M. Sc. (Mathematics) **Semester-I**

ABSTRACT ALGEBRA

Paper Code: 20MAT21C1

DIRECTORATE OF DISTANCE EDUCATION
MAHARSHI DAYANAND UNIVERSITY, ROHTAK
(A State University established under Haryana Act No. XXV of 1975)
NAAC 'A+' Grade Accredited University

Author

Dr. Jagbir Singh
Assistant Professor, Department of Mathematics
Maharshi Dayanand University, Rohtak

Maharshi Dayanand University
ROHTAK – 124 001

MASTER OF SCIENCE (MATHEMATICS)
First Semester
Paper code: 20MAT21C1
Abstract Algebra

M. Marks = 100
Term End Examination = 80
Assignment = 20
Time = 3 hrs

Course Outcomes

Students would be able to:

CO1 Apply group theoretic reasoning to group actions.

CO2 Learn properties and analysis of solvable & nilpotent groups, Noetherian & Artinian modules and rings.

CO3 Apply Sylow's theorems to describe the structure of some finite groups and use the concepts of isomorphism and homomorphism for groups and rings.

CO4 Use various canonical types of groups and rings- cyclic groups and groups of permutations, polynomial rings and modular rings.

CO5 Analyze and illustrate examples of composition series, normal series, subnormal series.

Section - I

Conjugates and centralizers in Sn, p-groups, Group actions, Counting orbits. Sylow subgroups, Sylow theorems, Applications of Sylow theorems, Description of group of order p2 and pq, Survey of groups upto order 15.

Section - II

Normal and subnormal series, Solvable series, Derived series, Solvable groups, Solvability of Sn-the symmetric group of degree $n \geq 2$, Central series, Nilpotent groups and their properties, Equivalent conditions for a finite group to be nilpotent, Upperandlower central series.
Composition series, Zassenhaus lemma, Jordan-Holder theorem.

Section - III

Modules, Cyclic modules, Simple and semi-simple modules, Schur lemma, Free modules,
Torsion modules, Torsion free modules, Torsion part of a module, Modules over principal ideal domain and its applications to finitely generated abelian groups.

Section - IV

Noetherian and Artinian modules, Modules of finite length, Noetherian and Artinian rings, Hilbert basis theorem.
HomR(R,R), Opposite rings, Wedderburn – Artin theorem, Maschk theorem, Equivalent statement for left Artinian rings having non-zero nilpotent ideals.
Radicals: Jacobson radical, Radical of an Artinian ring.

Note :The question paper of each course will consist of **five** Sections. Each of the sections **I to IV** will contain **two** questions and the students shall be asked to attempt **one** question from each. **Section-V** shall be **compulsory** and will contain **eight** short answer type questions without any internal choice covering the entire syllabus.

Books Recommended:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Lanski, C. Concepts in Abstract Algebra, American Mathematical Society, First Indian Edition, 2010.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
5. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
6. Musili, C., Introduction to Rings and Modules, Narosa Publication House, 1994.
7. Jacobson, N., Basic Algebra, Vol. I & II, W.H Freeman, 1980 (also published by Hindustan Publishing Company).
8. Artin, M., Algebra, Prentice-Hall of India, 1991.
9. Macdonald, I. D., The Theory of Groups, Clarendon Press, 1968.

Contents

1

PRELIMINARIES

Structure

1.1. Introduction.

1.2. Definitions.

1.1. Introduction. This chapter contains definitions and results related to groups, cyclic group, subgroups, normal subgroups, permutation group, centre of a group, homomorphism and isomorphism. All of these results will be helpful throughout the further study of the course.

1.1.1. Objective. The objective of the study of these results is to understand the basic concepts and have an idea to apply them in further study of the course.

1.2. Definitions.

1.2.1. Cartesian Product of Two Sets. Let A and B be two non-empty sets. Then, the set of all distinct ordered pairs whose first co-ordinate is an element of A and whose second co-ordinate is an element of B is called cartesian product of A and B and is denoted by $A \times B$. For example, let $A = \{1,2\}$, $B = \{4,5\}$, then

$A \times B = \{(1,4),(1,5),(2,4),(2,5)\}$ and $B \times A = \{(4,1),(4,2),(5,1),(5,2)\}$.

Thus, in general, $A \times B \neq B \times A$ if $A \neq B$. Also, $A \times B = \phi$ if A or B or both of A and B are empty sets.

1.2.2. Function. Let A and B be two given non-empty sets. A correspondence denoted by f, which associates to each member of A a unique member of B is called a function. The function f from A to B is denoted by $f : A \to B$.

1.2.3. Binary Operation. A mapping $f : S \times S \to S$ is called a binary operation on the set S.

1.2.4. Algebraic Structure. A non-empty set S equipped with one or more binary operations is called an algebraic structure. Suppose '*' is a binary operation on S. Then, (S,*) is called an algebraic structure.

1.2.5. Group. LetG be a non-empty set with a binary operation '*'. Then, G is called a group w.r.t. binary operation '*' if following postulates are satisfied:

(i) Associativity

(ii) Existence of Identity

(iii) Existence of Inverse.

1.2.6. Abelian Group. A group G is called an Abelian group or commutative group if in addition to above postulates G also satisfies the commutative law.

1.2.7. Important Results.

(i) The identity element in a group is unique.

(ii) Every element in a group have a unique inverse.

(iii) If a,b,c be elements of G such that ab = ac, then b = c (Left cancellation law)

and ba = ac, then b = c (right cancellation law)

(iv) If $a \in G$, then $\left(a^{-1}\right)^{-1} = a$.

(v) If $a,b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

(vi) If G is an Abelian group, then for all $a,b \in G$ and any integer n, we have $(ab)^n = a^n b^n$.

(vii) If every element of the group is its own inverse, then the group is Abelian.

(viii) If a group has a finite number of elements, this number is called the order of the group and the group is called finite group. A group with an infinite number of elements is called an infinite group.

(ix) If G is a group such that $(ab)^n = a^n b^n$ for three consecutive integers m and for all $a,b \in G$, then G is Abelian.

1.2.8. Subgroup. A non-empty subset H of a group G is said to be a subgroup of G if H itself is a group w.r.t. the same binary operation as in G.

1.2.9. Proper and Improper subgroups. The subgroups {e} and G itself are called improper subgroups of G. All other subgroups, other than {e} and G, are called proper subgroups of G.

1.2.10. Coset of a Subgroup. LetG be a group and H is any subgroup of G. Let 'a' be any element of G. Then, the set $Ha = \{ha : h \in H\}$ is called a right coset of H in G generated by 'a'. A left coset aH can be defined in a similar way. Also, a subset is called a coset of H in G generated by 'a' if Ha = aH.

1.2.11. Normal Subgroup. A subgroup N of a group G is said to be a normal subgroup of G iff Na = aN for all $a \in G$, that is, right and left cosets are same for every element of G. We denote a normal subgroup N of a group G by $N \trianglelefteq G$.

1.2.12. Remark. (i) A subset H of a group G is a subgroup iff $ab^{-1} \in H$ for all $a,b \in H$.

(ii) A finite subset H of a group G is a subgroup iff $ab \in H$ for all $a,b \in H$.

(iii) Let H and K be two subgroups of a group G. Then, the set

$HK = \{x : x = hk \text{ where } h \in H, k \in K\}$

is a subgroup of G iff HK = KH.

(iv) If H is a subgroup of G then Hg = H = gH iff $g \in H$.

(v) Any two right(left) cosets of a subgroup are either disjoint or identical.

(vi) If H is a finite subgroup of G. Then, $o(H) = o(Ha)$ for all $a \in G$.

(vii) A group $G \neq \{e\}$ which does not have any non-trivial normal subgroup is called a **simple group**.

(viii) A subgroup H of a group G is normal iff $g^{-1}hg \in H$ for every $h \in H, g \in G$.

(ix) Every subgroup of an Abelian group is a normal subgroup.

(x) Let H be a subgroup of G. The number of distinct right cosets of H in G is called the index of H in G and written as [G : H].

(xi) If [G : H] = 2, then H is normal in G.

(xii) A subgroup H of a group G is a normal subgroup of G iff the product of two right cosets of H in G is again a right coset of H in G.

(xiii) Every subgroup of a cyclic group is cyclic.

(xiv) Order of a finite cyclic group is equal to the order of its generator.

(xv) If the order of a group is a prime number, then the group is cyclic and hence Abelian.

1.2.13. Cyclic group. A group G is said to be cyclic group generated by an element $a \in G$ if every $g \in G$ is such that $g = a^t$ for some integer t.

1.2.14. Order of an element. Let G be a group and $a \in G$ and the composition being denoted by multiplication. By the order of an element $a \in G$, we mean the least positive integer n, if exists, such that $a^n = e$, the identity in G.

1.2.15. Results. (i) Let G be a finite group and $a \in G$, then $o(a) / o(G)$.

(ii) Let G be a finite group and $a \in G$, then $a^{o(G)} = e$.

(iii) If $a \in G$ and $o(a) = n$, then $a^t = e$ iff n / t (n divides t).

(iv) If $o(a) = n$, then $o(a^k) = \dfrac{n}{g.c.d.(n,k)}$.

1.2.16. Homomorphisms. If $(G,.)$ and $(\overline{G},*)$ are two groups. A mapping $f : G \to \overline{G}$ is called a homomorphism, if $f(x.y) = f(x) * f(y)$ for all $x, y \in G$.

1.2.17. Results. If f is a homomorphism from the group G to the group $\overline{G}$, then

(i) $f(e)=\bar{e}$, where e and $\bar{e}$ are identities of G and $\overline{G}$ respectively.

(ii) $f\left(g^{-1}\right)=\left(f(g)\right)^{-1}$ for all $g \in G$.

(iii) it is called epimorphism, if it is onto.

(iv) it is called monomorphism, if it is one – one.

(v) it is called isomorphism, if it is one – one and onto. We write as $G \cong \overline{G}$

(vi) it is called endomorphism, if $G=\overline{G}$.

1.2.18. Kernel of a Homomorphism. Let $f: G \to \overline{G}$ be a homomorphism. Then, the kernel of f is the set $Kerf=\left\{g \in G: f(g)=\bar{e}, \text{ the identity element of } \overline{G}\right\}$.

It should be noted that:

(i) $Kerf \trianglelefteq G$.

(ii) f is monomorphism iff $Kerf=\{e\}$.

(iii) A homomorphism from a simple group is eithe trivial or one-to-one.

1.2.19. Quotient Group. Let G be a group and H be a normal subgroup of G, then the set G/H (G mod H) of all cosets of H in G is a subgroup w.r.t. multiplication of cosets. Itis called quotient group or factor group of G by H. If $a, b \in G$, then HaHb = Hab. The identity element of G/H is H.

1.2.20. Canonical Homomorphism. The mapping $f: G \to G/H$ defined by $f(g)=Hg$ for all $g \in G$ is an onto homomorphism, where H be a normal subgroup of G. It is called natural or canonical homomorphism and $Kerf = H$.

1.2.21. Fundamental Theorem of Homomorphism. If $\overline{G}$ is homomorphic image of G under f (that is, f is onto), then $G/\ker f \cong \overline{G}$.

1.2.22. First Theorem of Isomorphism. Let f be a homomorphism of a group G onto a group $\overline{G}$. Let $\overline{K}$ is any normal subgroup of $\overline{G}$ and $K=\left\{x \in G: f(x) \in \overline{K}\right\}=f^{-1}\left(\overline{K}\right)$. Then, K is normal subgroup of G containing $\ker f$ and $G/K \cong \overline{G}/\overline{K}$.

1.2.23. Second Theorem of Isomorphism. Let H and K are subgroups of any group G, where $H \trianglelefteq G$. Then, $K/H \cap K \cong HK/H$.

1.2.24. Third Theorem of Isomorphism. Let G be any group and H, K be two normal subgroups of G such that $H \subseteq K$. Then, $G/K \cong \frac{G/H}{K/H}$.

1.2.25. Permutations. SupposeS is a finite set having n distinct elements. Then, a one-one mapping of S onto itself is called a permutation of degree n.

Let $S = \{a_1, a_2, ..., a_n\}$ be a finite set having n distinct elements. If $f : S \to S$ is a one-one onto mapping, then f is a permutation of degree n. Let $f(a_1) = b_1, f(a_2) = b_2, ..., f(a_n) = b_n$, where $\{a_1, a_2, ..., a_n\} = \{b_1, b_2, ..., b_n\}$. Then, f is written as $f = \begin{pmatrix} a_1 & a_2 \ldots a_n \\ b_1 & b_2 \ldots b_n \end{pmatrix}$.

If S is a finite set of n distinct elements, then we have $\lfloor \underline{n}$ distinct arrangements of these n elements. So there will be $\lfloor \underline{n}$ distinct permutations of degree n. the set of all permutations of degree n is called **symmetric set of permutations** and is denoted by P_n or S_n.

1.2.26. Product of Permutations. Product of two permutations f and g of degree n is given by first carrying out the operation defined by g and then by f. It is denoted by fog. If $f = \begin{pmatrix} a_1 & a_2 \ldots a_n \\ b_1 & b_2 \ldots b_n \end{pmatrix}$ and $g = \begin{pmatrix} b_1 & b_2 \ldots \mathrm{b}_n \\ c_1 & c_2 \ldots \mathrm{c}_n \end{pmatrix}$. Then, $gof = \begin{pmatrix} a_1 & a_2 \ldots a_n \\ c_1 & c_2 \ldots \mathrm{c}_n \end{pmatrix}$.

1.2.27. Results. (i) The set $S_n$of all permutations of n symbols is a finite group of order $\lfloor \underline{n}$ w.r.t. product of permutations.

(ii) This group is Abelian for $n \le 2$ and non-abelian for $n \ge 3$.

1.2.28. Cyclic Permutation. Let $f = \begin{pmatrix} a_1 & a_2 \ldots a_k & a_{k+1} \ldots a_n \\ a_2 & a_3 \ldots a_1 & a_{k+1} \ldots a_n \end{pmatrix}$. It is cyclic of length k and can be written as $f = (a_1\ a_2\ \ldots a_k)$.

1.2.29. Transposition. A cyclic permutation of length 2 is called a transposition.

1.2.30. Inverse of a Cycle. Let $f = (a_1\ a_2\ \ldots a_k)$ be a cycle of length k and degree n. Then, $f^{-1} = (a_1\ a_2\ \ldots a_k)^{-1} = (a_1\ a_k\ \ldots a_2)$.

1.2.31. Disjoint Cycles. Two cycles are said to be disjoint if they have no object in common in their one-rowed representation.

1.2.32. Results. (i) Any two disjoint cycles commute with each other.

(ii) A permutation is said to be an "even permutation" if it can be expressed as a product of an even number of transpositions and is called "odd permutation" if it can be expressed as a product of odd number of transpositions.

For example, (1 2 3 4 5) = (1 2)(1 3)(1 4)(1 5) which is product of even number of permutations and so is even permutations.

(iii) Product of two even(odd) permutations is again an even permutation.

(iv) The set of all permutations in S_n is a normal subgroup of S_n, is denoted by A_n and is called alternating group of order n and has $\frac{\lfloor n}{2}$ elements.

(v) The group A_n is simple for n = 1,2,3. But A_4 is not simple. However, A_n is simple for $n \geq 5$.

1.2.33. Centre of a group. Let G be a group then the centre of G is given by

$$Z(G) = C(G) = \{x \in G : xy = yx \text{ for all } y \in G\}.$$

1.2.34. Normalizer of a subgroup. Let G be any group and H be its subgroup. Then, normalizer of H in G is given by

$$N(H) = \{x \in G : xH = Hx\}.$$

N(H) is the largest subgroup of G in which H is normal. In particular, $H \Delta G$ iff $N(H) = G$.

1.2.35. Result. (i) If $o(G) = p^n$ for some prime p, then centre of G is non-trivial.

(ii) If $o(G) = p^2$, where $p$is a prime, then G is abelian.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
3. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
4. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
5. Artin, M., Algebra, Prentice-Hall of India, 1991.

2

THE SYLOW THEOREMS

Structure

2.1.Introduction.

2.2.Conjugate of an element.

2.3.Commutator.

2.4.The Sylow Theorems.

2.5.Structure of Finite Abelian Groups.

2.6.Survey of Groups.

2.7.Check Your Progress.

2.8.Summary.

2.1. Introduction. This chapter contains many important results related to the p-groups, Sylow p-subgroups, equivalent classes of the Sylow subgroups, number of sylow p-subgroups.

2.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Conjugate of an element.

(ii) Sylow First Theorem.

(iii) Sylow Second Theorem.

(iv) Sylow Third Theorem.

(v) Survey of groups.

2.2. Conjugate of an element. Let G be any group and $a, b \in G$, then a is called conjugate of b if there exists an element $x \in G$ such that $a = x^{-1} bx$.

2.2.1. Exercise. The relation of conjugacy is an equivalence relation.

2.2.2. Equivalence Class. Let $a \in G$, then equivalence class or conjugate class of 'a' is given by: $Cl(a) = \{x \in G : a \sim x\}$ = Set of all conjugates of 'a' = $\{g^{-1}ag : g \in G\}$

Remark. Since the conjugacy relation '$\sim$' is an equivalence relation on G, so G is union of all conjugate classes and any two conjugate class are either disjoint or identical. Keeping this in mind, we can say that $o(G) = \sum_a o\big(Cl(a)\big)$, where the sum runs over element a which is taken one each from each conjugate class. Clearly, $Cl\,(e) = \{e\}$ and $Cl\,(a) = Cl\,(b)$ iff $a \sim b$.

Result. If G is a finite group and $a \in G$, then $o\big(Cl(a)\big) = \dfrac{o(G)}{o\big(N(a)\big)}$

2.2.3. Class Equation. Let G be a finite group and $Z(G)$ denote the centre of G. Then, the equation

$$o(G) = o\big(Z(G)\big) + \sum_a \frac{o(G)}{o\big(N(a)\big)}$$

where 'a' ranges over each conjugate class containing more than one element, is called class-equation.

Another forms of class equation.

(i) $o(G) = \sum_a \dfrac{o(G)}{o\big(N(a)\big)}$, where the sum runs over 'a' taken one from each conjugate class.

(ii) $o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \dfrac{o(G)}{o\big(N(a)\big)}$, where the sum runs over 'a' taken one from each conjugate class.

(iii) $o(G) = o(Z(G)) + \sum_{N(a) \neq G} \dfrac{o(G)}{o\big(N(a)\big)}$, where the sum runs over 'a' taken one from each conjugate class.

(iv) $o(G) = o(Z(G)) + \sum_{a \notin Z(G)} [G : N(a)]$, where the sum runs over 'a' taken one from each conjugate class.

Results.

1. If $o(G) = p^n$ for some prime p then $Z(G) \neq \{e\}$ that is, $Z(G)$ is non-trivial, that is, $o\big(Z(G)\big) > 1$.
2. If $o(G) = p^2$ for some prime p, then G is abelian.
3. A group of order p^3 may not be abelian e.g. Q_8 whose order is 2^3.
4. If G is a non-abelian group of order p^3 for some prime p, then $o\big(Z(G)\big) = p$.
5. If Z is the centre of a group G such that G/Z is cyclic, then show that G is abelian.

2.3. Commutator. Let G be any multiplicative group. The commutator of two elements x and y of G is the element $x^{-1}y^{-1}xy \in G$. We denote it by $[x, y]$.

2.3.1. Proposition. G is abelian iff $[x, y] = e \;\forall\; x, y \in G$.

Proof. If G is abelian then

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e.e = e.$$

Conversely, let $[x, y] = e \ \forall \ x, y \in G$.

$$\Rightarrow \quad x^{-1}y^{-1}xy = e$$

$$\Rightarrow \quad (yx)^{-1}.(xy) = e$$

$$\Rightarrow \quad xy = yx \ \forall \ x, y \in G. \qquad \Rightarrow \quad G \text{ is abelian.}$$

2.3.2. Proposition. $a \in Z(G)$ iff $[a, x] = e \ \forall \ x \in G$.

Proof. Let $a \in Z(G)$ = centre of G

Then $[a, x] = a^{-1}x^{-1}ax = a^{-1}x^{-1}xa = a^{-1}a = e$ [Since $a \in Z(G)$]

Conversely. $[a, x] = e \ \forall \ x \in G$

$$\Rightarrow \quad a^{-1}x^{-1}ax = e \quad \Rightarrow \quad ax = xa \ \forall \ \in G \qquad \Rightarrow \quad a \in Z(G).$$

2.3.3. Commutator Element. The element y of G is said to be a commutator element of G if $\exists \ a, b \in G$ such that $[a, b] = y$ that is, $a^{-1}b^{-1}ab = y$. e.g. Identity element is always a commutator element.

Let us find the commutator elements of S_3. We know that

$$S_3 = \{I \ , \ (12) \ , \ (13) \ , \ (23) \ , \ (123) \ , \ (132)\}$$

Now, $[I, (12)] = I$, Similarly $[I, x] = I \ \forall \ x \in S_3$.

Now, $[(12), I] = I$, $[(12), (12)] = I$

$[(12),(13)] = (123)$, $[(12), (23)] = (132)$

$[(12), (123) = (132)$, $[(12), (132)] = (123)$

So, (123) and (132) are also commutator elements of S_3. We can show that I, (123), and (132) are the only commutator elements of S_3.

2.3.4. Derived Subgroup. The subgroup of G generated by all the commutators of G is called the derived subgroup of G. We denote it by $\delta(G)$ and G'

that is, $\delta(G) = G' = < [x, y] : x, y \in G >$

For example, let $G = S_3$, then

$$\delta(S_3) = < [x, y] : x, y \in S_3 > = < I, (123), (132) > = \{I, (123), (132)\}.$$

$\delta(G)$ is also known as first derived subgroup.

2.3.5. Exercises.

i) Derived subgroup of a group G is a normal subgroup of G, that is, $\delta(G) \trianglelefteq G$.

ii) A group G is abelian if and only if $G' = < e >$.

2.3.6. n^{th} Derived Subgroup. Let G be a group, for every non-negative integer n, define $G^{(n)}$ inductively as follows:

$$G^0 = G,\ G^{(n+1)} = \left(G^{(n)}\right)',$$

the commutator subgroup of $G^{(n)}$. The $G^{(n)}$ is called n^{th} commutator subgroup or n^{th} derived subgroup of G.

$$G^{(n+1)} = \left(G^{(n)}\right)' = [\,G^{(n)},\ G^{(n)}\,] = <[x, y] : x, y \in G^{(n)}>.$$

2.4. Sylow Theorems

2.4.1. Sylow's First Theorem. Let p be a prime number such that $p^m / o(G)$, where m is a positive integer. Then G has a subgroup of order p^m.

Proof. We shall prove the Theorem by induction on $o(G)$.

If $o(G) = 1$, then Theorem is trivially true.

As our induction hypothesis, we assume that Theorem is true for all groups of order less than order of G. In other words, we have assumed that if G' is a group such that $o(G') < o(G)$ and

$p^k / o(G')$, for some integer k, then G' has a subgroup of order p^k.

We shall prove the result for G. For this we consider two cases separately.

Case I. If p^m divides the order of a proper subgroup, say H, of G that is, $p^m / o(H)$ and

$o(H) < o(G)$. Then by induction hypothesis on H, we obtain that H (and hence G) has a subgroup of order p^m.

Case II. Let p^m does not divide the order of any proper subgroup of G that is, $p^m \nmid o(H)$, for all proper subgroup H of G.

We know that the class-equation for G is $o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$ (1)

If $N(a) \neq G$, then $N(a)$ is a proper subgroup of G, and so by hypothesis of this case,

$$p^m \nmid o(N(a))$$

Now, $o(G) = \frac{o(G)}{o(N(a))}.o(N(a))$

Given that $p^m / o(G)$, and if $p^m \nmid o(N(a))$ then by above expression, we obtain

$$p \Big/ \frac{o(G)}{o(N(a))}, \text{ whenever } N(a) \neq G.$$

$$\Rightarrow \qquad p \Big/ \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))}$$

Also, $p/o(G)$, so $p \Big/ \left[o(G) - \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))} \right] \quad \Rightarrow \quad p/o(Z(G)) \quad$ [By (1)]

As $Z(G)$ is abelian, so by Cauchy Theorem for finite abelian group, there exists an element $a(\neq e) \in Z(G)$ such that $a^p = e$. Let K be the cyclic subgroup of G generated by a that is,

$K = < a > = \{a, a^2, a^3, ..., a^p\}$ and $o(K) = p$. Now $a \in Z(G)$ implies that $K \subseteq ZG)$ and we know that a subgroup of $Z(G)$ is always a normal subgroup of G and so $K \underline{\Delta} G$ and so G/K is well-defined.

Now, $$o(G/K) = \frac{o(G)}{o(K)} = \frac{o(G)}{p} < o(G)$$

So, we can apply the induction hypothesis on G/K.

Now, $p^m/o(G) \Rightarrow \quad p^{m-1} \Big/ \frac{o(G)}{p}$

$$\Rightarrow \quad p^{m-1}/o(G/K)$$

By induction hypothesis on G/K for the divisor p^{m-1}, G/K must have a subgroup, say, T of order p^{m-1}, that is, $o(T) = p^{m-1}$.

Now, we know that every subgroup of G/K is of the form L/K where L is a subgroup of G containing K. So, we must have

$T = L/K$, where L is a subgroup of G containing K.

$$\Rightarrow \quad o(T) = o(L/K) = \frac{o(L)}{o(K)}$$

$$\Rightarrow \quad o(L) = o(T).o(K) = p^{m-1}.p = p^m$$

Thus G has a subgroup L of order p^m.

Remark. Sylow′s first Theorem can also be stated in following ways:

(i) If any power of prime divides the order of a group G, then G has a subgroup of order equal to that power of prime.

(ii) If $o(G) = p^k q$, where p is a prime number and q is a positive integer such that gcd(p,q)=1, then G has subgroups of orders $p, p^2, ..., p^k$.

Example of Sylow's first Theorem.

2.4.2. Example. Let G be a group such that $o(G) = 9000$. By Sylow first Theorem, find the order of subgroups which G certainly contains.

Solution. First we do the prime factorization of 9000 and obtain

$$o(G) = 2^3 \cdot 3^2 \cdot 5^2$$

Here, 2, 3 and 5 are prime numbers so by Sylow's first Theorem, G contains the subgroups of order 2^1, 2^2, 2^3, 3^1, 3^2, 5^1, 5^2 that is, 2, 4, 8, 3, 9, 5, 25.

However, by Sylow's first Theorem, nothing can be said about the existence of subgroups of order 6, 15, 10 etc. as they are not powers of a prime.

2.4.3. Sylow *p*-subgroup. Let p be a prime number such that p^k divides $o(G)$ and p^{k+1} does not divide $o(G)$. Then a subgroup of order p^k is called a Sylow p-subgroup of G.

-OR-

If $o(G) = p^k q$ where p is a prime number and gcd(p, q) = 1, then a subgroup of order p^k is called a Sylow p-subgroup of G.

-OR-

Sylow p -subgroup of a group G is a subgroup whose order is p^k where k is the largest power of p such that p^k divides $o(G)$.

-OR-

A subgroup of G is called a Sylow p-subgroup if its order is equal to the maximum power of p occurring in the order of the group.

2.4.4. Example. Find the order of different Sylow p–subgroups for G where

(i) $o(G) = 45$ **(ii)** $o(G) = 1125$.

Solution. (i) $o(G) = 45 = 3^2 5^1$.

Then, G has Sylow 3–subgroups and Sylow 5–subgroups. A sylow 3–subgroup is that whose order is 3^2, that is, 9 and a sylow 5-subgroup is that whose order is $5^1 = 5$.

(ii) $o(G) = 1125 = 3^2 5^3$.

In this case, a sylow 3-subgroup is that whose order is 9 and a sylow 5-subgroup is that whose order is 125.

Note. By above example, it is clear that in different groups Sylow p-subgroup may have different orders for some fixed prime p.

2.4.5. Example. If H is a Sylow p-subgroup of G, then prove that $x^{-1}Hx$ is also a sylow p-subgroup of G for any $x \in G$.

Solution. Let $p^n / o(G)$ and $p^{n+1} \nmid o(G)$.

As H is a Sylow p-subgroup of G, we have $o(H) = p^n$.

Let $H = \{h_1, h_2, h_3, ..., h_{p^n}\}$, then for any $x \in G$, we have

$$x^{-1}Hx = \{x^{-1}h_1x\ ,\ x^{-1}h_2x\ ,...,\ x^{-1}h_{p^n}x\} \qquad (1)$$

First we prove that $x^{-1}Hx$ is a subgroup of G. For this let $x^{-1}h_1x$ and $x^{-1}h_2x$ be any two arbitrary element.

Then $(x^{-1}h_1x)(x^{-1}h_2x)^{-1} = x^{-1}h_1x\,x^{-1}h_2^{-1}(x^{-1})^{-1}$

$$= x^{-1}h_1h_2^{-1}x \in x^{-1}Hx \ \left[\text{Since } h_1h_2^{-1} \in H \text{ as } H \text{ is a subgroup}\right]$$

Thus, $x^{-1}Hx$ is a subgroup.

Secondly, we prove that $o(x^{-1}Hx) = o(H)$.

For this it is sufficient to prove that all elements in (1) are distinct.

Let if, possible $x^{-1}h_1x = x^{-1}h_2x$, where $h_1 \neq h_2$

$$\Rightarrow \qquad xx^{-1}h_1xx^{-1} = xx^{-1}h_2xx^{-1}$$

$$\Rightarrow \qquad h_1 = h_2, \text{ which is a contradiction.}$$

Hence, $o(x^{-1}Hx) = o(H)$, that is, $o(x^{-1}Hx) = p^n$.

Thus, $x^{-1}Hx$ is a Sylow p-subgroup of G.

2.4.6. *p* group. Let p be a prime number. A group G is said to be a p – group if order of every element of G is some power of p. For example,

$$Q_8 = \{1, -1, i, -i\ ,\ j\ ,\ -j\ ,\ k\ ,\ -k\}$$

The group of quaternions is a 2–group because

$$o(1) = 2^0\ ,\ o(-1) = 2^1\ ,\ o(i, -i\ ,\ j, -j\ ,\ k, -k) = 2^2\ ,$$

that is, order of every element of Q_8 is a some power of 2.

2.4.7. Theorem. A finite group G is a p-group iff $o(G) = p^n$ for some integer n.

Proof. Suppose G is a p-group. We shall prove that $o(G) = p^n$ for some integer $n \geq 1$.

For this, it is sufficient to prove that p is the only prime dividing $o(G)$.

Let, if possible, $q(\neq p)$ be any other prime such that $q / o(G)$. By Cauchy Theorem, there exists an element $a(\neq e) \in G$ such that $o(a) = q$

Since $a \in G$ and G is a p-group, so $o(a) = p^r$ for some $r \geq 1$. Thus $p^r = q$

$\Rightarrow$ p/q, which is a contradiction since a prime can never divide other prime.

Hence p is the only prime dividing $o(G)$, so $o(G) = p^n$ for some n.

Conversely, Suppose $o(G) = p^n$. Let $a \in G$ be any element, then $o(a)/o(G)$

$\Rightarrow$ $o(a)/p^n \Rightarrow o(a) = p^r$ for some r.

Thus order of every element of G is some power of p. Hence G is a p-group.

Remark. Now we introduce the concept of Double Cosets which will be very useful in proving the Sylow's second and third Theorem.

2.4.8. Double Coset. Let H and K be two subgroups of a group G and $x \in G$ be any element. Then the set

$H \text{ x } K = \{hxk \ : \ h \in H \ , \ k \in K\}$ is called a double coset.

2.4.9. Double Coset Decomposition. If H and K are two subgroups of a group G then prove that

(i) any two double cosets are either disjoint or identical

(ii) G is the union of all distinct double cosets that is, $G = \bigcup_{x \in G} H\ x\ K$ where union runs over x taken one from each double coset.

Proof. We define a relation ~ for any two elements x and y of G as $x \sim y$ iff $x = hyk$ for some $h \in H$ and $k \in K$.

First we prove that this relation is an equivalence relation.

(i) Reflexivity: Clearly $x \sim x$ as $x = e\ x\ e$, where $e \in H$, $e \in K$.

(ii) Symmetry: Let $x \sim y \Rightarrow x = h\ y\ k$ for some $h \in H$, $k \in K$

$\Rightarrow h^{-1}\ x\ k^{-1} = h^{-1}\ h\ y\ k\ k^{-1}$

$\Rightarrow y = h^{-1}\ x\ k^{-1}$ where $h^{-1} \in H \ , \ k^{-1} \in K$

$\Rightarrow y \sim x$.

(iii) Transitivity: Let $x \sim y$ and $y \sim z$

$\Rightarrow$ $x = hyk$ and $y = h'zk'$ for some $h, h' \in H$ and $k, k' \in K$

$\Rightarrow$ $x = hh'zk'k$

Clearly $hh' \in H$ and $k'k \in K$, as H and K are subgroups and so $x \sim z$.

Hence ~ is an equivalence relation of G, so this relation partitions the group G into equivalence classes and so we can write

$$G = \bigcup_{x \in G} cl(x) \qquad (1)$$

where union runs over x taken one from each conjugate class.

Then,

$$\begin{aligned} cl(x) &= \{y \in G \ : \ y \sim x\} \\ &= \{y \in G \ : \ y = hxk \ \text{ for some } \ h \in H \ , k \in K\} \\ &= \{hxk \ : \ h \in H \ , \ k \in K\} = H\,x\,K \\ \Rightarrow \qquad cl(x) &= H\,x\,K \qquad (2) \end{aligned}$$

Thus equivalence class of any element comes out to be a double coset. Also we know that any two equivalence classes are either disjoint or identical. Thus we obtain that any two double cosets are either disjoint or identical, which proves (i).

Using (2) in (1), we obtain

$$G = \bigcup_{x \in G} H\ x\ K$$

where union runs over x taken one from each double coset which proves (ii).

This is called double coset decomposition of G by H and K.

2.4.10. Lemma. Let H and K be finite subgroups of a group G and $x \in G$ then

$$o(H\ x\ K) = \frac{o(H)\ o(K)}{o(H \cap x\ K\ x^{-1})}.$$

Proof. We define a mapping $\phi \ : \ H\ x\ K \to H\ x\ K\ x^{-1}$ by setting

$$\phi(hxk) = hxkx^{-1} \text{ for } h \in H \text{ and } k \in K.$$

We prove that ϕ is well-defined, one-one and onto.

(i) ϕ is well-defined: Let $h_1xk_1 = h_2xk_2$

$$\Rightarrow \qquad h_1xk_1x^{-1} = h_2xk_2x^{-1}$$

$$\Rightarrow \qquad \phi(h_1xk_1) = \phi(h_2xk_2)$$

So, ϕ is well-defined.

(ii) ϕ is one-one. Let $\phi(h_1xk_1) = \phi(h_2xk_2)$

$$\Rightarrow \qquad h_1xk_1x^{-1} = h_2xk_2x^{-1}$$

$$\Rightarrow \qquad h_1xk_1 = h_2xk_2$$

So, ϕ is one-one.

(iii) ϕ is onto. Let $hxkx^{-1} \in HxKx^{-1}$ be any element then clearly $hxk \in HxK$ and

$$\phi(hxk) = hxkx^{-1} \qquad \Rightarrow \qquad hxk \text{ is pre-image of } hxkx^{-1} \text{ under } \phi.$$

So, ϕ is onto.

Hence, there exists a one-to-one correspondence between $H\ x\ K$ and $HxK\ x^{-1}$ and so their orders must be same that is,

$$o(HxK) = o(HxKx^{-1}) \qquad (1)$$

Now we know that if K is a subgroup of G then xKx^{-1} is also a subgroup of G of the same order, that is,

$$o(K) = o(xKx^{-1}).$$

Also, we know a result that if A and B are two finite subgroups of G, then

$$o(AB) = \frac{o(A)\ o(B)}{o(A \cap B)}$$

Putting $A = H$ and $B = xKx^{-1}$ in above, we obtain

$$o(HxKx^{-1}) = \frac{o(H)\ o(xKx^{-1})}{o(H \cap xKx^{-1})}$$

$$\Rightarrow \qquad o(HxKx^{-1}) = \frac{o(H)\ o(K)}{o(H \cap xKx^{-1})} \quad [\text{Since } o(K) = o(xKx^{-1})] \ (2)$$

By (1) and (2), we obtain

$$o(HxK) = \frac{o(H)\ o(K)}{o(H \cap xKx^{-1})}$$

2.4.11. Sylow's Second Theorem. Any two Sylow p-subgroups of a finite group G are conjugates in G.

Proof. Let H and K be two Sylow p-subgroups of G. Let n be the highest power of p such that $p^n \,|\, o(G)$ that is,

$$p^{n+1} \nmid o(G) \qquad (1)$$

Then, $o(H) = o(K) = p^n$

We have to show that H and K are conjugate in G that is, $H = xKx^{-1}$ for some $x \in G$

Let, if possible this is false that is, $H \neq xKx^{-1}$ for all $x \in G$.

$\Rightarrow$ $H \cap xKx^{-1}$ is a subgroup of H which is properly contained in H

that is, $H \cap xKx^{-1} \subsetneq H \qquad (2)$

Now, by Lagrange's Theorem,

$$o(H \cap xKx^{-1}) \big/ o(H) = p^n$$

$$\Rightarrow \quad o(H \cap xKx^{-1}) = p^m \text{ for some } m \le n .$$

But in view of (2) clearly $m \neq n$, so $o(H \cap xKx^{-1}) = p^m$, where $m < n$.

By above Lemma, we have

$$o(HxK) = \frac{o(H)\ o(K)}{o(H \cap xKx^{-1})} = \frac{p^n . p^n}{p^m} = p^{2n-m}$$

$$= p^{n+1+n-m-1} = p^{n+1} . p^{n-m-1}$$

$$\Rightarrow \quad p^{n+1} \text{ divides } o(HxK)$$

$$\Rightarrow \quad p^{n+1} \text{ divides } \sum_{x \in G} o(HxK) \qquad (3)$$

Now, by double coset decomposition, we know that

$$G = \bigcup_{x \in G} H\ x\ K \text{ , where } H\ x\ K \text{ are mutually disjoint.}$$

$$\Rightarrow \quad o(G) = \sum_{x \in G} o(HxK) \qquad (4)$$

By (3) and (4), we have p^{n+1} divides $o(G)$, which is a contradiction to (1).

Hence $H = xKx^{-1}$ for some $x \in G$ that is, H and K are conjugates in G.

2.4.12. Lemma. Let P be a Sylow p -subgroup of a group G, then the number n_p of Sylow p-subgroups of G is equal to $\frac{o(G)}{o(N(P))}$.

Proof. We know that $o(cl(P)) = \frac{o(G)}{o(N(P))}$ (1)

Now, $cl(P)$ contains all subgroups which are conjugate to P.

But by Sylow second Theorem, all sylow p-subgroups are conjugate to each other and hence $cl(P)$ contains all Sylow p-subgroups of G.

Hence, number of Sylow p-subgroups = $n_p = o(cl(P))$ (2)

By (1) and (2), $n_p = \frac{o(G)}{o(N(P))}$.

2.4.13. Sylow's Third Theorem. The number n_p of Sylow p-subgroups of a finite group G is given by $n_p = 1 + kp$ such that $1 + kp \big/ o(G)$, and k is a non-negative integer.

Proof. Let P be a Sylow p-subgroup of G.

Let n be the highest power of p such that $p^n \mid o(G)$ that is, $p^{n+1} \nmid o(G)$.

By double coset decomposition of G, we know that

$$G = \bigcup_{x \in G} H\ x\ K \text{ , where union runs over } x \text{ taken one from each double coset.}$$

$$\Rightarrow \quad o(G) = \sum_{x \in G} o(HxK) \text{ where sum runs over } x \text{ taken one from each double coset.}$$

Taking $H = K = P$ in above, we get

$$o(G) = \sum_{x \in G} o(PxP)$$

$$\Rightarrow \quad o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP) \qquad (1)$$

We take up two sums in (1) one by one.

