Chapter 9 Normal subgroups and Factor Groups

Definition A subgroup H of a group is normal if $aH = Ha$ for all $a \in G$. We write $H \triangleleft G$.

Theorem 9.1 A subgroup H is normal if and only if H is normal, i.e., $gHg^{-1} \leq H$ for all $g \in G$.

Proof. Done in homework.

Theorem 9.2 Let $H \leq G$. Then $G/H = \{aH : a \in G\}$ is a group (known as the factor group) under the operation $(aH)(bH) = (ab)H$ if and only if $H \triangleleft G$.

Proof. Key step: The operation is well-defined if and only if H is normal.

Example In S_3, the left cosets of $H = \{\varepsilon, (1,2)\}$ do not form a factor group.

On the other hand, for each $n \geq 2$, S_n/A_n is a group isomorphic to $\mathbf{Z}_2$.

Remarks If G is Abelian (cyclic), then for any $H \leq G$ the factor group G/H is Ablian (cyclic). Factor groups of a cyclic (Abelian) group has the same property.

The order of $aH \in G/H$ is the smallest positive integer m such that $a^m \in H$.

Theorems 9.3, 9.4 Let $Z(G)$ be the center of G. Then $G/Z(G) \sim Inn(G)$.

If $G/Z(G)$ is cyclic, then G is Abelian.

Theorem 9.5 Let G be a finite Abelian group, and let p be a **prime** factor of $|G|$. Then G has an element of order p.

Chapter 10 Group Homomorphisms and Normal subgroups
Definition Let $(G_1, *_1), (G_2, *_2)$ be groups. Then a function $\phi : G_1 \to G_2$ is a group homomorphism if

$$\phi(a *_1 b) = \phi(a) *_2 \phi(b) \quad \text{ for all } a, b \in G_1.$$

The **kernel** of ϕ is the set $Ker(\phi) = \{a \in G_1 : \phi(a) = e_2\}$.
Theorem 10.2 Suppose $\phi : G_1 \to G_2$ is a group homomorphism.

1. If H is a normal subgroup in G_1 then $\phi(H)$ is a normal subgroup in $\phi(G_1)$.
2. If K is a (normal) subgroup of G_2, then $\phi^{-1}(K) = \{a \in G_1 : \phi(a) \in K\}$ is a (normal) subgroup of G_1. In particular, $Ker(\phi)$ is normal in G.

Remark Consider $\phi : \mathbf{Z}_2 \to S_3$ such that $\phi(1) = (1, 2)$. Then $H = \mathbf{Z}_2$ is a normal subgroup in $\mathbf{Z}_2$, but $\phi(\mathbf{Z}_2) = \{\varepsilon, (1, 2)\}$ is not a normal subgroup in S_3.

Theorem 10.3 If $\phi : G_1 \to G_2$, then the map $\Phi : G_1/Ker(\phi) \to \phi(G_1)$ defined by $\Phi(gKer(\phi)) = \phi(g)$ is an isomorphsim from $G_1/Ker(\phi)$ to $\phi(G_1)$.

Proof. Let $K = Ker(\phi)$.

(1) Φ is well-defined because $\Phi(aK) = \Phi(bK)$ implies ...

(2) Φ is 1-1 because ...

(3) Φ is onto because ...

(4) $\Phi(aKbK) = ... = \phi(aK)\phi(bK)$.

Theorem 10.4 A subgroup N is normal in G if and only if it is $N = Ker(\phi)$ for some group homomorphism from G to $\tilde{G}$.

Proof. If $N = Ker(\phi)$ then it is normal. If N is normal then $\phi : G \to G/N$ by $\phi(g) = gN$ is a homomorphism and $Ker(\phi) = N$.

Chapter 8/9 Internal and External Direct Products

Idea Decompose a large group into small subgroups, and combine several groups to form a larger group (to get desired or undesired properties).

Definition Let G_1, G_2 be groups. The external direct product of G_1 and G_2 is is the group $G_1 \oplus G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$ under the operation $(x_1, y_1) * (x_2, y_2) = (x_1 * x_2, y_1 * y_2)$.

