Group Theory SOS Report

Mentee: Sumit Kumar Adhya
Mentor: Sahil Kumar Rathour

July 2024

Contents

1 Groups

Definition 1.1. *A non empty set G, together with a binary composition * (star) is defined to be a group, if it satisfies the following postulates:*

1. *Associativity: a * (b * c) = (a * b) * c, for all a, b, c.*

2. *Existence of Identity: $\exists$ an element $e \in$ G, s.t., a * e = e * a = a for all a (e is then called identity).*

3. *Existence of Inverse: For every $a \in$ G, $\exists$ a' $\in$ G s.t., a * a' = a' * a = e (a' is then called inverse of a)*

Definition 1.2. *If a*b = b*a $\forall$ a,b $\in$ G. Then G is said to be an abelian group.*

Example 1.1. *Real numbers under addition form a group as $a + (b + c) = (a + b) + c$, $a + 0 = 0 + a = a$ and $a + (-a) = (-a) + a = 0$ where $a, b, c \in \mathbb{R}$ and 0 is the identity and inverse of a being (-a). It is an abelian group as $a + b = b + a$ for $a, b \in \mathbb{R}$.*

Definition 1.3. *Order of a group G: no. of elements in G, denoted by o(G) or $|G|$.*

Theorem 1.1. *In a group G, the properties hold true:*

1. *Identity element e is unique.*

2. *Inverse of each a is unique.*

3. $(a^{-1})^{-1}$=a $\forall$ a $\in$ G

4. $(ab)^{-1} = b^{-1}a^{-1}$

5. *Cancellation laws:* $ab=ac \implies b=c$ *and* $ba=ca \implies b=c \; \forall \; a,b,c \in G$.

Proof. 1. Let there be two identities e and e' in a group G. Then since e is an identity, $ee' = e'e = e'$ and since e' is an identity, $e'e = ee' = e$. So, $e = e'$

2. Let there be two inverses a' and a'' of a. Then $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$

3. Since, a^{-1} is inverse of a, $aa^{-1} = a^{-1}a = e$ which also implies a is inverse of a^{-1}. So, $(a^{-1})^{-1} = a$

4. $ab(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1} = [a(bb^{-1})]a^{-1} = (ae)a^{-1} = e$. Similarly, $(b^{-1}a^{-1})ab = e$ and the result follows

5. Let $ab = ac$, then $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = ec = c$

□

Theorem 1.2. *For elements* $a,b \in G$, $ax=b$ *and* $ya=b$ *have unique solutions for x and y in G.*

Theorem 1.3. *A non empty set together with a defined binary composition is a group iff:*

1. $(ab)c=a(bc) \; \forall \; a,b,c \in G$.

2. $ax=b$ *and* $ya=b$ *have solutions in* $G \; \forall \; a,b \in G$.

Theorem 1.4. *A set G with a binary composition forms a group iff:*

1. $(ab)c=a(bc) \; \forall \; a,b,c \in G$

2. $\exists \; e \in G$, *s.t* $ae=a \; \forall \; a \in G$.

3. $\forall \; a \in G, \exists \; a' \in G$ *s.t* $aa'=e$

The same theorem also holds if ea=a and a'a=e in 2. and 3. respectively.

2 Subgroups

Definition 2.1. *Let H be a non-empty subset of a group G, then it's a subgroup of G if it forms a group under the binary composition of G.*

Theorem 2.1. *A non-empty subset H of a group G is a subgroup of G iff:*

1. $a,b \in H \implies ab \in H$.
2. $a \in H \implies a^{-1} \in H$

Proof. It's easy to see if H is a subgroup then both of the conditions hold. Conversely, if (i) and (ii) hold true then, from (i), closure property is satisfied and as $H \subseteq G$, associative property would be satisfied in H as well. From (ii), the inverse exists and from (i) and (ii), $aa^{-1} \in H$ and so $e \in H$. So H is a subgroup. □

Theorem 2.2. *A non-empty subset H of a group G is a subgroup of G iff $a,b \in H \implies ab^{-1} \in H$.*