If $x \in N(P)$ then $xPx^{-1} = P \quad \Rightarrow \quad xP = Px$

$$\Rightarrow PxP = PPx$$

$$\Rightarrow PxP = Px \qquad [\text{Since } P \text{ is a subgroup , so } PP = P\ ]$$

$$\Rightarrow \bigcup_{x \in N(P)} P\ x\ P = \bigcup_{x \in N(P)} P\ x \qquad (2)$$

Now P is a subgroup of $N(P)$ and so Px is a right coset of P in $N(P)$. Further we know that union of all distinct right cosets of a subgroup is equal to the group, so we get

$$\bigcup_{x \in N(P)} P\ x = N(P)$$

Using this in (2), we get

$$\bigcup_{x \in N(P)} P\ x\ P = N(P)$$

$$\Rightarrow \qquad \sum_{x \in N(P)} o(PxP) = o(N(P)) \qquad (3)$$

Again, if $x \notin N(P)$ then $xPx^{-1} \neq P$

$\Rightarrow \quad P \cap xPx^{-1}$ is a subgroup of P properly contained in P,

that is, $o(P \cap xPx^{-1}) < o(P) = p^n$

Also by Lagrange's Theorem

$$o(P \cap xPx^{-1}) \mid o(P) = p^n$$

$\Rightarrow \qquad o(P \cap xPx^{-1}) = p^m$ with $m < n$.

Now we know that,

$$o(PxP) = \frac{o(P)\ o(P)}{o(P \cap xPx^{-1})} = \frac{p^n . p^n}{p^m} = p^{2n-m}$$

$$= p^{n+1+n-m-1} = p^{n+1} . p^{n-m-1}$$

$\Rightarrow \qquad p^{n+1}$ divides $o(P\,x\,P)$ whenever $x \notin N(P)$

that is, $p^{n+1} \Big/ \sum_{x \notin N(P)} o(PxP)$

$$\Rightarrow \qquad \sum_{x \notin N(P)} o(PxP) = p^{n+1}\ t \text{ for some integer } t \qquad (4)$$

Using (3) and (4) in (1), we obtain

$$o(G) = o(N(P)) + p^{n+1}\ t$$

$$\Rightarrow \qquad \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))} \qquad (5)$$

As $N(P)$ is a subgroup of G, by Lagrange's Theorem, $o(N(P))$ divides $o(G)$ and so $\frac{o(G)}{o(N(P))}$ is an integer.

So, by (5), we obtain that $\frac{p^{n+1}t}{o(N(P))}$ is an integer.

Now, P is a subgroup of $N(P)$, so by Lagrange's Theorem

$$o(P) \big/ o(N(P)) \qquad \Rightarrow \qquad p^n \big/ o(N(P))$$

$$\Rightarrow \qquad o(N(P)) = p^n\, r \text{ for some integer } r.$$

Thus, we obtain that $\frac{p^{n+1}t}{o(N(P))} = \frac{p^{n+1}t}{p^n r} = p\frac{t}{r}$ is an integer.

$$\Rightarrow \qquad \frac{t}{r} \text{ is an integer, say } k \qquad \Rightarrow \qquad \frac{p^{n+1}t}{o(N(P))} = kp$$

Using this in (5), we have

$$\frac{o(G)}{o(N(P))} = 1 + kp$$

By above Lemma, the number n_p of Sylow p-subgroups is given by $n_p = \frac{o(G)}{o(N(P))}$.

Hence, $n_p = \dfrac{o(G)}{o(N(P))} = 1 + kp$

Finally, $o(G) = o(N(P)).(1 + kp)$ implies that $1 + kp / o(G)$

Thus number of Sylow p-subgroups is $1 + kp$ such that $1 + kp / o(G)$.

2.4.14. Corollary. Show that a Sylow p-subgroup of a finite group G is unique iff it is normal.

Proof. *Condition is necessary*:

Suppose H be a unique Sylow p-subgroup of G. Let $p^n / o(G)$ and $p^{n+1} \nmid o(G)$, then

Clearly, $o(H) = p^n$

Let $x \in G$ be any arbitrary element, then we know that $x^{-1}Hx$ is also a Sylow p-subgroup.

Since H is the only Sylow p-subgroup of G, therefore

$$x^{-1}Hx = H \quad \text{for all } x \in G$$

$$\Rightarrow \quad Hx = xH \quad \text{for all } x \in G$$

$$\Rightarrow \quad H \text{ is a normal subgroup of } G.$$

Condition is sufficient :

Let H be a Sylow p-subgroup of G such that $H \trianglelefteq G$. We shall prove that H is unique. Suppose K be any other Sylow p -subgroup of G. Then, by Sylow second Theorem, H and K must be conjugate in G that is,

$K = x^{-1}Hx$ for some $x \in G$

$$\Rightarrow \quad K = x^{-1}xH \qquad [\text{Since } H \trianglelefteq G]$$

$$\Rightarrow \quad K = H$$

Hence H is unique Sylow p-subgroup of G.

2.4.15. Simple Group. A simple group is one having no proper normal subgroup.

Remark. To show that a finite group G of certain order is not simple, obtain a unique Sylow p -subgroup G for some prime p. Then, it becomes normal and obviously H is proper, which shows that G is not simple.

2.4.16. Example. Show that a group of order 28 is not simple.

-OR-

Let $o(G) = 28$, then show that group G has a normal subgroup of order 7.

Solution. We have $o(G) = 28 = 2^2 7^1$. By Sylow first Theorem, G has Sylow 2 – subgroups each of order 4 and Sylow 7 – subgroups each of order 7.

By Sylow third Theorem, the number n_7 of Sylow 7 – subgroups is given by $1 + 7k$ such that

$$1+7k/o(G) \Rightarrow 1+7k/28$$

$$\Rightarrow 1+7k/2^2.7$$

$$\Rightarrow 1+7k/4 \qquad \text{[Since } (1+7k, 7) = 1\text{]}$$

$$\Rightarrow k = 0$$

Thus, $n_7 = 1$ that is, there is unique Sylow 7 -subgroup say H and $o(H) = 7$

But we know that "a Sylow p -subgroup is unique iff it is normal".

Thus H is a normal subgroup of order 7. Obviously H is proper. Hence G is not simple.

2.4.17. Exercise.

1. Let G be a group of order $5^2.7.11$, then G has how many

(i) Sylow 5–subgroups

(ii) Sylow 7–subgroups

(iii) Sylow 11–subgroups.

Check whether G is simple or not.

2. Show that a group of order 40 is not simple.

-OR-

Show that a group of order 40 has a normal subgroup of order 5.

3. Show that a group of order 20499 is not simple.

-OR-

Show that a group of order 20499 has a normal subgroup of order 11.

4. Show that a group of order 56 is not simple.

2.4.18. Proposition. Let G be a finite group such that $o(G) = p^n$, where p is a prime. Prove that any subgroup of order p^{n-1} is a normal subgroup of G.

Proof. We shall prove the result by induction on n.

For $n = 1$, G is a group of order p and the only subgroup of order p^{n-1} that is, of order $p^{1-1} = p^0 = 1$ is $\{e\}$. The identity subgroup $\{e\}$ is obviously a normal subgroup of G. Thus the result is true for $n = 1$.

As our induction hypothesis, we assume that result is true for all groups of order p^m, where $m < n$.

Let H be a subgroup of G of order p^{n-1}. We shall prove that H is normal in G.

Now, $H \subseteq N(H) \subseteq G$ and so by Lagrange's Theorem,

$o(H)/o(N(H))$ and $o(N(H))/o(G)$

that is, $p^{n-1}/o(N(H))$ and $o(N(H))/p^n$

$\Rightarrow$ $o(N(H)) = p^{n-1}$ or p^n

If $o(N(H)) = p^n$, then $o(N(H)) = o(G) \Rightarrow N(H) = G$

$\Rightarrow$ H is normal in G, which is what we want to prove.

Now, we finish our proof by showing that $o(N(H)) = p^{n-1}$ is impossible.

Let, if possible, $o(N(H)) = p^{n-1}$, then as $o(H) = p^{n-1}$ and $H \subseteq N(H)$, we get

$$H = N(H) \qquad (1)$$

Now, $o(G) = p^n$, we know by class equation, that $o(Z(G)) > 1$ (2)

By Lagrange's Theorem, $o(Z(G))/o(G) = p^n$ $\Rightarrow$ $o(Z(G)) = p^s,\ 0 \le s \le n$

But if $s = 0$, then $o(Z(G)) = 1$, which is a contradiction by (1).

Hence, $o(Z(G)) = p^s, s > 0$ $\Rightarrow$ $p/o(Z(G))$

So, by Cauchy Theorem for finite groups, there exists an element $a(\neq e) \in Z(G)$ such that $o(a) = p$.

Let K be the cyclic subgroup of G generated by 'a' that is,

$$K = < a > = \{a, a^2, a^3, ..., a^p = e\}$$

As 'a' belongs to centre, every element $x \in G$ commutes with a and all its powers, so

$Kx = xK$ for all $x \in G$

$\Rightarrow$ K is a normal subgroup of G.

Hence G/K is well-defined and

$$o(G/K) = \frac{o(G)}{o(K)} = \frac{p^n}{p} = p^{n-1}, \text{ where } n-1 < n$$

Also, $o(H/K) = \dfrac{o(H)}{o(K)} = \dfrac{p^{n-1}}{p} = p^{n-2}$

So, by induction hypothesis, H/K must be a normal subgroup of G/K

$\Rightarrow$ H is a normal subgroup of G $\Rightarrow$ $N(H) = G$ (3)

By (1) and (3) we obtain, $H = G$, which is absurd.

Hence $o(H) = p^{n-1}$ is not possible.

2.4.19. Example. Show that no group of order 108 is simple.

-OR-

Let G be a group of order 108. Show that G has a normal subgroup of order 27 or 9.

Solution. We have $o(G) = 108 = 2^2.3^3$. By Sylow third Theorem, the number n_3 of Sylow 3–subgroups is given by $1 + 3k$ such that

$$1+3k/o(G) = 2^2.3^3 \quad \Rightarrow \quad 1+3k/4 \ \text{ [Since } (1+3k, 3^3) = 1]$$

$$\Rightarrow \quad k = 0 \text{ or } 1$$

$$\Rightarrow \quad n_3 = 1 + 3.0 \text{ or } 1 + 3.1$$

$$\Rightarrow \quad n_3 = 1 \text{ or } 4$$

We consider the two cases separately.

Case (i). $n_3 = 1$, that is, G has a unique Sylow 3 -subgroup, say H. Since H is unique, it must be normal and $o(H) = 3^3 = 27$. Thus G has a normal subgroup of order 27 in this case and hence G is not simple.

Case (ii). $n_3 = 4$, that is, G has four Sylow 3 – subgroups each of order 27. Let H and K be any two distinct sylow 3 – subgroups. We claim that $o(H \cap K) = 9$ and $H \cap K$ is a normal subgroup of G.

Clearly, $H \cap K \subseteq H$, and so by Lagrange's Theorem.

$$o(H \cap K)/o(H) = 27$$

$$\Rightarrow \quad o(H \cap K) = 1 \text{ or } 3 \text{ or } 9 \text{ or } 27.$$

If $o(H \cap K) = 27$ then since $o(H) = o(K) = 27$, we obtain $H = K$, which is a contradiction. Hence $o(H \cap K) \neq 27$.

If $o(H \cap K) = 1$ or 3 then $o(H\,K) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = \dfrac{27.27}{1\,or\ 3} > 108 = o(G)$, which is not possible.

Hence $o(H \cap K) \neq 1, 3$ and so $o(H \cap K) = 9$.

We now show that $H \cap K$ is normal in G. For this we shall prove that $N(H \cap K) = G$.

Now, we know a that, if $o(H) = p^{n-1}$ and $o(G) = p^n$ then H is a normal subgroup of G.

Using this, we conclude that $H \cap K$ is a normal subgroup of both H and K as $o(H \cap K) = 3^2$ and $o(H) = o(K) = 3^3$.

Let $x \in H$ be any element, then

$$(H \cap K)x = x(H \cap K) \qquad \text{[Since } (H \cap K) \trianglelefteq H]$$

$$\Rightarrow \quad x \in N(H \cap K), \text{ normalizer of } H \cap K.$$

$$\Rightarrow \quad H \subseteq N(H \cap K)$$

Similarly, $K \subseteq N(H \cap K) \quad \Rightarrow \quad HK \subseteq N(H \cap K)$

$$\Rightarrow \quad o\big(N(H \cap K)\big) \geq o(HK) = \frac{o(H).o(K)}{o(H \cap K)} = \frac{27.27}{9} = 81$$

$$\Rightarrow \quad o\big(N(H \cap K)\big) \geq 81 \qquad (1)$$

On the other hand, $N(H \cap K)$ is a subgroup of G so by Lagrange's Theorem

$$o\big(N(H \cap K)\big) \big/ o(G),$$

that is, $o\big(N(H \cap K)\big) \big/ 108 \qquad (2)$

Both (1) and (2) are possible only when

$$o\big(N(H \cap K)\big) = 108 = o(G)$$

$$\Rightarrow \quad o\big(N(H \cap K)\big) = o(G)$$

$$\Rightarrow \quad N(H \cap K) = G$$

$\Rightarrow \quad H \cap K$ is normal in G. [Since $N(H) = G$ iff $H \trianglelefteq G$]

Hence G is not simple.

2.4.20. Theorem. Let $o(G) = pq$, where p and q are distinct primes, $p < q$ and $p \nmid q - 1$, then show that G is cyclic.

Proof. By Sylow third Theorem, the number n_p of Sylow p-subgroups is given by $1 + kp$ such that $1 + kp \big/ o(G) = pq$

$$\Rightarrow \quad 1 + kp \big/ q \quad [\text{Since } (1 + kp, p) = 1]$$

$$\Rightarrow \quad 1 + kp = 1 \text{ or } 1 + kp = q \qquad [\text{Since } q \text{ is a prime}]$$

If $1 + kp = q$, then $kp = q - 1$

$$\Rightarrow \quad p \big/ q - 1, \text{ which is a contradiction.}$$

Hence $n_p = 1 + kp = 1$. Thus G has a unique Sylow p-subgroup, say, H of order p. Also since H is unique, it must be normal. Thus we obtained

$$o(H) = p \text{ and } H \trianglelefteq G \qquad (1)$$

Again, by Sylow third Theorem, the number n_q of Sylow q-subgroups is given by $1 + k'q$ such that $1 + k'q \big/ o(G) = pq \quad \Rightarrow \quad 1 + k'q \big/ p \qquad [\text{Since } (1 + k'q\ ,\ q) = 1]$

$$\Rightarrow \quad 1 + k'q = 1 \text{ or } 1 + k'q = p$$

If $1 + k'q = p$ then we get $q < p$, which is a contradiction.

Hence $n_q = 1 + k'q = 1$. Thus G has a unique Sylow q-subgroup, say, K of order q. Also since K is unique it must be normal. Thus we obtained

$$o(K) = q \text{ and } K \trianglelefteq G \qquad (2)$$

Now, we know that a group of prime order is always cyclic and here H and K both are of prime orders, so they must be cyclic.

Let $H = < a >$ and $K = < b >$ then $o(H) = o(a)$ and $o(K) = o(b)$ (3)

Using (1) and (2) in (3), we get

$$o(a) = p \text{ and } o(b) = q \qquad (4)$$

Now, we prove that $H \cap K = \{e\}$. Let $x \in H \cap K$ be any element.

Then $x \in H$ and $x \in K \Rightarrow o(x) / o(H)$ and $o(x) / o(K)$

$\Rightarrow o(x) / p$ and $o(x) / q$

$\Rightarrow o(x) / \gcd(p, q)$

$\Rightarrow o(x) = 1$

$\Rightarrow x = e$ for all $x \in H \cap K$

$\Rightarrow H \cap K = \{e\}$ (5)

Now, we prove that $ab = ba$.

For this consider the element $a^{-1}b^{-1}ab$. We see that

$$a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in H,$$

because $H \trianglelefteq G$, so that $b^{-1}ab \in H$ and also $a^{-1} \in H$.

Again, $a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)b \in K$, because $K \trianglelefteq G$, so that $a^{-1}b^{-1}a \in K$ and also $b \in K$.

Hence, we get $a^{-1}b^{-1}ab \in H \cap K$

$\Rightarrow a^{-1}b^{-1}ab = e$ [By (5)]

$\Rightarrow baa^{-1}b^{-1}ab = ba.e$

$\Rightarrow ab = ba$

Lastly, by (3), we see that $\gcd(o(a), o(b)) = \gcd(p, q) = 1$

We know that, if $a, b \in G$ such that $ab = ba$ and $\big(o(a), o(b)\big) = 1$ then $o(ab) = o(a).o(b)$.

Therefore, $o(ab) = o(a)\ o(b) = pq = o(\mathrm{G})$

$\Rightarrow$ G contains an element ab of order pq

$\Rightarrow G = < ab >$

$\Rightarrow$ G is cyclic.

Remark. Due to the above result, we can say that groups of order 15, 33, 35, 65, 51 etc. are cyclic.

2.4.21. Exercise.

1. Show that a group of order 15 always cyclic.
2. Let G be a group of order 231, then show that

   (i) G is not simple

   (ii) Sylow 11 -subgroup of G is contained in the centre of G.

2.4.22. Theorem. Let P be a Sylow p-subgroup of G and let $x \in N(P)$ be an element such that $o(x) = p^r$. Then show that $x \in P$.

Proof. Since P is given to be a Sylow p-subgroup of G and let

$$p^n / o(G) \text{ but } p^{n+1} \nmid o(G) \qquad (1)$$

Then, clearly $o(P) = p^n$.

We know that $P \trianglelefteq N(P)$, so $N(P)/P$ is well-defined.

As $x \in N(P)$, $Px \in N(P)/P$ and $(Px)^{p^r} = P.x^{p^r} = P.e$ [Since $o(x) = p^r$]

$\Rightarrow$ $(Px)^{p^r} = P =$ Identity of $N(P)/P$

$\Rightarrow$ $o(Px) / p^r \Rightarrow o(Px) = p^s$ for some $s \geq 0$

If $s = 0$, then $o(Px) = p^s = p^0 = 1 \Rightarrow Px = P$

$\Rightarrow$ $x \in P$, which is required to prove.

Now we finish the proof by showing that $s > 0$ is impossible.

Let, if possible, $s > 0$ and let $\overline{H}$ be the cyclic subgroup of $N(P)/P$ generated by Px that is,

$$\overline{H} = \langle Px \rangle \text{ then } o(\overline{H}) = o(Px) = p^s \qquad (2)$$

Since $\overline{H}$ is a subgroup of $N(P)/P$, it must be of the form $\overline{H} = H/P$ where H is a subgroup of $N(P)$ containing P.

Now, $o(\overline{H}) = p^s$ [By (2)]

$\Rightarrow$ $o(H/P) = p^s$

$\Rightarrow$ $\dfrac{o(H)}{o(P)} = p^s \quad \Rightarrow \quad o(H) = p^{n+s}$, $s > 0$

As H is a subgroup of $N(P)$ and $N(P)$ is a subgroup of G, so H is a subgroup of G and by Lagrange's Theorem, $o(H)/o(G)$

$\Rightarrow$ $p^{n+s} \mid o(G)$, which is a contradiction by (1), as $s > 0$.

Hence $s > 0$ is not possible and in case $s = 0$, we have already shown that $x \in P$.

2.5.Structure of Finite Abelian Groups.

If a group is direct product of some of its subgroups, then the structure of the group can be determined by determining the structures of subgroups appearing in the direct product. This simplifies our work as determination of structure of a big group is broken into determination of structures of comparatively smaller groups.

Let us call the subgroups appearing in the direct product as "building blocks". Now the procedure will be more simple if these building blocks are taken to be cyclic subgroups since cyclic groups are always easy to deal with.

Now a natural question arise "Is it always possible to write a group as the direct product of its cyclic subgroups".

The answer is no, in general. However, luckily, it is possible for finite abelian groups, due to Fundamental Structure Theorem for finite abelian groups.

Before the formal statement of this Theorem, let us study another Theorem in this regard.

2.5.1. Theorem. Prove that a finite abelian group is direct product of its Sylow subgroups.

Proof. Let G be a finite abelian group and $o(G) = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$, where $p_1, p_2, ..., p_r$ are distinct primes and $n_i \geq 1$ for all i. Since internal direct product is always isomorphic to external direct product, we shall prove that G is internal direct product of its Sylow subgroups.

Let $H_1, H_2, ..., H_r$ be the Sylow subgroups of G such that

$$o(H_1) = p_1^{n_1}, \quad o(H_2) = p_2^{n_2}, \ldots, \quad o(H_r) = p_r^{n_r}$$

To show that G is internal direct product of $H_1, H_2, ..., H_r$ we have to prove following three things.

(i) Each H_i is normal in G.

(ii) $H_i \cap H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_r = \{e\}$ for any i.

(iii) $G = H_1 H_2 \ldots H_r$

Let us prove all these one by one.

(i) Since G is abelian, so its every subgroup is normal. Hence each H_i is normal in G.

(ii) Let $x \in H_i \cap H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_r$ be any arbitrary element.

Then $x \in H_i$ and $x \in H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_r$

$\Rightarrow$ $x = h_1 h_2 \ldots h_{i-1} h_{i+1} \ldots h_r$ where $h_j \in H_j$ for all $j \neq i$

As $h_j \in H_j$ and $o(H_j) = p_j^{n_j}$, so $(h_j)^{p_j^{n_j}} = e$ for $j \neq i$ (1)

Now, let $t = p_1^{n_1} p_2^{n_2} ... p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} ... p_r^{n_r}$, then for $j \neq i$, we have

$$(h_j)^t = (h_j)^{p_1^{n_1} p_2^{n_2} ... p_{i-1}^{n_i - 1} p_{i+1}^{n_i + 1} ... p_r^{n_r}} = \left[\left(h_j \right)^{p_j^{n_j}} \right]^{\text{remaining factors}} \qquad \left[\text{Since } p_j^{n_j} \text{ appears in } t \right]$$

$$= [e]^{\text{remaining factors}} = e.$$

Thus, $h_1^t = h_2^t = ... = h_{i-1}^t = h_{i+1}^t = ... = h_r = e$ (2)

Now, $x^t = \left(h_1 h_2 ... h_{i-1} h_{i+1} ... h_r \right)^t$

$$= h_1^t h_2^t ... h_{i-1}^t h_{i+1}^t ... h_r^t$$

$$= e.$$

$\Rightarrow \quad o(x)/t \quad \Rightarrow \quad o(x) \big/ p_1^{n_1} p_2^{n_2} ... p_{i-1}^{n_i - 1} p_{i+1}^{n_i + 1} ... p_r^{n_r}$ (3)

Since $x \in H_i \Rightarrow o(x)/o(H_i)$

$\Rightarrow \quad o(x) \big/ p_i^{n_i} \quad \Rightarrow \quad o(x) = p_i^{m_i}, 0 \leq m_i \leq n_i$ (4)

Putting value of (4) in (3), we get

$$p_i^{m_i} \Big/ p_1^{n_1} p_2^{n_2} ... p_{i-1}^{n_i - 1} p_{i+1}^{n_i + 1} ... p_r^{n_r} \quad \Rightarrow \quad m_i = 0,$$

since p_i does not appear on R.H.S.. So by (4), we have $o(x) = p_i^{m_i} = p_i^0 = 1 \Rightarrow \quad x = e$

Thus, $H_i \cap H_1 H_2 ... H_{i-1} H_{i+1} ... H_r = \{e\}$ for any *i*, which proves (ii).

(iii) We know that a result that

If *A* and *B* are two finite subgroups then $o(AB) = \dfrac{o(A)\ o(B)}{o(A \cap B)}$ (5)

Using this result for $A = H_1$ and $B = H_2 H_3 ... H_r$, we get

$$o(H_1 H_2 ... H_r) = \frac{o(H_1) o(H_2 H_3 ... H_r)}{o(H_1 \cap H_2 H_3 ... H_r)} \tag{6}$$

Taking *i* = 1 in (ii), proved above, we have

$$H_1 \cap H_2 H_3 ... H_r = \{e\} \Rightarrow \quad o(H_1 \cap H_2 H_3 ... H_r) = 1$$

Using this in (6)

$$o(H_1 H_2 ... H_r) = o(H_1) o(H_2 H_3 ... H_r) = \frac{o(H_1)\ o(H_2)\ o(H_3 H_4 ... H_r)}{o(H_2 \cap H_3 H_4 ... H_r)} \tag{7}$$

Now, $H_2 \cap H_3 H_4 ... H_r \subseteq H_2 \cap H_1 H_3 H_4 ... H_r = \{e\}$ [By (ii) for *i* = 2]

$$\Rightarrow \quad H_2 \cap H_3 H_4 ... H_r = \{e\} \quad \Rightarrow \quad o(H_2 \cap H_3 H_4 ... H_r) = 1$$

Using this in (7), we get

$$o(H_1H_2...H_r) = o(H_1).o(H_2)o(H_3H_4...H_r)$$

Continuing in this way, we obtain

$$o(H_1H_2...H_r) = o(H_1).o(H_2)...o(H_r) = p_1^{n_1} p_2^{n_2} .....p_r^{n_r} = O(G)$$

$\Rightarrow$ $G = H_1H_2.....H_r$, which proves (iii).

Thus G is the internal direct product of its Sylow subgroups.

2.6. SURVEY OF GROUPS.

In our previous work we have obtained a complete description of number and nature of a finite abelian group. Unfortunately, there is no such general result for finite non-abelian groups. The Sylow Theorems and Cauchy Theorem (which is itself is a particular case of Sylow first Theorem) are a powerful tool in finding the number and nature of finite non-abelian groups.

However, to keep our study within the scope of the book, we shall study the groups of orders 6 and 8 only.

2.6.1. Example. Find all non-abelian groups of order 6.

Solution. Let G be a non-abelian group such that $o(G) = 6$. Now 3 and 2 are prime numbers dividing $o(G)$ so by Cauchy Theorem, there exist two non-identity element a and b in G such that $o(a) = 3$ and $o(b) = 2$.

Let $H = < a >$ be the cyclic subgroup of G generated by a that is,

$$H = \{e, a, a^2\} \text{ and } o(H) = 3.$$

Now, index of H in $G = \dfrac{o(G)}{o(H)} = \dfrac{6}{3} = 2$

Since every subgroup of index 2 is normal, H is normal in G.

If $b \in H$, then $o(b) / o(H) \Rightarrow 2/3$, which is a contradiction. Hence $b \notin H$

As index of H in G is 2, so there are two distinct right coset of H in G and clearly these are H and Hb. Then $G = H \cup Hb = \{e, a, a^2, b, ab, a^2b\}$.

Since $H \trianglelefteq G$, $b^{-1}ab \in H = \{e, a, a^2\} \Rightarrow$ $b^{-1}ab = e$ or a or a^2

If $b^{-1}ab = e$, then $bb^{-1}abb^{-1} = beb^{-1}$ that is, $a = e$, a contradiction.

If $b^{-1}ab = a$, then $ab = ba \Rightarrow G$ is abelian, a contradiction.

So, $b^{-1}ab = a^2 = a^{-1}$.

Hence there is only one non-abelian group of order 6 given by

$$G = \{e, a, a^2, b, ab, a^2b\} \text{ where } a^3 = b^2 = e \text{ and } b^{-1}ab = a^{-1}$$

2.6.2. Exercise.

1. Find all non-isomorphic abelian groups of order 6.
2. Find all non-isomorphic groups of order 6.
3. Find all non-isomorphic non-abelian groups of order 8.
4. Find all non-isomorphic groups of order 8.

2.7. Check Your Progress.

1. For any group G, G/G' is always abelian.

2. If G is a group, then $G^{(n)}/G^{(n+1)}$ is always abelian.

3. Show that a group of order 30 is not simple.

2.8. Summary.

In this chapter, we discussed about commutator elements, Sylow's theorems which is an important part of group theory. Also observed that for a finite group and a prime p dividing its order, if p^m is the largest power of p dividing order of group, then the group must have subgroups of orders $p^0, p^1, \ldots, p^m$. However, we have no idea about the number of subgroups of orders p^i for $i = 1, 2, \ldots, m-1$, but for $i = 0$, it is 1 and for $i = m$, it can be decided by Sylow's third theorem.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Lanski, C. Concepts in Abstract Algebra, American Mathematical Society, First Indian Edition, 2010.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
5. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
6. Musili, C., Introduction to Rings and Modules, Narosa Publication House, 1994.
7. Jacobson, N., Basic Algebra, Vol. I & II, W.H Freeman, 1980 (also published by Hindustan Publishing Company).
8. Artin, M., Algebra, Prentice-Hall of India, 1991.
9. Macdonald, I. D., The Theory of Groups, Clarendon Press, 1968.

3

SUBNORMAL SERIES

Structure

3.1. Introduction. This chapter contains definition of subnormal series and its examples. Definition and important properties related to that of a solvable group are discussed. One important result in this direction is that S_n is not solvable for $n > 4$. Also it is proved that every p-group is solvable.

3.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Every subgroup of a solvable group is solvable.

(ii) Every factor group of a solvable group is solvable.

(iii) Converse result of these results.

(iv) Every p-group is solvable.

(v) S_n is not solvable for $n > 4$.

(vi) A group is solvable iff nth derived subgroup is solvable.

3.1.2. Keywords. Subnormal Series, Solvable Groups, Abelian Groups, Order of Group, Quotient Groups.

3.2. Subnormal Series. A sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e >$$

of a group G is called a subnormal series of G if $G_{i+1} \Delta G_i$ for $0 \le i \le r-1$.

3.2.1. Refinement of a Series. Let G be a group and

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e >$$

be a subnormal series for G. A subnormal series

$$G = G_0' \supseteq G_1' \supseteq G_2' \supseteq ... \supseteq G_s' = < e >$$

is called a refinement of the former series if $\{G_0, G_1, G_2, ..., G_r\} \subseteq \{G_0', G_1', G_2', ..., G_s'\}$.

The refinement is said to be a proper refinement if $\{G_0, G_1, G_2, ..., G_r\} \subset \{G_0', G_1', G_2', ..., G_s'\}$. For example, let G = S_3, then $G = G_0 \supseteq G_1 = < I >$ is a subnormal series for G. Now consider the series $G = G_0 \supseteq G_1 = A_3 \supseteq G_2 = < I >$.

We note that $A_3 \Delta S_3$ and $< I > \Delta A_3$. So, this series is also a subnormal series for G. Also, $\{S_3, < I >\} \subset \{S_3, A_3, < I >\}$.

Hence this series is a proper refinement of the last one.

3.2.2. Length of a Series. Consider a subnormal series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e > \qquad (1)$$

Then, it is possible for some i, $G_i = G_{i+1}$ in (1). The number of distinct members of (1) different from (1) is called the length of the series (1).

Due to this definition, the length of series (1) is r, if all G_i's are distinct.

The subnormal series (1) is said to be redundant if for some i = 0,1,2,…,r-1; $G_i = G_{i+1}$, otherwise it is said to be irredundant. One can always construct an irredundant series from a redundant one by deleting G_i whenever for some i, $G_{i+1} = G_i$.

So, if (1) is irredundant, then length of (1) is r.

3.2.3. Factors of a Series. Let G be a group and $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e >$ is a subnormal series for G. Then, G_i / G_{i+1} is called factor group or quotient factor group of the series.

3.3. Solvable Group. A group G is said to be solvable if there exists a sequence of subgroups $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e >$ such that

(i) $G_{i+1} \Delta G_i,\ 0 \le i \le r-1$

(ii) G_i / G_{i+1} is abelian, $0 \le i \le r-1$.

3.3.1. Example. Every abelian group G is solvable. The series $G \supseteq < e >$ is a subnormal series, that is $< e > \Delta G$ and its only factor group is $G / < e >$, which being isomorphic to G, is abelian.

3.3.2. Results. (i) A subset H of a group G is a subgroup iff $ab^{-1} \in \mathrm{H}$ for all $a, b \in \mathrm{H}$.

(ii) A subgroup H of a group G is normal iff $g^{-1}hg \in H$ for every $h \in H, g \in G.$

(iii) Let G be a group and H be a normal subgroup of G, then the set G/H (G mod H) of all cosets of H in G is a subgroup w.r.t. multiplication of cosets. It is called quotient group or factor group of G by H. If $a, b \in G$, then HaHb = Hab. The identity element of G/H is H.

(iv) If $(G, .)$ and $(\bar{G}, *)$ are two groups. A mapping $f : G \to \bar{G}$ is called a homomorphism, if $f(x.y) = f(x) * f(y)$ for all $x, y \in G$. Also, it is called isomorphism, if it is one – one and onto. We write as $G \cong \bar{G}$

(v) **Fundamental Theorem of Homomorphism.** If $\bar{G}$ is homomorphic image of G under f (that is, f is onto) , then $G / \ker f \cong \bar{G}$. If f is not onto then $G / \ker f \cong f(G)$.

3.3.3. Proposition. Every subgroup of a solvable group is solvable.

Proof. Let G be a solvable group and let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$$

be a solvable series for G such that

(i) $G_{i+1} \Delta G_i,\ 0 \le i \le r-1$

(ii) G_i / G_{i+1} is abelian, $0 \le i \le r-1$.

Let H be any subgroup of G and let $H_i = H \cap G_i,\ 0 \le i \le r$, then

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_r = < e > \qquad \text{---(1)}$$

is a sequence of subgroups of H. For it, since $e \in H_i$ for $0 \le i \le r$. Therefore, $H_i \neq \phi$ for all $0 \le i \le r$.

Let $a, b \in H_i = H \cap G_i$ which implies $a, b \in H$ and $a, b \in G_i$.

Since H and G_i are subgroups, therefore, $ab^{-1} \in H$ and $ab^{-1} \in G_i$ and so $ab^{-1} \in H \cap G_i = H_i$. Hence H_i is a subgroup of H, $0 \le i \le r$.

Now, we claim that the series (1) is a solvable series for H.

First we prove that $H_{i+1} \Delta H_i,\ 0 \le i \le r-1$.

Let $h \in H_{i+1}$ and $k \in H_i$. Then $h \in H_{i+1} = H \cap G_{i+1} \Rightarrow h \in H$ and $h \in G_{i+1}$.

Similarly, $k \in H_i = H \cap G_i \Rightarrow k \in H$ and $k \in G_i$.

Since $G_{i+1} \Delta G_i$, thus $h \in G_{i+1},\ k \in G_i \Rightarrow k^{-1}hk \in G_{i+1}$ and $h, k \in H \Rightarrow k^{-1}hk \in H$. Therefore, $k^{-1}hk \in H \cap G_{i+1} = H_{i+1}$ and so $H_{i+1} \Delta H_i,\ 0 \le i \le r-1$.

Now, we shall prove that H_i / H_{i+1}, $0 \le i \le r-1$, are abelian.

To prove this we define a mapping $f : H_i \to G_i / G_{i+1}$ by considering

$$f(x) = xG_{i+1},$$

where $x \in H_i = H \cap G_i$.

We shall prove that f is well defined and a group homomorphism.

Let $x, y \in H_i$ such that $x = y \Rightarrow xy^{-1} = e \in G_{i+1}$.

So, $G_{i+1}xy^{-1} = G_{i+1} \Rightarrow G_{i+1}x = G_{i+1}y \Rightarrow xG_{i+1} = yG_{i+1} \Rightarrow f(x) = f(y)$.

Therefore, f is a well-defined mapping.

Again, let $x, y \in H_i$, then

$$f(xy) = xyG_{i+1} = xG_{i+1}.yG_{i+1} = f(x)f(y)$$

So, f is a group homomorphism. Thus, by fundamental theorem of group homomorphism, we have

$$H_i / \ker f \cong f(H_i) \subseteq G_i / G_{i+1}. \qquad (1a)$$

We shall prove that $Kerf = H_{i+1}$, where $Kerf = \{x \in H_i : f(x) = G_{i+1}\}$. For this, we have

$$x \in \ker f \Rightarrow f(x) = G_{i+1} \Rightarrow xG_{i+1} = G_{i+1} \Rightarrow x \in G_{i+1}$$

Now, $x \in H_i = H \cap G_i \Rightarrow x \in H$. So, $x \in H, x \in G_{i+1} \Rightarrow x \in H \cap G_{i+1} = H_{i+1}$

$$\Rightarrow \ker f \subseteq H_{i+1} \qquad (2)$$

Let $y \in H_{i+1} = H \cap G_{i+1} \Rightarrow y \in H$ and $y \in G_{i+1}$.

So,

$$f(y) = yG_{i+1} = G_{i+1} \Rightarrow y \in \ker f \Rightarrow H_{i+1} \subseteq \ker f \qquad (3)$$

By (2) and (3), $H_{i+1} = \ker f$.

Putting this value in (1a), we obtain

$$H_i / H_{i+1} \cong f(H_i) \subseteq G_i / G_{i+1}.$$

Since G_i / G_{i+1} is abelian and $f(H_i)$ is a subgroup of G_i / G_{i+1}, so $f(H_i)$ is also abelian.

Therefore, H_i / H_{i+1} is also abelian. Hence H is solvable.

3.3.4. Canonical Homomorphism. The mapping $f : G \to G/H$ defined by $f(g) = Hg$ for all $g \in G$ is an onto homomorphism, where H is a normal subgroup of G. It is called natural or canonical homomorphism and $Kerf = H$.

3.3.5. Proposition. Every quotient group of a solvable group is solvable.

-OR- Let G be a solvable group and H is a normal subgroup of G, then G/H is also solvable.

Proof. Let G be a solvable group and let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$$

be a solvable series for G, then

(i) $G_{i+1} \Delta G_i,\ 0 \le i \le r-1$

(ii) G_i / G_{i+1} is abelian, $0 \le i \le r-1$.

Let $q : G \to G/H$ be a canonical homomorphism, that is,

$$q(x) = xH \quad \text{for all } x \in G$$

Since $G_{i+1} \subseteq G_i$ so $q(G_{i+1}) \subseteq q(G_i)$.

Now consider the series

$$G/H = q(G_0) \supseteq q(G_1) \supseteq q(G_2) \supseteq \ldots \supseteq q(G_r) = < H >.$$

We claim that this series is a solvable series for G/H.

Let $x \in q(G_{i+1})$ and $y \in q(G_i)$, then there exist $\alpha \in G_{i+1}$ and $\beta \in G_i$ such that $x = q(\alpha)$ and $y = q(\beta)$.

Now $\alpha \in G_{i+1}, \beta \in G_i$ and $G_{i+1} \Delta G_i$, so $\beta^{-1}\alpha\beta \in G_{i+1}$.

Therefore, $q(\beta^{-1}\alpha\beta) \in q(G_{i+1}) \Rightarrow q(\beta^{-1})q(\alpha)q(\beta) \in q(G_{i+1})$

$\Rightarrow q(\beta)^{-1} q(\alpha)q(\beta) \in q(G_{i+1}) \Rightarrow y^{-1}xy \in q(G_{i+1})$ and hence $q(G_{i+1}) \Delta q(G_i)$.

Now we shall prove that $q(G_i)/q(G_{i+1})$ is abelian.

Let $\bar{\alpha}, \bar{\beta} \in q(G_i)/q(G_{i+1})$ be any two arbitrary elements. Then,

$\bar{\alpha} = \alpha q(G_{i+1})$ and $\bar{\beta} = \beta q(G_{i+1})$ for some $\alpha, \beta \in q(G_i)$.

Also, $\alpha, \beta \in q(G_i) \Rightarrow \alpha = q(\alpha')$ and $\beta = q(\beta')$ for some $\alpha', \beta' \in G_i$. Therefore,

$\bar{\alpha} = \alpha q(G_{i+1}) = q(\alpha')q(G_{i+1}) = q(\alpha' G_{i+1})$ and $\bar{\beta} = q(\beta' G_{i+1})$.

