ANNA ADARSH COLLEGE FOR WOMEN (AUTONOMOUS) CHENNAI – 600040
END SEMESTER EXAMINATIONS-NOVEMBER – 2025

Programme : M.Sc Mathematics	**Batch : 2025-2027**	**Semester : I**
Course Title: Algebra -I	**Course Code :24PMSMT101**	
Duration : 3 Hrs	**Maximum Marks : 75**	

Question No	Question	Mark	K Level (K1-K6)	(CO) (CO1-CO5)
	SECTION – A (10 X 1 = 10 Marks) Answer Any Ten Questions			
1	Show that S_4 is solvable. *Proof.* If $G = S_n$, by Lemma 5.7.2, $G^{(k)}$ contains all 3-cycles in S_n for every k. Therefore, $G^{(k)} \neq (e)$ for any k, whence by Lemma 5.7.1, G cannot be solvable.	**1**	**K1**	**CO1**
2	Predict that general polynomial of degree n ≥ 5 is not solvable by radicals. If f (x) is an irreducible polynomial over Q, of prime degree p, and if f has exactly p - 2 real roots, then its Galois group is Sp. By Galois Theory an arbitrary polynomial equation of degree ≥5≥5 is **not** solvable using radicals, unlike the polynomial equation of second degree which is solvable by radicals (because of the alternating group of order 5, the symmetry group is not soluble).	**1**	**K2**	**CO1**
3	Define Normalizer of a in G. DEFINITION If $a \in G$, then $N(a)$, the *normalizer of a in G*, is the set $N(a) = \{x \in G \mid xa = ax\}$.	**1**	**K1**	**CO1**
4	Define Internal direct product.	**1**	**K1**	**CO2**
5	Define the class equation. *If G is a .finite group, then c_a = o(G)fo(N(a)); in other words, the number of elements conjugate to a in G is the index of the normalizer of a in G.*	**1**	**K2**	**CO2**
6	What is meant by canonical form? Thus we need some canonical form for elements in $A_F(V)$ (or in F_n which presumes nothing about the location of the characteristic roots of it elements, a canonical form and a set of invariants created in $A_F(V)$ itsel using only its elements and operations. Such a canonical form is provided as by the rational canonical form which is described	**1**	**K2**	**CO3**
7	Define Invariant The integers $n_1, n_2, \ldots, n_r$ are called the *invariants* of T	**1**	**K1**	**CO3**
8	Define Jordan form. $\begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_k \end{pmatrix}$ is called the *Jordan form* of T. Note that Theorem 6.6.2,	**1**	**K1**	**CO4**
9	Define Trace of matrix. DEFINITION The *trace* of A is the sum of the elements on the main diagonal of A.	**1**	**K2**	**CO4**
10	Define Normal Transformation.	**1**	**K1**	**CO5**