Proof. Again it's easy to see that if H is a subgroup, the above condition holds true. Conversely, $aa^{-1} \in H \implies e \in H$. Now as $e, a \in H$, $ea^{-1} = a^{-1} \in H$. So the inverse exists. Finally for $a, b \in H \implies a, b^{-1} \in H \implies a(b^{-1})^{-1} \in H \implies ab \in H$. Now by the previous theorem, H is a subgroup of G. □

Theorem 2.3. *A non empty finite subset H of a group G is a subgroup of G iff H satisfies the closure property under multiplication.*

Definition 2.2. *Centre of a group G: $Z(G) = \{x \in G \mid xg=gx \; \forall \; g \in G.\}$*

Theorem 2.4. *Centre of a group G is a subgroup of G.*

If Z(G)=G $\longleftrightarrow$ G is abelian.

Definition 2.3. *Normalizer/Centralizer of a: N(a) = $\{x \in G \mid xa{=}ax\}$ for some $a \in G$.*

It is a subgroup of G.

Theorem 2.5. *Union of two subgroups is a subgroup iff one of them is contained in the other.*

Definition 2.4. *Let H be a subgroup of G. For a,b $\in$ G, if $ab^{-1} \in H$, we say a is congruent to b mod H or $a \equiv b$ mod H*

This relation is an equivalence relation. Corresponding to this, we therefore get equivalence classes. For any a $\in$ G, the equivalence class of a is cl(a)={x$\in$G | x $\equiv$a mod H}

3 Right and Left cosets

Definition 3.1. *Right or Left coset of H in G is Ha=$\{ha \mid h \in H\}$ or aH=$\{ah \mid h \in H\}$ respectively.*

A coset may not be a subgroup.

Theorem 3.1. *Ha=cl(a) for any $a \in G$. Therefore, Right cosets are equivalence classes.*

Proof. Let $x \in Ha$, then $x = ha$ for some $h \in H$. So, $xa^{-1} \in H \implies x \in cl(a) \implies Ha \subseteq cl(a)$. Again let $x \in cl(a) \implies x \equiv a \ mod \ H \implies xa^{-1} \in H \implies x = ha \in Ha$ for some $h \in H$. Thus $cl(a) \subseteq Ha$ and hence $Ha = cl(a)$ $\square$

Two important properties of equivalence classes:

- Two equivalence classes are either identical or disjoint
- Union of all equivalence classes is the original set

From this we can conclude the following theorem.

Theorem 3.2. *Two right cosets in G are either equal or have no element in common and the union of all right cosets in G is equal to G.*

Theorem 3.3. *There is always a one-one onto mapping between any two right cosets of H in G.*

Theorem 3.4. *If G is finite, all right cosets of a subgroup H in G have same number of elements as in H.*

Theorem 3.5. *Lagrange's theorem:- If H is a subgroup of a finite group G $\rightarrow$ o(H) divides o(G).*

Corollary 3.5.1. *If a group G is of prime order, then it will have only 2 subgroups, G and $\{e\}$.*

Corollary 3.5.2. *A subset $H \neq G$ with more than half the elements of G cannot be a subgroup of G.*

Definition 3.2. *The index of a subgroup H in G is the no. of distinct right(left) cosets of H in G, denoted by $i_G(H)$ or [G:H]*

Theorem 3.6. *If G is finite $\rightarrow i_G = \frac{o(G)}{o(H)}$.*

It is possible for an infinite group G to have a subgroup H with a finite index.

Example 3.1. G= $\langle Z, + \rangle$, H = {3n | n ∈ Z}. H has only 3 right cosets in G → H, H+1, H+2.

Definition 3.3. *Let H be a subgroup of G. Then C(H) =* $\{x \in G \mid xh{=}hx\ \forall h \in H\}$ *is called the centralizer of H in G and N(H) =* $\{x \in G \mid xH{=}Hx\}$ *is called the normalizer of H in G.*

It can be shown very simply that C(H) ⊆ N(H).