Then,

$\bar{\alpha}\bar{\beta} = q(\alpha' G_{i+1})q(\beta' G_{i+1}) = q(\alpha' G_{i+1}\beta' G_{i+1}) = q(\beta' G_{i+1}\alpha' G_{i+1}) = q(\beta' G_{i+1})q(\alpha' G_{i+1}) = \bar{\beta}\bar{\alpha}$.

Therefore, $q(G_i)/q(G_{i+1})$ is abelian. Hence G/H is solvable.

3.3.6. Proposition. Let G be a group and H be a normal subgroup of G. If H and G/H both are solvable, then G is also a solvable group.

Proof. Since H is solvable, so let $H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n = < e >$ be a solvable series for H. Therefore,

(i) $H_{i+1} \Delta H_i,\ 0 \le i \le n-1$

(ii) H_i/H_{i+1} is abelian, $0 \le i \le n-1$.

Now, since G/H is solvable, so let

$$G/H = G_0/H \supseteq G_1/H \supseteq G_2/H \supseteq \ldots \supseteq G_m/H = < H >$$

be a solvable series for G/H. Therefore,

(i) $G_{i+1}/\mathrm{H} \Delta G_i/\mathrm{H},\ 0 \le i \le m-1$

(ii) $\dfrac{G_i/H}{G_{i+1}/H}$ is abelian, $0 \le i \le m-1$.

Now consider the series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n = < e >$$

We claim that this is a solvable series for G, that is, we are to show that

(i) $G_{i+1} \Delta G_i,\ 0 \le i \le m-1$ and $H_{j+1} \Delta H_j,\ 0 \le j \le n-1$

(ii) $\dfrac{G_i}{G_{i+1}}$ is abelian, $0 \le i \le m-1$ and $\dfrac{H_j}{H_{j+1}}$ is abelian, $0 \le j \le n-1$.

(i) It is clear that $H_{j+1} \Delta H_j,\ 0 \le j \le n-1$.

So, we are to show that $G_{i+1} \Delta G_i,\ 0 \le i \le m-1.$

Let $x \in G_i$ and $y \in G_{i+1}$. Then, $xH \in G_i/\mathrm{H}$ and $yH \in G_{i+1}/H$. Due to solvability of G/H, we have

$G_{i+1}/\mathrm{H} \Delta G_i/\mathrm{H} \Rightarrow (xH)^{-1}(yH)(xH) \in G_{i+1}/\mathrm{H}$

$\Rightarrow x^{-1}yxH \in G_{i+1}/\mathrm{H} \Rightarrow x^{-1}yx \in G_{i+1}$

Thus, $G_{i+1} \Delta G_i$ for every *i*.

(ii) Again, it is clear that $\dfrac{H_j}{H_{j+1}}$ is abelian, $0 \le j \le n-1$.

So, we have only to prove that $\dfrac{G_i}{G_{i+1}}$ is abelian, $0 \le i \le m-1$. Due to Third Theorem of Isomorphism,

$\dfrac{G_i/H}{G_{i+1}/H} \cong \dfrac{G_i}{G_{i+1}} \Rightarrow \dfrac{G_i}{G_{i+1}}$ is abelian.

Hence G is solvable.

3.4. p-group. A finite group whose order is p^n for some integer $n \ge 1$, where p is a prime, is called a p-group.

3.4.1. Cyclic group. A group G is said to be cyclic group generated by an element $a \in G$ if every $g \in G$ is such that $g = a^t$ for some integer t. We denote it by G = <a>.

Remark. If the order of a group is a prime number, then the group is cyclic and every cyclic group is abelian and every abelian group is solvable.

3.4.2. Center of a group. Let G be a group then the center of G is given by

$$Z(G) = C(G) = \{x \in G : xy = yx \text{ for all } y \in G\}.$$

3.4.3. Corollary. Every finite p-group is solvable.

Proof. Let G be a finite p-group and let $o(G) = p^n$ for some $n \geq 1$.

If n=1, then $o(G) = p$ so G is cyclic. Hence G is abelian and so solvable.

So let n > 1 and suppose as our induction hypothesis that result is true for all p-groups with order p^rwherer < n

Now, if G is abelian then result is again true, so let G is non-abelian.

Then, Z(G), the center of G, is non- trivial by class equation. But we know that $Z(G)\ \Delta\ G.$ Now, $o(G) = p^n \ \Rightarrow\ o(Z(G)) = p^s$ for some $s < n.$

Since $Z(G)$ is non-trivial, so $o(Z(G)) > 1 \Rightarrow s \geq 1.$

Then, $o(G/Z(G)) = \dfrac{o(G)}{o(Z(G))} = p^{n-s} < p^n.$

So, by induction hypothesis, $G/Z(G)$ is solvable. Now, $Z(G)$ is abelian, so $Z(G)$ is also solvable. Then, by above proposition, G is solvable.

Remark. Let H and K be two groups. Then, the direct product of these groups is the group $H\text{x}K = \{(h,k) : h \in H, k \in K\}$.

Also, if $K \cong K'$, then $X/K \cong X/K'$ and $K\ \Delta\ H\text{x}K.$

3.4.3. Corollary. Direct product of two solvable groups is again solvable.

Proof. Let H and K be two solvable groups and X = HxK. We know that $K\ \Delta\ H\text{x}K = X$. Define a mapping $f : X \to H$ by setting

$$f(x) = f(h,k) = h \text{ for all } x \in X.$$

It is easy to show that f is well-defined.

To show that f is a homoporphism.

Let $x, y \in X$, then $x = (h,k)$ and $y = (h_1,k_1)$ for some $h, h_1 \in H; k, k_1 \in K.$ Therefore,

$$f(x,y) = f((h,k),(h_1,k_1)) = f(hh_1, kk_1) = hh_1 = f(x).f(y)$$

Hence, f is a homomorphism.

To show that f is onto.

Let $h \in H$, then for every $k \in K$, we have $(h,k) \in X$ and $f(h,k) = h.$

Hence f is onto.

Thus, by fundamental theorem of homomorphism, we have $X/Kerf \cong H$. ---(*)

Now, we claim that $\ker f \cong K$.

Let $k \in K$, we define $K' = \{(e,k) : e \in H, k \in K\}$.

We shall show that $\ker f \cong K'$.

For this, let $x \in \ker f \Rightarrow f(x) = e,$ where $e \in H.$

But $x = (h,k)$ for some $h \in H, k \in K.$ Therefore,

$f(h,k) = e \quad \Rightarrow h = e \quad \Rightarrow x = (e,k) \in K' \quad \Rightarrow \ker f \subseteq K'$ ---(1)

Let $x \in K' \quad \Rightarrow x = (e,k)$ for some $k \in K.$ Thus,

$f(x) = e \quad \Rightarrow x \in \ker f \quad \Rightarrow K' \subseteq \ker f$ ---(2)

By (1) and (2), we obtain

$K' = \ker f = \{(e,k) : e \in H, k \in K\}$

Now, by (*), we obtain

$$X/K' \cong H \qquad \text{---(**)}$$

We claim that $K \cong K' = \{e\} \text{x} K,$ where $e \in H$.

Define a mapping $\phi : K \to K'$, by setting

$$\phi(k) = (e,k) \qquad \text{for all } k \in K.$$

To show that ϕ is a homomorphism.

Let $x, y \in K$, then

$$\phi(x,y) = (e,xy) = (e,x)(e,y) = \phi(x)\phi(y)$$

To show that ϕ is one-one.

Let $k_1, k_2 \in K$ such that $\phi(k_1) = \phi(k_2) \quad \Rightarrow (e,k_1) = (e,k_2) \quad \Rightarrow k_1 = k_2.$

To show that ϕ is onto.

Let $(e,k) \in K'$, then for $k \in K$, $\phi(k) = (e,k)$

Hence ϕ is an isomorphism. Therefore, $K \cong K'$.

Thus, by (**), since $K \cong K'$, so $X/K \cong X/K' \Rightarrow X/K \cong H.$

Since H is solvable, so X/K is solvable.

Also subgroup K of X is solvable. Hence X = HxK is solvable.

3.4.4. Remark. (i) Let H and K be two subgroups of a group G. Then, HK is a subgroup of G iff HK = KH.If $H \Delta G$, then HK = KH and so HK is a subgroup of G.

(ii) Second Theorem of Isomorphism. Let H and K are subgroups of any group G, where $H \trianglelefteq G$. Then, $K/H \cap K \cong HK/H$.

3.4.5. Corollary. Let H and K are solvable subgroups of G and $H \Delta G$, then HK is also solvable.

Proof. Since $H \Delta G \Rightarrow HK = KH$, therefore HK is a subgroup of G. Now, by second theorem of isomorphism, we have

$$K/H \cap K \cong HK/H.$$

Now, K is solvable, so $K/H \cap K$ is solvable, since factor group of a solvable group is solvable. So HK/H being isomorphic to $K/H \cap K$ is solvable.But H is given to be solvable, so HK is also solvable, by above proposition.

3.4.6. Sylow p-subgroup. Let G be a finite group and p, a prime number, such that $p^k \mid o(G)$ and $p^{k+1} \nmid o(G)$. Then, any subgroup of G of order p^k is called a Sylow p-subgroup of G, where o(G) = $p^k q$, q is an integer.

3.4.7. Sylow's First Theorem. Let G be a finite group of order $p^k q$, $k \geq 1$, where p is a prime number and q is a positive integer such that g.c.d.(p, q) = 1. Then, for each i, $0 \leq i \leq k$, G has atleast one subgroup of order p^i.

3.4.8. Sylow's Third Theorem. Number of Sylow p-subgroups is of the form 1+mp, where p is a prime and m is non-negative integer such that $1 + mp \mid o(G)$.

3.4.9. Result. (i) If $o(G) = p^2$**,** where *p*is a prime, then G is abelian.

(ii) If G has only one Sylow subgroup of order p^i, then that subgroup will be normal in G.

3.4.10. Corollary. Every group of order pq is solvable, where p, q are prime numbers not necessarily distinct.

Proof. Let $o(G) = pq$. If $p = q$, then $o(G) = p^2$ and G is abelian and hence solvable.So, let us assume that $p > q$. Then, by Sylow's theorem, G has Sylow p-subgroups each of order p and number of sylow p-subgroups is of the form 1+mp such that $1 + mp \mid o(G)$ .That is, $1 + mp \mid pq \quad \Rightarrow 1 + mp \mid q \quad \Rightarrow m = 0$.

Hence, G has unique Sylow p-subgroup, say H, and $o(H) = p$. Also, we know that unique Sylow p-subgroup is always normal, so $H \Delta G$.

Now, $o(H) = p$ and $o(G/H) = \dfrac{o(G)}{o(H)} = q.$

Thus, H and G/H are both subgroups of prime order, so they are cyclic and hence abelian and in turn solvable. Therefore, by above proposition, G is solvable.

3.4.11. Corollary. Every group of order p^2q is solvable, where p, q are prime numbers not necessarily distinct.

Proof. Let $o(G) = p^2q$, we consider the following three cases

Case (i) $p = q$, **Case (ii)** $p > q$, and **Case (iii)** $p < q$.

Case (i). If $p = q$, then $o(G) = p^3$ and we know that a finite p-group is solvable hence G is solvable.

Case (ii). If $p > q$ then by Sylow theorems, G has Sylow p-subgroups each of order p^2 and number of these subgroups is 1+ mp such that $1 + mp/o(G)$, m is non-negative integer.

Since gcd (p , q) = 1, so $1 + mp/p^2q$, implies, $1 + mp/q$.

$\Rightarrow \quad m = 0$, as $p > q$.

Thus, G has unique Sylow p-subgroup, say H, and $o(H) = p^2$. Also, we know that unique Sylow p-subgroups is always normal so $H \Delta G$.

Now, $o(H) = p^2$ and $o(G/H) = \dfrac{o(G)}{o(H)} = q$.

Now, H is abelian, since a group of order p^2 is always abelian and so H is solvable.

Again, G/H , being of prime order, is cyclic hence abelian and therefore solvable.

Now, H and G/H both are solvable, so by above proposition, G is also solvable.

Case (iii). If $p < q$ then by Sylow theorems, G has Sylow p-subgroups each of order p^2 and number of these subgroups is n_p = 1+ mp such that $1 + mp/o(G)$, m is non-negative integer .

Since gcd (p , q) = 1, so $1 + mp/p^2q$, implies $1 + mp/q$, so n_p = 1+ mp = 1 or q.

Again, by Sylow theorems, G has Sylow q-subgroups each of order q and number of these subgroups is $n_q = 1 + m'q$ such that $1 + m'q / o(G)$, m is non-negative integer .

Since gcd (p , q) = 1, so $1 + m'q / p^2 q$, implies $1 + m'q / p^2$, so $n_q = 1 + m'q = 1$ or p or p^2. However, $p < q$ so $1 + m'q \neq p$ so $n_q = 1 + m'q = 1$ or p^2

Following four sub-cases arise:

(a) $n_p = 1, n_q = 1$

(b) $n_p = 1, n_q = p^2$

(c) $n_p = q, n_q = 1$

(d) $n_p = q, n_q = p^2$

If $n_p = 1$, then G is solvable according to case (ii). So, G is solvable in sub cases (a) and (b). In sub case (c) we have $n_q = 1$, that is, G has unique Sylow q-subgroup of order q, say K. Then K is a normal subgroup of G and $o(K) = q$ and $o(G/K) = \frac{p^2 q}{q} = p^2$. Then both K and G/K , being abelian, are solvable and hence G is solvable by above proposition.

Now we shall prove that sub-case (d) is impossible. In this case, we have p^2 Sylow q-subgroups each of order q, let these be $K_1, K_2, \ldots, K_{p^2}$. Every K_i has $q - 1$ element of order q.

Also, $K_i \cap K_j = \{e\}$. So , we have $p^2 (q - 1)$ element of order q.

Now , G has q Sylow p-subgroups of order p^2 , let there be $H_1 , H_2 , \ldots , H_q$ and $o(H_i) = p^2$

Now , $o(H_1 \cap H_2) / o(H_1) = p^2 \quad \Rightarrow \quad o(H_1 \cap H_2) = 1$ or p or p^2

But $o(H_1 \cap H_2) \neq p^2$, because if $o(H_1 \cap H_2) = p^2$, then $o(H_1 \cap H_2) = o(H_1)$

But $H_1 \cap H_2 \subseteq H_1$, so $H_1 \cap H_2 = H_1 \quad \Rightarrow \quad H_1 \subseteq H_2$.

Similarly $H_2 \subseteq H_1 \quad \Rightarrow \quad H_1 = H_2$ which is not so. So , $o(H_1 \cap H_2) = 1$ or p.

Now , $o(H_1 \cup H_2) = o(H_1) + o(H_2) - o(H_1 \cap H_2) = p^2 + p^2 - (1 \text{ or } p) \geq p^2 + p^2 - p$.

So , G has at least $p^2 + p^2 - p + p^2 (q - 1) = 2p^2 - p + p^2 q - p^2 = p^2 - p + p^2 q > p^2 q$, elements, which is a contradiction.

Therefore, G is solvable in all possible cases.

3.4.12. Exercise. The symmetric group S_n is solvable for $n \leq 4$.

Solution. For $n = 1$, $S_1 = < I >$, obviously solvable.

For $n = 2$, $S_2 = < I, (1\ 2) >$. Here, $o(S_2) = 2$, a prime number and so S_2 is abelian and hence solvable.

For $n = 3$, $S_3 = < I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) >$.

Consider the sequence $S_3 \supseteq A_3 \supseteq < I >$.

Clearly, $A_3 \Delta S_3$ and $< I > \Delta A_3$.

Here, $o(S_3/A_3) = 2 \Rightarrow S_3/A_3$ is cyclic and so abelian.

Also, $o(A_3/< I >) = 3 \Rightarrow A_3/< I >$ is cyclic and so abelian.

So, the above series is a solvable series for S_3 and hence S_3 is solvable.

For $n = 4$, consider the sequence $S_4 \supseteq A_4 \supseteq V_4 \supseteq < I >$.

We know that $A_4 \Delta S_4$, $V_4 \Delta A_4$ and $< I > \Delta V_4$.

Here, $o(S_4/A_4) = 2 \Rightarrow S_4/A_4$ is cyclic and so abelian.

$o(A_4/V_4) = 3 \Rightarrow A_4/V_4$ is cyclic and so abelian.

and $o(V_4/< I >) = 4 = 2^2 \Rightarrow V_4/< I >$ is cyclic and so abelian.

So, the above series is a solvable series for S_3 and hence S_3 is solvable.

3.4.13. Lemma. If a subgroup G of S_n (n > 4) contains all 3-cycles and H be any normal subgroup of G such that G/H is abelian. Then H contains all 3-cycles in G.

Proof. Given H is a normal subgroup of G. Consider the quotient group G/H and canonical homomorphism $\phi : G \to G/H$ given by

$$\phi(\sigma) = \sigma H \quad \text{for all } \sigma \in G.$$

We know that for this homomorphism, ϕ is onto and $\ker \phi = H$.

Let $\sigma, \eta \in G$ then σ and η are permutations in S_n. We compute,

$$\begin{aligned}
\phi(\sigma^{-1}\eta^{-1}\sigma\eta) &= \phi(\sigma^{-1})\phi(\eta^{-1})\phi(\sigma)\phi(\eta) \\
&= (\sigma^{-1}H)(\eta^{-1}H)(\sigma H)(\eta H) \\
&= (\sigma^{-1}\sigma H)(\eta^{-1}\eta H) \qquad [\because \text{ G/H is abelian}] \\
&= H.H = H = \text{ Identity of G/H.}
\end{aligned}$$

$\Rightarrow \sigma^{-1}\eta^{-1}\sigma\eta \in \ker \phi$ for all $\sigma, \eta \in G$

$\Rightarrow \sigma^{-1}\eta^{-1}\sigma\eta \in H$ for all $\sigma, \eta \in G$

Now, let $(i\ j\ k)$ be any 3-cycle in G. We shall prove that $(i\ j\ k) \in H$.

Since n > 4, so we can find l and m such that both do not belong to the set $\{i, j, k\}$. Let $\sigma = (i\ k\ l)$ and $\eta = (j\ k\ m)$ be any two elements in G. Then

$$\sigma^{-1}\eta^{-1}\sigma\eta = (i\ k\ l)^{-1}(j\ k\ m)^{-1}(i\ k\ l)(j\ k\ m)$$
$$= (i\ l\ k)(j\ m\ k)(i\ k\ l)(j\ k\ m) = (i\ j\ k) \in H$$

But $(i\ j\ k)$ was an arbitrary 3-cycle in G and hence H contains all 3-cycles of G.

3.4.14. Theorem. The group S_n is not solvable for n > 4.

Proof. Let, if possible, S_n (n > 4) is solvable and let

$$S_n = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$$

be a solvable series for S_n. Then, we have

(i) $G_{i+1} \Delta G_i,\ 0 \le i \le r-1$

(ii) G_i / G_{i+1} is abelian, $0 \le i \le r-1$.

Here, $G_0 = S_n$ and so G_0 contains all the 3-cycles. Now, since $G_1 \Delta G_0$ and G_0/G_1 is abelian and so by above lemma G_1 contains all 3-cycles in S_n. Again, G_1 is a subgroup of S_n containing all the 3-cycles and $G_2 \Delta G_1$ and G_1/G_2 is abelian and so by above lemma G_2 contains all 3-cycles in S_n. Continuing like this, we get $G_r = < I >$ contains all 3-cycles of S_n which is absurd. Therefore, S_n (n > 4) is not solvable.

3.4.15. Theorem. A finite group G is said to be solvable iff there exists a sequence of subgroups $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = < e >$ such that

(i) $G_{i+1} \Delta G_i,\ 0 \le i \le n-1$

(ii) G_i / G_{i+1} is cyclic group of prime order for $0 \le i \le n-1$.

Proof. Let G be a solvable group and

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$$

be a solvable series for G. Since G is finite, so each subgroup and its quotient group is finite. In particular, G_i / G_{i+1} is finite and abelian also.

If G_i / G_{i+1} is cyclic group of prime order, then we have nothing to prove.

If G_i/G_{i+1} is not cyclic group of prime order, then it has a proper subgroup, say $\bar{H}$. But then $\bar{H} = H/G_{i+1}$ for some subgroup H of G_i. Since $\bar{H}$ is a proper subgroup of G_i/G_{i+1}, so $H \neq G_i$ and $H \neq G_{i+1}$.

Therefore, we have a subgroup of G such that $G_{i+1} \subseteq H \subseteq G_i$. Then, either $o\left(H/G_{i+1}\right)$ is prime or there exists H' such that H'/G_{i+1} is a proper subgroup of H/G_{i+1}, then

$G_{i+1} \subseteq H' \subseteq H \subseteq G_i$

Since $G_i$is finite, so continuing like this at one stage after a finite number of steps, we get that H_i'/G_{i+1} is a cyclic group of prime order with

$G_{i+1} \subseteq H_i' \subseteq G_i$

for some subgroup H_i' of G_i. So, from the above discussion it follows that we can find subgroups

$G_i \supseteq H_{i0} \supseteq H_{i1} \supseteq \ldots \supseteq H_{im_i} \supseteq G_{i+1}$

such that $H_{i,j+1} \Delta H_{i,j}$ and $H_{i,j}/H_{i,j+1}$ is a cyclic group of prime order for $0 \leq j \leq m$.

Hence, we have a sequence

$G = G_0 = H_{00} \supseteq H_{01} \supseteq \ldots \supseteq H_{0m_0} = G_1 = H_{10} \supseteq H_{11} \supseteq \ldots \supseteq H_{1m_1} = G_2 = H_{20} \supseteq$
$H_{21} \supseteq \ldots \supseteq H_{2m_2} = G_3 \supseteq \ldots \supseteq H_{r-1m_{r-1}} = G_r = <e>$

such that $H_{i,k}/H_{i,k+1}$ is cyclic group of prime order.

Conversely, we know that every cyclic group is an abelian group, so converse is trivial.

3.5. Commutator. Let G be any multiplicative group. Then commutator of two elements x and y of G is the lement $x^{-1}y^{-1}xy$ of G. We denote it by [x, y].

If z is any other element of G, then the commutator of x, y, z is given by

$[x, y, z] = [[x, y], z] = [x^{-1}y^{-1}xy, z] = (x^{-1}y^{-1}xy)^{-1}z^{-1}(x^{-1}y^{-1}xy)z = y^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz$

3.5.1. Proposition. Prove that G is abelian iff [x, y] = e for all x and y in G

Proof. If G is abelian, then

$[x, y] = x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e.e = e.$

Conversely, let [x, y] = e for all x and y in G.

$\Rightarrow x^{-1}y^{-1}xy = e \quad \Rightarrow y^{-1}xy = x \quad \Rightarrow xy = yx$

Thus, G is abelian.

3.5.2. Proposition. $a \in Z(G)$ iff $[a,x] = e$ for all $x \in G$.

Proof. Let $a \in Z(G)$ = centre of G.

Then, [a, x] = $a^{-1}x^{-1}ax = a^{-1}ax^{-1}x$ = e.e =e

Conversely, let [a, x] = e for all $x \in G$.

$\Rightarrow a^{-1}x^{-1}ax = e$ for all $x \in G$

$\Rightarrow ax = xa$ for all $x \in G$

$\Rightarrow a \in Z(G)$.

3.5.3. Commutator Element. The element y of G is said to be a commutator element of G if there exist $a,b \in G$ such that y=[a,b] that is, y= $a^{-1}b^{-1}ab$

3.5.4. Derived Subgroup. The subgroup of G generated by all the commutator of G is called the derived subgroup of G. We denote it by $\delta(G)$ or G', that is,

$\delta(G) = G' = <[x,y] : x,y \in G>$

For example,

$\delta(S_3) = <[x,y] : x,y \in S_3>$

$= <I,(1\ 2\ 3),(1\ 3\ 2)> = \{I,(1\ 2\ 3),(1\ 3\ 2)\}$

$\delta(G)$ is also called first derived subgroup.

3.5.5. Results. (i) Derived subgroup of a group G is a normal subgroup of G.

(ii) A group G is abelian iff $G' = <e>$.

3.5.6. n^{th} Derived Subgroup. Let G be a group, for every non-negative integer n, define $G^{(n)}$ inductively as follows:

$G^0 = G$, $G^{(n+1)} = G^{(n)'}$, the commutator subgroup of $G^{(n)}$.

$G^{(n)}$ is called n^{th}commutator subgroup or n^{th} derived subgroup of G. Thus,

$G^{(n+1)} = G^{(n)'} = \left[G^{(n)}, G^{(n)}\right] = <[x,y] : x,y \in G^{(n)}>$

Thus,

$$G' = [G,G] = < [x,y] : x,y \in G >$$
$$G^{(2)} = [G',G'] = < [x,y] : x,y \in G' >$$
$$G^{(3)} = [G^{(2)},G^{(2)}] = < [x,y] : x,y \in G^{(2)} >$$
. . .
. . .
. . .
$$G^{(n+1)} = [G^{(n)},G^{(n)}] = < [x,y] : x,y \in G^{(n)} >$$

3.5.7. Result. For any group G, G/G' is always abelian. In general, we can say that $G^{(n)}/G^{(n+1)}$ is always abelian.

3.5.8. Theorem. A group G is solvable iff $G^{(n)} = <e>$ for some $n \geq 0$.

Proof. Let G be a solvable group and let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_t = < e >$$

be a solvable series for G such that

(i) $G_{i+1} \Delta G_i,\ 0 \leq i \leq t-1$

(ii) $G_i/G_{i+1},\ 0 \leq i \leq t-1$ is abelian.

To prove the theorem, first we shall prove that $G^{(k)} \subseteq G_k$ for all $0 \leq k \leq t$ by mathematical induction.

If k = 0, then $G^{(0)} \subseteq G_0 \Rightarrow G \subseteq G$ which is true. Thus, result is true for k = 0.

Now, assume that $G^{(k)} \subseteq G_k$ for some k. Then, by definition, we have

$$G^{(k+1)} = G^{(k)'} = [G^{(k)},G^{(k)}] \subseteq [G_k,G_k] = G_k' \qquad \text{---(1)}$$

Again, we claim that $G_k' \subseteq G_{k+1}$.

Here, $G_k' = < [a,b] : a,b \in G_k >$.

Let $[a,b] \in G_k'$. Then, consider

$$[a,b]G_{k+1} = a^{-1}b^{-1}abG_{k+1} = (a^{-1}G_{k+1})(b^{-1}G_{k+1})(aG_{k+1})(bG_{k+1})$$
$$= (a^{-1}G_{k+1})(aG_{k+1})(b^{-1}G_{k+1})(bG_{k+1}) = a^{-1}ab^{-1}bG_{k+1}$$
$$= G_{k+1}$$

$\Rightarrow [a,b] \in G_{k+1}$ for all $a,b \in G_k$

$\Rightarrow G_k' \subseteq G_{k+1}$ ---(2)

By (1) and (2), we obtain

$G^{(k+1)} \subseteq G_{k+1}$

So, result is true for k+1 and hence by induction hypothesis, result is true for all positive integers, that is, $G^{(k)} \subseteq G_k$ for $0 \le k \le t$. In particular, $G^{(t)} \subseteq G_t =< e >$ $\Rightarrow$ $G^{(t)} =< e >$.

Conversely, let $G^{(n)} =< e >$ for some $n \ge 0$. Then, consider the sequence

$$G = G^0 \supseteq G^1 \supseteq G^2 \supseteq ... \supseteq G^n =< e >$$

We claim that this is a solvable series for G. For this we have to prove that

(i) $G^{(i+1)} \Delta G^{(i)}$

(ii) $G^{(i)}/G^{(i+1)}$ is abelian for each *i*.

By definition, we have

$G^{(i+1)} = \left[G^{(i)}, G^{(i)} \right] =< [a,b] : a,b \in G^{(i)} >$

Let $[a,b] \in G^{(i+1)}$ and $c \in G^{(i)}$.

We shall prove that $c^{-1}[a,b]c \in G^{(i+1)}$.

Consider,

$$\begin{aligned} c^{-1}[a,b]c &= c^{-1}a^{-1}b^{-1}abc = c^{-1}a^{-1}cc^{-1}b^{-1}cc^{-1}acc^{-1}bc \\ &= \left(c^{-1}ac\right)^{-1}\left(c^{-1}bc\right)^{-1}\left(c^{-1}ac\right)\left(c^{-1}bc\right) \\ &= \left[c^{-1}ac, c^{-1}bc\right] \end{aligned}$$

Now, $c, a \in G^{(i)} \Rightarrow c^{-1}ac \in G^{(i)}$.

Also, $c, b \in G^{(i)} \Rightarrow c^{-1}bc \in G^{(i)}$.

Therefore, $c^{-1}[a,b]c = \left[c^{-1}ac, c^{-1}bc\right] \in \left[G^{(i)}, G^{(i)}\right] = G^{(i+1)}$.

Hence $G^{(i+1)} \Delta G^{(i)}$.

Now, we prove that $G^{(i)}/G^{(i+1)}$ is abelian.

Let $aG^{(i+1)}, bG^{(i+1)} \in G^{(i)}/G^{(i+1)}$, where $a,b \in G^{(i)}$.

Since $a,b \in G^{(i)}$ $\Rightarrow$ $[a,b] \in G^{(i+1)}$.

$\Rightarrow [a,b]G^{(i+1)} = G^{(i+1)} \quad \Rightarrow a^{-1}b^{-1}abG^{(i+1)} = G^{(i+1)}$

$\Rightarrow \mathrm{b}^{-1}abG^{(i+1)} = aG^{(i+1)} \quad \Rightarrow abG^{(i+1)} = baG^{(i+1)}$

$\Rightarrow \left(aG^{(i+1)}\right)\left(bG^{(i+1)}\right) = \left(bG^{(i+1)}\right)\left(aG^{(i+1)}\right) \quad \Rightarrow G^{(i)}/G^{(i+1)}$ is abelian.

Hence G is a solvable group.

3.5.9. Corollary. $\mathrm{A_n}$ is not solvable for $n \geq 5$ and hence $\mathrm{S_n}$ is also not solvable for $n \geq 5$.

Proof. We know that $\mathrm{A_n}$, $n \geq 5$, is a non-abelian group. So, we can say that $\mathrm{A}_n^{'} \neq < I >$.

Also, we know that $\mathrm{A_n}$, $n \geq 5$, is simple and so its only normal subgroups are $\mathrm{A_n}$ itself and the identity subgroup $<I>$. So, we must have $\mathrm{A}_n^{'} = \mathrm{A}_n$.

$\Rightarrow \left(\mathrm{A}_n^{'}\right)^{'} = \mathrm{A}_n^{'} = \mathrm{A}_n \quad \Rightarrow \mathrm{A}_n^{(2)} = \mathrm{A}_n$

In general, $\mathrm{A}_n^{(k)} = \mathrm{A}_n$ for all integers *k*.

Thus, $\mathrm{A}_n^{(k)} \neq < I >$ for any *k*.Hence $\mathrm{A_n}$ is not solvable.

Now, $\mathrm{A_n}$ is a subgroup of $\mathrm{S_n}$, $\mathrm{S_n}$ is also not solvable for $n \geq 5$, since subgroup of a solvable group is solvable.

3.5.10. Corollary. Let $G \neq < e >$ be a finite group. If G is solvable, then G contains a normal abelian subgroup $H \neq < e >$**.**

Proof. Let G be a solvable group, then by above theorem, for some $k \geq 1$, we have $G^{(k)} = < e >$ and then we have the solvable series

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots \supseteq G^{(k)} = < e >$$

We choose k such that $G^{(k-1)} \neq < e >$. Also, we have $G^{(k-1)}/G^{(k)}$ is abelian.

$\Rightarrow \; G^{(k-1)}$ is abelian .

So, $H = G^{(k-1)}$ is an abelian subgroup of G and $H \neq < e >$**.**

3.6. Lower Central Series. The **lower central series** (or **descending central series**) of a group *G* is the descending series of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_t = < e >$$

where each $G_{n+1} = [G_n, G]$, the subgroup of *G* generated by all commutators $[x, y]$ with *x* in G_n and *y* in *G*. Thus, $G_2 = [G, G] = G^{(1)}$, the derived subgroup of *G*; $G_3 = [[G, G], G]$, etc. The lower central series is often denoted $\gamma_n(G) = G_n$.

This should not be confused with the **derived series**, whose terms are $G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$, not $G_n := [G_{n-1}, G]$. The series are related by $G^{(n)} \subseteq G_n$.

3.7. Upper Central Series. The **upper central series** (or **ascending central series**) of a group G is the sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_t = < e >$$

where each successive group is defined by: $G_{i+1} = \{x \in G : \text{for all } y \in G, [x, y] \in G_i\}$ and is called the ***i*th center** of G (respectively, **second center**, **third center**, etc.). In this case, G_1 is the center of G, and for each successive group, the factor group G_i/G_{i+1} is the center of G/G_i, and is called an **upper central series quotient**.

3.8. Check Your Progress.

1. A group of order 1331 is solvable.
2. If G is a group of order 21, then it is solvable.
3. If G is a group having no proper subgroup, then it is solvable

Answers.

1. Every finite p-group is solvable.
2. A group of order pq is always solvable.
3. Since G has no proper subgroup, so it is a group of prime order and hence solvable.

3.9. Summary. In this chapter, we derived that a finite group is solvable if there exists a subnormal series in which factor groups are cyclic groups of prime order. However, any arbitrary group is solvable if some n^{th} derived subgroup of this group consists of only one element, namely the identity element and the solvability of S_n can be obtained independently or by using this result.

3.10. Exercise

1. A group of order pqr, where p, q, r are primes, not necessarily different, is solvable.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Lanski, C. Concepts in Abstract Algebra, American Mathematical Society, First Indian Edition, 2010.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
5. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
6. Musili, C., Introduction to Rings and Modules, Narosa Publication House, 1994.
7. Jacobson, N., Basic Algebra, Vol. I & II, W.H Freeman, 1980 (also published by Hindustan Publishing Company).
8. Artin, M., Algebra, Prentice-Hall of India, 1991.
9. Macdonald, I. D., The Theory of Groups, Clarendon Press, 1968.

4

NORMAL SERIES

Structure

4.1. Introduction. This chapter contains definition of normal series and its examples. Example of a subnormal series which is not normal is considered. Definition and important properties related to that of a nilpotent group, related to proper normal subgroup and center of a group, subgroup and its normalizer are discussed.

4.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Every subgroup of a nilpotent group is nilpotent.

(ii) Every factor group of a nilpotent group is nilpotent.

(iii) Converse result of these results is not true. But after imposing some condition it can be obtained.

(iv) Every p-group is nilpotent.

(v) S_n is not nilpotent for n > 3.

(vi) Maximal subgroup of a nilpotent subgroup is normal subgroup.

4.1.2. Keywords. Central Series, Center of a Group, Commutator Subgroup.

4.2. Normal Series. A sequence of subgroups $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e >$ of a group G is called a normal series of G if $G_i \ \Delta \ G$ for $1 \leq i \leq r$.

4.2.1. Remark. Every normal series of a group is also a subnormal series for that group. But the converse is not true. For this, consider

$$G = A_4 = \{I,(1\,2\,3),(1\,2\,4),(1\,3\,4),(1\,4\,2),(1\,4\,3),(2\,3\,4),$$
$$(2\,4\,3),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3),(1\,3\,2)\}$$

the alternating group of degree 4.

Let $G_1 = V_4 = \{I,(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$, which is known as the klein's four group. Again, let $G_2 = \{I,(1\,2)(3\,4)\}$.

Now consider the series

$$G = G_0 = A_4 \supseteq G_1 = V_4 \supseteq G_2 \supseteq G_3 = < I >$$

We know that V_4 is a normal subgroup of A_4 and also index of G_2 in G_1 is 2. Hence G_2 is a normal subgroup of G_1. Also, G_3 is a normal subgroup of G_2 as identity subgroup is always a normal subgroup. So, the series assumed is a subnormal series.

To show that it is not a normal series, we shall show that G_2 is not a normal subgroup of G. For this, since $(1\,2\,3) \in G$ and

$$(1\,2\,3)G_2 = \{(1\,2\,3)I,(1\,2\,3)(1\,2)(3\,4)\} = \{(1\,2\,3),(1\,3\,4)\}$$

and $$G_2(1\,2\,3) = \{I(1\,2\,3),(1\,2)(3\,4)(1\,2\,3)\} = \{(1\,2\,3),(2\,4\,3)\}$$

which shows that $G_2(1\,2\,3) \neq (1\,2\,3)G_2$. So, the above series is not a normal series.

4.2.2. Central Series. A sequence of subgroups $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$ of a group G is called a central series of G if

(i) $G_i \;\Delta\; G$ for $1 \le i \le r$

(ii) $G_{i-1}/G_i \;\subseteq Z(G/G_i\;)$ for $1 \le i \le r$.

4.2.3. Nilpotent Group. A group G is said to be nilpotent if it has a central series.

4.2.4. Example. Every abelian group G is nilpotent. The series $G \supseteq < e >$ is a central series, that is $< e > \;\Delta\; G$ and

$$G_0/G_1 \subseteq Z(G/G_1)$$
$$\Rightarrow G_0/< e > \subseteq Z(G/< e >)$$
$$\Rightarrow G \subseteq Z(G)$$
$$\Rightarrow G \subseteq G \qquad [\because \text{ G is abelian therefore, } G = Z(G)]$$

which is true. Hence G is nilpotent.

4.2.5. Exercise. Show that S_3 is not a nilpotent group.

Proof. Here, $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

We know that only proper subgroups of S_3 are

$$H_1 = \{I, (1\ 2)\}, \qquad H_2 = \{I, (1\ 3)\},$$
$$H_3 = \{I, (2\ 3)\}, \qquad A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}.$$

Since H_1, H_2, H_3 are not normal in S_3, so they cannot be the member of central series, if it exists. Further, $A_3 \ \Delta\ S_3$. We consider the series

$$S_3 = G = G_0 \supseteq G_1 = A_3 \supseteq G_2 = < I >$$

We check the condition $G_{i-1}/G_i \subseteq Z(G/G_i)$.

Firstly, for i = 1, $G_0/G_1 \subseteq Z(G/G_1)$ or $S_3/A_3 \subseteq Z(S_3/A_3)$ or $S_3/A_3 \subseteq S_3/A_3$, which is true.

Secondly, for $G_1/G_2 \subseteq Z(G/G_2)$ or $A_3/< I > \subseteq Z(S_3/< I >)$ or $A_3 \subseteq Z(S_3)$ or $A_3 \subseteq < I >$, which is never true.

So, above series is not a central series.

Again, we consider the series

$$S_3 = G = G_0 \supseteq G_1 = < I >$$

In this series, $< I > \ \Delta\ S_3$.

We check the condition $G_{i-1}/G_i \subseteq Z(G/G_i)$ for i = 1.

For this, $G_0/G_1 \subseteq Z(G/G_1)$ or $S_3/< I > \subseteq Z(S_3/< I >)$ or $S_3 \subseteq < I >$, which is not possible. So, this series is also not a central series. So we proved that both possible normal series of S_3 are not central series. Hence S_3 is not nilpotent.

4.2.6. Exercise. Every nilpotent group is solvable.

Proof. Let G be any nilpotent group and

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$$

be a central series of G. then,

(i) $G_i \ \Delta\ G$ for $1 \le i \le r$

(ii) $G_{i-1}/G_i \ \subseteq Z(G/G_i)$ for $1 \le i \le r$.

We shall prove that the above series is a solvable series for G. Since $G_i \Delta G \Rightarrow G_i \Delta G_{i-1}$ for all $1 \le i \le r$. Now,

$$G_{i-1}/G_i \subseteq Z(G/G_i)$$

Since centre of a group is always abelian, so $Z(G/G_i)$ is abelian. Also, every subgroup of an abelian group is abelian. So all factor groups are abelian. So, group G is solvable.

