Chapter - 2 : Structure of Finite Groups

Theorem .16 (Cauchy's Theorem for Finite Abelian Groups) *Let G be a finite abelian group, and let p be a prime such that p divides the order of G, denoted $|G|$. Then, G has an element of order p.*

Proof: Let $p \mid |G| \Rightarrow |G| = np$ for some integer n. We apply induction on n. If $n = 1$, then the result holds (In this case, G is cyclic, and there exists an element of order p, satisfying the result). Suppose the result is true for all abelian groups G' with $|G'| < |G|$. Since $|G| = np$ is not a prime, G must have a proper subgroup H (take any non-identity element a, and let H be the cyclic group it generates). By induction,

1. if $p \mid |H|$, there exists $a \in H$ such that $o(a) = p$. This a is in G as well.
2. if $p \nmid |H|$, we have $|G| = |H| \cdot |G/H|$ also $\Rightarrow p \mid |G/H|$ and $|G/H| < |G|$. By induction, there exists $bH \in G/H$ such that $|bH| = p$, i.e., $(bH)^p = H \Rightarrow b^p \in H \Rightarrow (b^p)^{|H|} = e \Rightarrow (b^{|H|})^p = e$. Choose $a = b^{|H|} \in G \Rightarrow a^p = e \Rightarrow o(a) \mid p$, and since p is prime, $o(a) = p$ (if $a = e$, then $b^{|H|} = e \Rightarrow (bH)^{|H|} = H \Rightarrow p \mid |H|$, which is a contradiction.

Hence the result. ■

Corollary .17 *The proof of the previous theorem is applicable exclusively to finite abelian groups G. For non-abelian groups, the process can be initiated from the point in the preceding theorem where $p \nmid |H|$.*

Hint(s): Then, by the class equation,

$$|G| = |Z(G)| + \sum_{a \in N} \frac{|G|}{|N(a)|}$$

Since G is non-abelian, there exists $a \in G$ such that $a \notin Z(G)$, leading to $N(a) \neq G$, and $|G| = |N(a)| \cdot \left|\frac{G}{N(a)}\right|$.

1. If $p \mid |N(a)|$ for any such $a \notin Z(G)$, then there exists $b \in N(a)$ such that $o(b) = p$, and $b \in G$.
2. If $p \nmid |N(a)|$ for all $a \notin Z(G)$, then from $p \mid \left|\frac{G}{N(a)}\right|$, we deduce $p \mid |Z(G)|$. Consequently, $Z(G)$ becomes a proper subgroup of G, with $p \mid |Z(G)|$. This implies the existence of $a \in Z(G)$ such that $o(a) = p$ and $a \in G$.

Thus, the result follows. ■

Note 17 *The converse of Lagrange's theorem is true for finite abelian groups, as shown in the next result.*

Theorem .18 *Let G be an abelian group such that $m \mid |G|$, where m is any integer. Then, G has a subgroup of order m.*

Proof: We use the induction method to prove the result. Let $|G| = n$. For $n = 1$, the result is trivial. Let $n > 1$. For $m = 1$, the result is obvious. For $m > 1$, there exists a prime p such that $p \mid m$, and consequently, $p \mid n$. Thus, there exists an element $a \in G$ with order $O(a) = p$. Construct the subgroup $H = \langle a \rangle$ (which is normal in G). If $m = p$, we are done. Now, consider $O(G/H) < O(G)$ and $O(G/H) = n/p$ and $(m/p) \mid (n/p)$. Therefore, there exists a subgroup K/H of G/H such that $O(K/H) = m/p$. Hence, there exists a subgroup K of G containing H such that $O(K) = O(H) \cdot O(K/H) = p \cdot m/p = m$. This concludes the result. ■

Remark 2 *As we know, the above result is not true for non-abelian groups; for example, A_4 has no subgroups of order 6.*

Theorem .19 (Sylow's First Theorem) *Let G be a finite group of order $n = p^k \cdot q$, where p is prime and q is any positive integer such that $(p,q) = 1$. Then, for each i, G has at least one subgroup of order p^i.*

Proof: We apply induction on the order of G. If $|G| = p$, *i.e.*, $k = 1$ and $q = 1$, the result is true. Let us assume that the result is true for all groups T of order less than $|G|$ and where $p \mid |T|$.

Case 1 If $p \mid |Z(G)|$, then there exists $a \in Z(G)$ such that $o(a) = p$. Let $H = \langle a \rangle$, and since a commutes with all elements in G, H is normal in G. If $k = 1$, H is the required subgroup. For $k > 1$, $|G/H| = p^{k-1} \cdot q < |G|$ and $p \mid |G/H|$. By induction, there exist subgroups $\frac{H_i}{H} \subseteq \frac{G}{H}$ for $i = 1, 2, \ldots, k-1$ with $o(H_i) = o(H) \cdot o(\frac{H_i}{H}) = p \cdot p^i = p^{i+1}$. Thus, G has subgroups H_i of order p^i for $i = 1, 2, \ldots, k$.

Case 2 If $p \nmid |Z(G)|$, then by the class equation, there exists $a \in G$ such that $p \nmid \frac{|G|}{|N(a)|}$, but $|G| = \frac{|G|}{|N(a)|} \cdot |N(a)| \Rightarrow p^k \mid |N(a)|$ and $|N(a)| < |G|$ (since G is non-abelian). By the induction hypothesis, $N(a)$ has a subgroup of order p^i, which is also a subgroup of G. Hence, the proof is complete. ∎

Note 18 *If G is abelian, then the proof of Sylow's first theorem is straightforward, the converse of lagrange's theorem for abelian groups.*

Definition .29 (p-group) *A group is a p-group if the order of each element is a power of p.*

The same condition applies to a p-subgroup.