	DEFINITION $T \in A(V)$ is said to be *normal* if $TT^* = T^*T$.			
11	Define Unitary transformation. **DEFINITION** The linear transformation $T \in A(V)$ is said to be *unitary* if $(uT, vT) = (u, v)$ for all $u, v \in V$.	**1**	**K1**	**CO5**
12	Infer that G is abelian and G is not simple if G is a group of order 11^2 x 13^2. by Sylow theorems, that if G has order $11^2 \times 13^2$then G=H.Kwith $\|H\|=11^2$, $\|K\|=13^2$and H,K	**1**	**K2**	**CO5**
	SECTION – B (5 X 5 = 25 Marks) **Answer Any Five Questions**			
13.	Explain the conjugacy relation defined on a group in an equivalence relation. The relation ~ defined on a group G by: for a, b ∈ G, a ~ b if b = cac−1 for some c ∈ G, is an equivalence relation on G, which is called conjugacy and the equivalence class Cl(a) = {cac−1 | c ∈ G} of a determined by ~ is called the conjugacy class of a. *Proof.* As usual, in order to establish this, we must prove that 1. $a \sim a$; 2. $a \sim b$ implies that $b \sim a$; 3. $a \sim b$, $b \sim c$ implies that $a \sim c$ for all a, b, c in G. We prove each of these in turn. 1. Since $a = e^{-1}ae$, $a \sim a$, with $c = e$ serving as the c in the definition of conjugacy. 2. If $a \sim b$, then $b = x^{-1}ax$ for some $x \in G$, hence, $a = (x^{-1})^{-1}b(x^{-1})$, and since $y = x^{-1} \in G$ and $a = y^{-1}by$, $b \sim a$ follows. 3. Suppose that $a \sim b$ and $b \sim c$ where $a, b, c \in G$. Then $b = x^{-1}ax$, $c = y^{-1}by$ for some $x, y \in G$. Substituting for b in the expression for c we obtain $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$; since $xy \in G$, $a \sim c$ is a consequence	**5**	**K3**	**CO1**
14	Examine that G is abelian, if $o(G) = p^2$, where p is a prime number. Our aim is to show that Z(G) = G. At any rate, we already know that Z(G) $\neq(e)$ is a subgroup of G so that o(Z(G)) = p or p^2 . Ifo(Z(G)) = p^2, then Z(G) = G and we are done. Suppose that o(Z(G)) = p; let $a \in G$, $a \notin$ Z(G). Thus $N(a)$ is a subgroup of G, Z(G) c $N(a)$,2 $a \in N(a)$,so that $o(N(a)) > p$, yet by Lagrange's theorem $o(N(a)) / o(G) = p^2$. The only way out is for $o(N(a)) = p^2$ implying that $a \in$ Z(G), a contradiction. Thus o(Z(G)) =p is not an actual possibility. COROLLARY *If $o(G) = p^2$ where p is a prime number, then G is abelian.* *Proof.* Our aim is to show that $Z(G) = G$. At any rate, we already know that $Z(G) \neq (e)$ is a subgroup of G so that $o(Z(G)) = p$ or p^2. If $o(Z(G)) = p^2$, then $Z(G) = G$ and we are done. Suppose that $o(Z(G)) = p$; let $a \in G$, $a \notin Z(G)$. Thus $N(a)$ is a subgroup of G, $Z(G) \subset N(a)$, $a \in N(a)$, so that $o(N(a)) > p$, yet by Lagrange's theorem $o(N(a)) \mid o(G) = p^2$. The only way out is for $o(N(a)) = p^2$, implying that $a \in Z(G)$, a contradiction. Thus $o(Z(G)) = p$ is not an actual possibility.	**5**	**K4**	**CO2**
15	Identify that G = A x B, the external direct product of A and B is a group. Let A and B be any two groups and consider the Cartesian product	**5**	**K4**	**CO3**

	$G = A$ x B of A and B. G consists of all ordered pairs (a, b), where $a \in A$ and b$\in B$ That is, let us define, for (a_1, b_1) and (a_2, b_2) in G, their product via $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1 b_2)$.Here, the product $a_1 a_2$ in the first component is the product of the elements a_1 and a_2 as calculated in the group A. The product $b_1 b_2$ in the second component is that of b_1 and b_2 as elements in the group B. With this definition we at least have a product defined in G. We do so now. First we do the associative law. Let $(a_1 b_1)$, (a_2, b_2), and (a_3, b_3) be three elements of G. Then $((a_1, b_1)(a_2, b_2))(a_3, b_3) = (a_1 a_2, b_1 b_2)(a_3, b_3) = ((a_1a_2)a_3, (b_1b_2)b_3)$, while $(a_1, b_1)((a_2, b_2)(a_3, b_3)) = (a_1, b_1)(a_2a_3, b_2 b_3) = (a_1(a_2a_3), b_1(b_2 b_3))$. The associativity of the product in A and in B then show us that our product in G is indeed associative. Now to the unit element. What would be more natural than to try (e,f), where e is the unit element of A and f that of B, as the proposed unit element for G. We have $(a, b)(e,f) = (ae, bf) = (a, b)$ and $(e,f)(a, b) = (ea,fb) = (a, b)$. Thus (e,f) acts as a unit element in G. Finally, we need the inverse in G for any element of G. Here, too, why not try the obvious? Let $(a, b) \in G$; try (a^{-1}, b^{-1}) as its inverse. Now $(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e,f)$ and $(a^{-1}, b^{-1})(a, b) = (a^{-1}a, b^{-1}b) = (e,j)$, so that (a^{-1}, b^{-1}) does serve as the inverse for (a, b).With this we have verified that $G = A$ x B is a group. We call it the *external direct product* of A and B .Since $G = A$ x B has been built			
16	Specify that Z (G) ≠ (e), if o(G) = p ^{n} , where p is a prime number.	**5**	**K4**	**CO4**
17	Prove that T = 0 when T∈ A(V) such that (vT, v) = 0 **LEMMA 6.10.1** *If $T \in A(V)$ is such that $(vT, v) = 0$ for all $v \in V$, then $T = 0$.* ***Proof.*** Since $(vT, v) = 0$ for $v \in V$, given $u, w \in V$, $((u + w)T, u + w) = 0$. Expanding this out and making use of $(uT, u) = (wT, w) = 0$, we obtain $$(uT, w) + (wT, u) = 0 \text{ for all } u, w \in V. \quad (1)$$ Since equation (1) holds for arbitrary w in V, it still must hold if we replace in it w by iw where $i^2 = -1$; but $(uT, iw) = -i(uT, w)$ whereas $((iw)T, u) = i(wT, u)$. Substituting these values in (1) and canceling out i leads us to $$-(uT, w) + (wT, u) = 0. \quad (2)$$ Adding (1) and (2) we get $(wT, u) = 0$ for all $u, w \in V$, whence, in particular, $(wT, wT) = 0$. By the defining properties of an inner-product	**5**	**K3**	**CO5**
18	If T∈ A(V) then prove that tr (T) is the sum of the characteristic roots of T.	**5**	**K4**	**CO5**