Theorem 3.7. *C(H)=G* $\iff$ *H ⊆ Z(G), for some subgroup H of group G.*

4 Cyclic groups

Definition 4.1. *Order of an element: o(a) or* $|a|$ *is the least positive integer n s.t* $a^n = e$

Definition 4.2. *Cyclic group:- A group G is defined to be a cyclic group if* $\exists$ *an element* $a \in$ *s.t every element of G can be expressed as a power of a. In that case a is called the generator of G, denoted by* $G = \langle a \rangle$ *or (a).*

Example 4.1. *The group of integers under addition is a cyclic group, 1 and -1 being it's generators.*

Example 4.2. *The group* $G = \{1, -1, i, -i\}$ *under multiplication is cyclic as we can express it's members as* i, i^2, i^3, i^4*, so, i is it's generator.*

It's easy to see that if a is a generator, a^{-1} is too. It can also be easily deduced that a cyclic group is abelian but the converse may not be true.

Theorem 4.1. *Order of a cyclic group is equal to the order of it's generator.*

Theorem 4.2. *Subgroup of a cyclic group is cyclic and $a^m \in H$ s.t m is least possible integer is the generator of H.*

Theorem 4.3. *If G is a finite group then order of any element of G divides order of G.$\rightarrow a^{o(G)} = e$*

Theorem 4.4. *If G is a finite cyclic group of order n, then the no. of distinct subgroups of G is the no. of distinct divisors of n and there is unique subgroup of G of any given order. If $m \mid n$, then for o(H) = $m \rightarrow H = \langle a^{\frac{m}{n}} \rangle$*

Theorem 4.5. *A group of prime order must be cyclic and every element of G other than the identity element can be taken as it's generator.*

Corollary 4.5.1. *A group of prime order is abelian.*

5 Normal Subgroups

Definition 5.1. *A subgroup H of a group G is called a normal subgroup of G if $Ha = aH$ for all $a \in G$. A normal subgroup is also called invariant or self conjugate subgroup. The notation $H \trianglelefteq G$ is used to convey that H is normal in G.*

G and {e} are normal subgroups of G and are referred to as the trivial normal subgroups.

Definition 5.2. *A group $G \neq \{e\}$ is called a simple group if the only normal subgroups of G are $\{e\}$ and G.*

Any group of prime order is simple.

Theorem 5.1. *A subgroup H of a group G is normal in G iff $g^{-1}Hg = H$ $\forall$ $g \in G$.*

Theorem 5.2. *A subgroup H of a group G is normal in G iff* $g^{-1}hg \in H \ \forall$ $h \in H$, $g \in G$.

Theorem 5.3. *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: HaHb=Hab.*

6 Quotient Groups

Definition 6.1. *Let G be a group and N, a normal subgroup of G. The set of all right or left (they are the same as N is normal) cosets of N is denoted by* $\frac{G}{N}$ *or G/N. This set satifies the closure property by the previous theorem and the associative property as well. It can be easily seen that the identity of this set is Ne (as* $NaNe = Nae = Na = Nea = NeNa$*, for any right coset Na where e is the identity of G). And also for any right coset Na,* Na^{-1} *is the inverse of Na, as* $NaNa^{-1} = Naa^{-1} = Ne = Na^{-1}a = Na^{-1}Na$*. So the set G/N satisfies the properties of a group. It is defined as the Quotient Group.*

Theorem 6.1. *For an abelian group G, any of it's quotient group will be abelian. The converse may not be true.*

From theorem 3.6 we can conclude the following:

Theorem 6.2. $o(\frac{G}{N}) = \frac{o(G)}{o(N)}$

Theorem 6.3. *For a cyclic group G, it's quotient groups will be cyclic.*

If G = $\langle a \rangle,\ o(\frac{G}{H}) = \langle Ha \rangle$

7 Homomorphisms and Isomorphisms

Definition 7.1. *Let $\langle G, *\rangle$ and $\langle G, \cdot\rangle$ be two groups. A map $f : G \to G$' is defined to be a homomorphism if $f(a * b) = f(a) \cdot f(b)$; a,$b \in G$ or $f(ab) = f(a)f(b)$.*

Definition 7.2. *In addition to the above if f happens to be a one-one onto map, then it is known as an isomorphism and in that case we write $G \cong G'$.*

7.1 Some more definitions:

1. An onto homomorphism is called an epimorphism.
2. A one-one homomorphism is called a monomorphism.
3. A homomorphism from group G to itself is called endomorphism of G.
4. An isomorphism from group G to itself is called an automorphism.
5. If $f : G \to G'$ is onto homomorphism, then G' is called homomorphic image of G.