Proposition .14 *A group G is a p-group if and only if $O(G) = p^k$ for some prime p and $k \geq 1$.*

Hint(s): *If q divides $O(G)$, then G has an element of order q.*

Example 1.9.2 (2-group) *1. D_4 2. K_4.*

If $O(G) = p^k.q$ such that $p^{k+1} \nmid O(G)$, where $(p,q) = 1$, then by Sylow's first theorem, there exists at least one subgroup of order p^k.

Definition .30 (Sylow p-subgroup) *A subgroup of G of order p^k is called a Sylow p-subgroup of G.*

Proposition .15 *All Sylow p-subgroups of G with $O(G) = p^k.q$ and $(p,q) = 1$ will have order p^k.*

Proposition .16 *Sylow p-subgroups of a group G may be more than one (not necessarily unique in general).*

Example 1.9.3 *Let $G = S_3$. Then $O(G) = 6 = 2.3$ and $2 \mid O(G)$, but $2^2 \nmid O(G)$. Thus, any subgroup of order 2 is a Sylow 2-subgroup of G. There are three subgroups of G of order 2:*

$$H_1 = \{e, (1\,2)\}$$
$$H_2 = \{e, (1\,3)\}$$
$$H_3 = \{e, (2\,3)\}$$

There are three Sylow 2-subgroups of S_3. However, there is only one subgroup of G of order 3, namely $K = \{e, (1\,2\,3), (1\,3\,2)\}$, which is the only Sylow 3-subgroup of S_3.

Definition .31 (Conjugate Groups) *Two subgroups K and H, of a group G, are said to be* ***conjugate*** *if there exists an element x in the group G such that*

$$K = x^{-1}Hx.$$

Observation in Example 1.9.3:

$$H_2 = (2\,3)H_1(2\,3)$$
$$H_3 = (1\,3)H_1(1\,3)$$
$$H_2 = (1\,2)H_3(1\,2)$$

In a general sense, it seems that these subgroups could be conjugate to each other.

Exercise 23 *Find all the Sylow 2-subgroups and Sylow 3-subgroups of A_4.*

Definition .32 (Double Coset) *Let H and K be two subgroups of a group G. For $x \in G$, define*

$$HxK = \{hxk : h \in H, k \in K\}$$

as a double coset.

Proposition .17 *The order of a group is given by $O(G) = \sum_{x \in H} \frac{O(H) \cdot O(K)}{O(x^{-1}Hx \cap K)} = \sum_{x \in H} \frac{O(H) \cdot O(K)}{O(H \cap xKx^{-1})}$ where $H, K \subseteq G$.*

Proof: *Let's define a relation for $a, b \in G$: $a \sim b$ if and only if $a = hbk$ for some $h \in H, k \in K$. This relation is clearly* *an equivalence relation and divides the group G into disjoint equivalence classes. Here,*

$$\begin{aligned} C_l(a) &= \{b : b \sim a\} \\ &= \{hak : h \in H, k \in K\} \\ &= HaK \\ \textit{Therefore, } O(G) &= \sum_{a \in M} O(HaK) \end{aligned}$$

where M is the set of representatives of double coset equivalence classes in G. Moreover, there is a one-to-one correspondence between

$$HaK \to HaKa^{-1}$$
$$hak \mapsto haka^{-1}$$

Hence, $O(HaK) = \frac{O(H)\cdot O(aKa^{-1})}{O(H \cap aKa^{-1})}$ *and* $O(aKa^{-1}) = O(K)$. *Therefore,*

$$O(G) = \sum_{a \in M} \frac{O(H)\cdot O(K)}{O(H \cap aKa^{-1})}$$

Using this result, we can prove Sylow's second theorem, which is about the relation among Sylow p-subgroups.

Theorem .20 (Sylow's Second Theorem) *All Sylow p-subgroups of a finite group G are conjugate to one another.*

Proof: *Let* $O(G) = p^k.q$ *where* $(p,q) = 1$. *Suppose P and Q are two Sylow p-subgroups of G such that* $O(P) = O(Q) = p^k$.
If possible, assume $P \neq gQg^{-1}$ *for any* $g \in G$. *Also, for all* $x \in G$, $O(PxQ) = \frac{O(P)\cdot O(Q)}{O(P \cap xQx^{-1})}$, *where PxQ is a double coset in G.*
Clearly, $P \cap xQx^{-1}$ *is contained in P. Let* $O(P \cap xQx^{-1}) = p^l$ *where* $l \leq k$.
If $l = k$, *then* $P \cap xQx^{-1} = P$, *implying* $P \subseteq xQx^{-1}$. *But* $O(Q) = O(xQx^{-1}) = p^k = O(P)$, *which leads to* $P = xQx^{-1}$, *contradicting our assumption.*
Thus, $l < k$. *Now,* $O(PxQ) = \frac{p^k \cdot p^k}{p^l} = p^{2k-l}$, *and since* $l < k$, *we have* $O(PxQ) = p^{k+1} \cdot p^{k-l-1}$ *where* $k - l - 1 \leq 0$.
Therefore, $p^{k+1} \mid O(PxQ)$ *for all* $x \in G$, *which contradicts the fact that* $(p,q) = 1$. *Hence, our assumption is false, and we conclude that P and Q are conjugate to each other.* ■

One-to-One Correspondence between $G/N(P)$ ***and*** $\mathbf{Cl}(P)$:

Let G be a group and P a subgroup of G. Consider the normalizer of P, denoted as $N(P)$, *which is defined as*

$$N(P) = \{g \in G \mid gPg^{-1} = P\}.$$

We aim to establish a one-to-one correspondence between the set of left cosets of $N(P)$ *in G, denoted as* $G/N(P)$, *and the collection of conjugates of P, denoted as* $Cl(P) = \{Q \,:\, Q = x^{-1}Px \;\; \text{for } x \in G\}$.