	be 0, the result is indeed true.			
19	Prove that N(a) is a subgroup of G *Proof.* In this result the order of G, whether it be finite or infinite, is of no relevance, and so we put no restrictions on the order of G. Suppose that $x, y \in N(a)$. Thus $xa = ax$ and $ya = ay$. Therefore, $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, in consequence of which $xy \in N(a)$. From $ax = xa$ it follows that $x^{-1}a = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = ax^{-1}$, so that x^{-1} is also in $N(a)$. But then $N(a)$ has been demonstrated to be a subgroup of G.	**5**	**K3**	**CO1**
SECTION – C (4 X 10 = 40 Marks) Answer ASny Four Questions				
20	State and prove Sylow's first theorem. ***If p is a prime number and p^{α} / o(G), then G has a subgroup of order p^{α}*** Before entering the first proof of the theorem we digress slightly to a brief number-theoretic and combinatorial discussion. The number of ways of picking a subset of k elements from a set of n elements can easily be shown to be ..nCk The question is, What power of p divides Looking at this number, written out as we have written it out, one can see that except for the terrn m in the numerator, the power of p dividing $(p^{a}m$ - i) is the same as that dividing so all powers of p cancel out except the power which divides m. Thus Let A be the set of all subsets of G which have p^{α} elements. Thus $\mathscr{M}$ has (p) elements. Given M_1 , $M_2 \in \mathscr{M}$ is a subset of G having p^{α} elements, and likewise so is $M2$) define M_1, M_2 if there exists an element g E G such that $M_1 = M2g$. It is mediate to verify that this defines an equivalence relation on A. We claim that there is at least one equivalence class of elements in $\mathscr{M}$. such that the number of elements in this class is not a multiple of p^{r+1}, for if p^{r+1} is divisor of the size of each equivalence class, then p^{r+1} would be a divisor of the number of elements in $\mathscr{M}$. Since $\mathscr{M}$ has ($p^{\alpha m}$) elements and this cannot be the case. Let $\{M_1., \ldots, M_n.\}$ be such an equivalence class in A where p^{r+1} n. By our very definition of equivalence in $\mathscr{M}$, if $g \in G$, for each $i = 1, \ldots, n$, $M_i g = M_j$ for some j, We let $H = \{g \in G / M_1 g = M_1\}$. Clearly H is a subgroup of G, for if $a, b \in H$, then $M_1 a = M_1$, $M_1 b = M_1$ whence $M_1 ab = (M_1 a)b = M_1 b = M_1$ • We shall be vitally concerned with $o(H)$. We claim that $no(H) = o(G)$; . Now $no(H) = o(G) = p^{\alpha}m$; since $p^{r+1} \nmid n$ and $p^{\alpha+r} / p^{\alpha}m = no(H)$, it must follow that . $p^{\alpha} / o(H)$, and so $o(H) \geq p^{\alpha}$.. However, if m_1 , then for all $h \in H$, $m_1 h \in M_1$ • Thus M_1 has at least $o(H)$ distinct elements. However, M_1 was a subset of G containing. p^{α} elements. Thus $p^{\alpha} \geq o(H)$. Combined with $o(H) \geq p^{\alpha}$. We have that $o(H) = p^{\alpha}$*But then we have exhibited a subgroup of G having exactly p« elements, namely H.* This proves the theorem	**10**	**K3**	**CO1**