Some basic properties of a homomorphism $f : G \to G'$: i. $f(e) = e'$ ii. $f(x^{-1}) = [f(x)]^{-1}$ iii. $f(x^n) = [f(x)]^n$

Definition 7.3. *Let $f : G \to G'$ be a homorphism. The Kernel of f (Ker f) is defined by:*

$$Ker f = \{x \in G \mid f(x) = e'\}$$

Theorem 7.1. *If $f : G \to G'$ be a homomorphism, then Ker f is a normal subgroup of G.*

Theorem 7.2. *If $f : G \to G'$ be a homomorphism, then it's one-one iff $Kerf = \{e\}$*

Theorem 7.3. Fundamental theorem of group homomorphism: If $f : G \to G'$ be an onto homomorphism, then $\frac{G}{Kerf} \cong G'$

8 Dihedral Group

Definition 8.1. *We define a group $G = \{x^i y^j \mid i = 0, 1; j = 0, 1, ..., n-1;\ x^2 = e;\ y^n = e;\ xy = yx^{-1}\}$*

So, $o(G) = 2n, G = D_{2n}$. If n = odd, $Z(G) = \{e\}$ otherwise $Z(G) = \{e, y^m\}$ where $n = 2m$.

9 Permutation Groups

Let S be a non-empty set. Any one-one onto map $f : S \to S$ is called a permutation of S.

Definition 9.1. *The set A(S) of all permutations of S satisfies the properties of a group, and is therefore defined as the symmetric group. Any subgroup of the symmetric group is the permutation group*

Let G be group and A(G) be the symmetric group on G. For any a∈G, let's define a map: $f_a : G \to G$ s.t, $f_a(x) = ax$ is a one-one onto map. So it's a permutation. Set of all these permutations is K which is a permutation group (a subgroup of A(G)).

Theorem 9.1. Cayley's Theorem: Every group G is isomorphic to a permutation group.

Example 9.1. *$\phi : G \to K$ s.t $\phi(a) = f_a$ is an isomorphism. So $G \cong K$.*

10 Generators of a subgroup

Let a non-empty subset of a group G be S. Now, let us define the following set:

$$H = \{x_1 x_2 x_3 \dots x_n | n \text{ is finite but not fixed}, x_i \in S\}$$

. Then H is a subgroup of G and contains S. S is then defined to be it's generator and we write $H = \langle S \rangle$

Theorem 10.1. *$H = \langle S \rangle$ is the smallest subgroup of G containing S. And it is the intersection of all groups of G containing S.*

11 Commutators

Definition 11.1. *Let G be a group and a,b∈G, then we define the commutator of a and b to be $a^{-1}b^{-1}ab$.*

Definition 11.2. *Let's denote the set of all commutators in a group G to be S and G' be the subgroup generated by S, then G' is called the commutator subgroup of G or the derived group of G.*

Theorem 11.1. *Let G' be the commutator subgroup of G, then the following statements hold:*

1. *G' is normal in G.*
2. *G/G' is abelian.*
3. *G' is the smallest subgroup of G s.t G/G' is abelian.*
4. *If $H \leq G$ s.t $G' \subseteq H$, then $H \trianglelefteq G$.*

12 Automorphisms and Inner Automorphisms

As defined earlier, it is an isomorphism $f : G \to G$, where G is a group.

Theorem 12.1. *Let Aut G denote the set of all automorphisms of a group G and A(G) the group of all permutations of G. Then Aut G is a subgroup of A(G), Aut* $G \leq A(G)$.