Let's define the mapping $\phi : G/N(P) \to Cl(P)$ *as follows:*

$$\phi : gN(P) \mapsto gPg^{-1}$$

where $g \in G$, *and* $gN(P)$ *represents the left coset of* $N(P)$ *containing g.*

1. (Well-definedness) Let $g_1, g_2 \in G$ *such that* $g_1N(P) = g_2N(P)$. *This means* $g_1^{-1}g_2 \in N(P)$. *Since* $g_1^{-1}g_2 \in N(P)$, *we have* $g_1^{-1}g_2Pg_1^{-1}g_2^{-1} = P$. *Thus,* $\phi(g_1N(P)) = g_1Pg_1^{-1} = g_2Pg_2^{-1} = \phi(g_2N(P))$, *demonstrating the well-definedness of* ϕ.

2. (Injective) Now suppose $\phi(g_1N(P)) = \phi(g_2N(P))$, *then* $g_1Pg_1^{-1} = g_2Pg_2^{-1}$. *This implies* $g_2^{-1}g_1 \in N(P)$, *so* $g_1N(P) = g_2N(P)$, *and* ϕ *is injective.*

3. (Surjective) Given any conjugate $gPg^{-1} \in Cl(P)$, *we can find the left coset* $gN(P) \in G/N(P)$ *such that* $\phi(gN(P)) = gPg^{-1}$. *This is true since* $\phi(gN(P)) = gPg^{-1}$ *by definition of* ϕ.

*Hence, **the number of Sylow p-subgroups** (which are actually conjugate to one another), denoted by n_p, equal to the order of the set $G/N(P)$.*

(Sylow's third theorem is concerned with the number of Sylow p-subgroups)

Theorem .21 (Sylow's Third Theorem) *Let G be a finite group of order $|G| = p^k \cdot q$, where p is a prime, q is any positive integer and p does not divide q. If n_p is the number of Sylow p-subgroups of G, then $n_p \equiv 1 \pmod p$ and n_p divides $|G|$.*

Proof: *Let P be a Sylow p-subgroup of G. Then $O(P) = p^k$.*

We can express G as the union of sets:

$$G = \bigcup_x PxP = \bigcup_{x\in N(P)} PxP \bigcup_{x\notin N(P)} PxP,$$

where $N(P)$ is the normalizer of P in G.

If $x \in N(P)$, then $Px = xP \Rightarrow PPx = PxP \Rightarrow Px = PxP$. Therefore, $\bigcup_{x\in N(P)} PxP = N(P)$.

On the other hand, when $x \notin N(P)$, it implies $x^{-1}Px \neq P \Rightarrow O(P\cap x^{-1}Px) = p^l$ where $l < k$ (if l=k, then $x^{-1}Px = P$). Consequently, $O(PxP) = \frac{O(P)\cdot O(P)}{O(P\cap x^{-1}Px)} = \frac{p^k \cdot p^k}{p^l} = p^{2k-l}$, where $l < k$.

Hence, we have:

$$O(G) = O(N(P)) + \sum_{x\notin N(P)} O(PxP) = O(N(P)) + \sum_{x\notin N(P)} p^{2k-l}$$

Therefore, $\frac{O(G)}{O(N(P))} = 1 + \sum_{x\notin N(P)} \frac{p^{2k-l}}{O(N(P))} = 1 + \sum_{x\notin N(P)} \frac{p^{k+1}.p^{k-l-1}}{O(N(P))}$, i.e., each term in the summation is a multiple of $\frac{p^{k+1}}{O(N(P))}$.

Since LHS is an integer n_p, so the summation is $\frac{u\cdot p^{k+1}}{O(N(P))}$ which is also an integer, where $u = \sum_{x\notin N(P)} p^{k-l-1}$. But since p^{k+1} does not divide $O(G)$, it follows that p^{k+1} does not divide $O(N(P))$. Hence, $\frac{u\cdot p^{k+1}}{O(N(P))}$ must be divisible by p.

Let us write $\frac{u\cdot p^{k+1}}{O(N(P))}$ as mp. Thus, $\frac{O(G)}{O(N(P)}(= n_p) = 1 + mp$, where $m \geq 0$. Clearly, $n_p \equiv 1 \pmod p$.
Also, $\frac{O(G)}{O(N(P)} = 1 + mp \Rightarrow 1 + mp$ divides $|G|$, i.e., n_p divides $|G|$.

Corollary .22 *Let G be a group of order $p^k q$, where p is a prime, q is any positive integer, and $(p,q) = 1$ $(k \geq 1)$. Then n_p must divide q.*

Proof: *Given n_p divides $p^k q$. Since $(1+mp, p) = (1+mp, p^k) = 1$, it follows that n_p must divide q (since if $a|bc$ and $(a,b) = 1$, implies $a|c$).*

Proposition .18 *A Sylow p-subgroup H of a finite group is unique if and only if H is normal in G.*

Proof: *Since xHx^{-1} is a conjugate of H and both are subgroups of G of some order, but if H is unique, then $xHx^{-1} = H \Rightarrow Hx = xH \ \forall\ x \in G \Rightarrow H$ is normal.*

Conversely, if H is normal and K is another Sylow p-subgroup of G, then $K = xHx^{-1}$ for some $x \in G$. But since $xH = Hx$, we have $K = Hxx^{-1} = H$, implying H is unique.