	THEOREM 2.12.1 (SYLOW) *If p is a prime number and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.* Before entering the first proof of the theorem we digress slightly to a brief number-theoretic and combinatorial discussion. The number of ways of picking a subset of k elements from a set of n elements can easily be shown to be $$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$ If $n = p^\alpha m$ where p is a prime number, and if $p^r \mid m$ but $p^{r+1} \nmid m$, consider $$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!}$$ $$= \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - i)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)\cdots(p^\alpha - i)\cdots(p^\alpha - p^\alpha + 1)}.$$ The question is, What power of p divides $\binom{p^\alpha m}{p^\alpha}$? Looking at this number, written out as we have written it out, one can see that except for the term m in the numerator, the power of p dividing $(p^\alpha m - i)$ is the same as that dividing $p^\alpha - i$, so all powers of p cancel out except the power which divides m. Thus $$p^r \mid \binom{p^\alpha m}{p^\alpha} \quad \text{but} \quad p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}.$$ *First Proof of the Theorem.* Let $\mathcal{M}$ be the set of all subsets of G which have p^α elements. Thus $\mathcal{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements. Given $M_1, M_2 \in \mathcal{M}$ (M is a subset of G having p^α elements, and likewise so is M_2) define $M_1 \sim M_2$ if there exists an element $g \in G$ such that $M_1 = M_2 g$. It is immediate to verify that this defines an equivalence relation on $\mathcal{M}$. We claim that there is at least one equivalence class of elements in $\mathcal{M}$ such that the number of elements in this class is not a multiple of p^{r+1}, for if p^{r+1} is a divisor of the size of each equivalence class, then p^{r+1} would be a divisor of the number of elements in $\mathcal{M}$. Since $\mathcal{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements and $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$, this cannot be the case. Let $\{M_1, \ldots, M_n\}$ be such an equivalence class in $\mathcal{M}$ where $p^{r+1} \nmid n$. By our very definition of equivalence in $\mathcal{M}$, if $g \in G$, for each $i = 1, \ldots, n$, $M_i g = M_j$ for some j, $1 \le j \le n$. We let $H = \{g \in G \mid M_1 g = M_1\}$. Clearly H is a subgroup of G, for if $a, b \in H$, then $M_1 a = M_1$, $M_1 b = M_1$ whence $M_1 ab = (M_1 a)b = M_1 b = M_1$. We shall be vitally concerned with $o(H)$. We claim that $no(H) = o(G)$; we leave the proof to the reader, but suggest the argument used in the counting principle in Section 2.11. Now $no(H) = o(G) = p^\alpha m$; since $p^{r+1} \nmid n$ and $p^{\alpha+r} \mid p^\alpha m = no(H)$, it must follow that $p^\alpha \mid o(H)$, and so $o(H) \ge p^\alpha$. However, if $m_1 \in M_1$, then for all $h \in H$, $m_1 h \in M_1$. Thus M_1 has at least $o(H)$ distinct elements. However, M_1 was a subset of G containing p^α elements. Thus $p^\alpha \ge o(H)$. Combined with $o(H) \ge p^\alpha$ we have that $o(H) = p^\alpha$. *But then we have exhibited a subgroup of G having exactly p^α elements, namely H.* This proves the theorem; it actually has done more—it has constructed the required subgroup before our very eyes!			
21	a) Test the fundamental result of finite abelian groups. That any finite abelian group G is the direct product of its Sylow subgroups. Ifwe knew that each such Sylow subgroup was a direct product of cyclic goups we could put the results together for these Sylow subgroups to realize G as a direct product of cyclic groups. Thus it suffices to prove the theorem for abelian groups of order pn where p is a prime. So suppose that G is an abelian group of order pn. Our objective is to find elements $a_{1,\ldots,}ak$ in G such that every element x E G can be written in a unique fashion as $x = a_{1\,11.}$ $_1 a_{2\,11.2} \cdots ak_{\,11.k}$ Note that if this were true and $a_{1,\cdots,}ak$ were of order $p^{n}{}_{1,\cdots,}P^{n}\backslash$ where $n_1 \sim n_2 \sim \cdots \sim nk$, then the maximal order of any element in G would be $p^{n}{}_{1}$(Prove!). The procedure	**10**	**K3**	**CO2**