Result. If in a group $\delta(G) \subseteq Z(G)$, that is, derived subgroup is contained in centre of the group, then $G/Z(G)$ is abelian.

4.2.7. Exercise. Any group G with $\delta(G) \subseteq Z(G)$ is nilpotent.

Solution. We consider the series

$$G = G_0 \supseteq G_1 = Z(G) \supseteq G_2 = < e > .$$

We know that $Z(G) \Delta G$ and $< e > \Delta G$.

Now, $G_0/G_1 = G/Z(G)$. But we are given that $\delta(G) \subseteq Z(G)$, so $G/Z(G)$ is abelian. Thus, $Z(G/Z(G)) = G/Z(G)$. Hence $G_0/G_1 \subseteq Z(G/G_1)$ is true.

Again, $G_1/G_2 = Z(G)/< e > = Z(G)$ and $Z(G/G_2) = Z(G/< e >) = Z(G)$.

Therefore, $G_1/G_2 \subseteq Z(G/G_2)$ is true.

So, the above series is a central series for G and hence G is nilpotent.

4.2.8. Definition. Let *H* and *K* be two subgroups of *G*. Then, commutator subgroup generated by *H* and *K* is denoted by

$$[H,K] = \langle [h,k] : h \in H, k \in K \rangle .$$

Remark. If $A \subseteq Z(G)$, then $ab = ba$ for all $a \in A, b \in G$.

4.2.9. Theorem. Let $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e >$ be a normal series for G. This series is a central series iff $[G_{i-1}, G] \subseteq G_i$, $1 \le i \le r$ or $G_{i-1}/G_i \subseteq Z(G/G_i)$ iff $[G_{i-1}, G] \subseteq G_i$, $1 \le i \le r$.

Proof. Suppose that the series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r = < e >$$

is a central series for *G*. Then, by definition, $G_i \Delta G$ and $G_{i-1}/G_i \subseteq Z(G/G_i)$ for $1 \le i \le r$.

Since $G_{i-1}/G_i \subseteq Z(G/G_i)$

$\Rightarrow \quad aG_i.bG_i = bG_i.aG_i \quad$ for all $a \in G_{i-1}, b \in G$

$\Rightarrow \quad abG_i = baG_i$

$\Rightarrow \quad a^{-1}b^{-1}abG_i = G_i$

$\Rightarrow \quad a^{-1}b^{-1}ab \in G_i$

$\Rightarrow \quad [a,b] \in G_i$

$\Rightarrow \quad \langle [a,b] : a \in G_{i-1}, b \in G \rangle \subseteq G_i$

$\Rightarrow \quad [G_{i-1}, G] \subseteq G_i$

Conversely, let $[G_{i-1}, G] \subseteq G_i$

We shall prove that $G_{i-1}/G_i \subseteq Z(G/G_i)$.

Now, let $aG_i \in G_{i-1}/G_i$, where $a \in G_{i-1}$ and $bG_i \in Z(G/G_i)$, where $b \in G$.

Further $[a,b] \in [G_{i-1}, G] \subset G_i$

$\Rightarrow \quad a^{-1}b^{-1}ab \in G_i \quad \Rightarrow \quad a^{-1}b^{-1}abG_i = G_i \quad \Rightarrow \quad abG_i = baG_i$

$\Rightarrow \quad aG_ibG_i = bG_iaG_i \quad \Rightarrow \quad G_{i-1}/G_i \subseteq Z(G/G_i)$

4.2.10. Theorem. Every subgroup of a nilpotent group is nilpotent.

Proof. Let G be a nilpotent group and let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$$

be a central series for G such that

(iii) $G_i \Delta G, \ 1 \le i \le r$

(iv) $[G_{i-1}, G] \subset G_i, \ 1 \le i \le r$.

Let H be any subgroup of G and let $H_i = H \cap G_i, \ 0 \le i \le r$, then consider the series

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_r = < e > \qquad (1)$$

of subgroups of H.

We claim that the series (1) is a central series for H.

First we prove that $H_i \Delta H, \ 1 \le i \le r$.

Let $x \in H_i$ and $y \in H$. Then $x \in H \cap G_i \Rightarrow x \in H$ and $x \in G_i$.

Since $G_i \Delta G$, thus $x \in G_i, \ y \in H \subset G \Rightarrow y^{-1}xy \in G_i$ and $x, y \in H \Rightarrow y^{-1}xy \in H$. Therefore, $y^{-1}xy \in H \cap G_i = H_i$ and so $H_i \Delta H, \ 1 \le i \le r$.

Now, we shall prove that $[H_{i-1}, H] \subset H_i$, $1 \le i \le r$.

Let $[x, y] \in [H_{i-1}, H]$.

Now $x \in H_{i-1} = H \cap G_{i-1} \Rightarrow x \in H$ and $x \in G_{i-1}$ and $y \in H \subset G$.

So we can say that $[x, y] \in [G_{i-1}, G] \subset G_i$ [By (ii) of given]

Also, $x \in H, y \in H \Rightarrow x^{-1}y^{-1}xy \in H \Rightarrow [x, y] \in H$.

Therefore, $[x, y] \in G_i, [x, y] \in H \Rightarrow [x, y] \in G_i \cap H = H_i$.

$\Rightarrow \langle [x, y] : x \in H_{i-1}, y \in H \rangle \subseteq H_i$

$\Rightarrow [H_{i-1}, H] \subseteq H_i$

It shows that (*) is a central series for H.

4.2.11. Theorem. Every quotient group of a nilpotent group is nilpotent.

-OR- Let G be a nilpotent group and H be a normal subgroup of G, then G/H is also nilpotent.

Proof. Let G be a nilpotent group and let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e >$$

be a central series for G such that

(iii) $G_{i+1} \Delta G$, $1 \le i \le r$

(iv) $[G_{i-1}, G] \subset G_i$, $1 \le i \le r$.

Now consider the series

$$GH/H = G_0H/H \supseteq G_1H/H \supseteq G_2H/H \supseteq \ldots \supseteq G_rH/H = < H >.$$

$$G/H = G_0H/H \supseteq G_1H/H \supseteq G_2H/H \supseteq \ldots \supseteq G_rH/H = < H > \qquad (*)$$

We claim that this series is a central series for G/H, that is (i) $G_iH/H \Delta G/H$ and (ii) $[G_{i-1}H/H, G/H] \subseteq G_iH/H$.

Since $H \Delta G$ and G_i is a subgroup of G. Therefore, $HG_i = G_iH$.

Thus, G_iH is a subgroup of G of $H \subseteq G_iH$.

Since $H \Delta G \Rightarrow H \Delta G_iH$.

Hence quotient group G_iH/H is well-defined.

To prove (i), let $\alpha \in G_iH/H$ and $\beta \in G/H$.

Therefore, $\alpha = xH$ for some $x \in G_i H$ and $\beta = yH$ for some $y \in G$.

Now, $x \in G_i H \quad \Rightarrow \quad x = g_i h$ for some $g_i \in G_i, h \in H$.

Therefore, $\alpha = xH = g_i hH = g_i H$.

Consider $\beta^{-1}\alpha\beta = (yH)^{-1}(g_i H)(yH) = y^{-1}g_i yH$.

Now, $G_i \ \Delta \ G$ and $g_i \in G_i, y \in G \quad \Rightarrow \quad y^{-1}g_i y \in G_i \subseteq G_i H \quad \Rightarrow \quad \beta^{-1}\alpha\beta \in G_i H/H$.

Thus, $G_i H/H \ \Delta \ G/H$.

To prove (ii), let $[\alpha, \beta] \in [G_{i-1}H/H, G/H]$.

Here, $\alpha \in G_{i-1}H/H \quad \Rightarrow \quad \alpha = xH$ for some $x \in G_{i-1}H$

and $\beta \in G/H \quad \Rightarrow \quad \beta = yH$ for some $y \in G$.

Also, $\alpha = xH = g_{i-1}hH = g_{i-1}H$ for some $g_{i-1} \in G_{i-1}, h \in H$.

Consider,

$$[\alpha, \beta] = (g_{i-1}H)^{-1}(yH)^{-1}(g_{i-1}H)(yH) = (g_{i-1}^{-1}y^{-1}g_{i-1}y)H = [g_{i-1}, y]H \in G_i H/H.$$

For, $[G_{i-1}, G] \subseteq G_i$. Therefore, $[g_{i-1}, y] \in G_i \subseteq G_i H$ for $g_{i-1} \in G_{i-1}, y \in G$.

Therefore, $\langle [\alpha, \beta] : \alpha \in G_{i-1}H/H, \beta \in G/H \rangle \subseteq G_{i-1}H/H$.

Thus, $[G_{i-1}H/H, G/H] \subseteq G_i H/H$.

4.2.12. Corollary. Every homomorphic image of nilpotent group is also nilpotent.

Proof. Let G be a nilpotent group and G' be its homomorphic image, then there exists an onto homomorphism $f : G \to G'$. So, by fundamental theorem of homomorphism

$$G/kerf \cong G'$$

Let $\ker f = H$, then $H \ \Delta \ G$ and $G/H \cong G'$. Now G is given to be nilpotent so by above theorem its quotient group G/H is nilpotent. Therefore, G' being isomorphic to G/H is nilpotent.

4.2.13. Corollary. S_n, $n \geq 3$ is not nilpotent.

Proof. We have proved earlier that S_3 is not a nilpotent group. Now, consider the function $f : S_3 \to S_n$ by

$$f(x) = x \quad \text{for all } x \in S_3$$

where *x*on L.H.S. belongs to S_3 and x on R.H.S. belongs to S_n, where x is represented in one-row representation and fixed elements are skipped.

Here, $f(I) = I, f((1\ 2)) = (1\ 2), f((1\ 3)) = (1\ 3)$ etc. Clearly, f is a homomorphism. Now, since S_3 is not nilpotent so $f(S_3)$ is also not nilpotent which is a subgroup of S_n and so S_n is not nilpotent.

4.2.14. Example. Show that if subgroup and quotient group of a group are nilpotent, then it is not necessary that the group is also nilpotent.

Solution. Consider the symmetric group $G = S_3$. This group is not nilpotent.

Further, let $H = A_3$. Clearly H is a subgroup of G and order of H is 3, a prime number, so H is a cyclic group and thus abelian. Further, we know that every abelian group is nilpotent, therefore, H is nilpotent.

Also, G/H is a subgroup of order 2, so it is also an abelian group and so it is also nilpotent.

4.3. Central Subgroup. A subgroup H is said to be a central subgroup of G if $H \subseteq Z(G)$, that is, H is contained in centre of G. Clearly, any central subgroup of a group is also a normal subgroup.

4.3.1. Theorem. If H is a central subgroup of G. Also, $H \Delta G$, both H and G/H are nilpotent subgroups of G. Then, G must be nilpotent.

Proof. Since H is a nilpotent subgroup. Let

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_t =< e >$$

be a central series for H. Therefore,

(iii) $H_i \Delta H,\ 1 \le i \le t$

(iv) $[H_{i-1}, H] \subseteq H_i,\ 1 \le i \le t$.

Since G/H is also nilpotent, so let

$$G/H = G_0/H \supseteq G_1/H \supseteq G_2/H \supseteq \ldots \supseteq G_r/H =< H >$$

be a central series for G/H. Therefore,

(iii) $G_i/\mathrm{H} \ \Delta\ G/\mathrm{H},\ 1 \le i \le r$

(iv) $[G_{i-1}/H, G/H] \subseteq G_i/H,\ 1 \le i \le r$.

Now consider the series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_t =< e >$$

We claim that this is a central series for G, that is, we are to show that

(i) $G_i \Delta G;\ H_j \Delta G,\ 1 \le i \le r,\ 1 \le j \le t$

(ii) $[G_{i-1}, G] \subseteq G_i,\ [H_{j-1}, G] \subseteq H_j,\ 1 \le i \le r, 1 \le j \le t$.

To prove (i), let $x \in G_i$ and $g \in G$, then $xH \in G_i/H$ and $gH \in G/H$. Since $G_i/H \ \Delta \ G/H$, therefore, $(gH)^{-1}(xH)(gH) \in G_i/H$.

So, $g^{-1}xgH \in G_i/H \quad \Rightarrow \quad g^{-1}xg \in G_i \quad \Rightarrow \quad G_i \ \Delta \ G$ for $1 \le i \le r$.

Now, we prove that $H_i \ \Delta \ G$ for $1 \le i \le t$.

We are given that H is a central subgroup and so $H \subseteq Z(G)$.

Further, $H_i \subseteq H \quad \Rightarrow \quad H_i \subseteq Z(G)$ for $1 \le i \le t$. Therefore, elements of H_i commutes with every element of *G*. Thus,

$$H_i g = gH_i \text{ for } 1 \le i \le t \text{ and for all } g \in G.$$

So, $H_i \ \Delta \ G$ for $1 \le i \le t$.

To prove (ii), we shall prove that $[G_{i-1}, G] \subseteq G_i$, $[H_{j-1}, G] \subseteq H_j$, $1 \le i \le r, 1 \le j \le t$.

Let $[x, y] \in [G_{i-1}, G]$. Then, $x \in G_{i-1}$, $y \in G \quad \Rightarrow \quad xH \in G_{i-1}/H$, $yH \in G/H$.

But we have $[G_{i-1}/H, G/H] \subseteq G_i/H \quad \Rightarrow \quad [xH, yH] \in G_i/H$

$$\Rightarrow \qquad [x, y]H \in G_i/H \qquad \Rightarrow \qquad [x, y] \in G_i$$

$$\Rightarrow \qquad \langle [x, y] : x \in G_{i-1}, y \in G \rangle \subseteq G_i \quad \Rightarrow \quad [G_{i-1}, G] \subseteq G_i$$

Again, let $[x, y] \in [H_{j-1}, G] \quad \Rightarrow \quad x \in H_{j-1}, y \in G$.

Since $x \in H_{j-1} \subseteq H \subseteq Z(G) \quad \Rightarrow \quad x \in Z(G)$.

Thus, $[x, y] = x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e \in H_j \quad \Rightarrow \quad [H_{j-1}, G] \subseteq H_j$.

Hence *G* is a nilpotent group.

4.3.2. Corollary. Every finite p-group is nilpotent.

Proof. Let G be a finite p-group and let $o(G) = p^n$ for some $n \ge 1$.

If n=1, then $o(G) = p$ so G is cyclic. Hence G is abelian and so nilpotent.

So let n > 1 and suppose as our induction hypothesis that result is true for all p-groups with order p^r where r < n.

Now, if G is abelian then result is again true, so let G is non-abelian.

Then, Z(G), the centre of G, is non- trivial by class equation. But we know that $Z(G) \ \Delta \ G$. Now, $o(G) = p^n \ \Rightarrow \ o(Z(G)) = p^s$ for some $s < n$.

Since $Z(G)$ is non-trivial, so $o\big(Z(G)\big) > 1 \Rightarrow s \geq 1$.

Then, $o\big(G/Z(G)\big) = \dfrac{o(G)}{o\big(Z(G)\big)} = p^{n-s} < p^n$.

So, by induction hypothesis, $G/Z(G)$ is nilpotent. Now, $Z(G)$ is abelian, so $Z(G)$ is also nilpotent. Then, by above Theorem, G is nilpotent.

4.3.3. Example. Prove that centre of a nilpotent group G is always non-trivial, where o(G)>1.

Proof. Let G be a nilpotent group and let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e > \qquad (1)$$

be the central series for G. Then, we have

(i) $G_i \ \Delta \ G$ for $1 \leq i \leq r$

(ii) $G_{i-1}/G_i \ \subseteq Z\big(G/G_i\ \big)$ for $1 \leq i \leq r$.

Since o(G)>1, so $G = G_0 \neq \{e\}$, so deleting the repeating subgroups from (1), we may take $G_{r-1} \neq \{e\}$. Using condition (ii) for $i = r$, we have

$$G_{r-1}/G_r \ \subseteq Z\big(G/G_r\big) \quad \Rightarrow \quad G_{r-1} \subseteq Z\big(G\big)$$

But $G_{r-1} \neq \{e\}$, so $Z\big(G\big) \neq \{e\}$.

Hence Z(G), the centre of G is non-trivial.

4.3.4. Result. If H is a subgroup of G such that $[H,G]=\{e\}$, then $H \subseteq Z\big(G\big)$.

Proof. Let $h \in H, g \in G$ be any arbitrary elements.

$$\Rightarrow \ \big[h,g\big] = e \ \Rightarrow \ h^{-1}g^{-1}hg = e \ \Rightarrow \ hg = gh \ \Rightarrow \ h = Z\big(G\big) \ \Rightarrow \ H \subseteq Z\big(G\big).$$

4.3.5. Result. If H is a normal subgroup of G, then $\big[H,G\big] \subseteq H$.

Proof. Let $\big[h,g\big] \in \big[H,G\big]$ be any arbitrary elements. Then,

$$\big[h,g\big] = h^{-1}g^{-1}hg = h^{-1}\big(g^{-1}hg\big) \in H \qquad \big[\because g^{-1}hg \in H \text{ as } H \ \Delta \ G\big].$$

Hence $\big[H,G\big] \subseteq H$.

4.3.6. Theorem. Let G be a non-trivial nilpotent group and H be a non-trivial normal subgroup of G, then $H \cap Z\big(G\big) \neq \{e\}$.

Proof. Since G is a nilpotent group. Let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = < e > \qquad (1)$$

be a central series of G. then,

(i) $G_i \ \Delta \ G$ for $1 \le i \le r$

(ii) $G_{i-1}/G_i \ \subseteq Z\left(G/G_i\right)$ for $1 \le i \le r$.

Deleting the repeated subgroups of this series, we may assume that $G_{r-1} \ne \{e\}$. Now,

$$\left[G_{r-1}, G\right] \subseteq G_r =< e > \quad \Rightarrow \quad \left[G_{r-1}, G\right] =< e > \quad \Rightarrow \quad G_{r-1} \subseteq Z\left(G\right) \qquad (2)$$

We consider the two cases: $H \cap G_{r-1} \ne < e >$ and $H \cap G_{r-1} =< e >$.

If $H \cap G_{r-1} \ne < e >$, then clearly $H \cap Z\left(G\right) \ne \{e\}$ $\quad \left[\because G_{r-1} \subseteq Z\left(G\right), \text{by (2)}\right]$

which is the required result.

Again, if $H \cap G_{r-1} =< e >$, then there exists a positive integer k such that

$$H \cap G_k \ne < e > \text{ and } H \cap G_{k+1} =< e > \qquad (3)$$

Such a positive integer k will surely exist as $H \cap G_{r-1} =< e >$ and $H \cap G_0 = H \ne < e >$.

Now consider $\left[H \cap G_k, G\right] \subseteq \left[G_k, G\right] \subseteq G_{k+1}$ $\quad \left[\because H \cap G_k \subseteq G_k\right]$.

Also, $\left[H \cap G_k, G\right] \subseteq \left[H, G\right] \subseteq H$ $\quad \left[\because H \ \Delta \ G\right]$.

By these two, we get

$$\left[H \cap G_k, G\right] \subseteq H \cap G_{k+1} =< e > \quad \Rightarrow \quad H \cap G_k \subseteq Z\left(G\right)$$

Now, $H \cap G_k \ne < e > \ \Rightarrow \ \left(H \cap G_k\right) \cap Z\left(G\right) = H \cap G_k \ne < e > \ \Rightarrow \ H \cap Z\left(G\right) \ne < e >$

which is the required result.

4.3.7. Theorem. Let G be a nilpotent group and H be a proper subgroup of G, then H is a proper subgroup of its normalizer, that is, $H \subset N\left(H\right)$.

Proof. Since G is nilpotent, so let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r =< e >$$

be a central series of G. then,

(i) $G_i \ \Delta \ G$ for $1 \le i \le r$

(ii) $\left[G_{i-1}, G\right] \subseteq G_i$ for $1 \le i \le r$.

Since $G_r =< e > \subseteq H$ and $H \ne G_0$, so there must exist an integer k such that $G_k \not\subseteq H$ but $G_{k+1} \subseteq H$

Now, $\left[G_k, H\right] \subseteq \left[G_k, G\right] \subseteq G_{k+1} \quad \Rightarrow \quad \left[G_k, H\right] \subseteq H$ ---(1) $\quad \left[\because G_{k+1} \subseteq H\right]$

Since $G_k \not\subseteq H$ so there exists an element x such that $x \in G_k$ and $x \notin H$. Let $h \in H$ be any arbitrary element. Then, $h^{-1} \in H$ and $\left[x, h^{-1}\right] \in \left[G_k, H\right] \subseteq H$. Thus,

$$x^{-1}hxh^{-1} \in H \quad \Rightarrow \quad x^{-1}hxh^{-1}h \in H \quad \Rightarrow \quad x^{-1}hx \in H \quad \Rightarrow \quad x^{-1}Hx \subseteq H$$

Also, $\left[x^{-1}, h^{-1}\right] \in \left[G_k, H\right] \subseteq H \quad \Rightarrow \quad xhx^{-1}h^{-1} \in H \quad \Rightarrow \quad xhx^{-1} \in H \quad \Rightarrow \quad h \in x^{-1}Hx$

$$\Rightarrow \quad H \subseteq x^{-1}Hx$$

Thus, we have $H = x^{-1}Hx \quad \Rightarrow \quad xH = Hx \quad \Rightarrow \quad x \in N(H)$.

But we have assumed that $x \notin H$, so $H \neq N(H)$ and hence $H \subset N(H)$.

4.4. Maximal subgroup. A subgroup H of a group G is called a maximal subgroup if $H \neq G$ and there does not exist any subgroup K of G such that $H \subset K \subset G$.

-OR-

H is said to be a maximal subgroup of G if $H \neq G$ and whenever K is any subgroup of G such that $H \subseteq K \subseteq G$, then $K = H$ or $K = G$.

4.4.1. Corollary. Prove that if a nilpotent group G has a maximal subgroup M, then M is a normal subgroup and G/M is a cyclic group of prime order.

Proof. We know that $M \subseteq N(M) \subseteq G$, where $N(M)$ is normalizer of M. But M is maximal, so $M \neq G$ and either $N(M) = M$ or $N(M) = G$. But by the above theorem $M \neq N(M)$. Therefore, $N(M) = G \quad \Rightarrow \quad M \;\Delta\; G \qquad \left[\because H \;\Delta\; G \text{ iff } N(H) = G\right]$.

Now, we claim that $o(G/M)$ is a prime number.

Let T be any proper subgroup of G/M. Then $T = K/M$, where $K \subseteq G$ and $M \;\Delta\; G$. Since T is proper subgroup, so

$$T \neq G/M \text{ and } T \neq M \quad \Rightarrow \quad K/M \neq G/M \text{ and } K/M \neq M$$
$$\Rightarrow \quad K \neq G \text{ and } K \neq M \qquad \Rightarrow \quad M \subset K \subset G,$$

which is a contradiction, since M is a maximal subgroup.

Hence G/M cannot have proper subgroups. Now, we know that a group having no proper subgroup is a cyclic group of prime order, so G/M is a cyclic group of prime order.

Notation. Set of all Sylow p-subgroups of a group G is denoted by Syl_pG. If we write $G_p \in Syl_pG$, it means G_p is a sylow p-subgroup of G.

4.4.2. Result. If G_p is a sylow p-subgroup, then $N(G_p) = N(N(G_p))$.

4.4.3. Corollary . Let G be a nilpotent group and $G_p \in Syl_p G$, then G_p is a normal subgroup of G.

Proof. We know that if G_p is a sylow p-subgroup, then $N\left(G_p\right) = N\left(N\left(G_p\right)\right)$.

Let, if possible, G_p is not a normal subgroup of G. then,

$$N\left(G_p\right) \neq G, \text{ that is, } N\left(G_p\right) \subset G$$

By above theorem, we know that if G is nilpotent and $H \subset G$, then $H \subset N\left(H\right)$. Taking $H = N\left(G_p\right)$, we have $N\left(G_p\right) \subset N\left(N\left(G_p\right)\right)$

which is a contradiction. Hence G_p is a normal subgroup of G.

4.4.4. Theorem. Direct product of finite set of nilpotent groups is again nilpotent.

Proof. Let $H_1, H_2, \ldots, H_n$ be any finite nilpotent groups.

We have to prove that $H_1 \text{x} H_2 \text{x} \ldots \text{x} H_n$ is also nilpotent.

For this it is sufficient to assume that n = 2.

Let H and K be two nilpotent groups. Then let

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_r = < e >$$

and $$K = K_0 \supseteq K_1 \supseteq K_2 \supseteq \ldots \supseteq K_s = < e >$$

are the central series for the groups H and K respectively.

Now, if $r < s$, then we can assume

$$H_{r+1} = H_{r+2} = \ldots = H_s = < e >$$

and, if $r > s$, then we can assume

$$K_{s+1} = K_{s+2} = \ldots = K_r = < e >$$

to make the lengths of both series equal and so W.L.O.G., we can assume that $r = s$. Now, consider the series

$$H \text{x} K = H_0 \text{x} K_0 \supseteq H_1 \text{x} K_1 \supseteq H_2 \text{x} K_2 \supseteq \ldots \supseteq H_r \text{x} K_r = \left\{\left(e, e\right)\right\}$$

We claim that this series is a central series for HxK.

For this we shall prove that

(i) $H_i \text{x} K_i \ \Delta \ H \text{x} K$ for $1 \leq i \leq r$

(ii) $\left[H_{i-1} \text{x} K_{i-1}, G\right] \subseteq H_i \text{x} K_i$ for $1 \leq i \leq r$

To prove (i), let $\alpha \in H_i \text{x} K_i$ and $\beta \in H \text{x} K$. Then,

$\alpha = (h_i, k_i)$ for some $h_i \in H_i$ and $k_i \in K_i$ and $\beta = (h, k)$ for some $h \in H$ and $k \in K$.

Consider,

$$\beta^{-1}\alpha\beta = (h,k)^{-1}(h_i,k_i)(h,k) = (h^{-1},k^{-1})(h_i,k_i)(h,k) = (h^{-1}h_ih, k^{-1}k_ik)$$

But $h_i \in H_i$, $h \in H$ and $H_i \Delta H \quad \Rightarrow \quad h^{-1}h_ih \in H_i$. Similarly, $k^{-1}k_ik \in K_i$.

Therefore, $\beta^{-1}\alpha\beta = (h^{-1}h_ih, k^{-1}k_ik) \in H_i \text{x} K_i \quad \Rightarrow \quad H_i \text{x} K_i \Delta H \text{x} K$.

To prove (ii), let $[x, y] \in [H_{i-1} \text{x} K_{i-1}, G]$.

Then, $x = (h, k)$, where $h \in H_{i-1}, k \in K_{i-1}$ and $y = (a, b)$ where $a \in H, b \in K$.

Consider,

$$[x,y] = x^{-1}y^{-1}xy = (h,k)^{-1}(a,b)^{-1}(h,k)(a,b) = (h^{-1}a^{-1}ha, k^{-1}b^{-1}kb) = ([h,a],[k,b]).$$

But $h \in H_{i-1}, a \in H \quad \Rightarrow \quad [h,a] \in [H_{i-1}, H] \subseteq H_i$

and $k \in K_{i-1}, \text{b} \in K \quad \Rightarrow \quad [k,b] \in [K_{i-1}, K] \subseteq K_i$.

Therefore, $H_i \text{x} K_i$ and hence $[H_{i-1} \text{x} K_{i-1}, G] \subseteq H_i \text{x} K_i$.

This proves that HxK is a nilpotent group.

For the generalization of the result, we can take $H=H_1 \text{x} H_2 \text{x} \ldots \text{x} H_{n-1}$ and $K=H_n$.

Then, $H \text{x} K = H_1 \text{x} H_2 \text{x} \ldots \text{x} H_n$ is nilpotent.

4.4.5. Note. Direct product is known as direct sum in case of finite sets.

4.5. Exercise.

1. A group G is nilpotent then there exists some non-negative integer n such that the n^{th} derived subgroup of G is the trivial subgroup <e>.

4.6. Check Your Progress:

1. If a group of finite order is nilpotent, then there exists a subnormal series of subgroups for which each factor group is a cyclic group of prime order.
2. If G is a group having no proper subgroup, then it is nilpotent.S

Answers:

1. Every nilpotent group is solvable, apply the result of a finite solvable group.
2. Since G has no proper subgroup, so it is a group of prime order and hence nilpotent.

4.7. Summary. In this chapter, we derived that if a nilpotent group G has a maximal subgroup M, then M is a normal subgroup and G/M is a cyclic group of prime order and if G is a non-trivial nilpotent group, H is a non-trivial normal subgroup of G, then $H \cap Z(G) \neq \{e\}$, which indicates that H contains atleast one element different from identity 'e' which commute with every element of the group.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Lanski, C. Concepts in Abstract Algebra, American Mathematical Society, First Indian Edition, 2010.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
5. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
6. Musili, C., Introduction to Rings and Modules, Narosa Publication House, 1994.
7. Jacobson, N., Basic Algebra, Vol. I & II, W.H Freeman, 1980 (also published by Hindustan Publishing Company).
8. Artin, M., Algebra, Prentice-Hall of India, 1991.
9. Macdonald, I. D., The Theory of Groups, Clarendon Press, 1968.

5

COMPOSITION SERIES

Structure

5.1. Introduction. This chapter contains definition of composition series and its examples. Important results related to composition series like Zassenhaus Lemma, Schrier's Refinement Theorem, Jordan Holder Theorems are discussed.

5.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Every Abelian group having a composition series must be finite.

(ii) Any two subnormal series of a group have equivalent refinements.

(iii) Every finite group must have a composition series.

(iv) All Composition series of a group are equivalent.

5.1.2. Keywords. Composition Series, Refinement of a Subnormal Series, Equivalent Series.

5.2. Maximal Normal Subgroup. A normal subgroup H of a group G is said to be maximal normal subgroup if $H \neq G$ and there does not exist any normal subgroup K of G such that $H \subset K \subset G$. For example, consider

$$S_3 = \{I, (1\ 2), (1\ 3), (3\ 2), (1\ 2\ 3), (1\ 3\ 2)\}$$

Then, $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$

is a maximal normal subgroup of S_3. But $H = \{I, (1\ 2)\}$ is not a maximal normal subgroup of S_3, since H is not normal in G.

5.2.1. Simple Group. If a group G has no proper normal subgroups, that is, if the only normal subgroups of G are {e} and G itself, then G is called a simple group.

5.2.2. Theorem. A subgroup $H\ (\neq G)$ is a maximal normal subgroup of G iff G/H is a simple group.

Proof. Let H be a maximal normal subgroup of G. We shall prove that G/H is simple.

Let, if possible, G/H is not simple. Then, G/H must have a proper normal subgroup, say K/H. Then, $K/H \neq G/H$ and $K/H \neq H$, H Δ K, K Δ G.

$$\Rightarrow K \neq G,\ H \neq K, \text{ H } \Delta \text{ K, K } \Delta \text{ G and H} \subset \text{K} \subset \text{G}$$

which is a contradiction to the fact that H is maximal normal subgroup of G. Hence G/H is a simple group.

Conversely, Let G/H is a simple group. Then, there exists no proper normal subgroup K/H of G/H and hence there exists no proper normal subgroup K of G such that H Δ K. This proves that H is a maximal normal subgroup of G.

5.3. Composition Series. An irredundant series $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n =< e >$ is called a composition series of G if each G_{i+1} is a maximal normal subgroup of G_i or each factor group G_i/G_{i+1} is a simple group.

Clearly, every composition series is a subnormal series. For example, consider the two series

$$S_4 \supset A_4 \supset V_4 \supset < I > \qquad \text{---(1)}$$

and

$$S_4 \supset A_4 \supset V_4 \supset A \supset < I > \qquad \text{---(2)}$$

where $A = \{I, (1\ 2)(3\ 4)\}$. Here, series (1) is only a subnormal series but not a composition series, since $<I>$ is not a maximal normal subgroup of V_4 as $V_4 \supset A \supset < I >$ and $A\ \Delta\ V_4$.

Series (2) is a composition series for S_4. Here, all factor groups $S_4/A_4, A_4/V_4, V_4/A, A/< I >$ are of order 2, 3, 2, 2 (prime) respectively and hence simple.

5.3.1. Lemma. If G is an abelian group having a composition series, then G is finite.

Proof. We know that a non-trivial group having no proper subgroup is a finite cyclic group of prime order. Let G be any simple abelian group, that is, G has no proper normal subgroup, which implies that G has no proper subgroup because all subgroups of an abelian group are always normal. Hence, by above result, G must be a finite cyclic group of prime order. Hence we have proved that a simple abelian group must be a finite cyclic group of prime order.

Now, we are given that G has a composition series. Let it be

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n =< e >$$

Then, each G_i/G_{i+1} is a simple group. But G is abelian. Hence G_i/G_{i+1} is simple abelian group for $0 \le i \le n-1$.

Therefore, by above discussion, each factor group G_i/G_{i+1} must be a finite cyclic group of prime order. We put $i = n-1$. Thus, $G_{n-1}/G_n = G_{n-1}/< e > = G_{n-1}$ must be of prime order.

Let $o(G_{n-1}) = p_{n-1}$.

Let $o(G_{n-2}/G_{n-1}) = p_{n-2}$ for some prime p_{n-2}.

Thus, $\dfrac{o(G_{n-2})}{o(G_{n-1})} = p_{n-2} \quad \Rightarrow \quad o(G_{n-2}) = p_{n-1}p_{n-2}$.

Continuing like this, we get

$o(G) = p_{n-1}p_{n-2}\cdots p_2p_1p_0$, where $o(G_i/G_{i+1}) = p_i$.

Hence G is finite.

5.3.2. Normal Subgroup. A subgroup N of a group G is said to be a normal subgroup of G iff Na = aN for all $a \in G$, that is, right and left cosets are same for every element of G. We denote a normal subgroup N of a group G by $N \underline{\Delta} G$.

5.3.3. Second Theorem of Isomorphism. Let H and K are subgroups of any group G, where $H \underline{\Delta} G$. Then, $K/H \cap K \cong HK/H$.

5.3.4. Lemma. Let H and K be two subgroups of G such that Hk = kH for all $k \in K$. Then, HK is a subgroup of G. H is a normal subgroup of HK and $H \cap K$ is a normal subgroup of K and $K/H \cap K \cong HK/H$.

Proof. Since Hk = kH for all $k \in K$, so HK = KH. We know that HK is a subgroup of G iff KH = HK. Hence HK is a subgroup of G.

Let $x \in HK$ be any arbitrary element.

Then, x = hk for all $h \in H$, $k \in K$.

Also, HK = KH so $x \in HK \Rightarrow x \in KH \Rightarrow x \in kH$

$$\Rightarrow x = kh_1 \text{ for some } h_1 \in H.$$

Then, Hx = Hhk = Hk = kH

and $xH = kh_1H = kH$.

Therefore, Hx = xH for all $x \in HK$.

Hence, $H \Delta HK$.

Now, we prove that $H \cap K$ is a normal subgroup of K.

Let $x \in H \cap K$ and $y \in K$ be any elements.

Since $x \in H \cap K \Rightarrow x \in H$ and $x \in K$.

Now, $x \in K,\ \mathrm{y} \in K \Rightarrow \mathrm{y}^{-1}xy \in K$.

Also, $x \in H,\ \mathrm{y} \in K \Rightarrow yH = Hy \Rightarrow \mathrm{xy} \in Hy = yH$

$$\Rightarrow \mathrm{xy} = yh' \text{ for some } h' \in H \Rightarrow \mathrm{y}^{-1}\mathrm{xy} = h' \text{ for some } h' \in H.$$

Hence $\mathrm{y}^{-1}\mathrm{xy} \in H$.

Therefore, $\mathrm{y}^{-1}\mathrm{xy} \in H,\ \mathrm{y}^{-1}\mathrm{xy} \in K \Rightarrow \mathrm{y}^{-1}\mathrm{xy} \in H \cap K$.

So $H \cap K$ is a normal subgroup of K.

Hence all the conditions of second theorem of isomorphism are satisfied and so

$$K/H \cap K \cong HK/H.$$

5.4. Zassenhaus Lemma (Butterfly Theorem). Let B and C be any two subgroups of a group G and B_0 and C_0 be normal subgroups of B and C respectively, then

$$B_0(B \cap C)/B_0(B \cap C_0) \cong C_0(C \cap B)/C_0(C \cap B_0).$$

Proof. Let $K = B \cap C$ and $H = B_0(B \cap C_0)$. Since $B_0 \,\Delta\, B \Rightarrow B_0 b = bB_0$ for all $b \in B$.

But $K = B \cap C \subseteq B \Rightarrow B_0 k = kB_0$ for all $k \in K$ ---(1)

Now, $C_0 \,\Delta\, C \Rightarrow B \cap C_0 \,\Delta\, B \cap C = K$

$$\Rightarrow B \cap C_0 \,\Delta K \quad \Rightarrow (B \cap C_0)k = k(B \cap C_0) \quad \text{for all } k \in K \qquad \text{---(2)}$$

Consider

$$Hk = B_0(B \cap C_0)k = B_0\left[(B \cap C_0)k\right] = (B_0k)(B \cap C_0)$$
$$= (kB_0)(B \cap C_0) = kB_0(B \cap C_0) = kH.$$

Hence by above lemma

$$HK/H \cong K/H \cap K \qquad \text{---(3)}$$

Now, $$HK = B_0(B \cap C_0)(B \cap C) = B_0(B \cap C) \qquad \text{---(4)}$$

We shall prove that $H \cap K = (C \cap B_0)(B \cap C_0)$.

Let $y \in H \cap K$ be any arbitrary element.

So, $y \in H$ and $y \in K \quad \Rightarrow \; y \in H = B_0(B \cap C_0)$ and $y \in K = B \cap C$.

Now, $y \in H = B_0(B \cap C_0) \quad \Rightarrow \quad y = b_0 b$ for some $b_0 \in B_0,\ b \in B \cap C_0$.

Also, $y \in B \cap C \quad \Rightarrow \quad y = d$ for some $d \in B \cap C$.

Thus, $d = b_0 b \;\Rightarrow\; db^{-1} = b_0$. But $d \in B \cap C \;\Rightarrow\; d \in C$ and $b^{-1} \in B \cap C_0 \subseteq C_0 \subseteq C$

$\Rightarrow \; d \in C$ and $b^{-1} \in C \;\Rightarrow\; db^{-1} \in C \;\Rightarrow\; b_0 \in C$.

Again, $b_0 \in B_0,\ b_0 \in C \;\Rightarrow\; b_0 \in C \cap B_0$.

Therefore, $y = b_0 b \in (C \cap B_0)(B \cap C_0) \;\Rightarrow\; H \cap K \subseteq (C \cap B_0)(B \cap C_0)$ ---(5)

On the other hand, $C \cap B_0 \subseteq C \cap B = B \cap C$ and $B \cap C_0 \subseteq B \cap C$. $[\because C_0 \subseteq C]$

Therefore, $(C \cap B_0)(B \cap C_0) \subseteq B \cap C = K$.

Also, $(C \cap B_0)(B \cap C_0) \subseteq B_0(B \cap C_0) = H$. $[\because C \cap B_0 \subseteq B_0]$

Thus, $(C \cap B_0)(B \cap C_0) \subseteq H \cap K$ ---(6)

From (5) and (6), $H \cap K = (C \cap B_0)(B \cap C_0)$ ---(7)

Using all the values of H, K, HK and $H \cap K$ in (3), we obtain

$$B_0(B \cap C) \Big/ B_0(B \cap C_0) \cong (B \cap C) \Big/ (C \cap B_0)(B \cap C_0). \quad \text{---(8)}$$

Interchanging roles of B and C in (7), we get

$$C_0(C \cap B) \Big/ C_0(C \cap B_0) \cong (C \cap B) \Big/ (B \cap C_0)(C \cap B_0). \quad \text{---(9)}$$

But $B \cap C_0 \;\Delta\; B \cap C$ and $C \cap B_0 \;\Delta\; B \cap C$ $[\because C_0 \;\Delta\; C]$

So, we must have $(C \cap B_0)(B \cap C_0) = (B \cap C_0)(C \cap B_0)$.