Definition .33 (External Direct Product) *Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, \ldots, G_n$, denoted as $G_1 \times G_2 \times \ldots \times G_n$, is defined as:*

$$G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\},$$

where $(g_1, g_2, \ldots, g_n)\cdot(g_{1'}, g_{2'}, \ldots, g_{n'})$ is defined to be $(g_1g_{1'}, g_2g_{2'}, \ldots, g_ng_{n'})$.

*Whereas the **internal direct product** of H and K, denoted as $G = H \otimes K$, if H and K are normal subgroups of G such that $G = HK$ and $H \cap K = \{e\}$.*

Exercise 24 *Let $G = H \times K$ such that H, K are cyclic. Prove that G is cyclic if and only if $(O(H), O(K)) = 1$.*

Hint(s): $O((a,b)) = lcm\{O(a), O(b)\}$.

Theorem .23 *Let G be a finite group of order pq, where p and q are distinct primes and $p < q$. Then G has a unique normal subgroup of order q. Moreover, if $p \nmid q-1$, then G is cyclic.*

Proof: *Since $O(G) = pq$, we have $n_q = 1 + kq \mid p$, where n_q is the number of Sylow q-subgroups. Therefore, $1 + kq = 1$ or $1 + kq = p$ (which is not possible since $p < q$). This implies $k = 0$, yielding $n_q = 1$. Hence, a unique subgroup exists of order q and it is a normal subgroup.*
Next, considering the condition $p \nmid q-1$, and observing that $n_p = 1 + mp \mid q$, we deduce that n_p can be either 1 or q. However, the latter option is contradictory (assuming $n_p = 1 + mp = q$, which implies $mp = q-1$, and then $p \mid q-1$). Thus, $m = 0$. As a result, the subgroup is unique, and so normal, of order p.

Now, let P and Q be two normal subgroups of G of order p and q respectively. Then $O(P \cap Q) \mid O(P)$ and $O(P \cap Q) \mid O(Q)$, i.e., $O(P \cap Q) \mid gcd(O(P), O(Q)) = (p,q) = 1$. This implies $O(PQ) = \frac{O(P) \cdot O(Q)}{1} = pq = O(G)$. Therefore, G is the direct product of P and Q, and since $(p,q) = 1$, P and Q are cyclic, making G a cyclic group.

Example 1.9.4 *Prove that every group of order 35 is cyclic.*

Solution: *Since $O(G) = 35 = 5 \cdot 7$, $p = 5$ and $q = 7$. Since $p < q$ and $p \nmid q$, we conclude that G is cyclic.*

Definition .34 (Simple Group) *A group G is said to be simple if it has no non-trivial normal subgroups.*

Example 1.9.5 *Prove that a group of order 40 is not simple.*

Solution: *Since $O(G) = 40 = 2^3 \cdot 5$, the number of Sylow 5-subgroups, denoted as n_5, must satisfy $1 + 5m \mid 8$. This implies $m = 0$, hence $n_5 = 1$, indicating the existence of a unique subgroup of order 5. Thus, G has a normal subgroup, so it is not simple.*

Exercise 25 *Prove that any group G of order pq is not simple, where p and q are distinct primes.*

Example 1.9.6 *Prove that in a group of order 14, there are only 6 elements of order 7.*

Solution: *By Cauchy's theorem, $7 \mid O(G) = 14$, which implies that there exists an element $a \in G$ with $O(a) = 7$. Construct the subgroup $H = \langle a \rangle = \{1, a, \cdots, a^6\}$ such that $O(a^i) = 7 \;\forall\; i = 1, 2, \cdots, 6$. We can prove that H is the unique subgroup of order 7. Suppose K is another subgroup; then $O(H \cap K) \mid 7$. If $O(H \cap K) = 7$, then $H = K$. If $O(H \cap K) = 1$, then $O(HK) = O(H) \cdot O(K) = 49 > O(G)$, which is a contradiction. Hence, H is the only subgroup of order 7.*

1.9.0.1. Finding the Number of Non-Isomorphic Abelian Groups

Exercise 26 *Let $m = n_1 n_2 \ldots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ if and only if n_i and n_j are relatively prime whenever $i \neq j$.*

For instance, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{30}$, but $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.

Fundamental Theorem of Finite Abelian Groups

Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Since a cyclic group of order n is isomorphic to $\mathbb{Z}_n$, this theorem implies that every finite Abelian group G is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}},$$

where the p_i's are not necessarily distinct primes, and the prime powers $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$ are uniquely determined by G.

Definition .35 *The partition of an integer is a way of representing it as a sum of positive integers, where the order of the summands doesn't matter. Formally, for a positive integer n, a partition of n is an expression of the form:*

$$n = a_1 + a_2 + \ldots + a_k,$$

where a_i are positive integers (possibly repeated), and k is the number of summands in the partition. The number of partitions of given n is denoted by $p(n)$.