	suggested by this is: let a1 be an element of maximal order in *G.* How shall we pick *a2 ?* Well, if A 1 = (a 1) the subgroup generated by a1, then *a2* maps into an element of highest order in *G/A 1 .*If we can successfully exploit this to find an appropriate *a2 ,* and if *A 2* =(a 2), then *a3* would map into an element of maximal order in *G/A 1A 2 ,* and so on. Let a1 be an element in *G* of highest possible order, p^n 1and let *A 1* =(a 1). Pick *b2* in *G* such that *52 ,* the image of *b2* in $G = GJA_1$, has maximal order p^n 2 Since the order of *52* divides that of *b2 ,* and since the order of *a1* is maximal, we must have that *n1 ~ n2* • In order to get a direct product of *A 1* with (b 2) we would need A1 *n* (b 2) = *(e);* this might not be true for the initial choice of *b2 ,* so we may have to adapt the element *b2* • Suppose that A 1 *n* (b 2) =*f:. (e);* then, since *b2 P"2* E *A 1* and is the first power of *b2* to fall in A1 (by our mechanism of choosing b2) we have that *b2 P"2* = *ai1* Therefore (a 1 i)P"t -n2 = (b 2P"2)P" 1 -n2 = b/"1 = *e,* whence a 1 iP"t-"2 = *e.* Since *a1* is of order P^n 1 we must have that p^n 1/ *ipn* 1 -n2 , and so *pn* 2/ *i.* we have *b2 P"2* = *a1i* = a/P"2 • This tells us that if *a2* =a 1 - *ib* 2 then *a2 P" 2* = *e.* The element *a2* is indeed the element we seek. Let *A 2* = *(a 2).* We claim that A 1 *n A 2* = *(e).* For, suppose that *a2 t* ε *A1 ;*since *a2* = *a 1 -ib2 ,* we get *(a 1 -ib2)tEA1* and so *b2tεA1* • By choice *ofb2,* this last relation forces *pn2* I *t,* and since a/"2 = *ewe* must have that *a2t* = *e.* In short A 1 *n A 2* = (e). We continue one more step in the program we have outlined. Let *b3* E *G* map into an element of maximal order in *G/(A 1A 2).* If the order of the image of *b3* in *G/(A 1 A2)* is *pn*\ we claim that *n3 ~ n2 ~* n1 . By the choice of *n2 , bl"2* E *A 1* so is certainly in *A 1A 2* • Thus *n3 ~ n 2* • Since *b3 P"3* E *A 1 A 2 , bl"3* = *a1 i 1 a2 i 2* • We claim that *pn* 3 1 i 1 and *pn* 3 1 i2 . For, *b3 P" 2* E A 1 hence *(a 1i 1a2 i 2)P" 2 -"3* = (bl"3)P"2 -"3 = b3P"2 E A 1 . This tells us that *a2 i 2 p"2 -n3* E A 1 and so *pn* 2/ *i2 pn* 2 -n3 , which is to say, *pn* 3 I i2 Also b3P"t :::::*e,* hence (a 1 i 1a 2 i 2)P"t-" 3 = *bl"1* = *e;* this says that a 1 itP"1 -"3 E *A 2 n* A1 = *(e),* that is, a 1itP"t -n3 = *e.* This yields that *pn* 3/ i 1 . Let i 1 = J_1P^n 3 , i 2 = *J2pn* 3 ; thus b3 P"3 = a/1 P"3 a/2 P"3 • Let *a3* = *a 1 -ha2 -hb3 , A 3* = (a 3); note that *al"3* =*e.* We claim that *A 3 n (A 1A2)* = (e). For if *a3 t* E *A1 A 2* then (a 1 -,'1 a2 -*hb3)t* E*A 1 A 2 ,* giving us *b3 t* E *A 1 A2* • But then *pn3*/ *t,* whence, since *a3 P"3* = *e,* we have *a3 t* = *e.* In other words, A3 ∩ (A 1 A 2) = (e).			
22	If T ∈ A(V) has all its characteristics roots lies in F,	**10**	**K4**	**CO3**