By this it is clear that R.H.S. of (8) and (9) are same and hence we get

$$B_0(B \cap C) \Big/ B_0(B \cap C_0) \cong C_0(C \cap B) \Big/ C_0(C \cap B_0).$$

5.5. Refinement of a series. Let G be a group and $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_r =< e >$ be a subnormal series for G. A subnormal series $G = G_0' \supseteq G_1' \supseteq G_2' \supseteq ... \supseteq G_s' =< e >$ is called a refinement of the former series if $\{G_0, G_1, G_2, ..., G_r\} \subseteq \{G_0', G_1', G_2', ..., G_s'\}$.

The refinement is said to be a proper refinement if $\{G_0, G_1, G_2, ..., G_r\} \subset \{G_0', G_1', G_2', ..., G_s'\}$.

5.5.1. Equivalent Series. Two subnormal series

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_n =< e >$$

and $$G' = G_0' \supset G_1' \supset G_2' \supset ... \supset G_n' =< e >$$

of a group G are said to be equivalent or isomorphic if there exists one-one correspondence between (1) and (2) such that corresponding factor groups are isomorphic, that is,

$$G_i / G_{i+1} \cong G_j' / G_{j+1}' \quad \text{for } 0 \le i \le n\text{-}1, 0 \le j \le n\text{-}1.$$

5.5.2. Scherier's Refinement Theorem. Any two subnormal series of a group have equivalent refinements.

Proof. Consider the subnormal series

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_s =< e > \qquad \text{---(1)}$$

and $$G = H_0 \supset H_1 \supset H_2 \supset ... \supset H_t =< e > \qquad \text{---(2)}$$

Then, $G_{i+1} \Delta G_i$ for $0 \le i \le s-1$, and $G_{j+1} \Delta G_j$ for $0 \le j \le t-1$.

We define, $G_{i,j} = G_{i+1}(G_i \cap H_j),\ 0 \le i \le s-1,\ 0 \le j \le t \qquad \text{---(3)}$

and $H_{k,l} = H_{k+1}(H_k \cap G_l),\ 0 \le k \le t-1,\ 0 \le l \le s \qquad \text{---(4)}$

Since $G_{i+1} \Delta G_i$, we must have

$$G_{i+1}(G_i \cap H_j) = (G_i \cap H_j) G_{i+1} \qquad [G_i \cap H_j \subseteq G_i]$$

So, $G_{i,j}$ is a subgroup of G.

Similarly, $H_{k,l}$ is also a subgroup of G.

Now, $H_{j+1} \Delta H_j \Rightarrow G_{i+1}(G_i \cap H_{j+1}) \Delta G_{i+1}(G_i \cap H_j) \Rightarrow G_{i,j+1} \Delta G_{i,j}$.

Similarly, $H_{k,l+1} \Delta H_{k,l}$.

Since $H_t =< e >$ and $H_0 = G$, we have

$$G_{i,t} = G_{i+1}(G_i \cap H_t) = G_{i+1}.< e >= G_{i+1}$$

and $G_{i,0} = G_{i+1}\left(G_i \cap H_0\right) = G_{i+1}\left(G_i \cap G\right) = G_{i+1}G_i = G_i.$

Therefore, $G_{i,t} = G_{i+1},\ G_{i+1,0} = G_{i+1}$ for all $0 \le i \le s-1$ ---(5)

Similarly, $H_{k,s} = H_{k+1},\ H_{k+1,0} = H_{k+1}$ for all $0 \le k \le t-1$ ---(6)

Now, we consider two series

$$G = G_0 = G_{0,0} \supseteq G_{0,1} \supseteq \ldots \supseteq G_{0,t} = G_1 = G_{1,0} \supseteq G_{1,1} \supseteq G_{1,2} \supseteq \ldots \supseteq G_{1,t}$$
$$= G_2 = G_{2,0} \supseteq G_{2,1} \supseteq \ldots \supseteq G_{s-1,0} \supseteq G_{s-1,1} \supseteq \ldots \supseteq G_{s-1,t} = G_s =< e > \quad ---(7)$$

$$G = H_0 = H_{0,0} \supseteq H_{0,1} \supseteq \ldots \supseteq H_{0,s} = H_1 = H_{1,0} \supseteq H_{1,1} \supseteq H_{1,2} \supseteq \ldots \supseteq H_{1,s}$$
$$= H_2 = H_{2,0} \supseteq H_{2,1} \supseteq \ldots \supseteq H_{t-1,0} \supseteq H_{t-1,1} \supseteq \ldots \supseteq H_{t-1,s} = H_t =< e > \quad ---(8)$$

Clearly (7) and (8) have same number of terms (*ts+1*). Also, each of $G_0, G_1, G_2, \ldots, G_s$ occurs in (7). Thus, (7) is a refinement of (1). Similarly (8) is a refinement of (2).

Now, since $G_{r+1} \Delta G_r$ and $H_{k+1} \Delta H_k$, by Zassenhaus Lemma, we have

$$G_{r+1}\left(G_r \cap H_k\right) \Big/ G_{r+1}\left(G_r \cap H_{k+1}\right) \cong H_{k+1}\left(H_k \cap G_r\right) \Big/ H_{k+1}\left(H_k \cap G_{r+1}\right).$$

Thus, $G_{r,k} \Big/ G_{r,k+1} \cong H_{k,r} \Big/ H_{k,r+1}$ for all $0 \le r \le s-1, 0 \le k \le t-1.$

Hence, the refinement (7) and (8) are equivalent because every factor group of (7) is isomorphic to some factor group of (8).

5.6. Jordan Holder Theorem. If a group G has a composition series then all its composition series are pairwise equivalent.

Proof. Let

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_s =< e > \quad ---(1)$$

be a composition series for G.

Suppose $G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_t =< e >$ be a refinement of the series (1). This refinement will be proper if for some *j*, H_j is a not equal to any G_i. Then, we must have for some $i, G_i \supset H_j \supset G_{i+1}.$

Further, we choose *j* to be such that $G_i \not\supset H_{j-1}$. Then, $H_{j-1} \supseteq G_i \supset H_j \supset G_{i+1}.$

But $H_j \Delta H_{j-1} \Rightarrow H_j \Delta G_i$. Also, $G_{i+1} \Delta G_i \Rightarrow G_{i+1} \Delta H_j$. So, H_j becomes a proper normal subgroup of G_i which contains G_{i+1} properly, that is, $G_i \supset H_j \supset G_{i+1}$ and $H_j \Delta G_i$, which is a contradiction, because G_{i+1} is maximal normal subgroup of G_i.

Hence, we get that (1) cannot have a proper refinement and so we can say that any composition series of a group cannot have a proper refinement.

Now, let $G = G_0' \supset G_1' \supset G_2' \supset ... \supset G_n' =< e >$ ---(2)

be another composition series for G.

As (1) and (2) are subnormal series also, so by Scherier's Refinement Theorem, (1) and (2) must have equivalent refinements. But we have proved above that (1) and (2) cannot have proper refinements. Therefore, both of them must be equivalent.

Hence all composition series of a group must be pairwise equivalent as (1) and (2) are any two arbitrary series for G.

5.6.1. Jordan Holder Theorem For Finite Groups.

(i) Every finite group having atleast two elements has a composition series.

(ii) Any two composition series for G are equivalent, that is, if $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_k =< e >$ and $G = H_0 \supset H_1 \supset H_2 \supset ... \supset H_l =< e >$ be two composition series for finite group G, then $k = l$ and for all $0 \le i \le k-1$, $G_i / G_{i+1} \cong H_{\pi(i)} / H_{\pi(i+1)}$ for some permutation π on the set $\{0,1,2,...,k-1\}$, that is $G_i / G_{i+1} \cong H_j / H_{j+1}$ for some j.

Proof. (i) We shall prove the result by induction on order of G. Let $o(G) = n$.

When $n = 2$,then $G = G_0 \supset G_1 =< e >$ is the only composition series for G because $G_0 / G_1 \cong G$ being a cyclic group of prime order is simple. So, the theorem is true for $n = 2$.

As our induction hypothesis, we assume that result is true for all groups of order less than $o(G) = n$, that is, all groups of order less than n has a composition series. We discuss two cases:

Case I. If G is simple, then G has no proper normal subgroup. Consequently, $G = G_0 \supset G_1 =< e >$ is the only composition series for G.

Case II. If G is not simple. Let N be a proper normal subgroup of G. Since G is finite so there exist only finitely many proper normal subgroups of G containing N and let M be one such normal subgroup having largest number of elements. Then, M is a maximal normal subgroup of G. Clearly, G/M is a simple group and $M \ne G$, so $o(M) < n = o(G)$.

Hence, by induction hypothesis, M has a composition series, say

$$M = M_0 \supset M_1 \supset M_2 \supset ... \supset M_t =< e >$$

then M_i / M_{i+1} is a simple group for $0 \le i \le t-1$.

Now consider the series

$$G \supset M = M_0 \supset M_1 \supset M_2 \supset ... \supset M_t =< e > \quad \text{---(1)}$$

Here, G/M is one other extra factor group which is also simple as said above. Hence (1) is a composition series for G.

(ii) Suppose $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_k =< e >$ ---(2)

and $G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_l =< e >$ ---(3)

are two composition series for the finite group G. We shall prove the result by induction.

Let $o(G) = n$ and if $n = 2$, then $G = G_0 \supset G_1 =< e >$ is the only composition series for *G*, so the result is trivial. Hence result is true for all groups of order 2.

As our induction hypothesis, we assume that result is true for all groups of order less than $o(G) = n$.

Let $o(G) = n$. We shall discuss two cases:

Case I. When $G_1 = H_1$. Then,

$G_1 \supset G_2 \supset \ldots \supset G_k =< e >$ ---(4)

and $H_1 \supset H_2 \supset \ldots \supset H_l =< e >$ ---(5)

are two composition series for the groups G_1, whose order is less than $o(G) = n$. So by induction hypothesis series (4) and (5) are equivalent. So, we must have $k - 1 = l - 1 \Rightarrow k = l$ and in series (2) and (3), we also have

$$G_0/G_1 = G/G_1 = G/H_1 = H_0/H_1$$

Hence, series (2) and (3) are equivalent.

Case II. When $G_1 \neq H_1$.

Now, series (2) and (3) are composition series, so G_1 and H_1 are maximal normal subgroups of G, then $K = G_1 \cap H_1$ is a normal subgroup of G_1 as well as H_1. Also, since $G_1 \neq H_1$, so *K* is properly contained in G_1 as well as H_1, that is, $K \subset G_1$ and $K \subset H_1$.

Since G_1 and H_1 are normal subgroups of *G*, so G_1H_1 is also a subgroup of *G* [since HK is a subgroup of G iff HK = KH]. We claim that $G_1H_1 \Delta G$.

Let $x \in G_1H_1$ and $y \in G$, so $x = g_1h_1$ for some $g_1 \in G_1$ and $h_1 \in H_1$.

Consider,

$$y^{-1}xy = y^{-1}g_1h_1y = y^{-1}g_1yy^{-1}h_1y = \left(y^{-1}g_1y\right)\left(y^{-1}h_1y\right) \in G_1H_1 \quad [\because G \Delta G, H \Delta H]$$

Also, $G_1 \subset G_1H_1$ and $H_1 \subset G_1H_1$ $[\because G_1 \neq H_1]$.

Because G_1 and H_1 are maximal normal subgroups of *G* and $G_1H_1 \Delta G$, so we must have $G_1H_1 = G$.

Since every finite group has a composition series so let

$$K = K_0 \supset K_1 \supset K_2 \supset \ldots \supset K_l =< e >$$ ---(*)

be a composition series for the group K.

Now, we consider the series

$$G = G_0 \supset G_1 \supset K = K_0 \supset K_1 \supset K_2 \supset \ldots \supset K_l =< e > \quad \text{---(6)}$$

$$G = H_0 \supset H_1 \supset K = K_0 \supset K_1 \supset K_2 \supset \ldots \supset K_l =< e > \quad \text{---(7)}$$

First, we claim that (6) and (7) are composition series. For this, it is sufficient to prove that G_1/K and H_1/K are simple groups.

$\left[\because K_i/K_{i+1}, G/G_1 \text{ and } G/H_1 \text{ are simple by (2), (3) and (*)}\right]$

By second theorem of isomorphism, we have

$$G_1H_1/H_1 \cong G_1/G_1 \cap H_1 \qquad \left[\because H_1 \Delta G_1H_1\right]$$

$$\Rightarrow \quad G/H_1 \cong G_1/K \qquad \left[\because G_1 = G_1H_1 \ \& \ K = G_1 \cap H_1\right] \quad \text{---(8)}$$

But G/H_1 is simple since (3) is a composition series, so G_1/K must also be simple. Similarly,

$$G_1H_1/G_1 \cong H_1/G_1 \cap H_1 \quad \Rightarrow \quad G/G_1 \cong H_1/K \qquad \text{---(9)}$$

But G/G_1 is simple since (2) is a composition series, so H_1/K must be simple.

By (8) and (9) it is clear that the series (6) and (7) are equivalent because first factor group of (6) is isomorphic to second factor group of (7) and first factor group of (7) is isomorphic to second factor group of (6) and all other factor groups are same.

Now, by case I, series (2) and (6) are equivalent, so $k = m+2$. Again, by case I, series (3) and (7) are equivalent, so $l = m+2$.

Hence, $k = l$. Also, series (6) and (7) are equivalent; therefore, the series (2) and (3) are equivalent.

5.6.2. Exercise.

1. Give example of a group having no composition series.

5.7. Check Your Progress.

1. All the composition series for a group of order 121 are equivalent.

Answers.

1. Directly obtained from Jordan Holder Theorem for finite groups.

5.8. Summary

In this chapter, we derived results for composition series and also derived that every finite group must have a composition series. Also it was discussed that any abelian group having a composition series is always finite. Thus the only possibility for a group having no composition series is an infinite abelian group.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Lanski, C. Concepts in Abstract Algebra, American Mathematical Society, First Indian Edition, 2010.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
5. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
6. Musili, C., Introduction to Rings and Modules, Narosa Publication House, 1994.
7. Jacobson, N., Basic Algebra, Vol. I & II, W.H Freeman, 1980 (also published by Hindustan Publishing Company).
8. Artin, M., Algebra, Prentice-Hall of India, 1991.
9. Macdonald, I. D., The Theory of Groups, Clarendon Press, 1968.

6

MODULES

Structure

6.1. Introduction. In this chapter Module theory is discussed in detail. The concepts of generating sets, rank of a finitely generated module and direct sum of two submodules are detailed.

6.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Simple Modules, Unital Modules, Free Module, Irreducible Module, Quotient Modules.

(ii) Submodules.

(iii) Kernel and Null Space of a homomorphism.

(iv) Schurs' Lemma.

(v) Fundamental Theorem on Finitely Generated Modules.

Keywords. Modules, Submodules, Free Module. Rank.

6.2. Module. Let R be a ring. A non empty set M is said to be a left module R (or a left R - module) if M is an abelian group under an operation '+' such that for every $r \in R$, $m \in M$, there exists a unique element $rm \in M$ subject to the conditions:

(i) r(a+b) = ra+rb

(ii) (r+s)a = ra+sa

(iii) r(sa) =(rs)a

In a similar way, we can define a right R – module by modifying the conditions (i), (ii), (iii) in the above definition in the following manner,

(i) $(a+b)r = ar + br$

(ii) $a(r + s) = ar + as$

(iii) $(ar)\, s = a\,(rs)$

6.2.1. Note. The theory of right R-modules can be developed in same manner as the theory of left R-module . We shall develop here the theory of left R-modules and shall be omitting the adjective left.

6.2.2. Unital R-Module. If R is a ring with unity, then a R – module is said to be unital if

$$1.m = m \text{ for all } m \in M.$$

Remark. If a ring R is a field, then a unital R-Module is a vector space over the field R . So we can say that concept of a module is a generalisation of the concept of a vector space.

6.2.3. Example. Every abelian group G is a module over the ring of integers, Z.

Solution. Let G be an abelian group, the operation in G being denoted by + and identity of G being 0. For any integer n and for element $a \in G$, we define

$$na = a + a + \ldots + a \quad (n\text{-times})$$

Then by closure property $na \in G$.

Now to prove that G is a module over I, we have to prove that

(i) $m(a + b) = (a + b) + (a + b) + \ldots + (a + b)$ (m-times)

$= (a + a + \ldots + a) + (b + b + \ldots + b)$ [$\because$ G is abelian]

$= ma + mb$

(ii) $(m + n)\, a = a + a + \ldots + a$ (m + n times)

$= (a + a + \ldots + a) + (a + a + \ldots + a)$

m- times n- times

$= ma + na$

(iii) $m(na) = na + na + \ldots + na$ (m-times)

$= n(a + a + \ldots + a)$ (m-times)

$= (a + a \ldots + a) + (a + a \ldots + a) + \ldots + (a + a \ldots + a)$ [n-times]

$= a + a + \ldots + a$ (mn - times)

$= (mn)\, a$

Hence G is a module over I.

6.2.4. Exercise.

1. Every ring R is an R – module over itself.

2. Every ring R is an module over its subring S, OR, If R is a ring and S be its subring then R is an S – module.

Remark. With this, we confirm that ring R of real numbers is a Q – module and a Z – module.

3. Every abelian group G is module over the ring of integer Z.

4. Let R be a ring and n be a positive integer. Then $R^n = \{(a_1, a_2, ..., a_n) : a_i \in R\}$ is an R – module under the operations defined by

$$(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$$

and $$r(a_1, a_2, ..., a_n) = (ra_1, ra_2, ..., ra_n)$$

for all $(a_1, a_2, ..., a_n), (b_1, b_2, ..., b_n) \in R^n$ and for all $r \in$ R .

5. (Elementary properties of module) Let R be a ring and M be an R – module. Then for all $a, b, c \in$ M, we have

(i) $a + b = a \Rightarrow b = 0$

(ii) $a + b = 0 \Rightarrow a = -b$

(iii) $a + b = a + c \Rightarrow b = c$

(iv) $b + a = c + a \Rightarrow b = c$

6. Let R be a ring and M be an R – module . Then

(i) $r0 = 0$ for all $r \in$ R

(ii) $0a = 0$ for all $a \in$ M

(iii) $(-r)a = -(ra) = r(-a)$ for all $r \in$ R , $a \in$ M

(iv) $r(a - b) = ra - rb$ for all $r \in$ R , $a, b \in$ M

(v) $(r - s)a = ra - sa$ for all $r, s \in$ R, $a \in$ M .

7. Let R be any ring and λ be a left ideal of R. Let M consist of all cosets a + λ, where a ∈ R, of λ in R Thus, M = { a + λ : a ∈ R} Then, M is an R- module if the two requisite composition are defined as follows:

$$(a + \lambda) + (b + \lambda) = (a + b) + \lambda$$

$$r(a + \lambda) = ra + \lambda$$

Remark. M is written as R- λ or R/λ and is called the difference (or quotient) module of R by λ.

6.2.5. Sub- module. A non – empty subset N of an R – module M is said to be submodule of M if N itself is an R – module under the operations of addition and scalar multiplication as defined for M.

If M is an R-module then M itself and {0} are always submodules of M and are termed as improper submodules. Any submodules of M other than M and {0} are called proper submodule.

6.2.6. Exercise.

1. Let R be a ring and let M be an R – module. A non –empty subset N of M is a submodule of M iff N is additive subgroup of M and is closed under scalar multiplication

Alternatively, A non – empty subset N of R – module M is a submodule of M iff $a-b \in N$ for all $a,b \in N$ and $ra \in N$ for all $a \in N$, $r \in R$.

2. If A and B are two submodule of an R- module M. Then A∩B is also a sub-module of M.

3. Arbitrary intersection of submodules of a module is a submodule.

4. Let $\{M_\lambda\}$ be a family of submodules of module M. Suppose this family is totally ordered or linearly ordered, that is, given $M_{\lambda_1}, M_{\lambda_2} \in \{M_\lambda\}_{\lambda \in \wedge}$ then either $M_{\lambda_1} \subseteq M_{\lambda_2}$ *or* $M_{\lambda_2} \subseteq M_{\lambda_1}$ then $\bigcup_{\lambda \in \wedge} M_\lambda$ is a submodule of M.

5. If M is an R – module and $a \in M$ then the set $Ra = \{ra \ : \ r \in R\}$ is a sub module of M.

6. Let M be an R – module. Define $S = \{ra + ma \ : \ r \in R, m \in Z\}$, Z being the ring of integers, then S is an R – submodule of M containing 'a'.

7. If A and B are submodules of an R-module M, then A+B is also a submodule of M .

6.2.7. Submodule generated by a subset of module. Let M be an R- module and S be a non-empty subset of M. If A is a submodule containing S and is itself contained in every submodule of M containing S, then A is called the submodule of M generated by S.The submodule of M generated by S will be denoted by < S >. It should be noted that < S > is the smallest submodule of M containing S. It can be seen that the intersection of all the submodule of M containing Sis the submodule of M generated by S.

6.2.8. Theorem. The submodule of a unital R- module M generated by a subset S of M consists of all linear combinations of elements in S.

Proof. Let L(S) denote the set of all linear combinations of the elements of S, that is,

$$L(S)= \{r_1a_1 + r_2a_2 + \ldots + r_na_n : a_i \in S, r_i \in R\}$$

First we shall prove that L(S) is a sumodule of M.

Let $a = r_1a_1 + r_2a_2 + \ldots + r_na_n$ and $b = s_1b_1 + s_2b_2 + \ldots + s_nb_n$ be any two elements of L(S), where $r_i, s_i \in R$ and $a_i, b_i \in S$.

We have,

$$a-b = r_1a_1 + r_2a_2 + \ldots + r_na_n + (-s_1)b_1 + (-s_2)b_2 + \ldots + (-s_n)b_n$$

is a linear combination of some elements of S, which implies a-b ∈ S. Thus, L(S) is an additive subgroup of M.

If $r \in R$ and $a = r_1a_1 + r_2a_2 + \ldots + r_na_n \in L(S)$, then

$$ra = r(r_1a_1 + r_2a_2 + \ldots + r_na_n)$$

$$= r(r_1a_1) + r(r_2a_2) + \ldots + r(r_na_n) = rr_1(a_1) + rr_2(a_2) + \ldots + rr_n(a_n)$$

which implies, $ra \in L(S)$, as $rr_1, rr_2, \ldots rr_n \in R$. Hence, L(S) is a submodule of M.

Next, we claim that S is contained in L(S).

Let $a \in S$, then $a \in S$, $1 \in R$, so $a.1 \in L(S)$, or, $a \in L(S)$. Hence S is contained in L(S).

Thus, L(S) is a submodule of M containing S.

Now, if W is any submodule of M containing S,then each element of L(S) must be in W, as W is closed under scalar multiplication & addition.

Therefore, L(S) will be contained in W. Hence, $L(S) = < S >$, that is, L(S) is the smallest submodule generated by S.

6.3. Homomorphism of Modules.

Let M and N be two R-modules. A mapping $T : M \rightarrow N$ is called a homomorphism or module homomorphism if

(i) $T(m_1+m_2) = T(m_1) + T(m_2)$ for all $m_1,m_2 \in M$

(ii) $T(rm) = rT(m)$ for all $m \in M$, $r \in R$

The kernel K(T) of T is defined as

$$K(T) = \{m \in M: T(m) = 0 \text{ where 0 is the additive identity of } N\}$$

8.3.1. Theorem. The kernel of a homomorphism is a submodule.

Proof. Let K(T) be the kernel of homomorphism T of R-module M in to an R-module N, then $K(T) = \{m \in M : T(m) = 0\}$. We are to prove that K(T) is a submodule of M. Since

$$T(0) = 0 \Rightarrow 0 \in K(T) \Rightarrow K(T) \neq \emptyset$$

Let $m_1,m_2 \in K(T) \Rightarrow T(m_1) = 0 = T(m_2)$, then $T(m_1 - m_2) = T(m_1) - T(m_2) = 0 - 0 = 0$

$$\Rightarrow m_1 - m_2 \in K(T)$$

Hence, K(T) is an additive subgroup of M.

Again, $r \in R$ and $m \in K(T) \Rightarrow T(m) = 0$, then $T(rm) = rT(m) \Rightarrow r.0 = 0 \Rightarrow rm \in K(T)$

Hence, K(T) is a submodule of M.

6.3.2. Theorem. The range of a homomorphism is a submodule.

Proof. Let $T: M \rightarrow N$ is a homomorphism where M and N are R-submodules. Then, T(M) is the range of M under T. So, $T(M) = \{T(m) : m \in M\}$.

We claim that T(M) is a submodule of N. Let $T(m_1)$ and $T(m_2)$ be any two element of T(M) where $m_1, m_2 \in M$

We have, $T(m_1 - m_2) = T(m_1) - T(m_2) \Rightarrow T(m_1 - m_2) \in T(M)$ $[\because m_1 - m_2 \in M]$

$\therefore$ T(M) is an addtive subgroup of N.

Let $r \in R$ and $T(m) \in T(M)$ where $m \in M$, then we have $rT(m) = T(rm) \in T(M)$, as $rm \in M$.

Hence T(M) is a submodule of N.

6.3.3. Theorem. Let $T: M \to N$ be a module homomorphism. Then, T is a monomorphism iff $K(T) = \{0\}$

Proof. Let T be homomorphism of an R-module M in to an R-module N and assume that $K(T) = \{0\}$. We claim that T is a monomorphism

If $m_1, m_2 \in M$ such that $T(m_1) = T(m_2)$

$\Rightarrow T(m_1) - T(m_2) = 0 \quad \Rightarrow T(m_1 - m_2) = 0$

$\Rightarrow m_1 - m_2 \in K(T) = \{0\} \quad \Rightarrow m_1 - m_2 = 0$

$\Rightarrow m_1 = m_2 \quad \Rightarrow$ T is one-one

Conversely, suppose that t is one-one

Let $m \in K(T)$ then $T(m) = 0$. We know that $T(0) = 0 \Rightarrow T(m) = T(0) \Rightarrow m = 0$, since T is one-one. Hence Ker T = K(T) = {0}.

6.3.4. Quotient Modules. Let A be any submodule of an R-module M. Then A is an additive abelian subgroup of M. If $m \in M$, then $m + A$ is coset of A in M. Then,

$$M/A = \{ m + A : m \in M \}$$

is an R-module unknown as quotient module with addition and scalar multiplication defined as:

$$(m_1 + A) + (m_2 + A) = (m_1 + m_2) + A$$

and $r(m_1 + A) = rm_1 + A; r \in R, m_1 \in M.$

6.3.5. Exercise.

1. If M is an R-module and N is an R-submodule of M. The mapping $T : M \to M/N$ defined as $T(m) = m + N$ for all $m \in M$. Then, T is an R- homomorphism of M onto M/N and $\ker T = N$.

2. **Fundamental Theorem of Homomorphism on Modules.** If T is a homomorphism of an R-module M onto an R-module N such that ker T = A then N is isomorphic to M/A, that is, $M/\ker T \cong N$.

Hint. To derive it define a mapping $\Psi: M/A \to N$ as $\Psi(m + A) = T(m)$ for all $m \in M$, and then prove that this mapping is an isomorphism.

6.3.6. Cyclic Module. An R-module M is said to be cyclic if there is an element $m_o \in M$ such that every $m \in M$ is of the form $m = rm_o$, where $r \in R$. Also m_o is called a generator of M and we can write $M = \langle m_o \rangle = \{rm_o : r \in R\}$.

6.3.7. Theorem. Let M be a unital R-module and for a fixed element m ∈ M, let A = {rm : r ∈ R}. Then, A is cyclic submodule of M generated by m.

Proof. Let a, b ∈ A Then, a = r_1m and b= r_2m for r_1,r_2 ∈ R. We have

a - b = r_1m - r_2m = (r_1- r_2)m ∈A [∵ r_1- r_2∈ R]

For r ∈ R and a ∈A such that a = r_1m for some r_1∈R

ra = r(r_1m)=(rr_1)m ∈ A [∵ rr_1 ∈R]

=> ra ∈A

Hence, A is a submodule of M. Also 1 ∈ R, so 1.m ∈ A => m ∈ A. Due to the definition of A, we conclude that A is cyclic submodule of M generated by m.

6.3.8. Theorem. If A and B are submodules of M. Then, $A+B/B \cong A/A\cap B$.

Proof. Consider the mapping Ψ: A+ B → $A/A\cap B$ defined by

Ψ(x + y) = x + (A ∩ B) for all x ∈ A, y ∈ B.

(i) **Ψ is well defined.** Let $x_1 + y_1$, $x_2 + y_2$ ∈ A + B are such that

$x_1 + y_1 = x_2 + y_2$ => $x_1 - x_2 = y_2 - y_1$

Since A and B are submodules of M, so x_1, x_2 ∈ A and y_1, y_2 ∈ B => $x_1 - x_2$ ∈ A, $y_2 - y_1$ ∈ B.

Now, $x_1 - x_2 = y_2 - y_1$ => $x_1 - x_2$ ∈ B [∵ $y_2 - y_1$∈B]

and $y_2 - y_1$ ∈ A [∵ $x_1 - x_2$∈A]

=> $x_1 - x_2 = y_2 - y_1$ ∈ A ∩ B

=> $x_1 - x_2$ ∈ A ∩ B

=> x_1 + A ∩ B = x_2 + A ∩ B

=> Ψ(x_1+ y_1) = Ψ(x_2 + y_2)

(ii) **Ψ is a module homomorphism.** Let $x_1 + y_1$, $x_2 + y_2$ ∈ A + B. Then

Ψ[(x_1+y_1) + (x_2+ y_2)] = Ψ[(x_1 +x_2)+(y_1 + y_2)]

=(x_1+ x_2) + A ∩ B= (x_1 + A ∩ B) + (x_2 + A ∩ B)

= Ψ(x_1+y_1) + Ψ (x_2+ y_2)

and Ψ[r(x+y)]= Ψ(rx+ry) = rx + A ∩ B

= r(x + A ∩ B)=r Ψ(x+y)

Therefore, Ψ is a module homomorphism.

(iii) **Ψ is onto.**

Let $x+ A \cap B \in {}^{A}\!/_{A\cap B}$, where $x \in A \Rightarrow x + y \in A+B$ for $y \in B$ and $\Psi(x+y) = x+ A \cap B$

$\Rightarrow \Psi$ is onto.

By Fundamental Theorem of module homomorphism, we have

$$ {}^{A+B}\!/_{\ker\psi} \cong {}^{A}\!/_{A\cap B} \qquad (*)$$

We claim that $\ker \Psi = B$.

By definition, $\ker \Psi = \{x+y : \Psi(x+y)= A \cap B\} = \{x+y : x+A \cap B = A \cap B\}$

$= \{x+y : x \in A \cap B\} = \{x+y : x \in B, y \in B\}$

$= \{z : z \in B\} = B$

Hence by (*), we have ${}^{A+B}\!/_{B} \cong {}^{A}\!/_{A\cap B}$.

6.3.9. Irreducible Module. A R-module having no proper submodule is called an Irreducible module.

6.3.10. Theorem. Prove that any unital, Irreducible R-module is cyclic.

Proof. Let M be any unital irreducible R-module, then the only submodule of M are <0> and M itself. We claim that M is cyclic

If $M = < 0 >$, then obviously M is cyclic. Let $M \neq < 0 >$. Then, there exists atleast one element $m_o \in M$ such that $m_0 \neq 0$.

Let $A = \{rm_o : m_o \in M, r \in R\}$

We shall prove that A is a submodule of M

Let $a, b \in A$, then $a= r_1m_o$ and $b = r_2m_o$ for $r_1, r_2 \in R$ and $m_o \in M$.

We have, $a - b = r_1m_o - r_2m_o = (r_1- r_2)m_o \in A \Rightarrow a - b \in A$

Therefore, A is an additive subgroup of M.

Now let $r \in R$ and $a= r_1m_o \in A$.

Then $ra = r(r_1m_o) = (rr_1)m_o \in A \quad [\because rr_1 \in R]$

$\Rightarrow ra \in A$ for all $r \in R$

$\Rightarrow$ A is submodule of M

As given M is unital module, so $1.m_o = m_o$, where 1 is unity of R.

Since $1 \in R, m_o \in M \Rightarrow 1.m_o \in A \Rightarrow m_o \in A$.

However, $m_o \neq 0$, so $A \neq < 0 >$, but M is irreducible. So we must have A=M.

Since A is cyclic, so M must be cyclic.

6.3.11. Exercise.

1. If λ is a left ideal of R and M is an R-module, then for $m \in M$, $\lambda m=\{xm : x \in \lambda\}$ is a submodule of M.

2. Let M be an R- module. If I is a right ideal of R, then the collection of elements $y \in M$ such that $by = 0$ for all $b \in I$ is a submodule of M.

Hint. Let $A = \{y : y \in M, by = 0 \text{ for all } b \in I\}$, Then A is a submodule of M

6.3.12. Theorem. Suppose that R is a ring with unity and M is a module over R but is not unital. Then, there exists some non-zero m in M such that $rm = 0$ for all $r \in R$.

Proof. Since M is not unital then there exists $m \in M$ such that $1.m \neq m$

$\Rightarrow 1.m - m \neq 0$ But $1.m - m \in M$ [$\because 1.m \in M$ as $1 \in R, m \in M$]

Let $m_0 = 1.m - m \neq 0$

Then $rm_0 = r(1.m - m) = r(1.m) - rm = 0$, that is, $rm_0 = 0$ where $m_0 \neq 0$ for all $r \in R$

In particular, $rm_0 = 0$ for all $r \in R$.

6.3.13. Exercise. If M is an irreducible R- module. Then, either M is cyclic module or for every $m \in M$ and $r \in R$, $rm = 0$.

Solution. Given M is irreducible, that is, $< 0 >$ and M are the only submodules of M.

Let $m \in M$. Consider $N= \{rm : r \in R\}$

We claim that N is a submodule of M

Let $\alpha, \beta \in N \Rightarrow \alpha = r_1m, \beta = r_2m$ for some $r_1, r_2 \in R$. Then $\alpha - \beta = r_1m - r_2m = (r_1 - r_2)m \in N$, as $r_1 - r_2 \in R$. Therefore, N is an additive subgroup of M.

Let $\alpha \in N$ and $r \in R$ then $r\alpha = r(r_1m) = (rr_1)m \in N$. [$\because rr_1 \in R$]

Thus, N is a submodule of M .

$\Rightarrow N = < 0 >$ or $N = M$

If $N = < 0 >$ then $rm=0$ for all $r \in R, m \in M$.

If $N = M$, then $M = \{rm: r \in R, m \in M\}$

$\Rightarrow$ M is a cyclic submodule.

6.3.13. Exercise.

1. Suppose M and N are submodules of a module P over R, then

$$M \cap N = \{0\}$$

iff every element $z \in M+N$ can be uniquely expressible as $z=x+y$ with $x \in M, y \in N$.

2. The necessary and sufficient condition for a module M to be the direct sum of its two submodules M_1 and M_2 are that (i) $M = M_1 + M_2$, (ii) $M_1 \cap M_2 = \{0\}$.

Finitely Generated Module. An R-module M is said to be finitely generated if there exist elements a_1, $a_{2,\ldots,} a_n \in M$ such that every m in M can be written as:

$$m = r_1a_1 + r_2a_2 + \ldots + r_na_n; \qquad r_i\text{'s} \in R$$

Then, $\{a_1, a_{2,\ldots,} a_n\}$ is called the generating set of M.

6.4. Minimal Generating Set. The generating set of a module which has as few elements as possible is called minimal generating set, that is, if we remove even a single element from this set, this set is no longer a generating set.

6.4.1. Rank of a Module. The number of elements in a minimal generating set of module is known as the rank of module.

6.4.2. Fundamental Theorem on Finitely Generated Module.

Let R be a Euclidean ring, then any finitely generated R-module M, is the direct sum of a finite number of cyclic modules.

Proof. We shall prove the theorem by induction on the rank of M. If rank of M is 1, then M is generated by a single element and hence M is cyclic. The theorem is true in this case. Now as an induction hypothesis, we assume that the theorem holds for all R-modules of rank k - 1.

Now consider R-modules M with rank k.

Given any minimal generating set $a_1, a_2, \ldots, a_k$ of M, if any relation of the form

$$n_1a_1 = n_2a_2 = \ldots = n_ka_k = 0,$$

then M is the direct sum of $M_1, M_2, \ldots, M_K$ where each M_i is cyclic generated by a_i and the theorem is proved.

So, let given any minimal generating set $b_1, b_2, \ldots, b_k$ there exists $r_{1,} r_2, \ldots, r_k \in R$ such that $r_1b_1 + r_2b_2 + \ldots + r_kb_k = 0$ but not all of $r_1b_1, r_2b_2, \ldots, r_kb_k$ are zero.

Now among all possible such relations for all minimal generating sets, let s_1 be the element of R with minimum d-value $d(s_1)$ and let the generating set for which it occurs be $a_1, a_2, \ldots, a_k$. Thus we have

$$s_1a_1 + s_2a_2 + \ldots + s_ka_k = 0. \qquad (1)$$

Now, if for any $r_1, r_2, \ldots, r$;

$$r_1a_1 + r_2a_2 + \ldots + r_ka_k = 0, \qquad (2)$$

then we claim that s_1/r_1.

Since $r_1, s_1 \in R$, a Euclidean ring, so there exist $m, t \in R$ with $r_1 = ms_1 + t$, where either $t = 0$ or $d(t) < d(s_1)$.

Multiplying (1), by m and subtracting from (2), we get

$$(r_1 - ms_1)a_1 + (r_2 - ms_2)a_2 + \ldots + (r_k - ms_k)a_k = 0 \quad \Rightarrow \quad ta_1 + (r_2 - ms_2)a_2 + \ldots + (r_k - ms_k)a_k = 0$$

Thus by choice of s_1 we must have $d(s_1) < d(t)$

$$\Rightarrow d(t) \not< d(s_1) \quad \Rightarrow \quad t = 0 \quad \Rightarrow \quad r_1 = ms_1 \quad \Rightarrow \quad s_1/r_1.$$

We further claim that s_1/s_i for i = 2, 3, …, k.

Suppose not, then let s_1 does not divide s_2, so there exists m_2, $t_2 \in R$ such that $s_2 = m_2s_1 + t_2$, where $d(t_2) < d(s_1)$ [if $t_2 = 0$ then s_1/s_2].

Now clearly $a_1' = (a_1 + m_2a_2), a_2, ..., a_k$ generates M.

Consider, $s_1 a_1' + t_2a_2 + s_3a_3 + \ldots + s_ka_k = s_1(a_1 + m_2a_2) + t_2a_2 + s_3a_3 + ... + s_ka_k$

$$= s_1a_1 + (s_1m_2 + t_2)a_2 + s_3a_3 + ... + s_ka_k$$

$$= s_1a_1 + s_2a_2 + s_3a_3 + ... + s_ka_k = 0.$$

Thus, t_2 occurs as a coefficient in some relation among elements of a minimal generating set. so by choice of s_1 we have $d(s_1) < d(t_2)$, which is a contradiction to the statement that

$$d(t_1) < d(s_1) \Rightarrow s_1/s_2 .$$

Similarly it can be proved that s_1/s_i for all i.