Example 1.9.7

- *For n=1:*
  - *There is only one partition: $\{1\}$.*
- *For n=2:*
  - *There are two partitions: $\{2\}$, $\{1,1\}$.*
- *For n=3:*
  - *There are three partitions: $\{3\}$, $\{2,1\}$, $\{1,1,1\}$.*
- *For n=4:*
  - *There are five partitions: $\{4\}$, $\{3,1\}$, $\{2,2\}$, $\{2,1,1\}$, $\{1,1,1,1\}$.*
- *For n=5:*
  - *There are seven partitions: $\{5\}$, $\{4,1\}$, $\{3,2\}$, $\{3,1,1\}$, $\{2,2,1\}$, $\{2,1,1,1\}$, $\{1,1,1,1,1\}$.*

One practical application of the fundamental theorem is utilizing it as an algorithm for constructing all Abelian groups of any order. Consider groups whose orders follow the pattern p^k, where p is a prime and $k \le 4$.

For each set of positive integers whose sum is k (known as a partition of k), there exists one group of order p^k. That is, if k can be expressed as $k = n_1 + n_2 + \ldots + n_t$, where each n_i is a positive integer, then $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \ldots \times \mathbb{Z}_{p^{n_t}}$ is an Abelian group of order p^k.

Order of G	Partitions of k	Possible Direct Products for G
p	1	$\mathbb{Z}_p$
p^2	$2, 1+1$	$\mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p$
p^3	$3,\ 2+1,\ 1+1+1$	$\mathbb{Z}_{p^3},\ \mathbb{Z}_{p^2} \times \mathbb{Z}_p,\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
p^4	$4,\ 3+1,\ 2+2,\ 2+1+1,\ 1+1+1+1$	$\mathbb{Z}_{p^4},\ \mathbb{Z}_{p^3} \times \mathbb{Z}_p,\ \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2},\ \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p,\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Furthermore, the uniqueness aspect of the Fundamental Theorem ensures that distinct partitions of k result in distinct isomorphism classes. For instance, $\mathbb{Z}_9 \times \mathbb{Z}_3$ is not isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Procedure: *We begin by writing n in prime-power decomposition form:*

$$n = p^{n_1} p^{n_2} \ldots p^{n_k}.$$

Next, we individually construct all Abelian groups of order p^{n_1}, then p^{n_2}, and so on, as described earlier. The number of non-isomorphic Abelian groups of order n is then $p(n_1) \cdot p(n_2) \cdot \ldots \cdot p(n_k)$.

Example 1.9.8 *Let $n = 1176 = 2^3 \cdot 3 \cdot 7^2$. Then, the complete list of the distinct isomorphism classes of Abelian groups of order 1176 is:*

- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{49}$,
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{49}$,
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{49}$,
- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$,
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$,
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$.

Here $p(3) = 3, p(1) = 1, p(2) = 2$, and so $p(3)p(1)p(2) = 6$, the number of abelian non-isomorphic groups of order 1176.

1.10. Solvable Groups

Definition .36 (Subnormal Series) *A finite sequence of proper subgroups $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{e\}$ of a group G is called a subnormal series of G if G_{i+1} is a normal subgroup of G_i for all $i = 0, 1, 2, \ldots, k-1$.*

Definition .37 *The groups $\frac{G_i}{G_{i+1}}$ are called the factor groups of the subnormal series. If each G_i is a normal subgroup of G, then the series is called a* ***normal series****.*

Example 1.10.1 *1. Every non-trivial group G has at least one subnormal series, namely $G \supseteq \{e\}$.*

Note 19 *1. A normal series is a subnormal series. However, the converse is not true.*

2. For abelian groups, the concept of subnormal series and normal series coincides.

Example 1.10.2 *$S_4 \supset V_4 \supset \{(1), (12)(34)\} \supset \{e\}$, where $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ is a subnormal series but not a normal series. The subgroup $\{(1), (12)(34)\}$ is not normal in S_4.*

Use the following code in the calculator available at: http://magma.maths.usyd.edu.au/calc/

```
//Define the symmetric and alternating groups of order 4
S := SymmetricGroup(4);
A := AlternatingGroup(4);

//Define two subgroups: I and J
I := sub<S | (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)>;
J := sub<S | (1,2)(3,4)>;

//Initialize G and H as the entire group and subgroup J
G := S;
H := J;

// Create a set C containing the elements of subgroup H
C := {a : a in H};

//Initialize the set T for the conjugate elements
T := {};

//Calculate the conjugates of elements in subgroup H by elements in group G
for a in G, b in H do
    T join:= {a * b * a^(-1)};
end for;
//Check if the difference in the number of elements between C and T is zero
if #C - #T eq 0 then
    "The subgroup H is normal within the symmetric group G.";
else
    "The subgroup H is not normal within the symmetric group G.";
end if;
```

Modify the above code for more examples.

Definition .38 (Solvable) *A group G is considered solvable when it possesses a subnormal series of the type $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{e\}$, with each of its quotient groups $\frac{G_i}{G_{i+1}}$ being abelian.*
This series is referred to as a solvable series.

Example 1.10.3 *1. Every abelian group is solvable, as $G \supseteq \{e\}$ and $\frac{G}{\{e\}} \simeq G$ is abelian.*

2. S_3 is solvable.

Solution: *Note that the index of A_3 in S_3 is 2, so A_3 is normal in S_3. Consider the subnormal series $S_3 \supset A_3 \supset \{i\}$, where $\frac{S_3}{A_3}$ is of order 2 (hence abelian), and $\frac{A_3}{\{e\}}$ is of order 3 (hence abelian).*

Exercise 27 *Prove that S_4 is solvable.*

Hint(s): *Consider the subnormal series $S_4 \supset A_4 \supset V \supset \{i\}$, where $V = \{i, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.*

Exercise 28

1. *Prove that Q_8 is solvable.*
2. *Prove that K_4 is solvable.*

Proposition .19 *Prove that any group G of order pq is solvable, where p and q are primes.*