Definition 12.1. *Let* $g \in G$, *where G is a group. We define the map* $T_g : G \to G$ *s.t* $T_g(x) = gxg^{-1}\ \forall x \in G$ *an inner automorphism.*

Theorem 12.2. *The I(G) of all inner automorphisms of G is a subgroup of Aut G.*

Theorem 12.3. *If* T_{g_1} *and* T_{g_2} *are inner automorphisms on G, for some* $g_1, g_2 \in G$, *then* $T_{g_1} = T_{g_2}$ *when* $g_2 g_1^{-1} \in Z(G)$ *or* $g_1 Z(G) = g_2 Z(G)$, *where Z(G) is the centre of the group G.*

Theorem 12.4. $\frac{G}{Z(G)} \cong I(G)$,*for some group G, where Z(G) and I(G) are as defined above.*

13 Characteristic Subgroup

Definition 13.1. *A subgroup H of G is called a characteristic subgroup of G if:* $T(H) \subseteq H\ \forall\, T\ \in\ AutG$.

Theorem 13.1. *A characteristic subgroup of a group G is a normal subgroup on G.*

14 Conjugates and Conjugacy Classes

Definition 14.1. *Let G be a group and $a, b \in G$, we say a is conjugate to b or that a and b are conjugates, denoted by $a \sim b$ if $\exists\ c \in G$, s.t $a = c^{-1}bc$ and relation $\sim$ (which is an equivalence relation) is called the conjugate relation on G. And the set of all conjugates of a in G, denoted by $cl(a) = \{x \in G | x \sim a\} = \{y^{-1}ay | y \in G\}$, is known as the conjugate class or conjugacy class of a in G.*

Theorem 14.1. *$cl(a) = \{a\}$ iff $a \in Z(G)$ and if this holds true for all $a \in G$, then G is abelian and vice-versa.*

Theorem 14.2. *Let K(G) or K denote the number of conjugacy classes in G. Now, if $o(G) = K(G)$ then G is abelian and vice-versa.*

Definition 14.2. *Let $H \leq G$ and $g \in G$. Then $g^{-1}Hg$ is known as the conjugate of H in G and the set $\{g^{-1}Hg \mid g \in G\} = cl(H)$ is conjugacy class of H in G.*

Theorem 14.3. Cauchy's Theorem: Let G be a finite group and p be a prime s.t $p \mid o(a)$, then $\exists x \in G$ s.t o(x)=p.

15 Similar Permutation

Theorem 15.1. *Two permutations $\sigma, \rho \in S_n$, (where S_n is the symmetric group on n elements, or the group of all possible bijections of a set X with n elements to itself) are called similar if they have the same cycle structure when decomposed as product of disjoint cycles.*

Theorem 15.2. *Two permutations σ and ρ are similar iff they are conjugate in S_n.*

16 p-Groups

Definition 16.1. *A group in which every element has order p^r, where p is prime and $r \in \mathbb{Z}$ (which may vary for different elements) is known as a p-group.*

Theorem 16.1. *A finite group G is a p-group iff $o(G) = p^r$.*

17 Sylow p-subgroups and Sylow's theorems

Definition 17.1. *Let p be a prime s.t $p^n|o(G)$ and $p^{n+1} \nmid o(G)$. Then a subgroup H of G is called a Sylow p-subgroup of G if $o(H) = p^n$.*

Theorem 17.1 (Sylow's First theorem)**.** *Let p be a prime and m, a positive integer s.t $p^m|o(G)$. The there exists a subgroup H of G such that $o(H) = p^m$*

Definition 17.2 (Double cosets)**.** *Let H,K be subgroups of G and $a, b \in G$. Define a relation $' \sim'$ on G as:*
$a \sim b$ iff $\exists\ h \in H,\ k \in K$ s.t $a = hbk$
$' \sim'$ is an equivalence relation on G. So it divides G into disjoint equivalence classes. Equivalence class of $a \in G$ is therefore:
$cl(a) = x \in G|a \sim x = HaK$, called double coset of H and K in G.