Let $s_2 = m_2s_1, s_3 = m_3s_1, ..., s_k = m_ks_1,$ [2(a)]

Now consider the elements $a_1^* = a_1 + m_2a_2 + ... + m_ka_k, a_2, a_3, \ldots, a_k$. Clearly $a_1^*, a_2, ..., a_k$ generate M. Let M_1 be the cyclic submodule of M generated by a_1^* and M_2 be the submodule of M generated by $a_2, ...,a_k$. We claim that $M = M_1 \oplus M_2$ (*)

Since $a_1^*, a_2, ...,a_k$ generate m, so clearly $M = M_1 + M_2$ in order to prove (*) only we have to prove now is that $M_1 \cap M_2 = \{0\}$. For this, let $p \in M_1 \cap M_2$

$\Rightarrow p \in M_1$ and $p \in M_2$

Now, $p \in M_1 \Rightarrow p = r_1 a_1^*,$ for some $r_1 \in R$ [$\because$ M_1 is generated by a_1^*]

Also, $p \in M_2 \Rightarrow p = r_2a_2 + ... + r_ka_k$ for some $r_2, r_3, ..., r_k \in R$

Now we have $r_2 a_1^* = r_2 a_2 + ... + r_ka_k,$

$\Rightarrow r_1 a_1^* - r_2 a_2 + ... + r_ka_k = 0$

$\Rightarrow r_1(a_1 + a_2m_2 + ... + a_km_k) - r_2a_2 - ... - r_ka_k = 0$

$\Rightarrow r_1a_1 + (r_1m_2 - r_2)a_2 + ... + (r_1m_k - r_k)a_k = 0$ (3)

Thus we have obtained a relation between $a_1, a_2, ..., a_k$ in which coefficient of a_1 is r_1. Hence by what we have proved above s_1/r_1. Let $r_1 = ls_1$ where $l \in R$, so we have

$$p = r_1a_1*$$

$$= l[s_1(a_1 + m_2a_2 + ... + m_ks_k)] = l[s_1a_1 + s_1m_2a_2 + \ldots + s_1m_ka_k]$$

$$= l[s_1a_1 + s_2a_2 + ... + s_ka_k] = l(0) = 0.$$

$$\Rightarrow M_1 \cap M_2 = \{0\}$$

and this proves (*), that is, M is direct sum of $M_1 + M_2$. Now, M_2 is generated by $a_2, a_3, ..., a_k$. Thus, rank of M_2 is atmost k - 1. So by induction hypothesis, M_2 is the direct sum of cyclic submodules. Therefore, M is the direct sum of cyclic modules.

6.4.3. Schur's Lemma. If M is an irreducible or simple R-module, then the endomorphism ring End_R (M) is a division ring.

Proof. Let $\emptyset$ ($\neq 0$) $\in End_R(M)$, since $ker\emptyset$ is a submodule of M and $ker\emptyset \neq M$, so $ker\emptyset = \{0\}$, thus $\emptyset$ is one one. Also, the image of $\emptyset(M)$ is an R- submodule of M.

Since $\emptyset \neq 0 \Rightarrow \emptyset(M) \neq 0$.

But M is irreducible $\Rightarrow \emptyset(M) = M \Rightarrow \emptyset$ is onto. Thus $\emptyset$ is one one and onto, hence has an inverse in End_R (M). Hence, we have shown that every non zero element of $End_R(M)$ is invertible. Hence $End_R(M)$ is a division ring.

6.4.4. Free Module. An R-module M is called a free module if M has a basis, that is, there exists a subset S of M such that M is generated by S and S is linearly independent set.

6.4.5. Theorem. Let M be a free module with a basis $\{e_1,e_2,...e_n\}$ then

$$M \cong R^n$$

6.4.6. Annihilator of an element.

Let M be an R-module and x ϵ M. The subset $\{r \epsilon R: rx = 0\}$ is called annihilator of x and is denoted by Ann(x).

6.4.7. Exercise. Ann(x) is a left ideal of R.

6.4.8. Theorem. Suppose 1 ϵ R, then M is a cyclic module iff $M \cong R/I$, where I is a left ideal of R.

Proof. First suppose that M is cyclic R-module, then M = Rx for some x ϵ M

Define a mapping f: R$\rightarrow$M by f(r) = rx

Now we shall show that f is a homomorphism of left R- module

$$f(r + s) = (r + s)x = rx + sx = f(r) + f(s) \qquad \forall\ r, s \epsilon R$$

and $$f(sr) = (sr)x = s(rx) = sf(r) \qquad \forall\ r, s \epsilon R$$

Hence, f is an R-module homomorphism.

We shall prove that f is onto.

Let y ϵ M = Rx. Then, y = rx for some r ϵ R. Now, r ϵ R $\Rightarrow$ f(r) = rx = y. Hence, f is onto.

Thus, by Fundamental Theorem of Homomorphism $R/I \cong M$, where I = ker f is a left ideal of R.

Conversely, suppose that $R/I \cong M$

Let f: $R/I \rightarrow M$ be the given homomorphism. Since 1+I ϵ R/I .

So let f(1+I) = x

Let y ϵ M. Now, f is onto, so there exists r+I ϵ R/I such that f(r+I) = y.

$\Rightarrow$ f(r (1+I)) = y $\Rightarrow$ r f(1+I) = y $\Rightarrow$ rx = y.

Hence y ϵ M $\Rightarrow$ y = rx ϵ Rx $\Rightarrow$ M $\subseteq$ Rx.

Again x ϵ M $\Rightarrow$ Rx $\subseteq$ M.

Hence, M = Rx

$\Rightarrow$ M is a cyclic module.

6.4.9. Theorem. Let R be a ring with unity and M be an R-Module. Then the following conditions are equivalent:

(i) M is a simple R-module.

(ii) Every non-zero element of M generates M.

(iii) $M \cong R/I$ where I is a maximal ideal of R.

Proof. (i) $\Rightarrow$ (ii)

Let M be a simple R- module. Then, {0} and M are the only submodules.

Let x ≠ 0 ϵ M. Since 1 ϵ R and 1x = x ≠ 0, therefore x ϵ Rx = N = < x >

Now, N is a non zero submodule of M and M is simple, so N = M $\Rightarrow$ M = Rx, that is, every non zero element of M generates M.

(ii) $\Rightarrow$ (i)

Suppose that M is generated by every non zero element of M. So let N ≠ {0} be a submodule of N. Take 0 ≠ x ϵ N. Then, by the given condition M = Rx

Now, x ϵ N $\Rightarrow$ Rx $\subseteq$ N, that is, M $\subseteq$ N. Also, N $\subseteq$ M $\Rightarrow$ M = N.

Thus the only non zero submodule of M is M itself. Therefore M must be simple.

(i) $\Rightarrow$ (iii)

Let 0 ≠ x ϵ M then N = Rx is a non zero submodule of M, since M is simple so N = M, that is, M = Rx.

Define a map f : R$\rightarrow$ Rx = M by f(r) = rx, for all r ϵ R

It is easy to see that f is an onto homomorphism (as proved in previous theorem). Then by Fundamental Theorem of Homomorphism for modules, we have

$$R/\ker f \cong M$$

Let I = ker f. Then, I is a module and $R/I = M$.

We shall prove that I is maximal ideal of R.

Suppose J is a left ideal of R such that $I \subseteq J \subseteq R$. Now J/I is a submodule of R/I

Since $R/I \cong M$ and M is simple, therefore, R/I is also simple. But then either J/I is zero submodule or $J/I = R/I$, that is, $J/I = \{I\}$ or $J/I = R/I$.

$\Rightarrow$ J = I or J = R.

Hence, I is a maximal left ideal of R.

(iii) $\Rightarrow$ (i)

Suppose $M \cong R/I$ where I is a maximal ideal of R.

Now, I is a maximal left ideal of R $\Rightarrow$ $I \neq R$.

Now $1 \in R \Rightarrow 1+I \in R/I$ and $1+I \neq I$ (zero of R/I)

By definition,

$$1(1+I) = 1 \cdot 1+I = 1+I \neq I \quad \Rightarrow \quad R(1+I) \neq I \quad \Rightarrow \quad R(R/I) \neq I \quad \Rightarrow \quad RM \neq \{0\}$$

Let N be a submodule of M. Since $M \cong R/I$, so there exists some isomorphism $\phi : M \to R/I$. Then ϕ (N) is a submodule of R/I and precisely of the form J/I where J is a left ideal of R containing I.

Now I is maximal left ideal of R and $I \subseteq J \subseteq R$.

$\Rightarrow$ either J = I, then J/I = I = zero element of R/I.

$\Rightarrow \phi$ (N) = {I}

But ϕ is one one $\Rightarrow$ N = {0}

If J = R, then ϕ (N) = $R/I \cong M \Rightarrow$ N = M

Hence {0} and M are the only submodules of M.

Therefore, M must be simple.

6.4.10. Definition. Let M be an R-module and N be a submodule. We say that N is a direct summand of M if there exists another submodule N' of M such that

$$M = N \oplus N' .$$

6.4.11. Theorem. Let M be an R-module and N be a submodule of M such that M/N is a free R-module then N is a direct summand of M.

Proof. Let $\{x_\lambda + N\}_{\lambda\in\wedge}$ be a basis of M/N over R, where $x_\lambda \in M \ \ \forall\lambda\in\wedge$. Since a basis is linearly independent, therefore this basis will not contain zero element.

Thus, $x_\lambda + N \neq N \ \ \forall\lambda\in\wedge$, that is, $x_\lambda \notin N \quad \forall\lambda\in\wedge$.

Let B = $\{x_\lambda\}_{\lambda\in\wedge} \subseteq M$ and $M' = \langle x_\lambda \rangle_{\lambda\in\wedge}$, that is, M' is a submodule of M generated by B. We shall prove that M = $N \oplus M'$

Let x ϵ M, then x + N ϵ M/N. Now $\{x_\lambda + N\}_{\lambda\in\wedge}$ is a basis of M/N, so there exists $r_1, r_2, \ldots, r_n \in R$ such that

$$x+N = r_1(x_{\lambda_1} + N) + r_2(x_{\lambda_2} + N) + \ldots + r_n(x_{\lambda_n} + N)$$

$$= (r_1 x_{\lambda_1} + N) + (r_2 x_{\lambda_2} + N) + \ldots + (r_n x_{\lambda_n} + N)$$

$$= (r_1 x_{\lambda_1} + r_2 x_{\lambda_2} + \ldots + r_n x_{\lambda_n}) + N$$

$$= \sum_{i=1}^{n} r_i x_{\lambda_i} + N$$

$$\Rightarrow x - \sum_{i=1}^{n} r_i x_i \in N$$

Let $x - \sum_{i=1}^{n} r_i x_i = y, \quad y \in N \qquad \Rightarrow x = y + \sum_{i=1}^{n} r_i x_i \in N + M$.

Thus M = N + M'. Let Z ϵ N ∩ M', then Z ϵ N & Z ϵ M'. Now Z ϵ M' =<B>

$$\Rightarrow Z = t_1 x_{\lambda_1} + t_2 x_{\lambda_2} + \ldots + t_n x_{\lambda_n}, \qquad t_i \in R$$

$$\Rightarrow Z + N = \sum_{i=1}^{n} t_i x_{\lambda_i} + N = \sum_{i=1}^{n} t_i (x_{\lambda_i} + N)$$

$$\Rightarrow \sum_{i=1}^{n} t_i (x_{\lambda_i} + N) = Z + N = N \ [\because Z \in N].$$

Since $\{x_\lambda + N\}_{\lambda\in\wedge}$ is a basis of M/N, therefore, $t_i = 0 \ \ \forall i \qquad 1 \le i \le n$

But then $Z = \sum_{i=1}^{n} t_i x_{\lambda_i} = 0 \qquad \Rightarrow N \bigcap M' = \{0\}$

Now it is clear that $M = N \oplus M'$, that is, N is direct summand of M.

6.4.12. Theorem. Let M_1, M_2 be free submodules of M such that $M_1 + M_2 = M_1 \oplus M_2$, then M_1+M_2 is also a free R-module.

Proof. Now M_1 is a free R-submodule of M, so M has a basis say $\{x_i\}_{i\in I} \subseteq M_1$.

Similarly, M_2 has a basis say $\{y_j\}_{j\in J} \subseteq M_2$

Let $B = \{x_i\}_{i\in I} \cup \{y_j\}_{j\in J}$

Then, $B \subseteq M_1+M_2$ $\quad [\because M_1, M_2 \subseteq M_1+M_2\ ]$

Let $x \in M_1+M_2$, then $x = x'+y'$ where $x' \in M_1$ and $y' \in M_2$. Now $\{x_i\}_{i\in I}$ is a basis of M_1 over R.

$\Rightarrow x'$ is a linear combination of finite number of elements, say $x_1, x_2, \ldots, x_m$, that is,

$$x' = \sum_{k=1}^{m} r_k x_k \ , \quad r_k \in R .$$

Similarly, there exist elements $y_1, y_2, \ldots, y_n$ such that

$$y' = \sum_{t=1}^{n} s_t y_t \ , \quad s_t \in R$$

Therefore, $x = x'+y' = \sum_{k=1}^{m} r_k x_k + \sum_{t=1}^{n} s_t y_t .$

$\Rightarrow M_1+M_2$ is generated by B.

Next, suppose $B = \{z_k\}_{k\in K}$. Let $r_1, r_2, \ldots, r_n$ be such that $r_1 z_{k_1} + r_2 z_{k_2} + \ldots + r_n z_{k_n} = 0$, $z_i \in R$.

Since '+' is commutative, we may assume that $z_{k_1}, z_{k_2}, \ldots, z_{k_m} \in \{x_i\}_{i\in I}$ and

$$z_{k_{m+1}}, z_{k_{m+2}}, \ldots, z_{k_n} \in \{y_j\}_{j\in J} .$$

Hence, $r_1 z_{k_1} + r_2 z_{k_2} + \ldots + r_m z_{k_m} = -(r_{m+1} z_{k_{m+1}} + r_{m+2} z_{k_{m+2}} + \ldots + r_n z_{k_n})$.

$r_1 z_{k_1} + r_2 z_{k_2} + \ldots + r_m z_{k_m} \in M_1$ and $-(r_{m+1} z_{k_{m+1}} + r_{m+2} z_{k_{m+2}} + \ldots + r_n z_{k_n}) \in M_2$.

Hence, $r_1 z_{k_1} + r_2 z_{k_2} + \ldots + r_m z_{k_m} \in M_1 \cap M_2 = \{0\}$, that is, $r_1 z_{k_1} + r_2 z_{k_2} + \ldots + r_m z_{k_m} = 0$.

Similarly $r_{m+1} z_{k_{m+1}} + r_{m+2} z_{k_{m+2}} + \ldots + r_n z_{k_n} = 0$.

Since $\{x_i\}_{i\in I}$ and $\{y_j\}_{j\in J}$ are linearly independent. It follows that $r_i = 0$, $1 \le i \le n$

Hence B is linearly independent.

From this it follows that B is a basis for $M_1 + M_2 = M_1 \oplus M_2$ over R.

Hence $M_1 + M_2$ is a free R-modules.

6.4.13. Theorem. Let R be a commutative ring with unity and e be an idempotent (that is, $e^2 = e$ and $e \neq 0, e \neq 1$). Let M = Re, then M is not a free R-module.

Proof. Since $e \neq 0, e \neq 1$. Thus $\{0\} \subset M \subset R$.

Suppose M is a free R-module. Since M = R e, so M is finitely generated R-module. Thus every basis of M has finite number of elements. Let $\{x_1, x_2, \ldots, x_m\}$ be a basis of M. now $x_i \in M = R\,e$.

$$\Rightarrow x_i = r_i e\ ,\ \ 1 \leq i \leq m,\ \ r_i \in R\ .$$

Since $\{x_1, x_2, \ldots, x_m\}$ is a basis of M, so each $x_i \neq 0 \Rightarrow r_i \neq 0$

Now, $r_2x_1+(-r_1)x_2 = r_2r_1e + (-r_1)r_2e$

$$= r_2r_1e - r_1r_2e = 0 \qquad [\because R \text{ is commutative}]$$

Now $-r_1 \neq 0, r_2 \neq 0 \Rightarrow x_1$ and x_2 are linearly dependent, a contradiction. Therefore, the basis has only one element, namely $x_1 = r_1e$.

Now, $e \neq 0, 1 \Rightarrow 1 - e \neq 0$. $1\text{-}e \in R$, so $(1 - e)x_1 = (1 - e)r_1e = r_1(e - e^2) = r_1(e - e) = 0$.

But $1 - e \neq 0$ and so x_1 is linearly dependent, again a contradiction.

Thus, M is not a free R-module.

6.4.14. Theorem. Let N be a finitely generated free module over a commutative ring R. Then all its basis are finite.

Proof. Suppose N is generated by $\{x_1, x_2, \ldots, x_n\}$ and $\{e_i\}_{i \in \Lambda}$ be a basis of N and let us denote this basis by B. We shall prove that B is a finite set.

Now, $x_i \in N$ and B is a basis of N, so there exists a finite subset B_i of B such that x_i is a linear combination of elements of B_i with coefficients in R.

Let $S = \bigcup_{i=1}^{n} B_i$, then clearly S is finite since each B_i is finite.

Now, B is linearly independent, so S, being a subset of B, is also linearly independent. Let $x \in N$ be any arbitrary element, then

$$x = r_1 x_1 + r_2 x_2 + \ldots + r_n x_n,\ r_i \in R$$

But each x_i is a linear combination of elements of B_i, so x is a linear combination of elements of S. Hence S generates N. Thus, S is a basis of N. Now $S \subseteq B$ and B is also a basis, so we must have

S = B. herefore, B is finite since S is finite.

6.4.15. Theorem. Let N be a finitely generated free module over a commutative ring R. Then all basis of N have the same number of elements.

Proof. Suppose N has two basis containing m and n elements respectively. We shall prove that m = n. Since N is a free module, so we must have (by a previous theorem), that $N \cong R^m$ and $N \cong R^n$

$$\Rightarrow \qquad R^m \cong R^n\ .$$

Let, if possible, m < n.

Let $\phi : R^m \to R^n$ be an isomorphism and since ϕ is one-one and onto, so ϕ is invertible and let $\psi = \phi^{-1}$, then $\psi : R^n \to R^m$ is an isomorphism.

Let $\{e_1, e_2, \ldots, e_n\}$ and $\{f_1, f_2, \ldots, f_n\}$ be standard basis of R^m and R^n respectively.

Now $\phi(e_i) \in R^n$, $1 \le i \le m$, so let us write

$$\phi(e_i) = a_{1i} f_1 + a_{2i} f_2 + \ldots + a_{ni} f_n, \quad 1 \le i \le m$$

that is, we have

$$\begin{aligned}
\phi(e_1) &= a_{11} f_1 + a_{21} f_2 + \ldots + a_{n1} f_n \\
\phi(e_2) &= a_{12} f_1 + a_{22} f_2 + \ldots + a_{n2} f_n \\
&\cdot \qquad\qquad \cdot \qquad\qquad \cdot \\
\phi(e_m) &= a_{1m} f_1 + a_{2m} f_2 + \ldots + a_{nm} f_n
\end{aligned}$$

Then, matrix of $\phi = A = \begin{bmatrix} a_{11} & a_{12} \ldots & a_{1m} \\ a_{21} & a_{22} \ldots & a_{2m} \\ \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} \ldots & a_{nm} \end{bmatrix}_{n \times m.}$

Again, $\psi(f_i) \in R^m$, $1 \le j \le n$, so let us write

$$\psi(f_i) = b_{1j} e_1 + b_{2j} e_2 + \ldots + b_{mj} e_m$$

that is, we have

$$\begin{aligned}
\psi(f_1) &= b_{11} e_1 + b_{21} e_2 + \ldots + b_{m1} e_m. \\
\psi(f_2) &= b_{12} e_1 + b_{22} e_2 + \ldots + b_{m2} e_m \\
&\vdots \qquad \vdots \qquad \vdots \\
\psi(f_n) &= b_{1n} e_1 + b_{2n} e_2 + \ldots + b_{mn} e_m
\end{aligned}$$

$$\text{Matrix of } \psi = B = \begin{bmatrix} b_{11} & b_{12} \ldots b_{1m} \\ b_{21} & b_{22} \ldots b_{2m} \\ \vdots & \vdots \quad \vdots \\ b_{m1} & b_{m2} \ldots b_{mn} \end{bmatrix}_{m \times n.}$$

Now, we see that $\phi : R^m \to R^n$, $\psi : R^n \to R^m$ implies that $\psi\,\phi : R^m \to R^m$ and $\psi\,\phi$ is identity mapping on R^m because $\psi = \phi^{-1}$.

So matrix associated with the mapping $\phi\,\psi$ is identity matrix, but matrix of $\psi\,\phi$ is also given by BA.

Hence, $BA = I_m$ = Identity matrix of $m \times m$.

that is, $\begin{bmatrix} b_{11} & b_{12}\cdots & b_{1n} \\ b_{21} & b_{22}\cdots & b_{2n} \\ \vdots & \vdots & \vdots \\ b_{m1} & b_{m2}\cdots & b_{mn} \end{bmatrix}_{m\times n} \begin{bmatrix} a_{11} & a_{12}\cdots & a_{1m} \\ a_{21} & a_{22}\cdots & a_{2m} \\ \vdots & \vdots & \vdots \\ a_{n1} & a_{n2}\cdots & a_{nm} \end{bmatrix}_{n\times m} = \begin{bmatrix} 1 & 0\cdots & 0 \\ 0 & 1\cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0\cdots & 1 \end{bmatrix}_{m\times m}$

$$\Rightarrow \quad \sum_{k=1}^{m} b_{ik}\, a_{kj} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \qquad (1)$$

Similarly, $AB = I_n$, implies

$$\sum_{k=1}^{m} a_{ik}\, b_{kj} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \qquad (2)$$

Let $A' = [A\ O]$ and $B' = \begin{bmatrix} B \\ O \end{bmatrix}$ be $n\times n$ augmented matrices, where each of the O blocks is a matrix of appropriate size, that is,

$$A' = \begin{bmatrix} a_{11} & a_{12}\cdots & a_{1m} & 0\cdots & 0 \\ a_{21} & a_{22}\cdots & a_{2m} & 0\cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2}\cdots & a_{nm} & 0\cdots & 0 \end{bmatrix}_{n\times n}, \quad B' = \begin{bmatrix} b_{11} & b_{12}\cdots & b_{1n} \\ b_{21} & b_{22}\cdots & b_{2n} \\ \vdots & \vdots & \vdots \\ b_{m1} & b_{m2}\cdots & b_{mn} \\ 0 & 0\cdots & 0 \\ 0 & 0\cdots & 0 \end{bmatrix}_{n\times n}$$

Form these two matrices we note that

$$A'B' = \begin{bmatrix} 1 & 0\cdots & 0 \\ 0 & 1\cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0\cdots & 1 \end{bmatrix}_{n\times n} = I_n \qquad \text{[Using (2)]}$$

and $$B'A' = \begin{bmatrix} 1 & 0\cdots & 0 & 0\cdots & 0 \\ 0 & 1\cdots & 0 & 0\cdots & 0 \\ \vdots & \vdots & & \vdots & \\ 0 & 0\cdots & 1 & 0\cdots & 0 \\ 0 & 0\cdots & 0 & 0\cdots & 0 \\ 0 & 0\cdots & 0 & 0\cdots & 0 \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix} \qquad \text{[Using (1)]}$$

So, we have

$$\det(A'B') = \det(I_n) = 1 \quad \text{and} \quad \det(B'A') = \det\begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix} = 0.$$

$$\Rightarrow \quad \det(A'B') \neq \det(B'A') \qquad \ldots(3)$$

But A' and B' are $n \times n$ matrices over a commutative ring so we must have $\det(A'B') = \det(B'A')$, which is contradicted by (3).

Hence $m \geq n$.

Similarly $n \geq m$.

So, $m = n$, that is, all basis of N have the same number of elements.

6.4.16. Rank. The number of elements in any basis of a finitely generated free module N over a commutative ring R with unity is called the rank of N.

6.4.17. Theorem. Every finitely generated module is a homomorphic image of a finitely generated free module.

Proof. Let N be an finitely generated R-module with generators $x_1, x_2, \ldots, x_n$.

Let $e_1 = (0, 0, \ldots, 1, 0, \ldots, 0)$ be the n-tuple with all entries 0 except the i^{th} place, where the entry is 1. Then, we know that $\{e_1, e_2, \ldots, e_n\}$ are linearly independent over R and generated a free module R^n. Hence R^n is a finitely generated free module. We shall prove that N is homomorphic image of R^n. We define a mapping

$$\phi : R^n \to N \text{ by setting } \quad \phi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} r_i x_i$$

(i) ϕ **is well-defined.** Let $x = \sum_{i=1}^{n} r_i e_i$ and $y = \sum_{i=1}^{n} r_i' e_i$ be two elements of R^n such that $x = y$, that is $\sum_{i=1}^{n} (r_i - r_i')\, e_i = 0 \quad \Rightarrow \quad r_i - r_i' = 0,\ 1 \leq i \leq n$ [Since e_i' are L. I.]

$$\Rightarrow \quad r_i = r_i' ,\ 1 \leq i \leq n \quad \Rightarrow \quad \sum_{i=1}^{n} r_i x_i = \sum_{i=1}^{n} r_i' x_i \quad \Rightarrow \quad \phi(x) = \phi(y).$$

(ii) ϕ **is homomorphism.**

Let $x = \sum_{i=1}^{n} r_i e_i$, $y = \sum_{i=1}^{n} r_i' e_i$ and $r \in R$, then

$$\phi(x + y) = \phi\left(\sum_{i=1}^{n} (r_i + r_i')\, e_i\right) = \sum_{i=1}^{n} (r_i + r_i')\, x_i$$

$$= \sum_{i=1}^{n} r_i x_i + \sum_{i=1}^{n} r_i' x_i = \phi(x) + \phi(y)$$

and $\phi(rz) = \phi\left(\sum_{i=1}^{n} r r_i e_i\right) = \sum_{i=1}^{n} r r_i x_i = r\phi(x)$.

(iii) ϕ **is onto.** Let m = $\sum_{i=1}^{n} r_i x_i$ be any arbitrary element. Then $r_i \in R$ and consider the element

$x = \sum_{i=1}^{n} r_i e_i \in R^n$. Then $\phi(x) = \phi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} r_i x_i = m$. So, x is pre-image of m. Hence ϕ is onto and so, $\phi(R^n) = N$, that is, N is homomorphic image of R^n which is a finitely generated free-module.

6.4.18. Theorem. Every finitely generated module is isomorphic to a quotient group of a finitely generated free module.

Proof. Proof can be obtained by using Theorem 6.4.14 and then using fundamental theorem of module homomorphism

$$R^n / \ker\phi \cong M.$$

Thus, N is isomorphic to a quotient group of finitely generated free-module.

6.4.19. Fundamental Structure Theorem (or Decomposition Theorem) of finitely generated modules over Principal Ideal Domain.

Let R be a PID and let N be any finitely generated R-module, then

$$N \cong R^s \oplus R/Ra_1 \oplus R/Ra_2 \oplus \ldots \oplus R/Ra_r$$

a direct sum of cyclic modules, where a_i's are non zero non-units and a_i / a_{i+1}, i = 1, 2,.., r – 1.

Proof. Since N is a finitely generated R-module and we know that every finitely generated module is isomorphic to a quotient group of a finitely generated free module, so

$$M \cong R^n / K.$$

Now, since R^n is a free R-module, where R is a PID and K is a sub module of R^n, so we must have

$$K \cong R^m, \text{ where } m \leq n.$$

Let ϕ be this isomorphism from R^m to K, that is, $K = \phi(R^m)$. Let $\{e_1, e_2, \ldots, e_m\}$ be a basis of R^m. Let us write

$$\phi(e_1) = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{bmatrix} \in R^n$$

$$\vdots$$

$$\vdots$$

$$\phi(e_m) = \begin{bmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{bmatrix} \in R^n$$

Then, $\phi(R^m) = AR^m$, where $A = (a_{ij})$ is an $n \times m$ matrix. We choose invertible matrices P and Q of order $n \times n$ and $m \times m$ respectively such that

$$PAQ = \text{diag.}((a_1, a_2, \ldots, a_k, 0, 0, \ldots, 0), \text{ where } a_1 | a_2 | \ldots | a_k .$$

Then we have

$$M \cong R^n/K \cong R^n/\phi(R^m) \cong R^n/AR^m \cong R^n/PAQR^m$$

$$= R^n \begin{bmatrix} a_1 & & & & & & \\ & a_2 & & & O & & \\ & & \ddots & & & & \\ & & & \ddots & & & \\ & & & & a_k & & \\ & & & & & 0 & \\ & O & & & & & \ddots \\ & & & & & & & 0 \end{bmatrix} \begin{bmatrix} R \\ R \\ \vdots \\ \vdots \\ R \end{bmatrix}$$

$$= [R \oplus R \oplus \ldots \oplus R]/[Ra_1 \oplus Ra_2 \oplus \ldots \oplus Ra_k]$$

$$\cong R/Ra_1 \oplus R/Ra_2 \oplus \ldots \oplus R/Ra_k \oplus \underbrace{R \oplus \ldots \oplus R}_{(n-k) \text{ times}}$$

By deleting the zero terms on R.H.S., if any (corresponding to those a_i's that are units) and renumbering if necessary we obtain

$$M \cong R/Ra_1 \oplus R/Ra_2 \oplus \ldots \oplus R/Ra_r \oplus R^s .$$

6.4.20. Application to finitely generated abelian groups. Since the ring of integers $\mathbb{Z}$ is a PID and any abelian group is a $\mathbb{Z}$ module, so by above theorem it follows that:

Let A be a finitely generated abelian group, then

$$A \cong \mathbb{Z}^s \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z}$$

where 's' is a non-negative integer and a_i's are non-zero non units in $\mathbb{Z}$ s.t. $a_1 | a_2 | \ldots | a_r$.

6.5. Torsion Element. Let M be an R-module, then an element m of M is said to be a torsion element if $rm=0$ for some nonzero element $r \in R$. The collection of all torsion elements is denoted by M_t or Tor(M), so

$$\text{Tor}(M) = \{m \in M : rm=0 \text{ for some non-zero } r \in R\}.$$

Also, it is known as **Torsion part of the module.** It is the largest torsion submodule of M.

65.1. Exercise. Prove that if R is an integral domain, then Tor(M) is a submodule of M.

6.5.2. Torsion module. A module is said to be a torsion module if its every element is a torsion element.

6.5.3. Torsion free moldule. A module having no non-zero torsion elements is called a torsion-free module or we can say that the only torsion element in a torsion-free module is the zero element, which means that every non-zero element of this module is linearly independent.

Now according to the definition of Torsion part of a module, we can say that M is torsion free if its torsion part M_t is $\{0\}$.

6.5.4. Proposition. For any module M over a commutative integral domain R, the quotient module M/M_t is a torsion free module.

Proof. Let $x + M_t \in M/M_t$ be any arbitrary element. If $x + M_t$ is a torsion element of M/M_t, then $r.(x + M_t) = 0$ for some non-zero $r \in R$ and, therefore, $r.x \in M_t$. So by definition of torsion part of M, there exists some non-zero element $a \in R$ such that $a(r.x) = 0$. Then, $(ra).x = 0$, since R is an integral domain and a, r are non-zero, so ra is also non-zero element of R. Therefore, x is a torsion element of M and thus $x \in M_t$. Hence $x + M_t = M_t$, which is zero element of M/M_t. Hence zero element is the only torsion element of M/M_t and so M/M_t is a torsion free module.

6.5. Check Your Progress.

1. Let M_1, M_2 be free R-module. Then $M=M_1\times M_2$ is also a free module.

2. Q is not free Z-module.

Answers.

1. First prove $M_1\times M_2 \cong M_1 \oplus M_2$. Since direct sum of two free modules is again free module, the result follows.

2. Let M = Q. We know that every abelian group can be treated as Z-module. Thus, Q is a Z-module. Suppose M is a free Z-module. Let $\{x_\lambda\}_{\lambda\in\wedge}$ be a basis of M over Z. Let $x_1, x_2 \in \{x_\lambda\}_{\lambda\in\wedge}$. Suppose

$x_1=\frac{m_1}{n_1}$, $x_2=\frac{m_2}{n_2}$ where $m_1, m_2, n_1, n_2 \in Z$ and $n_1 \neq 0, n_2 \neq 0$.

Now $(n_1m_2)x_1 + (-n_2m_1)(x_2) = n_1m_2 \cdot \frac{m_1}{n_1} - n_2m_1 \cdot \frac{m_2}{n_2} = m_1m_2 - m_1m_2 = 0$, $n_1m_2 \neq 0, -n_2m_1 \neq 0$. Thus x_1, x_2 are linearly dependent, a contradiction. Hence, basis of M contains only a single element, say x.

Suppose $x = \frac{m_1}{n_1}$, where $m_1, n_1 \in Z$. and $n_1 \neq 0$.

Now $\{x\}$ is a basis of M over Z. Thus, every element of M is of the form lx, $l \in Z$.

Take a prime p such that $p > n_1$

Now, $\frac{1}{p} \in M = Q$

$\Rightarrow \frac{1}{p} = l \times \frac{m_1}{n_1}$ for some $l \in Z$.

$\Rightarrow n_1 = lm_1 p \Rightarrow p/n_1$, a contradiction. ($\because$ p > n_1)

Hence, M = Q is not a free Z-module.

6.6. Summary. In this Chapter, we discussed about various properties of modules, structures that become module, their direct sum, rank etc. Also, it was derived that for a finitely generated free module over a commutative ring all basis have same number of elements.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Lanski, C. Concepts in Abstract Algebra, American Mathematical Society, First Indian Edition, 2010.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
5. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
6. Musili, C., Introduction to Rings and Modules, Narosa Publication House, 1994.
7. Jacobson, N., Basic Algebra, Vol. I & II, W.H Freeman, 1980 (also published by Hindustan Publishing Company).
8. Artin, M., Algebra, Prentice-Hall of India, 1991.
9. Macdonald, I. D., The Theory of Groups, Clarendon Press, 1968.

7

NOETHERIAN AND ARTINIAN MODULES

Structure

7.1. Introduction. In this chapter the concept of ascending and descending sequences of submodules, definitions, examples and properties of Noetherian and Artinian Modules are given. Further nil ideal and nilpotent ideals are discussed in detail.

7.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Noetherian Module and equivalent conditions for a module to be Noetherian.

(ii) Artinian Module and equivalent conditions for a module to be Artinian.

(iii) Hilbert Basis Theorem.

(iv) Wedderburn Artin Theorem.

7.1.2. Keywords. Noetherian Module, Artinian Module, Nil Idels, Finitely Generated Module.

7.2. Noetherian and Artinian Modules. Let M be a left R-module and $\{M_i\}_{i \geq 1}$ be a family of submodules of M

1) The family $\{M_i\}_{i \geq 1}$ is called an ascending chain or sequence if

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq ... \subseteq M_n \subseteq M_{n+1} \subseteq ...$$

2) The family $\{M_i\}_{i \geq 1}$ is called a descending chain or sequence if

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq ... \supseteq M_n \supseteq M_{n+1} \supseteq ...$$

7.2.1. Noetherian Module.

An R-Module M is called Noetherian if for every ascending chain

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq ... \subseteq M_n \subseteq M_{n+1} \subseteq ...$$

of submodules of M, there exists a positive integer K such that

$$M_K = M_{K+1} = M_{K+2} = \ldots$$

that is, $M_K = M_{K+i}$, for all $i \geq 0$.

-OR-

Every ascending chain of submodules of M becomes stationary after a finite number of steps.

-OR-

Every properly ascending chain $M_1 \underset{\neq}{\subset} M_2 \underset{\neq}{\subset} M_3 \underset{\neq}{\subset} ...$ of submodules of M terminates after a finite number of steps, that is, every properly ascending chain of sub modules of M is finite.

7.2.2. Theorem. For an R-module M the following conditions are equivalent:

(i) M is Noetherian.

(ii) Every non-empty family of R-modules has a maximal element.

(iii) Every sub-module of M is finitely generated.

Proof : **(i) $\Rightarrow$ (ii)**

Suppose M is Noetherian R-module and let $\rho = \{M_\lambda\}_{\lambda \in \Lambda}$ be a non-empty family of sub-modules of M. Since the family ρ is non-empty so let M_{λ_1} be any member of ρ.

If M_{λ_1} is maximal element, then we are done, otherwise there exist $M_{\lambda_2} \in \rho$ such that

$$M_{\lambda_1} \subsetneq M_{\lambda_2}.$$

Again, if M_{λ_2} is maximal, then we are through, otherwise there exist $M_{\lambda_3} \in \rho$ such that

$$M_{\lambda_2} \subsetneq M_{\lambda_3}.$$

Now, ρ has no maximal element is equivalent to saying that there exists an infinite ascending chain

$$M_{\lambda_1} \subset M_{\lambda_2} \subset M_{\lambda_3} \subset ...$$

of sub-modules of M, which is a contradiction as M is assumed to be Noetherian. Hence the family ρ must have a maximal element.

(ii) $\Rightarrow$ (iii)

We are given that every non-empty family of sub-modules of M has a maximal element. Let N be a sub-module of M and we shall prove that N is finitely generated.

Let, if possible, N is not finitely generated. For any positive integer k let $a_1, a_2, \ldots, a_k \in N$.

Then $N \neq < a_1, a_2, \ldots, a_k >$. Choose $a_{k+1} \in N$ such that $a_{k+1} \notin < a_1, a_2, \ldots, a_k >$.

We then obtain an infinite properly ascending chain

$$< a_1 > \subsetneq < a_1, a_2 > \subsetneq \ldots \subsetneq < a_1, a_2, \ldots, a_k > \subsetneq \ldots$$

of submodules of M.

Let us denote $N_k = < a_1, a_2, \ldots, a_k >$, then $N_1 \subsetneq N_2 \subsetneq \ldots \subsetneq N_k \subsetneq \ldots$

Let family of all these sub-modules be ρ, that is, $\rho = \{N_k\}$, $k \geq 1$, then by the given hypothesis ρ has a maximal element, say L.

Now, $L \in \rho \Rightarrow L = N_m$ for some m. But $L = N_m \subsetneq N_{m+1}$ so L is not a maximal element, a contradiction. Hence N must be finitely generated.

(iii) $\Rightarrow$ (i)

Suppose every submodule of M is finitely generated. We shall prove that M is Noetherian.

Let $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots \subseteq N_k \subseteq N_{k+1} \subseteq \ldots$ be an ascending chain of sub-modules of M.

Consider $N = \bigcup_i N_i$. We claim that N is also a sub-module of M.

Let $x, y \in \bigcup_i N_i$ and $r \in R$. Then $x \in N_r$ and $y \in N_s$ for some integers r and s.

Since either $N_r \subseteq N_s$ or $N_s \subseteq N_r$, therefore both x and y lie in one sub-module N_r or N_s, and hence $x - y$ and rx lie in same sub-module. However, both N_r and N_s are subsets of N, so $x - y, rx \in N$, and hence N is a submodule of M.

Now, by (iii), N is finitely generated. So there exist elements $a_1, a_2, \ldots, a_n \in N$ such that

$N = < a_1, a_2, \ldots, a_n >$. Now for each j, $1 \leq j \leq n$, $a_j \in N = \bigcup_i N_i$

$\Rightarrow \quad a_j \in N_{\lambda_j}$ for some natural number λ_j

Let $k = \max \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$, then clearly $a_j \in N_k$, $1 \leq j \leq n$ that is,, $\quad a_1, a_2, \ldots, a_n \in N_k$

But $N = < a_1, a_2, \ldots, a_n >$, so N is smallest submodule containing $a_1, a_2, \ldots, a_n$.

This implies $N \subseteq N_k$. Also $N_k \subseteq N$. Hence $N = N_k$ and so $N_k = N_{k+1} = N_{k+2} = \ldots$, therefore, M is a Noetherian R-module.

7.2.3. Definition. If the left R-module M is noetherian then M is called a **left-Noetherian module**. Similarly, if a right R-module M is Noetherian then M is called a **right Noetherian module**.