Solution: *G is not simple (already proved). Let K be its normal subgroup. $O(K) = p$ or $O(K) = q$, i.e., $G \supset K \supset \{1\}$ is a subnormal series such that $\frac{G}{K}$ is abelian and $\frac{K}{\{e\}}$ is abelian.*

Recalling: Fundamental Theorem of Homomorphisms: *Let $\phi : G \to H$ be a group homomorphism. Then:*

1. *The kernel of ϕ, denoted as $\ker(\phi)$, is a normal subgroup of G.*
2. *The image of ϕ, denoted as $Im(\phi)$ or $\phi(G)$, is a subgroup of H.*
3. *The quotient group $G/\ker(\phi)$ is isomorphic to $Im(\phi)$:*

$$G/\ker(\phi) \cong Im(\phi).$$

Exercise 29 *Revisit the proof of the theorem mentioned above.*

Theorem .24 *A subgroup of a solvable group is solvable.*

Proof: *Let G be a solvable group and $H \subseteq G$. Now, $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$ be a solvable series for G. Consider: $H = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_n = \{e\}$, where $H_i = G_i \cap H$. Clearly, H_{i+1} is normal in H_i, since G_{i+1} is normal in G_i. We define a map*

$$f : H_i \to \frac{G_i}{G_{i+1}}$$
$$x \mapsto xG_{i+1} \quad \forall\ x \in H_i$$

Here, $f(xy) = xyG_{i+1} = (xG_{i+1})(yG_{i+1}) = f(x)f(y) \Rightarrow f$ is a homomorphism. Now

$$\begin{aligned}
\ker f &= \{x \in H_i \subseteq H \text{ such that } f(x) = G_{i+1}\} \\
&= \{x \in H \text{ such that } xG_{i+1} = G_{i+1}\} \\
&= \{x \in H \text{ such that } x \in G_{i+1}\} \\
&= H \cap G_{i+1} = H_{i+1}
\end{aligned}$$

By the Fundamental Theorem of Homomorphism,

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

Since $\frac{G_i}{G_{i+1}}$ is abelian, $\frac{H_i}{H_{i+1}}$ is also abelian, here $f(H_i)$ is a subgroup of $\frac{G_i}{G_{i+1}}$. Therefore, the claimed series is solvable, i.e., H is solvable.

— Recall the statement of the Third Isomorphism Theorem: If H and K are normal subgroups of a group G with $H \subseteq K$, then $\frac{G}{K} \equiv \frac{G/H}{K/H}$.

Theorem .25 *If H is a normal subgroup of a solvable group G, then the quotient group G/H is also solvable. In other words, the quotient of a solvable group remains solvable.*

Proof: *Let $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$ be a solvable series for G.*
Consider

$$\frac{G}{H} = \frac{G_0}{H} \supseteq \frac{G_1H}{H} \supseteq \cdots \supseteq \frac{G_nH}{H} = \{\bar{e}\}.$$

We claim that $G_{i+1}H$ is normal in G_iH.
Let $x \in G_iH$, i.e., $x = gh$, where $g \in G_i$ and $h \in H$.
Consider

$$\begin{aligned}
xG_{i+1}H &= gh[G_{i+1}H] = gh[HG_{i+1}] = gHG_{i+1} \quad (\because H \trianglelefteq G \text{ and } K \leq G \text{ implies } HK = KH) &(1)\\
&= gG_{i+1}H = G_{i+1}.g.H \quad (\because G_{i+1} \trianglelefteq G_i) &(2)\\
&= G_{i+1}.gh.H = G_{i+1}xH = G_{i+1}Hx &(3)
\end{aligned}$$

Thus, $G_{i+1}H$ is a normal subgroup of G_iH.

By the Third Isomorphism Theorem,

$$\frac{G_iH}{G_{i+1}H} \cong \frac{G_iH/H}{G_{i+1}H/H}.$$

Define $f : G_i \to G_iH/G_{i+1}H$ by $f(x) = G_{i+1}Hx$. Check that f is a homomorphism and onto.

Also, we find that $G_{i+1} \subseteq \mathrm{Ker}(f)$ (check it), and so f induces a homomorphism defined as:

$$\bar{f} : \frac{G_i}{G_{i+1}} \to \frac{G_iH}{G_{i+1}H}, \text{ by } \quad \bar{f}(G_{i+1}x) = G_{i+1}Hx.$$

$\bar{f}$ is a homomorphism and onto. Therefore, $\frac{G_iH}{G_{i+1}H}$ is abelian , since the homomorphic image of an abelian group is abelian. Consequently, $\frac{G_iH}{G_{i+1}H} \cong \frac{G_iH/H}{G_{i+1}H/H}$ is also abelian. Hence, G/H is solvable.

Theorem .26 *Let H be a normal subgroup of a group G. If both H and G/H are solvable, then G is solvable.*

Proof: *Given that H is solvable, there exists a subnormal series for H:*

$$H = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = \{e\},$$

where each quotient group H_i/H_{i+1} is abelian.

Similarly, since G/H is solvable, there exists a subnormal series for G/H:

$$\frac{G}{H} = \frac{G_0}{H} \trianglerighteq \frac{G_1}{H} \trianglerighteq \ldots \trianglerighteq \frac{G_m}{H} = \{H\},$$

where each quotient group $\frac{G_i}{H}/\frac{G_{i+1}}{H}$ is abelian.