Theorem 17.2 (Sylow's Second theorem)**.** *Any two p-Sylow subgroups of a finite group G are conjugate in G.*

Theorem 17.3. *Number of Sylow p-subgroups of G is equal to $\frac{o(G)}{o(N(P))}$, where P is a p-Sylow subgroup of G.*

Theorem 17.4 (Sylow' Third theorem)**.** *Number of p-Sylow subgroups of G is of the form $1 + cp$ where $(1 + cp)|o(G)$, c being a non-negative integer.*

18 Direct Products

Definition 18.1. *For two groups G_1 and G_2, we define the direct product or external direct product (EDP) of G_1 and G_2 to be $G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}$ with the binary composition defined in it as $(g_1,\ g_2)(g_1',\ g_2') = (g_1g_1',\ g_2g_2')$. G forms a group under this composition.*

We can similarly define the direct product of n groups.
Now, let $G = G_1 \times \ldots \times G_n$
Define $H_i = \{e_1, e_2, \ldots, g_i, \ldots, e_n \mid g_i \in G\}$

Theorem 18.1. *H_i are normal subgroups of G and any element $g \in G$ can be uniquely written as a product of elements from $H_1, H_2, \ldots, H_n$*

Definition 18.2. *Let $H_1, H_2, \ldots, H_n$ be normal subgroups of G. G is said to be an internal direct product (IDP) of H_i if $G = H_1, \ldots, H_n$ and each $g \in G$ can be uniquely written as product of elements from $H_1, H_2, \ldots, H_n$*

Theorem 18.2. *Let H_1, H_2 be normal subgroups of G. Then G is an IDP of H_1 and H_2 iff:*

1. $G = H_1H_2 \ldots H_n$
2. $H_1 \cap H_2 = \{e\}$

Theorem 18.3. *Let $H_1, H_2, \ldots, H_n$ be normal subgroups of G. Then G is an IDP of $H_1, H_2, \ldots, H_n$ iff:*

1. $G = H_1H_2 \ldots H_n$
2. $H_i \cap H_1H_2 \ldots H_{i-1}H_{i+1} \ldots H_n = \{e\}$

Remark 1. *If G is an IDP of $H_1, H_2, \ldots, H_n$, then $H_i \cap H_j = \{e\}$ for some i,j s.t $i \neq j$*

Theorem 18.4. *Let G be the IDP of $H_1, H_2, \ldots, H_n$ and T be it's EDP. Then $G \cong T$.*

Theorem 18.5. *Let G and F be finite groups, their order being m and n respectively. If $gcd(m, n) = 1$, then $Aut(G) \times Aut(F) \cong Aut(G \times F)$*

19 Finite Abelian Groups

Definition 19.1. *Groups which can be written as the direct product of some 'simple looking groups'*

Theorem 19.1. *A finite abelian group can be written as a direct product of its Sylow p-subgroups.*

Theorem 19.2 (Fundamental Theorem on Finite Abelian Groups)**.** *A finite abelian group can be written as a direct product of cyclic groups of prime power order.*

20 Group Actions

Definition 20.1. *Let G be a group and A be a non-empty set, then G is said to act on A if $\exists$ a map $*$ from $G \times A \to A$ satisfying the following:*

1. $g_1 * (g_2 * a) = (g_1 g_2) * a$
2. $e * a = a \ \forall \ g_1, \ g_2 \in \ G$, *$e$ is the identity element of G and $a \in A$*

This mapping $*$ is called a group action of G on A and A is called a G-set.

This is an action on the left. We can similarly define action on the right.

Theorem 20.1. *Let A be a non-empty set and G be a group. Then any homomorphism $G \to Sym(A)$ defines an action of G on A. Conversely every action of G on A induces a homomorphism $G \to Sym(A)$. This homomorphism is sometimes called the associated (or corresponding) permutation representation of the given action.*

Definition 20.2. *For a group action $*$ of a group G on A, we define the Kernel $K(*)$ is defined to be: $K(*) = \{g \in G \mid g * a = a \; \forall \; a \in A\}$*

It can easily be seen that $K(*)$ is a subgroup of G.