7.2.4. Finitely Co- generated Module.

Let M be a left R- module then M is called finitely co- generated if for any non- empty family $\{M_\lambda\} = £$ of sub modules of M, having $\{0\}$ intersection, that is, if $\bigcap_{\lambda\in\Lambda} M_\lambda = \{0\}$. Then, there exists $\lambda_1, \lambda_2, \ldots, \lambda_n \in \Lambda$ such that $\bigcap_{i-1}^{n} M_{\lambda_i} = \{0\}$.

7.2.5. Artinian Module.

Let M be a left R- module. M is called left- Artinian if for every decreasing chain

$$M_1 \supseteq M_2 \supseteq \ldots \supseteq M_k \supseteq \ldots$$

we have $M_k = M_{k+1} = \cdots = M_{k+l} = \cdots$ for some k $\in$ N, that is, have $M_k = M_{k+i}$ for all $i \geq 0$, that is, every descending chain of sub modules of M becomes stationary after a finite number of steps.

OR

Every properly descending chain of $M_1 \underset{\neq}{\supseteq} M_2 \underset{\neq}{\supseteq} M_3 \ldots \underset{\neq}{\supseteq} M_n \underset{\neq}{\supseteq} \ldots$ of submodules of M is finite.

OR

Every properly descending chain of sub modules of M terminates after a finite number of steps.

7.2.6. Theorem. For an R-module M the following conditions are equivalent:

(i) M is Artinian.

(ii) Every non-empty family of sub-modules of M has a minimal element.

(iii) Every quotient module of M is finitely co-generated.

Proof. (i) $\Rightarrow$ (ii)

Let us suppose that M is Artinian and let $\rho = \{M_\lambda\}_{\lambda\in\Lambda}$ be a non-empty family of sub – modules of M. We shall prove that ρ has a minimal element. Now $\rho \neq \phi$ so there exist $M_{\lambda_1} \in \rho$, then either M_{λ_1} is a minimal element of ρ or there exists $M_{\lambda_2} \in \rho$ such that $M_{\lambda_1} \supsetneq M_{\lambda_2}$.

Again, either M_{λ_2} is a minimal element of ρ or there exists $M_{\lambda_3} \in \rho$ such that

$$M_{\lambda_2} \supsetneq M_{\lambda_3}.$$

If this process continues indefinitely (that is, ρ has no minimal element) then we get an infinite properly descending chain $M_{\lambda_1} \supsetneq M_{\lambda_2} \supsetneq M_{\lambda_3} \ldots$ of sub-modules of M, which is a contradiction since M is given to be Artinian. Hence ρ must have a minimal element.

(ii) $\Rightarrow$ (iii)

Let us suppose that every non-empty family of sub-modules of M has a minimal element. We shall prove that every quotient module of M is finitely co-generated. Let N be a sub-module of M. Consider the quotient module M/N.

Let $\{M_\lambda/N\}_{\lambda \in \Lambda}$ be a family of sub-modules of M/N such that $\bigcap_{\lambda \in \Lambda} (M_\lambda/N) = \{N\}$

Now, $\{N\} = \bigcap_{\lambda \in \Lambda} (M_\lambda/N) = \left(\bigcap_\lambda M_\lambda\right)\Big/N \Rightarrow \bigcap_\lambda M_\lambda = N$ (1)

Let $\rho = \{M_\lambda\}_{\lambda \in \Lambda}$, where M_λ's are sub-modules of M and let

$$\rho' = \{A : A \text{ is the intersection of finite number of sub-modules of } M \text{ in } \rho\}$$

Then clearly $\rho \subseteq \rho'$ *that is,*, $M_\lambda \in \rho' \ \forall \ \lambda \in \Lambda$.

Now ρ' is a family of sub-module of M so by the given condition (ii) it must have a minimal element say, A.

Then, $A = M_{\lambda_1} \cap M_{\lambda_2} \ldots \cap M_{\lambda_n}$, $\lambda_i \in \Lambda$

Let $M_\lambda \in \rho$ be any member, then $A \cap M_\lambda = M_\lambda \cap M_{\lambda_1} \cap M_{\lambda_2} \cap \ldots \cap M_{\lambda_n} \in \rho'$, being finite intersection of members of ρ.

Now $A \cap M_\lambda \subseteq A$. But A is minimal element of ρ' so $A \cap M_\lambda = A$

$\Rightarrow$ $A \subseteq M_\lambda \ \forall \ \lambda \in \Lambda$

$\Rightarrow$ $A \subseteq \bigcap_\lambda M_\lambda = N$ [By (1)]

Again, $N = \bigcap_\lambda M_\lambda \subseteq \bigcap_{i=1}^{n} M_{\lambda_i} = A$. Hence $A = N = \bigcap_{i=1}^{n} M_{\lambda_i}$

Now, $\bigcap_{i=1}^{n} (M_{\lambda_i}/N) = \left(\bigcap_{i=1}^{n} M_{\lambda_i}\right)\Big/N = N/N = \{N\}$.

Hence, there exist a finite sub-family $\{M_{\lambda_i}/N\}_{i=1}^{n}$ of $\{M_\lambda/N\}_{\lambda \in \Lambda}$ such that

$$\bigcap_{i=1}^{n} (M_{\lambda_i}/N) = \{N\}$$

Hence every quotient module of M is finitely co-generated.

(iii) $\Rightarrow$ (i)

Let us suppose that every quotient module of M is finitely co-generated and shall prove that M is Artinian. Let $M_1 \supseteq M_2 \supseteq ... \supseteq M_k \supseteq M_{k+1} \supseteq ...$ be a descending chain of sub-modules of M.

Let $N = \bigcap_i M_i$. Then N is a sub-module of M and $N \subseteq M_i$ for all i. Consider the family $\{M_i/N\}_i$ of sub-modules of M/N. We see that

$$\bigcap_i (M_i/N) = \left(\bigcap_i M_i\right)\Big/N = N/N = \{N\}$$

Since by the given condition (iii), M/N is finitely co-generated therefore there exists a finite sub-family, say, $\{M_{n_i}/N\}_{i=1}^{r}$ of $\{M_i/N\}_i$ such that $\bigcap_{i=1}^{r} M_{n_i}/N = \{N\}$

Let $k = \max. \{n_1, n_2,...,n_r\}$ then

$$\bigcap_{i=1}^{r} M_{n_i} = M_k,$$

since the chain is descending.

Now $\{N\} = \bigcap_{i=1}^{r} (M_{n_i}/N) = \left(\bigcap_{i=1}^{r} M_{n_i}\right)\Big/N = M_k/N$ and so $M_k = N$.

But then $N \subseteq M_{k+j} \subseteq M_k = N$ gives that $M_k = M_{k+1} = M_{k+2} = ...$

Hence, the R-module M is Artinian.

7.2.7. Proposition. Let M be a left R-Module

1) If M is Noetherian then every submodule and factor module of M is also Noetherian.

2) If N is a submodule of M such that bot h N and M/N are Noetherian then so is M.

Proof. 1) We know that "a R-module M is Noetherian iff every sub-module of M is finitely generated."

(i) Let N be a sub-module of M then N must be finitely generated. Now let N_1 be any sub-module of N then it is also finitely generated as every sub-module of a finitely generated module is finitely generated. Hence N is Noetherian.

(ii) Let M/N be any quotient module of M. To prove M/N Noetherian, we shall prove that every sub-module of M/N is finitely generated. So let A/N be any submodule of M/N, where A is a sub-module of M. Now A is a sub-module of M and M is Noetherian, therefore A is finitely generated.

Suppose $A = < x_1, x_2,...,x_n >$. We claim that $A/N = < x_1 + N, x_2 + N, ..., x_n + N >$

Let $x + N \in A/N$ be any element.

Then, $x \in A \Rightarrow x = r_1x_1 + r_2 x_2 + ... + rn\, x_n,\ r_i \in R$

$\Rightarrow x + N = (r_1x_1 + r_2 x_2 + ... + rn\, x_n) + N$

$$= r_1 (x_1+N) + r_2 (x_2+N) +...+ rn (x_n + N)$$

Hence $A/N = < x_1+N, x_2 +N, ...,x_n+N >$, that is, A/N is finitely generated. Therefore, M/N is Noetherian.

2) To prove that M is Noetherian, we shall prove that every sub-module of M is finitely generated. So, let A be any sub-module of M. Then A + N is also a submodule of M containing N. Therefore $^{A+N}/_{N}$ is a sub-module of M/N. Since M/N is Noetherian, therefore, $^{A+N}/_{N}$ must be finitely generated.

Now, we know that $^{A+N}/_{N} \cong A/A \cap N$

$\Rightarrow$ $A/A \cap N$ is also finitely generated.

Also, $A \cap N$ being a sub-module of Noetherian R- module N, is also finitely generated.

Suppose $A \cap N = < x_1, x_2,..., x_m >$ and $A/A \cap N = < y_1 + A \cap N, y_2 + A \cap N,..., y_n + A \cap N >$,

where $x_i, y_i \in A$.

We claim that $A = < x_1, x_2,...,x_m, y_1, y_2,...,y_n >$

Let $x \in A$ be any arbitrary element, then

$x + A \cap N \in A/A \cap N$ and $A/A \cap N = < y_1+A \cap N, y_2 + A \cap N,...,y_n+A \cap N >$

so $x + A \cap N = \sum_{j=1}^{n} r_j \left(y_j + A \cap |N| \right),\ r_j \in R$

$$= \sum_{j=1}^{n} r_j y_j + A \cap N$$

$$\Rightarrow \left(x - \sum_{j=1}^{n} r_j y_j \right) + A \cap N = A \cap N$$

$$\Rightarrow x - \sum_{j=1}^{n} r_j y_j \in A \cap N .$$

Since $A \cap N = < x_1, x_2,...,x_m >$, so $x - \sum_{j=1}^{n} r_j y_j = s_1x_1 + s_2x_2 +...+ s_mx_m, \quad s_i \in R$

$$\Rightarrow x = \sum_{j=1}^{n} r_j y_j + \sum_{i=1}^{m} s_i x_i$$

$\Rightarrow$ $A = < x_1, x_2,...,x_m, y_1, y_2,...,y_n >$

Hence A is finitely generated and therefore M is Noetherian R-module.

7.2.8. Proposition. Let M be a left R-module and N be a sub module of M. Then M is Artinian iff both N and $^{M}/_{N}$ are Artinian.

Proof. First suppose that both N and $^{M}/_{N}$ are Artinian.

We shall prove that M is Artinian.

Let $A_1 \supseteq A_2 \supseteq ... \supseteq A_n \supseteq A_{n+1}$ be a descending chain of sub-modules of M. We shall prove that this chain becomes stationary after a finite number of steps.

Now, A_i is a sub-module of M and N is also a sub-module, so $A_i + N$ is also a sub-module of M and N $\subseteq A_i + N$ for all *i*.

Since, $A_i \supseteq A_{i+1}$ so $A_i + N \supseteq A_{i+1} + N$ for all *i*.

$$\Rightarrow \quad A_i + N/N \supseteq A_{i+1} + N/N,$$

where $A_i + N/N$ is a sub-module of M/N for all *i*.

Hence, we have a descending chain $A_1 + N/N \supseteq A_2 + N/N \supseteq ... \supseteq A_n + N/N \supseteq ...$ of submodules of M/N.

Since M/N is Artinian, so there exist a positive integer *r* such that

$$A_r + N/N = A_{r+1} + N/N = A_{r+2} + N/N = ...$$

that is, $A_r + N/N = A_{r+i} + N/N \quad \forall\ i \geq 0$

$$\Rightarrow \quad A_r + N = A_{r+i} + N \quad \forall\ i \geq 0 \qquad (1)$$

Now, again $A_i \cap N$ is a sub-module of N and since $A_i \supseteq A_{i+1}$.

We have $A_i \cap N \supseteq A_{i+1} \cap N$ for all *i*. Hence, we have a descending chain

$$A_1 \cap N \supseteq A_2 \cap N \supseteq ... \supseteq A_n \cap N \supseteq ...$$

of sub-modules of N. However, N is artinian, so there exist a positive integer *s* such that

$$A_s \cap N = A_{s+1} \cap N = A_{s+2} \cap N = ...$$

that is,, $A_s \cap N = A_{s+i} \cap N$ for all $i \geq 0$. (2)

Let $k = \max\{r, s\}$, then by (1) and (2), we must have

$$A_k + N = A_{k+i} + N \quad \text{for all } i \geq 0 \qquad (3)$$

and $A_k \cap N = A_{k+i} \cap N \quad \text{for all } i \geq 0. \qquad (4)$

We claim that $A_k = A_{k+i} \quad \text{for all } i \geq 0.$

Let $x \in A_k$ be any arbitrary element. Then $x \in A_k \subseteq A_k + N = A_{k+i} + N$ [By(3)]

$$\Rightarrow \quad x = y + z, \text{ for some } y \in A_{k+i}, z \in N$$

$$\Rightarrow \quad x - y = z \in N.$$

Now, $x \in A_k, y \in A_{k+i} \subseteq A_k \Rightarrow x - y \in A_k$

Hence $x - y \in A_k \cap N = A_{k+i} \cap N$ [By (4)]

$\Rightarrow \quad x - y \in A_{k+i} \cap N \subseteq A_{k+i}$

$\Rightarrow \quad x - y \in A_{k+i}$ and $y \in A_{k+i}$

$\Rightarrow \quad x - y + y = x \in A_{k+i}$.

So, $A_k \subseteq A_{k+i}$, also $A_{k+i} \subseteq A_i$.

Hence, we have $A_k = A_{k+i}$ for all $i \geq 0$.

Therefore, the considered chain of sub-modules of M becomes stationary after a finite number of steps. Hence M is Artinian.

Conversely, suppose that M is an Artinian module.

(i) Let N be any sub-module of M. We shall prove that N is Artinian.

Suppose that $N_1 \supseteq N_2 \supseteq N_3 \supseteq \ldots \supseteq N_k \supseteq N_{k+1} \supseteq \ldots$ be a descending chain of sub-modules of N. Since sub-modules of N are also the sub-modules of M, it follows that above chain is a descending chain of sub-modules of M. Since M is Artinian, therefore, there exists a positive integer k such that

$$N_k = N_{k+1} = N_{k+2} = \ldots$$

Hence N is Artinian.

(ii) Let M/N be any quotient module of M. To prove M/N Artinian, let us consider a descending chain of sub-modules of M/N, that is,

$$M_1/N \supseteq M_2/N \supseteq M_3/N \supseteq \ldots \supseteq M_k/N \supseteq \ldots$$

Here, M_i are sub-modules of M and since $M_i/N \supseteq M_{i+1}/N \supseteq$, so $M_i \supseteq M_{i+1}$.

Thus, we have a descending chain $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_k \supseteq \ldots$ of sub-modules of M. Since M is Artinian, so there exists a positive integer k such that $M_k = M_{k+1} = M_{k+2} = \ldots$ and then, we have

$$M_k/N = M_{k+1}/N = M_{k+2}/N = \ldots$$

Hence, M/N is a Artinian R-module.

7.2.9. Remark. Since every homomorphic image of a module is isomorphic to some quotient module. Thus, if the module is Noetherian (Artinian), then its homomorphic image is also Noetherian (Artinian).

7.2.10. Result. Let M_1 and M_2 be R-modules and N_1 and N_2 be submodules of M_1 and M_2 respectively. Let $M = M_1 \times M_2 = \{(x, y) : x \in M_1, y \in M_2\}$. Define addition and scalar product as

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$r(x, y) = (rx, ry).$$

Then, M is a module with respect to this addition and scalar multiplication.

Also, let $N = N_1 \times N_2$. Then, N is a submodule of M. Consider the factor module

$$M/N = M_1 \times M_2 / N_1 \times N_2 .$$

Consider the quotient module M_1/N_1 and M_2/N_2 and let $M_1/N_1 \times M_2/N_2$ be their direct product. Define a map $\phi : M_1 \times M_2 \to M_1/N_1 \times M_2/N_2$ by

$$\phi(x, y) = (x + N_1, y + N_2) .$$

It is easy to see that ϕ is the homomorphism of left R-modules.

Now, ϕ is onto. For, let $(x + N_1, y + N_2) \in M_1/N_1 \times M_2/N_2$, where $x \in M_1$ and $y \in M_2$. Therefore, $(x, y) \in M_1 \times M_2$ and $\phi(x, y) = (x + N_1, y + N_2)$.

Also, let $(x, y) \in Ker\phi \subseteq M_1 \times M_2$. Then,

$$\phi(x, y) = \text{zero of } M_1/N_1 \times M_2/N_2 = (N_1, N_2) \text{ iff } (x + N_1, y + N_2) = (N_1, N_2)$$

iff $x + N_1 = N_1$ and $y + N_2 = N_2$ iff $x \in N_1$ and $y \in N_2$

$$\Rightarrow Ker\phi = N_1 \times N_2 .$$

Hence, by fundamental theorem of homomorphism $M_1 \times M_2 / N_1 \times N_2 \cong M_1/N_1 \times M_2/N_2$.

Generalising this we get

$$M_1 \times M_2 \times ... \times M_n / N_1 \times N_2 \times ... \times N_n \cong M_1/N_1 \times M_2/N_2 \times ... \times M_n/N_n .$$

Remark. If M_1 is a left R-module, then $M_1/M_1 \cong \{0\}$.

7.2.11. Proposition. Let $M_1, M_2, ..., M_k$ be left R-modules.

(i) If each of M_i is Noetherian, then so is $M_1 \times M_2 \times ... \times M_k$.

(ii) If each of M_i is Artinian, then so is $M_1 \times M_2 \times ... \times M_k$.

Proof. We shall prove the result by induction on k.

Suppose k = 2. We know that "If N is a submodule of M, then M is Noetherian iff both N and M/N are Noetherian."

Now, $M_1 \times M_2 / M_1 \times \{0\} \cong M_1/M_1 \times M_2/\{0\} \cong \{0\} \times M_2/\{0\} \cong M_2/\{0\} \cong M_2$.

Since M_2 is Noetherian, therefore $M_1 \times M_2 / M_1 \times \{0\}$ is Noetherian.

Now both $M_1 \times \{0\}$ and $M_1 \times M_2 / M_1 \times \{0\}$ are Noetherian, therefore, $M_1 \times M_2$ is also Noetherian.

Suppose k > 2 and the result holds for modules $M_1, M_2, ..., M_{k-1}$.

Now $M_1 \times M_2 \times ... \times M_{k-1}$ is Noetherian and M_k is also Noetherian, therefore by above discussion $M_1 \times M_2 \times ... \times M_k$ is Noetherian. Hence the Proof.

7.2.12. Proposition. Let $M_1, M_2, ..., M_k$ be Noetherian submodules of M, then $\sum_{i=1}^{k} M_i$ is also Noetherian.

Proof. We know that finite direct product of Noetherian Modules is again Noetherian. Now, each of $M_1, M_2, ..., M_k$ is Noetherian, therefore, $M_1 \times M_2 \times ... \times M_k$ is Noetherian.

Define a map $\phi : M_1 \times M_2 \times ... \times M_k \to \sum_{i=1}^{k} M_i$ by

$$\phi(x_1, x_2, ..., x_k) = x_1 + x_2 + ... + x_k, \; x_i \in M_i.$$

Now, ϕ is a homomorphism:

Let $(x_1, x_2, ..., x_k)$, $(y_1, y_2, ..., y_k) \in M_1 \times M_2 \times ... \times M_k$. Then,

$$\begin{aligned} \phi((x_1, x_2, ..., x_k) + (y_1, y_2, ..., y_k)) &= \phi(x_1 + y_1, x_2 + y_2, ..., x_k + y_k) \\ &= \sum_{i=1}^{k} (x_i + y_i) = \sum_{i=1}^{k} x_i + \sum_{i=1}^{k} y_i \\ &= \phi(x_1, x_2, ..., x_k) + \phi(y_1, y_2, ..., y_k). \end{aligned}$$

and $\phi(r(x_1, x_2, ..., x_k)) = \phi(r x_1, r x_2, ..., r x_k) = \sum_{i=1}^{k} r x_i = r \sum_{i=1}^{k} x_i = r\phi(x_1, x_2, ..., x_k).$

Hence, ϕ is a homomorphism.

ϕ is onto:

Let $x \in M_1 \times M_2 \times ... \times M_k$. Then, $x = x_1 + x_2 + ... + x_k$, $x_i \in M_i$.

Now, $(x_1, x_2, ..., x_k) \in M_1 \times M_2 \times ... \times M_k$ and $\phi(x_1, x_2, ..., x_k) = x_1 + x_2 + ... + x_k = x.$

Thus, ϕ is onto.

Hence, $\sum_{i=1}^{k} M_i$ is a homomorphic image of a Noetherian module $M_1 \times M_2 \times ... \times M_k$.

Therefore, $M_1 + M_2 + ... + M_k$ is Noetherian.

Exercise. If the submodules $M_1, M_2, ..., M_k$ are Artinian, then so is their sum.

7.2.13. Left Noetherian Ring. Let R be a ring. R is called left Noetherian, if left R-module R^R is Noetherian.

7.2.14. Right Noetherian Ring. Let R be a ring. R is called right Noetherian, if right R-module R_R is Noetherian.

7.2.15. Noetherian Ring. If R is both left as well as right Noetherian, R is called Noetherian ring.

7.2.16. Remark. Suppose R is a commutative ring, then it is clear that R is left Noetherian

iff R is right Noetherian iff R is Noetherian.

7.2.17. Artinian Ring. Let R be a ring. Then,

(1) R is called left Artinian if Left R module R^R is Artinian.

(2) R is called right Artinian if right R module R_R is Artinian.

(3) If R is both left as well as right Artinian, R is called Artinian ring.

(4) If R is a commutative ring, then it is clear that R is left Artinian iff R is right Artinian iff R is Artinian.

7.2.18. Proposition. Let R be a right Noetherian ring and M be a finitely generated R-module, then M is also Noetherian.

Solution. We know that finite direct product of Noetherian left R-Modules is again Noetherian, therefore finite direct product of R^R's is also Noetherian.

Therefore, $M' = R^R \times R^R \times ... \times R^R \cong R^{(n)}$ is Noetherian.

Now, M is finitely generated R-module, thus there exist $x_1, x_2, ..., x_n \in M$ such that

$$M = \sum_{i=1}^{n} Rx_i = \langle x_1, x_2, ..., x_n \rangle$$

Now, $R^{(n)} = M' = \{(r_1, r_2, ..., r_n) : r_i \in R\}$ is Noetherian R-module.

Define a map $\phi : M' \to M$ by

$$\phi(r_1, r_2, ..., r_n) = r_1x_1 + r_2x_2 + ... + r_nx_n.$$

Then, ϕ is a homomorphism:

Let $(r_1, r_2, ..., r_n) \in M'$ and $(s_1, s_2, ..., s_n) \in M'$. Then,

$$\begin{aligned}\phi((r_1, r_2, ..., r_n) + (s_1, s_2, ..., s_n)) &= \phi(r_1 + s_1, r_2 + s_2, ..., r_n + s_n) \\ &= \sum_{i=1}^{n} r_i x_i + \sum_{i=1}^{n} s_i x_i \\ &= \phi(r_1, r_2, ..., r_n) + \phi(s_1, s_2, ..., s_n).\end{aligned}$$

Let $r \in R^R$, then

$$\phi(r(r_1, r_2, ..., r_n)) = \phi(rr_1, rr_2, ..., rr_n) = \sum_{i=1}^{n} rr_i x_i = r\sum_{i=1}^{n} r_i x_i = r\phi(r_1, r_2, ..., r_n).$$

Hence, ϕ is a homomorphism of left R-modules.

Let $x \in M$, then, there exists $r_1, r_2, ..., r_n \in R$ such that $x = \sum_{i=1}^{n} r_i x_i$.

But then $(r_1, r_2, ..., r_n) \in R^{(n)}$ and $\phi(r_1, r_2, ..., r_n) = \sum_{i=1}^{n} r_i x_i = x.$

Hence, ϕ is onto.

Thus, $\phi : M' \to M$ is epimorphism that is, M is homomorphic image of M' and so, M is Noetherian.

7.2.19. Exercise. Let R be a left Artinian ring and M be a finitely generated left R-module, then M is also Artinian.

Proof. Proof of this exercise is similar to that of the above if we change Noetherian by Artinian.

7.3. Hilbert Basis Theorem. Let R be a left Noetherian ring then so is the polynomial ring R[x] and conversely.

Proof. Let the ring R be left Noetherian and let R[x] be the polynomial ring over R in the indeterminate x.

We shall prove that every left ideal of R[x] is finitely generated as a left R-module.

Let A be a left ideal of R[x].

If A = {0}, then clearly it is finitely generated left R[x] module.

Suppose A $\neq$ {0}. Let

I_k = { $a \in R$: a is leading co-efficient of some polynomial of degree k in A} $\cup$ {0}.

Here $k \geq 0$. We prove that I_k is left ideal of R.

Clearly, $I \neq \phi$ as $0 \in I_k$.

Let a, b $\in I_k$. If a = b, then a - b = $0 \in I_k$.

Suppose $a \neq b \Rightarrow a - b \neq 0$.

Then either $a \neq 0$ or $b \neq 0$.

If $a \neq 0$, then there exist $f(x) = ax^k + a^1x^{k-1} + ... \in A$. Now, $a \neq 0 \Rightarrow -a \neq 0$.

Now $f(x) \in A$ and A is left ideal.

$$\Rightarrow -f(x) \in A \Rightarrow -a \in I_k .$$

Similarly, if $b \neq 0 \Rightarrow -b \in I_k$.

(i) if $b = 0$, then $a - b = a \in I_k$.

(ii) if $a = 0$, then $a - b = -b \in I_k$.

(iii) if $a \neq 0$, $b \neq 0$ and $a - b \neq 0$. Then,

$$f(x) - g(x) = (a-b)x^k + (a^1-b^1)x^{k-1} + ... \in A,$$

where $g(x) = bx^k + b^1x^{k-1} + ... \in A$

$$\Rightarrow a - b \in I_k.$$

Hence, I_k is a subgroup of R under addition.

Let $r \in R$ and $a \in I_k$.

If $ra = 0$., then $ra \in I_k$.

If $ra \neq 0$, then $a \neq 0$. Now, $r \in R \subseteq R[x]$ and $f(x) \in A$

$$\Rightarrow rf(x) \in A.$$

Now, $rf(x) = rax^k + ra^1x^{k-1} + ...$ is of degree k so $ra \in I_k$.

Hence, I_k is a left ideal of R.

If $a \in I_k$ and $a \neq 0$, then

$$xf(x) = ax^{k+1} + a^1x^k + ... \in A \text{ is of degree } k + 1.$$

$$\Rightarrow a \in I_{k+1}.$$

Hence, $I_k \subseteq I_{k+1} \; \forall \, k \geq 0.$

Now, we have an ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq ... \subseteq I_{k+1} \subseteq ...$ of left-ideals of R.

Since R is left Noetherian, therefore there exists a positive integer d such that

$$I_d = I_{d+i} \quad \forall \, i \geq 0.$$

Since R is left Noetherian, therefore each ideal of R is finitely generated as a left R-module. Let $I_k = \left\langle a_{k_1}, a_{k_2}, ..., a_{k_{n_k}} \right\rangle$, that is, $I_k = \sum_{j=1}^{n_k} Ra_{k_j}$.

Now, by definition of I_k; there exists polynomial

$$f_{k_j}(x) = a_{k_j} x^k + a_{k_j}^1 x^{k-1} + ..., \text{ where } 1 \le j \le n_k .$$

Let $T = \left\{ f_{k_j}(x) \right\}_{k=0, j=1}^{d, n_k} = \bigcup_{k=0}^{d} \left\{ f_{k_j}(x) \right\}_{j=1}^{n_k}$.

Let $B = \langle T \rangle$ (The left ideal generated by T)

$$B = \sum_{k=0}^{d} \sum_{j=1}^{n_k} R[x] f_{k_j}(x).$$

We shall prove that A = B.

Let $f(x) \in A$ and suppose deg(f(x)) = n. We write

$$f(x) = ax^n + a^1 x^{n-1} + ...$$

We prove the result by induction on n.

If n = 0, then $f(x) = ax^0$ ($a \neq 0$) and $a \in I_0$.

$$I_0 = \left\langle a_{01}, a_{02}, ..., a_{0n_0} \right\rangle = \sum_{j=1}^{n_0} Ra_{0j}$$

$$\Rightarrow a = r_1 a_{01} + r_2 a_{02} + ... + r_{n_0} a_{0n_0}, \quad r_j \in R$$

$$= \sum_{j=1}^{n_0} r_j f_{0j}(x)$$

$$\Rightarrow a \in B,$$

that is, $f(x) \in B$

Let $n \ge 1$ and suppose that the result holds for all polynomials in A. that is, $g(x) \in A$ and deg(g(x)) < n.

$$\Rightarrow g(x) \in B.$$

Now either $n \ge d$ or $n < d$.

Case-I**.** Suppose $n \ge d$ and $a \in I_n = I_d$ and

$$I_d = \sum_{j=1}^{n_d} Ra_{dj} \qquad [\because k = d]$$

$$\Rightarrow I_d = \sum_{j=1}^{n_d} r_j a_{dj}.$$

Consider the polynomial

$$g(x) = \sum_{j=1}^{n_d} r_j x^{n-d} f_{dj}(x) \in B.$$

Now, $f_{dj}(x)$ is a polynomial of degree d with leading co-efficient $r_j a_{dj}$.

Hence, the leading co-efficient of g(x) is $\sum_{j=1}^{n_d} r_j a_{dj} = a$ and it is a polynomial of degree n.

Now $g(x) \in B$ and $B \subseteq A$

$\therefore$ $f(x) - g(x) \in A$ and it is a polynomial of degree n - 1 and hence by induction hypothesis $f(x) - g(x) \in B.$

Since $g(x) \in B$, it follows that $f(x) \in B.$ This completes the induction.

Case-II**.** n < d.

Now, $I_n = \sum_{j=1}^{n_m} Ra_{nj}$ and $a \in I_n$

$$\Rightarrow a = \sum_{j=1}^{n_m} r_j a_{nj}, \ r_j \in R.$$

Consider $g(x) = \sum_{j=1}^{n_m} r_j f_{nj}(x) \in B.$

Now, g(x) is of degree n and leading co-efficient is $\sum_{j=1}^{n_m} r_j a_{nj} = a.$

Hence $f(x) - g(x) \in A$ is of degree atmost n - 1 and hence by induction hypothesis $f(x) - g(x) \in B.$

Since $g(x) \in B \Rightarrow f(x) \in B.$

Hence, in either case $A \subseteq B.$

But $B \subseteq A.$

$$\Rightarrow \text{A} = \text{B}.$$

Since B is finitely generated, therefore A is finitely generated.

7.3.1. Proposition. (Converse to Hilbert Basis Theorem) If R[x] is left Notherian, then so is R.

Proof. Let I be the ideal of R[x] generated by x over R[x].

that is, I = <x> = R[x]x.

Then I is an ideal of R[x].

Define a map $f : R \to R[x]/I$ by

f(a) = a + I.

Now, f(a + b) = a + b + I = (a + I) + (b + I) = f(a) + f(b)

and f(ab) = ab + I = (a + I)(b + I) = f(a)f(b).

Thus, f is ring homomorphism.

Now, let f(a) = f(b)

$\Rightarrow$ a + I = b + I

$\Rightarrow$ a - b + I = I = R[x]x

$\Rightarrow$ a - b $\in$ I = R[x]x

$\Rightarrow$ a - b = f(x)x for some f(x) $\in$ R[x]

$\Rightarrow$ f(x)/ a - b.

If $a \neq b$, then deg(a - b) = deg(f(x)) + 1.

$\Rightarrow$ 0 = deg(f(x)) + 1, a contradiction.

Thus, a = b.

Hence f is one-one.

Let $g(x) + I \in R[x]/I$, $g(x) \in R[x]$.

Suppose, $g(x) = b_0 + b_1x + ... + b_nx^n$

$= b_0 + (b_1 + b_2x + ... + b_nx^{n-1})x$

$= b_0 + h(x)x$

$\Rightarrow g(x) + I = b_0 + h(x)x + I = b_0 + I.$ [$\because$ h(x) $\in$ R[x] $\Rightarrow$ h(x) x $\in$ I]

Now, $b_0 \in R$ and $f(b_0) = b_0 + I = g(x) + I.$

Hence, f is onto.

Therefore, f is an isomorphism of ring R. that is, $R \cong R[x]/I$.

Since R[x] is left Noetherian and a factor ring of Noetherian is again Noetherian. It follows that R is Noetherian.

7.3.2. Theorem. Let R be a left Noetherian ring and $x_1, x_2, ..., x_n$ be n independent indeterminants. Then, $R[x_1, x_2, ..., x_n]$ is also Noetherian.

Proof. We know that R is left Noetherian iff polynomial ring R[x] is Noetherian.

We prove the result by induction on n.

If n = 1, then, $R[x_1]$ is left Notherian.

If n = 2, then, $R[x_1, x_2] = R[x_1][x_2]$, is left Noetherian, since $R[x_1]$ is Noetherian.

Suppose that n > 2 and $R[x_1, x_2, ..., x_{n-1}]$ is left Noetherian.

Then, $R[x_1, x_2, ..., x_n] = R[x_1, x_2, ..., x_{n-1}][x_n]$ is left Noetherian.

This completes the proof.

7.3.3. Theorem. Let S be a sub-ring of R such that $1 \in R \Rightarrow 1 \in S$. Suppose S is left Noetherian and R is generated by finite number of elements as an algebra over S. Then, R is also left Noetherian.

Proof. Let $x_1, x_2, ..., x_n \in R$ and R is generated by $x_1, x_2, ..., x_n$ as an algebra over S, that is, every element of R is a polynomial function in the variables $x_1, x_2, ..., x_n$ with co-efficient in S, that is, $R[x_1, x_2, ..., x_n]$.

Since S is left Noetherian, by above theorem, $S[x_1, x_2, ..., x_n]$ is left Noetherian and so is R.

7.4. Nil Left Ideal.

Let R be a ring and I be a left ideal. If given $a \in I$, there exists a positive integer n depending upon 'a' such that $a^n = 0$, then I is called nil left ideal of R.

If $a \in R$ and $a^n = 0$ for some positive integer n, then a is called nilpotent element of R. Thus, a left ideal I of R is nil if every element of I is nilpotent.

7.4.1. Nilpotent Ideal.

A left ideal I of R is called nilpotent if there exists a positive integer n such that $I^n = \{0\}$. that is, for every $a_1, a_2, ..., a_n \in I$,

$$a_1.a_2...a_n = 0.$$

In particular, for every $a \in I$,

$\underbrace{a.a...a}_{\text{n times}} = 0$, that is, $a^n = 0$

that is, a is nilpotent element of R. Hence, a nilpotent left ideal is a nil left ideal.

7.4.2. Theorem. In a left Artinian ring, every nil left ideal is nilpotent.

Proof. Let R be a left Artinian ring and I be a nil left ideal of R.

We shall prove that I is nilpotent.

Consider the decreasing chain $I \supseteq I^2 \supseteq I^3 \supseteq ... \supseteq I^m \supseteq I^{m+1} \supseteq ...$ of left ideals of R.

Since R is left Artinian, there exists a positive integer k such that $I^k = I^{k+1} = ...$

that is, $I^k = I^{k+i} \quad \forall\, i \geq 0.$

Let $J = I^k$. Then, J is left ideal of R such that $J^2 = I^k.I^k = I^k = J$.

We claim that $J = \{0\}$.

Suppose $J \neq \{0\}$.

Let £ = {A : A is left ideal of R contained in J such that $JA \neq \{0\}$}

Now, $JJ = J^2 = J \neq \{0\}$ and J is left ideal of R contained in J.

$\Rightarrow J \in £ \Rightarrow £ \neq \phi.$

We know that if R is left Artinian, then every non-empty set of left ideals of R has a minimal element.

Let A be the minimal element of £ such that $JA \neq \{0\}$.

Hence, there exists $a(\neq 0) \in A$ such that $Ja \neq \{0\}$, otherwise $JA = \{0\}$.

Also, $a \in A$ and A is left ideal of R contained in J.

$$\Rightarrow B = Ja \subseteq A \subseteq J.$$

Thus, B is a left ideal of R and

$$JB = JJa = Ja = B \neq \{0\}.$$

$$\Rightarrow B \in £.$$

Since $B \subseteq A$ and A is the minimal element of £.

$$\therefore B = A.$$

that is, $A = Ja = B$.

Now, $a \in A = Ja$.

$$\Rightarrow a = xa \text{ for some } x \in J.$$

Now, $a = x(xa) = x^2a$, a simple induction shows that $a = x^na \ \forall\, n \geq 1$.

Now, $x \in J \subseteq I$ implies that x is a nilpotent element.

Let m be a positive integer such that $x^m = 0$.

Then, $a = x^ma = 0a = 0$, that is, $a = 0$, a contradiction.

Thus, $J = 0$, that is, $I^k = \{0\}$, that is, I is a nilpotent left ideal of R.

Note. A ring with unity is called a division ring if every non-zero element of R is invertible.

7.4.3. Proposition. An Artinian domain is a division ring (Skew-field).

Proof. To prove that R is a division ring, we shall prove that every non-zero element of R is invertible. Let a ∈ R be a non-zero element.

Let $I_k = \langle a^k \rangle = Ra^k$, that is, left ideal of R is generated by a^k.

Now, if $y \in I_{k+1} \Rightarrow y = ra^{k+1} = (ra)a^k \in I_k$, $r \in R$, thus $I_{k+1} \subseteq I_k \quad \forall\, k \geq 0$.

So, we have a decreasing chain

$$I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n \supseteq I_{n+1} \supseteq \ldots$$

of left ideals of R.

Since R is left Artinian, so there exists a positive integer k such that

$$I_k = I_{k+i} \quad \forall\, i \geq 0$$

that is, $\langle a^k \rangle = \langle a^{k+i} \rangle \quad \forall\, i \geq 0$.

Now $a^k \in \langle a^k \rangle = \langle a^{k+1} \rangle$

$\Rightarrow a^k = ra^{k+1}$ for some $r \in R$

$\Rightarrow a^k = raa^k$

$\Rightarrow (1 - ra)a^k = 0.$

Now, R is a division ring and $a \neq 0 \Rightarrow a^k \neq 0$ and therefore $1 - ra = 0$, that is, $ra = 1$, that is, every element of R is left invertible. By the same reasoning, there exists $b \in R$ such that $1 = br$.

Then, $a = (br)a = b(ra) = b.1 = b.$

Hence, r is the inverse of a and hence R is a division ring.

7.4.4. Prime Ideal. Let R be a ring. An ideal P of R is called a prime ideal if given ideals A and B such that $AB \subseteq P$ implies either $A \subseteq P$ or $B \subseteq P$.

Remark. In a left Artinian ring every prime ideal is maximal.

7.4.5. Theorem. Let R be a left Noetherian ring. Every ideal I of R contains a finite product of prime ideals.

Proof. Let R be a left Noetherian ring. We shall prove that every ideal of R contains a finite product of prime ideals. Let

£ = {I : I is ideal of R such that I does not contain a finite product of prime ideals}.

To prove the result, we prove that £ = ϕ.

Suppose $£ \neq \phi$.

Since every ideal is a left ideal and R is left Noetherian, therefore £ must have a maximal element, say I.

Now, I∈£, so I is not prime ideal, so there exist ideals A and B of R such that the product $AB \subseteq I$ implies neither $A \subseteq I$ nor $B \subseteq I$.

Consider the ideals, $I_1 = I + A$ and $I_2 = I + B$.

Since I is maximal ideal of £, therefore I_1 and $I_2 \notin$ £.

Hence there exist finite number of prime ideals, say $P_1, P_2, ..., P_m$ and $P_1', P_2', ..., P_n'$ such that

$$P_1P_2...P_m \subseteq I_1 \text{ and } P_1'P_2'...P_n' \subseteq I_2.$$

Now, $P_1P_2...P_mP_1'P_2'...P_n' \subseteq I_1I_2$

Let $x \in I_1I_2$, then $x = \sum_{finite} y_iz_i, \quad y_i \in I_1, z_i \in I_2$.