Now, let's consider the preimages of these quotient groups under the natural projection $\pi : G \to G/H$ given by $g \to \bar{g}$ (since for $x \in G_0$, $g_1 \in G_1$, $\bar{x} \in \frac{G_0}{H}$, and $\bar{g_1} \in \frac{G_1}{H}$, we can infer that $\bar{x}\bar{g_1}\bar{x^{-1}} \in \frac{G_1}{H}$ (normal) and $\bar{x}\bar{g_1}\bar{x^{-1}} = \overline{xg_1x^{-1}}$, which implies $xg_1x^{-1} \in G_1$. Therefore, we conclude that:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m = H.$$

Note that each quotient group G_i/G_{i+1} is isomorphic to $\frac{G_i/H}{G_{i+1}/H}$ (as per the Third Isomorphism Theorem), and these are abelian groups.

By combining these two subnormal series, we obtain the following subnormal series for G:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m = H \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = \{e\}.$$

Each factor group G_i/G_{i+1} and H_i/H_{i+1} is abelian.

Thus, G is solvable.

Theorem .27 *The direct product of two solvable groups is solvable.*

Proof: *Let G_1 and G_2 be solvable groups, and consider their direct product $G = G_1 \times G_2$.*

Consider the natural projection homomorphism $\pi : G \to G_2$ defined by $\pi(g_1, g_2) = g_2$ for $(g_1, g_2) \in G_1 \times G_2$, which is onto also.

The kernel of π is the set of elements in G that get mapped to the identity element e_2 in G_2, i.e.,

$$\ker(\pi) = \{(g_1, g_2) \in G \mid g_2 = e_2\} = G_1 \times \{e_2\} \cong G_1.$$

By the Fundamental Theorem of Group Homomorphisms, we have $G/G_1 \cong G_2$. Now, since G_2 is solvable, it implies that G/G_1 is solvable. Additionally, G_1 is solvable, gives G is solvable. Hence, the result follows.

Exercise 30 *The converse of the above theorem is also true.*

Hint(s): *If $G_1 \times G_2$ is solvable, then the quotient groups G/G_1 and G/G_2 are also solvable. Moreover, $G/G_1 \cong G_2$ and $G/G_2 \cong G_1$ imply that G_1 and G_2 are solvable.*

Exercise 31 *Prove that any finite p-group is solvable.*
Hint(s): *Use induction on n, where order of group is p^n.*

Definition .39 (Composition series) *A composition series for a group G is a finite sequence of normal subgroups $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$, where each factor group G_{i+1}/G_i is simple (i.e., it has no nontrivial normal subgroups).*

Example 1.10.4

1. *Consider the group A_4, the alternating group on four elements. A composition series for A_4 is given by $\{e\} \trianglelefteq \langle(12)(34)\rangle \trianglelefteq \langle(12),(34)\rangle \trianglelefteq A_4$. Here, the factor groups $\frac{A_4}{\langle(12),(34)\rangle}, \frac{\langle(12),(34)\rangle}{\langle(12)(34)\rangle}$ are isomorphic to the cyclic groups of order $3, 2$, which are simple groups.*

2. *Let $G = D_8$ be the dihedral group of order 8 (symmetries of a square). A composition series for D_8 is $\{e\} \trianglelefteq \langle r^2\rangle \trianglelefteq \langle r^2, s\rangle \trianglelefteq D_8$. Where the factor groups are simple groups.*

3. *Consider the symmetric group S_3 on three elements. A composition series for S_3 is $\{e\} \trianglelefteq \langle(123)\rangle \trianglelefteq S_3$. Here, the factor groups $\frac{\langle(123)\rangle}{\{e\}}, \frac{S_3}{\langle(123)\rangle}$ are isomorphic to the cyclic groups of order $3, 2$, which are simple groups.*

4. *Let $G = \mathbb{Z}_{30}$ be the cyclic group of order 30. A composition series for $\mathbb{Z}_{30}$ is $\{e\} \trianglelefteq \langle 15\rangle \trianglelefteq \langle 3\rangle \trianglelefteq \langle 1\rangle \trianglelefteq \mathbb{Z}_{30}$. In this case, all factor groups in the series are isomorphic to cyclic groups of prime order, which are simple groups.*

5. *Consider the Klein four-group K_4 which has elements $\{e, a, b, c\}$ where $a^2 = b^2 = c^2 = e$ and $ab = c$.*

   A composition series for K_4 is given by $\{e\} \trianglelefteq \langle a\rangle \trianglelefteq K_4$. In this case, each factor group in the series is isomorphic to the cyclic group of order 2, which is a simple group.

Exercise 32

1. *Write a composition series for S_4.*

2. *Write all possible composition series for $\mathbb{Z}_{12}$.*

Definition .40 *Two composition series $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ and $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_m = G$ for a group G are said to be* equivalent *if there exists a bijection $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ such that the corresponding factor groups are isomorphic, i.e., $G_{i+1}/G_i \cong H_{\sigma(i)+1}/H_{\sigma(i)}$ for all $i = 0, 1, \ldots, n-1$.*

Example 1.10.5 *Consider the quaternion group Q_8 with elements $\{1, -1, i, -i, j, -j, k, -k\}$. Here are three possible composition series for Q_8:*

Series 1: $\{1\} \trianglelefteq \{1, -1\} \trianglelefteq \{\pm 1, \pm i\} \trianglelefteq Q_8$

Series 2: $\{1\} \trianglelefteq \{1, -1\} \trianglelefteq \{\pm 1, \pm j\} \trianglelefteq Q_8$

Series 3: $\{1\} \trianglelefteq \{1, -1\} \trianglelefteq \{\pm 1, \pm k\} \trianglelefteq Q_8$