Definition 20.3. *Let $a \in A$ be any fixed element. Then the set $G_a = \{g \in G \mid g * a = a\}$ is defined to be the stabilizer of a in G.*

G_a is a subgroup of G.

Definition 20.4. *For a group action $*$ of a group G on a set A, we then define the orbit of $a \in A$ under G to be: $Ga = \{g * a \mid g \in G\}$*

Theorem 20.2. *There exists a one-one onto map from Ga to the set of all left cosets of G_a, for some group G acting on set A and $a \in A$.*

Definition 20.5. *An action $G \times A \to A$ is called transitive if there exists only one orbit, said in a different way for $a,\ b \in A$, $a = g * b$ for some $g \in G$.*

21 Normal Series

Definition 21.1. *A normal subgroup $H \trianglelefteq G$ is said to be the maximal normal subgroup of G if $H \neq G$ and there $\nexists$ any normal subgroup K of G s.t., $H \subset K \subset G$.*

In a similar way, we can define maximal subgroups.

Definition 21.2. *A normal subgroup $H \trianglelefteq G$ is said to be the minimal normal subgroup of G if the only normal subgroups of G contained in H are e and H.*

Theorem 21.1. *H is a maximal normal subgroup of G iff G/H is simple.*

Definition 21.3. *Let G be a group. A sequence of subgroups $\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$ is called a normal series of G if G_i is a normal subgroup of G_{i+1}, $\forall\ i = 0,\ 1,\ 2, \ldots,\ n-1$*

The quotient groups $\frac{G_{i+1}}{G_i}$ $\forall\ i$ are called the factors of the normal series. The number of distinct members of the series is called the length of the normal series.

Definition 21.4. *Let G be a group. A sequence of subgroups $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ is called a composition series of G if G_i is a maximal normal subgroup of G_{i+1} and $G_i \neq G_{i+1}$ for any i.*

Theorem 21.2. *Every finite group G (with more than one element) has a composition series.*

Definition 21.5. *Two composition series:*
$C_1 : \{e\} = N_0 \subset N_1 \subset \ldots \subset N_t = G$
$C_2 : \{e\} = H_0 \subset H_1 \subset \ldots \subset H_m = G$
are equivalent if $t = m$ and each factor group of C_1 is isomorphic to some factor group of C_2

Theorem 21.3 (Jordan-Holder)**.** *Let G be a finite C_1 and C_2 be 2 composition series:*
$C_1 : \{e\} = N_0 \subset N_1 \subset \ldots \subset N_t = G$
$C_2 : \{e\} = H_0 \subset H_1 \subset \ldots \subset H_m = G,$
then $m = t$ and C_1 and C_2 are equivalent.

22 Solvable Groups

Definition 22.1. *A group G is said to be solvable or soluble if $\exists$ a series of subgroups:*

$$e = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$$

s.t. each H_i is a normal subgroup of H_{i+1} and $\frac{H_{i+1}}{H_i}$ is abelian.

Theorem 22.1. *Every cyclic group is solvable.*

Theorem 22.2. *A group G is a solvable group if and only if $G^{(m)} = \{e\}$ for some positive integer m.*

Theorem 22.3.

1. *A subgroup of a solvable group is solvable.*
2. *A homomorphic image of a solvable group is solvable.*
3. *A quotient group of a solvable group is solvable.*

23 Nilpotent Groups

Definition 23.1. *A group G is defined to be nilpotent if it has a normal series:*

$$e = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$$

such that $\frac{G_i}{G_{i-1}} \subseteq Z\left(\frac{G}{G_{i-1}}\right)$ for all i.

Theorem 23.1. *A nilpotent group is solvable. But the converse may not be true.*

Theorem 23.2. 1. *A subgroup of a nilpotent group is nilpotent.*

2. *A homomorphic image of a nilpotent group is nilpotent.*

3. *Any quotient group of a nilpotent group is nilpotent.*

References

[1] V.K. Khanna and S.K. Bhambri A course in Abstract Algebra, 4th ed.