Now, $y_i \in I_1 = I + A \Rightarrow y_i = c_i + a_i$ where $c_i \in I, a_i \in A$

and $z_i \in I_2 = I + B \Rightarrow z_i = d_i + b_i$ where $d_i \in I, b_i \in B$.

Then, $y_iz_i = (c_i + a_i)(d_i + b_i) = c_i d_i + c_ib_i + a_i d_i + a_ib_i \in I$ [$\because c_i, d_i \in I, a_i \in A, b_i \in B$ & $AB \subseteq I$]

Hence, $x = \sum_{finite} y_iz_i \in I$.

From this, it follows that $P_1P_2...P_mP_1'P_2'...P_n' \subseteq I$, that is, I contains a finite product of prime ideals, a contradiction and this contradiction proves that £ = ϕ, that is, every ideal of R contains a finite product of prime ideals.

7.4.6. Boolean Ring. A ring R is called Boolean Ring if $x^2 = x \; \forall \; x \in R$. Suppose R is a Boolean ring, then $x^2 = x \; \forall \; x \in R$. Then

$$(x + y)^2 = (x + y)$$

$$\Rightarrow x^2 + y^2 + xy + yx = x + y$$

$$\Rightarrow x + y + xy + yx = x + y$$

$$\Rightarrow xy = -yx \quad \forall \; x, y \in R.$$

Also, $(x + x)^2 = (x + x)$

$$\Rightarrow x + x = 0$$

$$\Rightarrow x = -x \quad \forall \; x \in R.$$

Now, $xy = -xy = -(-yx) = yx$.

Therefore, R is a commutative ring.

Remark. Let R be a Boolean Noetherian ring, then

$$R \cong Z/2Z \times Z/2Z \times \ldots \times Z/2Z$$

and so if a Boolean ring which is also Noetherian, then number of elements in R is 2^n where n is a positive integer.

Remark. If $a, b \in R$ (ring) such that ab = 1 and $ba \neq 1$. Define $e_{ij} = b^{i-1}a^{j-1} - b^i a^j$.

We shall prove that (i) $e_{ij}e_{kl} = \begin{cases} 0 & if\ j \neq k \\ e_{il} & if\ j = k \end{cases}$

(ii) $e_{ii} \neq 0$

(iii) $e_{ii} \neq 1$.

We have, $e_{ij}e_{kl} = (b^{i-1}a^{j-1} - b^i a^j)(b^{k-1}a^{l-1} - b^k a^l)$

$$= b^{i-1}a^{j-1}b^{k-1}a^{l-1} - b^i a^j b^{k-1}a^{l-1} - b^{i-1}a^{j-1}b^k a^l + b^i a^j b^k a^l.$$

Suppose $j \neq k$. Then, either $j > k$ or $j < k$.

First suppose that $j > k$.

$$\Rightarrow j - 1 > k - 1.$$

Now, $e_{ij}e_{kl} = b^{i-1}a^{j-k}a^{k-1}b^{k-1}a^{l-1} - b^i a^{j-k+1}a^{k-1}b^{k-1}a^{l-1} - b^{i-1}a^{j-1-k}a^k b^k a^l + b^i a^{j-k}a^k b^k a^l$

Since $a^m b^m = 1 \ \forall\ m \geq 0.$

$\therefore\ e_{ij}e_{kl} = b^{i-1}a^{j-k}a^{l-1} - b^i a^{j-k+1}a^{l-1} - b^{i-1}a^{j-1-k}a^l + b^i a^{j-k+1}a^{l-1}$

$$= b^{i-1}a^{j+l-k-1} - b^i a^{j+l-k} - b^{i-1}a^{j+l-1-k} + b^i a^{j+l-k} = 0.$$

Similarly, we can prove that $e_{ij}e_{kl} = 0$ if $j < k$.

Suppose $j = k$, then

$e_{ij}e_{kl} = e_{ij}e_{jl} = b^{i-1}a^{j-1}b^{j-1}a^{l-1} - b^i a^j b^{j-1}a^{l-1} - b^{i-1}a^{j-1}b^j a^l + b^i a^j b^j a^l$

$$= b^{i-1}a^{l-1} - b^i a^l - b^i a^l + b^i a^l = b^{i-1}a^{l-1} - b^i a^l = e_{il}.$$

Hence, $e_{kl} = \begin{cases} 0 & if\ j \neq k \\ e_{il} & if\ j = k \end{cases}$.

(ii) Take $f_i = e_{ii}$.

Then, $f_i f_i = e_{ii}e_{ii} = e_{ii} = f_i$.

$\Rightarrow f_i$ is idempotent.

Suppose $f_i = 0$, then

$f_i = e_{ii} = b^{i-1}a^{i-1} - b^i a^i = 0$

$\Rightarrow b^{i-1}a^{i-1} = b^i a^i$

$\Rightarrow a^{i-1}b^{i-1}a^{i-1}b^{i-1} = a^{i-1}b^i a^i b^{i-1}$

$\Rightarrow 1 = ba,$ a contradiction.

Hence $e_{ii} \neq 0.$

(iii) Suppose $f_i = 1.$ Take $j \neq i$, then

$f_i f_j = e_{ii} f_j = f_j.$ $(\because e_{ii} = 1)$

Again, $f_i f_j = e_{ii} e_{jj} = 0.$ $[\because i \neq j]$

Hence $f_j = 0$, a contradiction.

Hence, $e_{ii} \neq 1.$

7.4.7. Theorem. Let R be left Noetherian ring and $a, b \in \mathrm{R}$ such that $ab = 1$, then $ba = 1.$

Proof. Let R be a left Noetherian ring and $a, b \in \mathrm{R}$ such that $ab = 1$. We have to show that $ba = 1.$

Suppose that $ba \neq 1$. Now, $ab = 1$

$\Rightarrow a(ab)\mathrm{b} = ab$

$\Rightarrow a^2 b^2 = 1.$

A simple induction shows that $a^m b^m = 1 \ \forall\ m \geq 0.$

Define, $e_{ij} = b^{i-1}a^{j-1} - b^i a^j.$ $(\mathrm{i} \geq 1, \mathrm{j} \geq 1)$

Now, as shown in above remark

$$e_{ij}e_{kl} = \begin{cases} 0 & if\ j \neq k \\ e_{il} & if\ j = k \end{cases},$$

$e_{ii} \neq 0$ and $e_{ii} \neq 1.$

Define, $f_i = e_{ii}$ and let $I_k = Rf_1 + Rf_2 + ... + Rf_k.$

Then, $\mathrm{I_k}$ is a left ideal of R and is contained in $\mathrm{I_{k+1}}$ $\forall\ k \geq 1.$

that is, $I_k \subseteq I_{k+1} \; \forall \; k \geq 1$.

Now, $f_{k+1} \in Rf_{k+1} \subset Rf_1 + Rf_2 + ... + Rf_{k+1} = \mathrm{I}_{k+1}$.

Suppose, $f_{k+1} \in \mathrm{I}_k$. Then, $f_{k+1} = r_1 f_1 + r_2 f_2 + ... + r_k f_k$ where $r_i \in R$

$\Rightarrow f_{k+1} f_{k+1} = r_1 f_1 f_{k+1} + r_2 f_2 f_{k+1} + ... + r_k f_k f_{k+1} = 0$ $\quad [\because f_r f_s = 0 \; if \; r \neq s]$

$\Rightarrow f_{k+1} = 0$, a contradiction. [$\because f_r$ is idempotent]

Hence $I_k \underset{\neq}{\subset} I_{k+1}$.

Hence, we get an infinite properly ascending chain

$$I_1 \underset{\neq}{\subset} I_2 \underset{\neq}{\subset} I_3 \underset{\neq}{\subset} ... \underset{\neq}{\subset} I_k \underset{\neq}{\subset} I_{k+1} \underset{\neq}{\subset} ...$$

of left ideals of R, a contradiction because R is left Noetherian.

Hence, ba = 1.

7.4.8. Theorem. Let R be a Noetherian ring having no non-zero nilpotent ideals. Then R has no non-zero nil ideals.

Proof. Let, if possible, A be a non-zero nil ideal of R.

Let $\rho = \{ l(a) : a \in \mathrm{A}, a \neq 0 \}$ be a family of left annihilators of all non-zero elements of A. Since each $l(a)$ is a left ideal of R and $\mathrm{A} \neq \{0\}$, so ρ is a non-empty family of left ideals of R. Since R is a Noetherian ring, so ρ must have a maximal element, say, $l(a)$.

Now, let $x \in$ R be any arbitrary element, then $ax \in$ A $\quad [\because$ A is an ideal of R]

But A is a nil ideal so ax must be a nilpotent element that is, there exist a smallest positive integer k such that

$$(ax)^k = 0 \Rightarrow (ax)(ax)^{k-1} = 0 \Rightarrow ax \in l\left((ax)^{k-1}\right) \qquad (1)$$

Now, we see that $(ax)^{k-1} \neq 0$ and $(ax)^{k-1} \in \mathrm{A} \Rightarrow l\left((ax)^{k-1}\right) \in \rho$

Now, we prove that $l(a) \subseteq l\left((ax)^{k-1}\right)$

Let $y \in l(a) \Rightarrow ya = 0 \Rightarrow (ya)x = 0 \Rightarrow \quad y(ax) = 0$

$\Rightarrow y(ax)^{k-1} = 0 \Rightarrow y \in l\left((ax)^{k-1}\right) \Rightarrow l(a) \subseteq l\left((ax)^{k-1}\right)$

But $l(a)$ is a maximal element of ρ, so $l(a) = l\left((ax)^{k-1}\right)$ $\qquad (2)$

By (1) and (2), we have $\quad ax \in l(a)$

$\Rightarrow \quad a\,x\,a = 0 \; \forall \; x \in \mathrm{R}$

$\Rightarrow \quad a\,\mathrm{R}\,a = 0$

Let J = R a R, then, J^2 = R a R R a R $\subseteq$ R a R a R [$\because$ R R $\subseteq$ R]

= R (a R a) R = {0}

that is,, J is a nilpotent ideal of R.

But R has no non-zero nilpotent ideal, so we must have

J = {0} that is,, RaR = {0} (3)

Now, consider the ideal

B = < a > = R a + a R + R a R + a $\mathbb{Z}$

Let D = R a + a R + R a R = R a + a R [By-(3)]

Then, D^2 = (Ra + aR) (Ra + aR) = R a R a + a R R a + R a a R + a R a R

$\subseteq$ R a R a + a R a + R a R + a R a R [$\because$ $R^2 \subseteq$R, RaaR $\subseteq$RaR] = {0}

as R a R = a Ra = 0, that is, D is a nilpotent ideal of R. But R has no non-zero nilpotent ideal, so we must have D = {0}

Hence, we obtain B = $a\mathbb{Z}$

Now, $a \in$ A and A is a nil ideal so 'a' must be a nilpotent element that is, there exists a smallest positive integer t such that $a^t = 0$.

Then, $B^t = a\mathbb{Z}\ .a\mathbb{Z}\ ...a\mathbb{Z}$ (t times) = $a^t\ \mathbb{Z}$ = {0}, that is, B is nilpotent ideal of R. But R has no non-zero nilpotent ideal, so B = {0}

$\Rightarrow$ $a\ \mathbb{Z}$ = {0}

Now $a.1 \in a\mathbb{Z}$ = {0}

$\Rightarrow$ $a.1 = 0$

$\Rightarrow$ a = 0, a contradiction.

Hence R has no non-zero nil ideal.

7.4.9. Proposition. Let R be a left Noetherian ring. Prove that sum of nilpotent ideals of R is again a nilpotent ideal of R.

Proof. Let R be a left Noetherian ring and $\{I_\lambda\}_{\lambda\in\Lambda}$ be a family of nilpotent ideals of R.

Suppose, $I = \sum_{\lambda\in\Lambda} I_\lambda$.

Then, I is an ideal of R, since sum of ideals is again an ideal.

Since R is left Noetherian, therefore I is generated by finite number of elements, say $x_1, x_2, ..., x_n \in I$.

Now, $x_i \in I \Rightarrow$ there exists a finite subsets Λ_i of Λ such that $x_i = \sum_{\lambda\in\Lambda_i} I_\lambda$.

Take, $\Lambda' = \bigcup_{i=1}^{n} \Lambda_i$. Then, $x_i = \sum_{\lambda \in \Lambda'} I_\lambda \quad \forall\, i$

$$\Rightarrow I = \langle x_1, x_2, ..., x_n \rangle = \sum_{\lambda \in \Lambda'} I_\lambda \subseteq I \qquad \Rightarrow I = \sum_{\lambda \in \Lambda'} I_\lambda$$

and Λ' is a finite subset of Λ. Thus, we may assume that $I = I_1 + I_2 + I_3 + ... + I_m$ and each I_k is nilpotent.

Thus, to prove the result it is equivalent to prove that sum of finite number of nilpotent ideals is again a nilpotent ideal.

We prove the result by induction on m.

If m = 2, then

$$I_1 + I_2 \big/ I_2 \cong I_1 \big/ I_1 \cap I_2 .$$

Now, I_1 is nilpotent ideal of R, so $I_1 \big/ I_1 \cap I_2$ is nilpotent ideal of $R \big/ I_1 \cap I_2$. Hence, $I_1 + I_2 \big/ I_2$ is a nilpotent ideal. since I_2 is a nilpotent ideal of R, it follows that I_1+I_2 is a nilpotent ideal of R.

Thus, the sum of two nilpotent ideals is again a nilpotent ideal of R.

Let m > 2 and suppose that the result hold for (m - 1) nilpotent ideals, that is, $I_1 + I_2 + I_3 + ... + I_{m-1}$ is nilpotent.

Now, sum of two nilpotent ideals is again nilpotent, so the sum of $I_1 + I_2 + I_3 + ... + I_{m-1}$ and I_m, that is, $I_1 + I_2 + I_3 + ... + I_m$ is also nilpotent.

Remark. Let R be a ring and A and B be ideals of R such that $A \subseteq B$. Then, B is nilpotent iff both A and $B \big/ A$ are nilpotent.

7.4.10. Proposition. In a left Noetherian ring, every nil ideal is nilpotent.

Proof. Let £=$\{I_\lambda\}_{\lambda \in \Lambda}$ be the family of all nilpotent ideals of R and $I = \sum_{\lambda \in \Lambda} I_\lambda$.

Then, I is an ideal of R. Also, we know that in a left Noetherian ring sum of nilpotent ideals is again nilpotent and hence I is nilpotent ideal of R.

Consider the quotient ring $R \big/ I$.

Let $J \big/ I$ be the nilpotent ideal of $R \big/ I$, where J is an ideal of R containing I. Now, $J \big/ I$ is an nilpotent ideal of $R \big/ I$ and I is nilpotent ideal of R. Hence, $J \in$ £.

Thus, there exists $\lambda_0 \in \Lambda$ such that $J = I_{\lambda_0}$.

Now, $I = \sum_{\lambda \in \Lambda} I_\lambda \supseteq I_{\lambda_0} = J \supseteq I$

$\Rightarrow I = J.$

Hence, J/I is the zero ideal. that is, $J/I = \{I\}$.

Therefore, R/I has no non-zero nilpotent ideal. Since R is left nilpotent, therefore, R/I is left Noetherian.

Thus, R/I is left Noetherian ring such that R/I has no non-zero nil ideal.

Let k be a nil ideal of R, then K + I is an ideal of R

$\Rightarrow K+I/I$ is an ideal of R/I.

Now, $K+I/I \cong K/K \cap I$ and K is nil ideal, so $K+I/I$ is nil ideal. Hence, $K+I/I$ is a nil ideal of R/I. Since $K+I/I$ has no non-zero nil ideal.

Therefore, $K+I/I = \{I\} \qquad \Rightarrow K + I = I \Rightarrow K \subseteq I.$

Since I is a nilpotent ideal, it follows that K is also a nilpotent ideal of R. Thus, every nil ideal in R is nilpotent.

7.4.11. Example. Example of a ring which is both Noetherian as well as Artinian.

Proof. Let R be a ring having only finite number of left ideals. Clearly, every properly ascending chain or a properly descending chain is finite and therefore R is left Noetherian as well as left Artinian.

7.4.12. Example. Example of a ring which is Noetherian but not Artinian.

Solution. Let R=Z, the ring of integers. Now, since Z is a P.I.D., so every ideal of R is generated by a single element that is, if I is an ideal of R, then ∃ m ∈ I, m≥0 such that I=mZ. that is, every ideal of R is finitely generated, therefore R is Noetherian.

Let $I_k = 2^k Z$, $k \geq 0$

Now, $2^{k+1} \in I_{k+1,}$ and $2^{k+1} = 2.\ 2^k \in 2^k Z = <2^k> = I_k$, so $<2^{k+1}> \subseteq I_k$ and thus $I_{k+1} \subseteq I_k$

Now, $2^k \in I_{k.}$. If $2^k \in I_{k+1}$, then $2^k = 2^{k+1}z$, where $z \in Z$, so $1=2z$, ehich implies

$z = \frac{1}{2} \in Z$, a contradiction.

Hence $2^k \notin I_{k+1}$ and so $I_{k+1} \subsetneq I_k$

Thus,

$$I_0 \supset I_1 \supset \ldots \supset I_n \supset \ldots$$

is an infinite properly descending chain of ideals of R.

Therefore, R is not Artinian.

7.4.13. Example. Example of a ring which is neither Noetherian nor Artinian.

Solution. Let R be a ring and $x_1, x_{2,} ..., x_{n...}$ be infinite numbers of commutingindeterminants over R. Consider the polynomial ring $R[x_1, x_{2,} ..., x_n]=S$. Let I_k be the left ideal of S generated by $x_1, x_{2,} ..., x_n$, that is,

$$I_k =< x_1, x_{2,} ..., x_n> = Sx_1 +Sx_2+...+Sx_K.$$

Now, it is clear that $I_k \subseteq I_{k+1}$

If $x_{k+1} \in I_{k+1}$.Then,

$$x_{k+1}= r_1x_1+ r_2x_2+...+ r_kx_k \text{ where } r_i \in S = R[x_1, x_{2,} ..., x_n...]$$

The L.H.S. is a polynomial in the single indeterminates x_{k+1} while the R.H.S. is a polynomial in the indeterminants $x_1, x_{2,} ..., x_n$.

Therefore these two polynomials cannot be equal.

Hence, $x_{k+1} \notin I_k \Rightarrow I_k \subseteq I_{k+1}$. Thus, we have

$$I_1 \subset I_2 \subset ... \subset I_n \subset ...$$

is an infinite properly ascending chain of left ideals of S

Hence,S is not left Noetherian.

Similarly, we can prove that S is not right Noetherian.

Let, $B_0=\{x_1,x_{2,...} x_{n,...}\}$

$B_{1=} B_0-\{x_1\}$

$B_2= B_0-\{x_1,x_2\}$

. . .

$B_n =B_0-\{x_1,x_{2,...} x_n\}$

Let J_n be the left ideal of $R[x_1,x_{2,...} x_{n,...}]=S$ generated by B_n.

Now, it is clear that

$$J_0 \supset J_1 \supset ... \supset J_n \supset ...$$

is an infinite properly descending chain of left ideals of S.

Therefore, S is not left Artinian.

Similarly, we can prove that S is not right Artinian.

7.4.14. Proposition. Let *R be* a P.I.D and $I \neq \{0\}$ be an ideal of R. Then, R/I is both Noetherian and Artinian.

Proof. Since R is P.I.D.,so every ideal of R is generated by a single element. Thus, every ideal of R is finitely generated and so R is Noetherian.

Now, R is Noetherian and a quotient ring of a Noetherian ring is a Noetherian, so R/I is Noetherian.

Let a ∈I be such that a= aR=$< a >$. Since I≠ {0}, so a ≠0.

If a=1 or a unit, then I=R and

R/I= R/R ≅ {R}= the zero ring .

But zero ring is trivially Artinian ring so R/I is Artinian.

Suppose, a is not a unit, then $a = a_1^{\alpha_1} a_2^{\alpha_2} ... a_m^{\alpha_m}$ where each $a_{i\,\mathrm{i}}$ is an irreducible element of R and each α_{i}' s are positive integers.

Let J/I be an ideal of R/I. Here, J is an ideal of R, so there exists an element b∈ J such that

J = bR = < b>

I = < a >⊆ J = <b>

which implies a= br for some r∈ R .

So, b/a.

Thus, $b = a_1^{\alpha_1} a_2^{\alpha_2} ... a_m^{\alpha_m}$ where $0 \le \beta_i \le \alpha_i$

Now each β_i can be selected in (α_i +1) ways.

Therefore, the number of choices for b is (α_1 +1) (α_2 +1)... (α_n +1), so the number of choices for b is (α_1 +1) (α_2 +1)... (α_n +1), which means the number of choice for J/I is

(α_1 +1) (α_2 +1)... (α_n +1)

Thus, R/I has only finite number of ideals.

We know that a ring which has finite number of ideals is an Artinian ring.

7.5. Ring of Homomorphisms. The collection of all homomorphisms from a R-module M to itself is denoted by $Hom_R(M, M)$ and is a ring.

7.5.1. Opposite ring. Let (R, +, .) be a ring. Then the opposite ring of R, denoted by R^{op}, is defined as the ring (R,+, o), where the operation o is given as

$$x \circ y = y.x \text{ for all } x, y \in R$$

Results.

(i) Let R be a ring and R_n denote the ring of $n \times n$ matrices over R then $(R_n)^{op} \cong (R^{op})_n$

(ii) If R is a division ring then R^{op} is also a division ring.

(iii) If a ring R is direct sum of rings $R_1, R_2, \ldots, R_k$ that is,, $R = R_1 \oplus R_2 \oplus ... \oplus R_k$, then

$R^{op} = R_1^{op} \oplus R_2^{op} \oplus ... \oplus R_k^{op}$.

(iv) Let M be a R-module such that $M = \sum_{\lambda\in\Lambda} M_\lambda$ is the sum of a family of simple R-modules $\{M_\lambda\}_{\lambda\in\Lambda}$, then there exists a sub- family $\{M_\lambda\}_{\lambda\in\Lambda'}$ such that $M = \oplus \sum_{\lambda\in\Lambda'} M_\lambda$

In words, we can say that if a R-module M is sum of simple R-modules, then it can be represented as the direct sum of a sub family of family of these simple R-modules.

Now, we will state some lemma´s, which will be useful for proving the Wedderburn- Artin Theorem.

7.5.2. Lemma. Let $M = M_1 \oplus M_2 \oplus ... \oplus M_n$ be a left R-module (M_i ´s are submodules of M) and let $A_{ij} = Hom_R(M_i M_j)$. Then,

$$Hom_R(M, M) = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix}.$$

7.5.3. Lemma. Let $M = M_1 \oplus M_2 \oplus ... \oplus M_n$, where $M_i \ncong M_j$, $i \neq j$ and each M_i is a simple R-sub module of M. Then

$$Hom_R(M, M) = \begin{pmatrix} D_1 & 0 & 0 & \dots & 0 \\ 0 & D_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & D_n \end{pmatrix}$$

where each Di=Aii and is a division ring.

7.5.4. Lemma. Let $M = M_1 \oplus M_2 \oplus ... \oplus M_n$, where M_i is simple and $M_i \cong M_j$ $\forall$ i and j. Suppose $Hom_R(M_1, M_1) = End_R(M_1) = D$ then, $Hom_R(M, M) \cong M_n(D)$

where, $M_n(D) = \begin{pmatrix} D & D & \dots & D \\ D & D & \dots & D \\ \dots & \dots & \dots & \dots \\ D & D & \dots & D \end{pmatrix}$, where D is a division ring.

7.5.5. Lemma. Let A be minimal left ideal of R. Then either $A^2=\{0\}$ or A=Re, e is an idempotent in A.

7.5.6. Wedderburn- Artin Theorem. Let R be left (or right) artinian ring with unity and no nonzero nilpotent ideal. Then, R is isomorphic to a finite direct sum of matrix rings over division rings.

Proof. First, we prove the following lemmas:

7.5.6.1. Lemma. Let R be a left Artinian ring with unity having no nonzero nilpotent ideals. Prove that every nonzero left ideal of R contains nonzero idempotents.

Proof. Let A be a nonzero left ideal of R and let

J_1={ B⊆A : B is a nonzero left ideal of R}

Now, A≠ {0}and A⊆A ⇨A∈ J_1, then

$J_1 \neq \emptyset$

Since R is left Artinian, therefore, J_1 has a minimal element, say B.

Then, B is a minimal left ideal of R.

Then, either $B^2 = \{0\}$ or B = Re for some idempotent e ∈ B.

Suppose B = {0}.

Consider the ideal J= BR

Then, $J^2 = BRBR \subseteq BBR = B^2R = \{0\}$.

Thus, J is a nilpotent ideal of R. By the given condition J = {0}, that is, BR = {0}.

Now, b = b.1∈ bR⊆ BR = {0}, which implies b=0 for all b∈ B and so B = {0}, a contradiction. Hence, B= Re

Now, B⊆ A and e = e.1 ∈ Re = B ⊆A, so

e ∈ A.

Thus, A contains nonzero idempotents.

7.5.6.2. Lemma. Let R be a left artinian ring with unity having no nonzero nilpotent ideals. Then, every left ideal of R is generated by an idempotent.

Proof. Let A be any left ideal of R and let S be the set of all nonzero idempotent of A. Then, S ≠ ∅, since by lemma 7.5.6.1., there exists an idempotent e ∈ A.

Now, consider the left ideal R(1-e) ∩ A, e ∈ S.

and let

J = { R(1-e) ∩ A, e ∈ S }

Since S is nonempty, so J ≠∅

Again R is left Artinian, since J has a maximal element, say R(1-e) ∩ A where e ∈ S.

We claim that R(1-e) ∩ A= {0}

Suppose R(1-e) ∩ A ≠ {0}. Then, it is a nonzero left ideal of R. Therefore, by lemma 7.5.6.1., this left ideal has a nonzero idempotent, say e_1.

Now, e_1 ∈ R(1-e) and e_1 ∈A

Now, e_1 ∈A $e_1 \neq 0$ ⇨ e_1 ∈ S.

Also, e_1∈ R(1-e) ⇨ e_1 = r(1-e) for some r∈ R, so

$e_1 e = r(1-e)e = r(e-e^2) = r(e-e) = r.0 = 0$

Let $e' = e + e_1 - e\,e_1 \in A$. Then

$e'^2 = e'e' = (e + e_1 - e\,e_1)(e + e_1 - e\,e_1)$

$= e^2 + e\,e_1 - e^2\,e_1 + e\,e_1 + e_1^2 - e_1\,e\,e_1 - e\,e_1\,e - e\,e_1^2 + e\,e_1\,e\,e_1$

$= e + e\,e_1 - e\,e_1 + 0 + e_1 - 0.e_1 - e.0 - e\,e_1 + e.0.e_1$

$= e + e_1 - e\,e_1 = e'$

and $e_1 e' = e_1 e + e_1^2 - e_1 e e_1 = 0 + e_1 - 0.e_1$

$= e_1 \neq 0$

Thus, $e_1 e' \neq 0 \Rightarrow e' \neq 0$ (*)

Hence,e' is an idempotent and so $e' \in S$.

But then $R(1-e') \cap A \in J$

Now, $r_1(1-e') = r_1(1-e-e_1 + e\,e_1) = r_1(1-e) - r_1 r(1-e) + r_1 e\,r(1-e) = R(1-e)$ [$r, r_1, e \in R$)

So, $R(1-e') \subseteq R(1-e)$

and thus, $R(1-e') \cap A \subseteq R(1-e) \cap A$.

Now, $e_1 \in R(1-e) \cap A$.

Suppose, $e_1 \in R(1-e') \cap A$. Then, $e_1 = s(1-e')$, $s \in R$, therefore

$e_1 e' = s(e' - e'^2) = s(e' - e') = 0$

a contradiction, because $e_1 e' \neq 0$ (by *)

Hence, $e_1 \notin R(1 - e') \cap A$

However, in that case $R(1 - e') \cap A \subsetneq R(1 - e) \cap A$.

Now, $R(1 - e') \cap A$ and $R(1 - e) \cap A \in J_2$ and $R(1 - e) \cap A$ is the minimal element of J_2, a contradiction.

The contradiction proves that

$R(1 - e) \cap A = \{0\}$ (**)

Let $a \in A$, then $a(1 - e) = a - ae \in A$ and $a(1 - e) \in R(1 - e)$

implies, $a(1 - e) \in R(1 - e) \cap A = \{0\}$

implies, $a(1 - e) \in \{0\}$

implies, $a(1-e) = 0$ for all $a \in A$

implies, $a = ae$ for all $a \in A$

implies, $A \subseteq Ae \subseteq Re \subseteq A$

implies, $A = Re$

Hence, every left ideal of R is generated by an idempotent.

7.5.6.3. Lemma. Let R be a left Artinian ring with unity having no non-zero nilpotent ideal. Let J be the set of all non -zero minimal left ideals of R. Prove that R= $\sum_{\lambda\in\Lambda} I_\lambda$; J ={ I_λ:$\lambda\in\Lambda$}.

Proof. Let J be the set of all minimal left ideals of R.

Since R is left Artinian, so J ≠φ. Let J = { I_λ }$_{\lambda\in\Lambda}$. Put I= $\sum_{\lambda\in\Lambda} I_\lambda$. Then, I is a left ideal of R. By lemma 7.5.6.2., there exists an idempotent e ∈ I such that I = Re.

We claim that R(1-e) ={0}. Now, this left ideal will contain a minimal left ideal of R, say B, so

B ∈ J, which implies B ⊆ I = Re

Now, B ⊆ Re ∩ R(1 - e) = {0} (By (**))

which implies B = {0}

A contradiction. Hence,

R(1-e) ={0} ⇨R =Re.

Hence, I = Re = R, and so R= $\sum_{\lambda\in\Lambda} I_\lambda$.

Proof of the theorem . We know that a minimal left ideal is a simple submodule of R^R.

⇨ R^R is the sum of simple submodules.

Therefore, there exists a subset $\Lambda' \subseteq \Lambda$ such that

$R^R = \oplus\sum I_\lambda$.

Now, $1 \in R = R^R$, therefore

$1 = x_{\lambda 1} + x_{\lambda 2} + ... + x_{\lambda n}$, where $\lambda_i \in \Lambda'$

so, $r = rx_{\lambda 1} + r x_{\lambda 2} + ... + r x_{\lambda n}$,

so, $R \subseteq I_{\lambda 1} + I_{\lambda 2} + ... + I_{\lambda n} \subseteq R^R$

so, $R^R \subseteq I_{\lambda 1} + I_{\lambda 2} + ... + I_{\lambda n}$

We may assume that

$R = R^R = I_1 \oplus I_2 \oplus ... \oplus I_n$.

where each I_j is a minimal left ideal of R.

Suppose $I_j = R_{ej}$ where $e_j \in I_j$ is an idempotent.

Thus we may write

$R = R^R = R_{e1} \oplus R_{e2} \oplus ... \oplus R_{en}$

Suppose

$$R = R^R = (R_{e1} \oplus R_{e2} \oplus \ldots \oplus R_{en}) \oplus (R_{e1} \oplus R_{e2} \oplus \ldots \oplus R_{en})$$

where $n_k = n$, where every two ideals in every bracket are isomorphic as left R-module and the ideals in the different brackets are not isomorphic. (This can be done if necessary by rearranging and renumbering the ideals in the desired form).

Take $R = M_1 \oplus M_2 \oplus \ldots \oplus M_k$, where M_i is the sum of left ideals in the ith bracket.

Then, $\mathrm{Hom}(R^R, R^R) \cong \begin{pmatrix} A_{11} & A_{12} & \ldots & A_{1k} \\ \ldots & \ldots & \ldots & \ldots \\ A_{k1} & A_{k2} & \ldots & A_{kk} \end{pmatrix}_{n \times n}$

where $A_{ij} = \mathrm{Hom}_R(M_i, M_j)$

We know that

(i) if $X = X_1 \oplus X_2 \oplus \ldots \oplus X_m$, where each X_i is a left R- module of M such that

$\mathrm{Hom}_R(X_j, X_i) = \{0\}$ for all $i \neq j$.

Then, $\mathrm{Hom}_R(X_i, X_j) = \begin{pmatrix} A_{11} & 0 & \ldots & 0 \\ 0 & A_{22} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & A_{mm} \end{pmatrix}$, where $A_{ij} = \mathrm{Hom}_R(X_j, X_i)$.

(ii) If $B = B_1 \oplus B_2 \oplus \ldots \oplus B_m$ and $C = C_1 \oplus C_2 \oplus \ldots \oplus C_t$, where B_i's & C_i's are simple submodules of M & $B_i \ncong C_j$ for all $i \neq j$, then $\mathrm{Hom}_R(B, C) = \{0\}$

(iii) if $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ and each A_i is simple and $A_i \cong A_j$ for all $i \neq j$, then,

$\mathrm{Hom}_R(A, A) \cong M_m(D)$, where $D = \mathrm{Hom}_R(A_1, A_1)$ is a division ring.

Using all these, we conclude that

$A_{ij} = \mathrm{Hom}_R(M_j, M_i) = \{0\}$ if $i \neq j$.

and $A_{ii} = \mathrm{Hom}_R(M_i, M_i) \cong M_{t_i}(D_i)$,

where $D_i \cong \mathrm{Hom}_R\left(\mathrm{Re}_{n_{i-1}+1}, \mathrm{Re}_{n_{i-1}+1}\right)$ and $M_i = \left(\mathrm{Re}_{n_{i-1}+1} \oplus \ldots \oplus \mathrm{Re}_{n_i}\right)$

Hence,

$$\mathrm{Hom}\left(R^R, R^R\right) \cong \begin{pmatrix} M_{t_1}(D_1) & 0 & \ldots & 0 \\ 0 & M_{t_2}(D_2) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & M_{t_k}(D_k) \end{pmatrix}$$

$$\cong M_{t_1}(D_1) \times M_{t_2}(D_2) \times \ldots\ldots\ldots \times M_{t_k}(D_k)$$

We Know that $R^{op} \cong Hom_R(R^R, R^R)$

Hence, R^{op} is isomorphic to finite direct product of matrix rings over the division rings .

From this we conclude that $R = (R^{op})^{op}$ is also isomorphic to finite direct product of matrix rings over the division ring.

7.5.7. Maschke Theorem. If F is the field of complex numbers and G is a finite group, then

$$F(G) \simeq F_{n_1} \oplus ... \oplus F_{n_k}$$

for some positive integers $n_1, ..., n_k$.

Proof. We first prove that $F(G)$ has no non zero nilpotent ideals.

Let $G = \{g_1 = e, g_2, ..., g_n\}$, and $x = \sum \alpha_i g_i \in F(G)$. Set $x^* = \sum \bar{\alpha}_i g_i^{-1}$, where $\bar{\alpha}_i$ denotes the complex conjugate of α_i. Then

$$xx^* = \sum_{i=1}^{n} |\alpha_i|^2 + \sum_{i=2}^{n} \beta_i g_i$$

for some $\beta_i \in F$. Hence, $xx^* = 0$ implies $\sum_{i=1}^{n} |\alpha_i|^2 = 0$, so each $\alpha_i = 0$; that is $x = 0$. Thus, $xx^* = 0$ implies $x = 0$. Let A be a nilpotent ideal in $F(G)$. Let $a \in A$. Then $aa^* \in A$, so aa^* is nilpotent, say $(aa^*)^r = 0$. (We may assume *r* is even.) Set $b = (aa^*)^{\frac{r}{2}}$. Then $b^2 = 0$ and $b = b^*$. Thus, $bb^* = 0$, which gives $(aa^*)^{\frac{r}{2}} = b = 0$. Proceeding like this, we get $aa^* = 0$. Hence, $a = 0$, which proves that $A = (0)$. Hence, $F(G)$ has no nonzero nilpotent ideals.

Further, $F(G)$ is a finite-dimensional algebra with unity over the field F. Therefore, $F(G)$ is an artinian ring. Then by the Wedderburn –Artin theorem,

$$F(G) \simeq D_{n_1}^{(1)} \oplus ... \oplus D_{n_k}^{(k)},$$

Where $D^{(i)}, 1 \le i \le k$, are division rings. Now each $D_{n_i}^{(i)}$ contains a copy K of F in its center. In this way each $D_{n_i}^{(i)}$ is a finite dimensional algebra over K (How?). Let $\left[D^{(i)} : K\right] = n$, and $a \in D^{(i)}$. Then $1, a, a^2, ..., a^n$ are linearly dependent over K. Thus, there exist $\alpha_0, \alpha_1, ..., \alpha_n$ (not all zero) in K such that $\alpha_0 + \alpha_1 a + ... + \alpha_n a^n = 0$. But since K is algebraically closed, $\alpha_0 + \alpha_1 x + ... + \alpha_n x^n \in K[x]$ has all its roots in K. Hence, $a \in K$, which shows that $D^{(i)} = K \simeq F$ and completes the proof.

7.6. Radical ideal. A two-sided ideal I in a ring R with unity is called a radical ideal with respect to a specified property P if

1 . the ideal I possesses the property P and

2. the ideal I is maximal for the property P, that is, if J is a 2-sided ideal of R having the property P, then $J \subseteq I$.

7.6.1. Jacobson radical. Let R be a ring with unity, then the Jacobson radical denoted by J(R) is a radical ideal of R defined as

$J(R) = \{a \in R : 1 - a \text{ is a unit in } R\}$.

7.6.2. Example. In the ring of integers, $J(Z) = (0)$.

7.6.3. Radical of an Art inian Ring.

7.6.4. Proposition. The Jacobson radical of an Artinian ring is the intersection of some finitely many maximal left (right) ideals.

Proof. Let R be an Artinian ring and τ be the family of all maximal left ideals of R. Let F be the family of all left ideals of R each of which is an intersection of finitely many maximal left ideals of R. Obviously $F \neq \phi$ as $\tau \subseteq F$. Since R is Artinian, therefore, F has a minimal member, say $J_0 = \bigcap_{i=1}^{n} M_i$, where $M_i \in \tau$. By definition of Jacobson radical, $J(R) \subseteq J_0$.

If $M \in \tau$, then $J_0 \cap M \in F$ and so $J_0 \cap M = J_0$, by the minimality of J_0 which means that $J_0 \subseteq M$, for all $M \in \tau$. Thus we get that $J(R) \subseteq J_0 \subseteq \bigcap_{m \in \tau} M_i = J$ and hence $J = J_0$, as required.

7.6.5. Exercise. In a commutative Artinian ring, the only maximal ideals are $M_i, 1 \leq i \leq n$, where $J(R) = \bigcap_{i=1}^{n} M_i$.

7.7. Check Your Progress.

1. Every division ring is Noetherian.

2. An Artinian integral domain with atleast two elements is a field.

3. Subring of an Artinian ring need not be Artinian.

7.8. Summary.

In this section, we obtained results for Noetherian and Artinian. The relation between nil and nilpotent ideals. Also, observed that every nil ideal is nilpotent but the converse statement need not be true. Also the difference between these two is really interesting to study.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. I: Groups, Vol. III: Modules, Narosa Publishing House (Vol. I – 2013, Vol. III –2013).
2. Lanski, C. Concepts in Abstract Algebra, American Mathematical Society, First Indian Edition, 2010.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Malik, D.S., Mordenson, J.N. and Sen, M.K., Fundamentals of Abstract Algebra, McGraw Hill, International Edition, 1997.
5. Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
6. Musili, C., Introduction to Rings and Modules, Narosa Publication House, 1994.
7. Jacobson, N., Basic Algebra, Vol. I & II, W.H Freeman, 1980 (also published by Hindustan Publishing Company).
8. Artin, M., Algebra, Prentice-Hall of India, 1991.
9. Macdonald, I. D., The Theory of Groups, Clarendon Press, 1968.