideal domain that is not a unique factorization domain? ($Z[X]$ is the ring of polynomials in the variable X with integer.)
6) How many elements does the quotient ring $\frac{Z_5[X]}{X^2+1}$ have? Is it an integral domain? Justify your answers.

2008

1) Let R_0 be the set of all real numbers except zero. Define a binary operation $*$ on R_0 as $a*b = |a|b$ where $|a|$ denotes absolute value of a. Does $(R_0,*)$ form a group? Examine.
2) Suppose that there is a positive even integer n such that $a^n = a$ for all the elements a of some ring R. Show that $a+a=0$ for all $a \in R$ and $a+b=0 \Rightarrow a=b$ for all $a,b \in R$
3) Let G and $\bar{G}$ be two groups and let $\phi: G \to \bar{G}$ be a homomorphism. For any element $a \in G$
   (i) Prove that $O(\phi(a))/O(a)$
   (ii) $\mathrm{Ker}\ \phi$ is normal subgroup of G.

4) Let R be a ring with unity. If the product of any two non-zero elements is non-zero. Then prove that $ab=1 \Rightarrow ba=1$. Whether Z_6 has the above property or not explain. Is Z_6 an integral domain?
5) Prove that every Integral Domain can be embedded in a field.
6) Show that any maximal ideal in the commutative ring $F[x]$ of polynomial over a field F is the principal ideal generated by an irreducible polynomial.

2007

1) If in a group $G, a^5 = e, e$ is the identity element of G , $aba^{-1} = b^2$ for $a, b \in G$, then find the order of b

2) Let $R = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $a, b, c, d \in Z$. Show that R is a ring under matrix addition and multiplication $\left\{A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, a, b \in Z\right\}$. Then show that A is a left ideal of R but not a right ideal of R.

3) Prove that there exists no simple group of order 48.

4) Show $1 + \sqrt{-3}$ and $Z[\sqrt{-3}]$ is an irreducible element, but not prime. Justify your answer.

5) Show that in the ring $R = \{a + b\sqrt{-5}/a, b \in Z\}$. The element $\alpha = 3$ and $\beta = 1 + 2\sqrt{-5}$ are relatively prime, but αy and βy have no g.c.d in R, where $\gamma = 7(1 + 2\sqrt{-5})$

2006

1) Let S be the set of all real numbers except -1. Define on S by $a * b = a + b + ab$. Is $(S,*)$ a group? Find the solution of the equation $2 * x * 3 = 7$ in S.

2) If G is a group of real numbers under addition and N is the subgroup of G consisting of integers, prove that $\frac{G}{N}$ is isomorphic to the group H of all complex numbers of absolute value 1 under multiplication

3) Let $O(G) = 108$. Show that there exists a normal subgroup or order 27 or 9 .

4) Let G be the set of all those ordered pairs (a, b) of real numbers for which $a \neq 0$ and define in G, an operation as follows: $(a, b) \otimes (c, d) = (ac, bc + d)$ Examine whether G is a group w.r.t the operation $\otimes$. If it is a group, is G abelian?

5) Show that $Z[\sqrt{2}] = \{a + b\sqrt{2}: a, b \in Z\}$ is a Euclidean domain.

2005

1) If M and N are normal subgroups of a group G such that $M \cap N = \{e\}$, show that every element of M commutes with every element of N.

2) Show that $(1 + i)$ is a prime element in the ring R of Gaussian integers.

3) Let H and K be two subgroups of a finite group G such that $|H| > \sqrt{|G|}$ and $|K| > \sqrt{|G|}$. Prove that $H \cap K \neq \{e\}$

4) If $f: G \to G$ is an isomorphism, prove that the order $a \in G$ of is equal to the order $f(a)$

5) Prove that any polynomial ring $F[x]$ over a field F is U.F.D

2004

1) If p is prime number of the form $4n + 1, n$ being a natural number, then show that congruence $x^2 \equiv -1(\text{mod}p)$ is solvable.

2) Let G be a group such that of all $a, b \in G$ (i) $ab = ba$ (ii) $(O(a), O(b)) = 1$ then show that $O(ab) = O(a)O(b)$

3) Verify that the set E of the four roots of $x^4 - 1 = 0$ forms a multiplicative group. Also prove that a transformation $T, T(n) = i^n$ is a homomorphism from I_+(Group of all integers with addition) onto E under multiplication.

4) Prove that if cancellation law holds for a ring R then $a(\neq 0) \in R$ is not a zero divisor and conversely

5) The residue class ring $\frac{Z}{(m)}$ is a field iff m is a prime integer.

6) Define irreducible element and prime element in an integral domain D with units. Prove that every prime element in D is irreducible and converse of this is not (in general) true.

2003

1) If H is a subgroup of a group G such that $x^2 \in H$ for every $x \in G$, then prove that H is a normal subgroup of G

2) Show that the ring $Z[i] = \{a + ib/a, b \in Z, i = \sqrt{-1}\}$ of Gaussian integers is a Euclidean domain

3) Let R be the ring of all real-valued continuous functions on the closed interval $[0,1]$. Let $M = \left\{f(x) \in R/f\left(\frac{1}{3}\right) = 0\right\}$. Show that M is a maximal ideal of R

4) Let M and N be two ideals of a ring R. Show that $M \cup N$ is an ideal of R if and only if either $M \subseteq N$ or $N \subseteq M$

5) Show that $Q(\sqrt{3}, i)$ is a splitting field for $x^5 - 3x^3 + x^2 - 3$ where Q is the field of rational numbers

6) Prove that $x^2 + x + 4$ is irreducible over F the field of integers modulo 11 and prove further that $\frac{F[x]}{(x^2+x+4)}$ is a field having 121 elements.

7) Let R be a unique factorization domain (U.F.D), then prove that $R[x]$ is also U.F.D

2002

1) Show that a group of order 35 is cyclic.

2) Show that polynomial $25x^4 + 9x^3 + 3x + 3$ is irreducible over the field of rational numbers

3) Show that a group of p^2 is abelian, where p is a prime number.

4) Prove that a group of order 42 has a normal subgroup of order 7.

5) Prove that in the ring $F[x]$ of polynomial over a field F, the ideal $1 = |p(x)|$ is maximal if and only if the polynomial $p(x)$ is irreducible over F.

6) Show that every finite integral domain is a field

7) Let F be a field with q elements. Let E be a finite extension of degree n over F. Show that E has q^n elements

2001

1) Let K be a field and G be a finite subgroup of the multiplicative group of non-zero elements of K. Show that G is a cyclic group.

2) Prove that the polynomial $1 + x + x^2 + x^3 + \cdots + x^{p-1}$ where p is prime number is irreducible over the field of rational numbers.

3) Let N be a normal subgroup of a group G. Show that $\frac{G}{N}$ is abelian if and only if for all $x, y \in G, xyx^{-1}y^{-1} \in N$

4) If R is a commutative ring with unit element and M is an ideal of R, then show that maximal ideal of R if and only if $\frac{R}{M}$ is a field

5) Prove that every finite extension of a field is an algebraic extension. Give an example to show that the converse is not true.