	then there exists a basis of V in which matrix of T is triangular.			
23	Prove that the elements S and T in $A_F(V)$ are similar in $A_F(V)$ if and only if they have the Same elementary divisors.	**10**	**K4**	**CO4**
24	Examine the class equation. *If G is a ,finite group, then c_a = o(G)fo(N(a)); in other words, the number of elements conjugate to a in G is the index of the normalizer of a in G.* ***Proof.*** To begin with, the conjugate class of *a* in *G, C(a),* consists exactly of all the elements $x^{-1}ax$ as *x* ranges over *G.* c_a measures the number of distinct $x^{-1}ax$'s. *The* two elements in the same right coset of *N(a)* in *G* yield the same conjugate of *a* whereas two elements in different right cosets of *N(a)* in *G* give rise to different conjugates of *a.* In this way we shall have a one-to-one correspondence between conjugates of *a* and right cosets of *N(a).* Suppose that *x,y* ε *G* are in the same right coset of *N(a)* in *G.* Thus *y = nx,* where *n* E *N(a),* and so *na = an.* Therefore, since $y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$, $y^{-1}ay = x^{-1}n^{-1}anx = x^{-1}n^{-1}nax = x^{-1}ax,$ whence *x* and *J* result in the same conjugate of *a.* If, on the other hand, *x* andy are in different right cosets of *N (a)* in *G* we claim that $x^{-1}ax ::/= y^{-1}ay.$ Were this not the case, from $x^{-1}ax = y^{-1}a)$ we would deduce that $yx^{-1}a = ayx^{-1};$ this in turn would imply that yx^{-1} E *N(a).* However, this declares *x* and y to be in the same; right *coset* of *N(a)* in *G,* contradicting the fact that they are in different cosets. *sum runs over one element a in each conjugate class.* , using the theorem the corollary becomes immediate. The equation in this corollary is usually referred to as the *class equation* of *G.* Before going on to the applications of these results let us examine these concepts in some specific group. There is no point in looking at abelian groups because there two elements are conjugate if and only if they are equal (that is, $c_a = 1$ for every a). So we turn to our familiar friend, the, group S_3 .Its elements are *e,* (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, THEOREM 2.11.1 *If G is a finite group, then $c_a = o(G)/o(N(a))$; in other words, the number of elements conjugate to a in G is the index of the normalizer of a in G.* *Proof.* To begin with, the conjugate class of *a* in *G*, $C(a)$, consists exactly of all the elements $x^{-1}ax$ as *x* ranges over *G*. c_a measures the number of distinct $x^{-1}ax$'s. Our method of proof will be to show that two elements in the same right coset of $N(a)$ in *G* yield the same conjugate of *a* whereas two elements in different right cosets of $N(a)$ in *G* give rise to different conjugates of *a*. In this way we shall have a one-to-one correspondence between conjugates of *a* and right cosets of $N(a)$. Suppose that $x, y \in G$ are in the same right coset of $N(a)$ in *G*. Thus $y = nx$, where $n \in N(a)$, and so $na = an$. Therefore, since $y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$, $y^{-1}ay = x^{-1}n^{-1}anx = x^{-1}n^{-1}nax = x^{-1}ax$, whence x and y result in the same conjugate of *a*. If, on the other hand, x and y are in different right cosets of $N(a)$ in *G* we claim that $x^{-1}ax \neq y^{-1}ay$. Were this not the case, from $x^{-1}ax = y^{-1}ay$ we would deduce that $yx^{-1}a = ayx^{-1}$; this in turn would imply that $yx^{-1} \in N(a)$. However, this declares x and y to be in the same right coset of $N(a)$ in *G*, contradicting the fact that they are in different cosets. The proof is now complete.	**10**	**K4**	**CO5**

25	Explain the Cauchy's theorem for a group G.	**10**	**K3**	**CO1**

THEOREM 2.11.3 (CAUCHY) *If p is a prime number and $p \mid o(G)$, then G has an element of order p.*

Proof. We seek an element $a \neq e \in G$ satisfying $a^p = e$. To prove its existence we proceed by induction on $o(G)$; that is, we assume the theorem to be true for all groups T such that $o(T) < o(G)$. We need not worry about starting the induction for the result is vacuously true for groups of order 1.

If for any subgroup W of G, $W \neq G$, were it to happen that $p \mid o(W)$, then by our induction hypothesis there would exist an element of order p in W, and thus there would be such an element in G. Thus we may assume that p is not a divisor of the order of any proper subgroup of G. In particular, if $a \notin Z(G)$, since $N(a) \neq G$, $p \nmid o(N(a))$. Let us write down the class equation:

$$o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}.$$

Since $p \mid o(G)$, $p \nmid o(N(a))$ we have that

$$p \left| \frac{o(G)}{o(N(a))}, \right.$$

and so

$$p \left| \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}; \right.$$

since we also have that $p \mid o(G)$, we conclude that

$$p \left| \left(o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} \right) = o(Z(G)). \right.$$

$Z(G)$ is thus a subgroup of G whose order is divisible by p. But, after all, we have assumed that p is not a divisor of the order of any proper subgroup of G, so that $Z(G)$ cannot be a proper subgroup of G. We are forced to accept the only possibility left us, namely, that $Z(G) = G$. But then G is abelian; now we invoke the result already established for abelian groups to complete the induction. This proves the theorem.