Equivalence of Series 1 and Series 2:

The factors in Series 1 are:

$$
\begin{aligned}
Q_8/\{\pm 1, \pm i\} &\cong \{\bar{1} = \{\pm 1, \pm i\}, \bar{j} = \{\pm j, \pm k\}\} \\
\{\pm 1, \pm i\}/\{1, -1\} &\cong \{\bar{1}, \bar{i}\} \\
\{1, -1\}/\{1\} &\cong \{1, -1\}
\end{aligned}
$$

The factors in Series 2 are:

$$
\begin{aligned}
Q_8/\{\pm 1, \pm j\} &\cong \{\bar{1}, \bar{i}\} \\
\{\pm 1, \pm j\}/\{1, -1\} &\cong \{\bar{1}, \bar{j}\} \\
\{1, -1\}/\{1\} &\cong \{1, -1\}
\end{aligned}
$$

Both Series 1 and Series 2 have the same factor groups, up to isomorphism and irrespective of the order. Hence, the series are equivalent. Similarly, Series 2 and Series 3 are equivalent.

Theorem .28 (Jordan-Hölder Theorem) *Let G be a group and assume G has a decomposition series. Let $G = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = \{e\}$ $G = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_s = \{e\}$ be any two decomposition series for G. Then $r = s$ and there exists $\sigma \in S_r$ such that for all k: $G_k/G_{k+1} \cong H_{\sigma(k)}/H_{\sigma(k)+1}$.*

Proof: *We use induction on the length of the composition series of group G. The result is true for length 1. Let us assume that the result is true for all subgroups of G of order less than G. Then,*

Case 1: *When $H_1 = G_1$,*

$$\frac{G}{G_1} = \frac{G}{H_1} \quad \text{and so} \quad G/G_1 \cong G/H_1.$$

In this case, the two composition series for G_1 are

$$G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_s = \{e\} \text{ and } G_1 = H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_t = \{e\}.$$

Also, the corresponding quotient groups are

$$\frac{G_1}{G_2}, \frac{G_2}{G_3}, \ldots, \frac{G_{s-1}}{G_s} \text{ and } \frac{G_1}{H_2}, \frac{H_2}{H_3}, \ldots, \frac{H_{t-1}}{H_t}.$$

Since $|G_1| < |G|$, therefore by the induction hypothesis, the theorem is true for G_1. Consequently, the corresponding quotient groups are isomorphic. Since $G/G_1 \equiv G/H_1$, all the quotient groups are isomorphic.

Case 2: *When $H_1 \neq G_1$, since H_1 and G_1 are normal subgroups of G, it implies that H_1G_1 is a normal subgroup of G and contains H_1 and G_1. However, if H_1 is a maximal normal subgroup of G, this implies $G = H_1G_1$.*

By the third isomorphism theorem,

$$H_1G_1/H_1 \cong G_1/(H_1 \cap G_1),$$

or equivalently,

$$G/H_1 \cong G_1/(H_1 \cap G_1).$$

Also, since G/H_1 is simple, it follows that $G_1/(H_1 \cap G_1)$ is simple, and $H_1 \cap G_1$ is a maximal normal subgroup of G_1.

Similarly, $G/G_1 \cong H_1/(H_1 \cap G_1)$, and $H_1 \cap G_1$ is a maximal normal subgroup of H_1.

Suppose

$$H_1 \cap G_1 \trianglelefteq M_2 \trianglelefteq M_3 \ldots \trianglelefteq M_k = \{e\}$$

is a composition series for $H_1 \cap G_1$.

Now consider the two composition series for $G = H_1G_1$:

$$G = H_1G_1 \trianglelefteq H_1 \trianglelefteq H_1 \cap G_1 \trianglelefteq M_1 \ldots \trianglelefteq M_k \quad \text{and} \quad G = H_1G_1 \trianglelefteq G_1 \trianglelefteq H_1 \cap G_1 \trianglelefteq M_2 \ldots \trianglelefteq M_k.$$

Since $G/G_1 \cong H_1/(H_1 \cap G_1)$, and $G/H_1 \cong G_1/(H_1 \cap G_1)$, thus...

$$\begin{tikzcd}
\frac{G}{H_1} \arrow[dr] & \frac{H_1}{H_1 \cap G_1} \arrow[dl] & \frac{H_1 \cap G_1}{M_2} \arrow[d] & \frac{M_2}{M_3} \arrow[d] & \cdots & \frac{M_{k-1}}{M_k} \arrow[d] \\
\frac{G}{G_1} & \frac{G_1}{H_1 \cap G_1} & \frac{H_1 \cap G_1}{M_2} & \frac{M_2}{M_3} & \cdots & \frac{M_{k-1}}{M_k}
\end{tikzcd}$$

The first two quotient groups are isomorphic in the reverse order, and the remaining factors are equal. Continuing in this way, if $H_2 = G_2$ or $H_2 \neq G_2$, and so on, we have $t = s$ and so the required result.

Exercise 33 *Let G be a finite group. Then G is solvable if and only if for every composition series of G, the quotient groups are cyclic of prime order.*

Hint(s): *Consider the "if" part first. Assume that G is solvable. This means that there exists a chain of subgroups $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{e\}$ where each quotient group G_i/G_{i+1} is abelian. Now, use the fact that every abelian group is cyclic of prime order or a direct product of cyclic groups of prime order.*

For the "only if" part, assume that for every composition series of G, the quotient groups are cyclic of prime order, i.e., abelian, and hence G is solvable.

***********CHAPTER END**********