One can extend the results to $G = G_1 \oplus \cdots \oplus G_k$.

Some basic results

Theorem 8.1 Let $g = (g_1, \ldots, g_k) \in G_1 \oplus \cdots \oplus G_k$. If $|g_1|, \ldots, |g_k|$ are finite, then $|g| = \text{lcm}(|g_1|, \ldots, |g_k|)$; if one of the $|g_i|$ is infinite, then $|g|$ is infinite.

Theorem 8.2 Let $G_1, \ldots, G_k$ be finite cyclic groups. Then $G_1 \oplus \cdots \oplus G_k$ is cyclic if and only if

$$\gcd(|G_i|, |G_j|) = 1 \text{ for all } 1 \le i, j \le k, \text{ equivalently, } \text{lcm}(|G_1|, \ldots, |G_k|) = \prod_{j=1}^{k} |G_j|.$$

In particular, $\mathbf{Z}_{n_1 \cdots n_k} = \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_k}$ if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Remark If $k > 1$ and one of the cyclic group G_i is infinite, then $G_1 \oplus \cdots \oplus G_k$ is not cyclic.

Remark If H_1, H_2 are subgroups of G_1, G_2, then $H_1 \oplus H_2$ is a subgroup of $G_1 \oplus G_2$. In particular, $G_1 \oplus \{e_2\}$ and $\{e_1\} \oplus G_2$ are normal subgroup of $G_1 \oplus G_2\}$.

Theorem If H, K are normal subgroups of G such that $G = HK$ and $H \cap K = \{e\}$. Then G is isomorphic to $H \oplus K = \{(h,k) : h \in H, k \in K\}$.

Proof. Define $\phi : H \oplus K \to G$ by $\phi(h,k) = hk$.

To prove that ϕ is bijective, we only use the fact that H, K are subgroups, $H \cap K = \{e\}$ and $HK = G$. Clearly, ϕ is onto because for every $hk \in HK = H \times K$, $\phi(h,k) = hk$. For one-one, if $\phi(h,k) = hk = e$, then $h = k^{-1} \in H \cap K$ so that $h = k = e$.

To prove that ϕ is a homomorphism, we will use the fact that H, K are normal subgroups of G. Let $(h_1, k_1), (h_2, k_2) \in H \oplus K$. We need to show the equality of $\phi((h_1,k_1)(h_2,k_2)) = \phi(h_1h_2, k_1k_1) = h_1h_2k_1k_2$ and $\phi(h_1,k_1)\phi(h_2,k_2) = (h_1k_1)(h_2k_2)$. We only need to prove that $h_2k_1 = k_1h_2$, i.e., $h_2k_1h_2^{-1}k_1^{-1} \in H \cap K = \{e\}$, which is true because $h_2k_1h_2^{-1} \in K$ and $k_1h_2^{-1}h_1^{-1} \in H$. □

Remark If H, K satisfy the conditions in the above theorem, we say that G is the internal direct product of G. One may further decompose H and K, and write G is the internal direct product of normal subgroups $H_1, \dots, H_k$.

Theorem 9.7 If G has p^2 elements for a prime p, then G is isomorphic to $\mathbf{Z}_{p^2}$ or G is isomorphic to $\mathbf{Z}_p \oplus \mathbf{Z}_p$. Consequently, G is Abelian.

Proof. Note that elements in G has order $1, p$ or p^2. If G has an elements of order p^2, then G is isomorphic to $\mathbf{Z}_{p^2}$. Otherwise, all elements in G not equal to e has order p. Let $a \neq e$ and $H = \langle a \rangle = \{e, a, \dots, a^{p-1}\}$.

We show that H is normal. If not, there is $b \in G$ such that $bab^{-1} \notin H$. Note that bab^{-1} has order p, and $\tilde{H} \cap H = \{e\}$. Else, bab^{-1} and a will generate the same subgroup, and $bab^{-1} = a^j \in H$.

By the counting theorem, $|H\tilde{H}| = p^2$ so that $H\tilde{H} = G$, Hence, $b^{-1} = a^j(bab^{-1})^k = a^jba^kb^{-1}$ for some $0 \leq j, k < p$. Hence, $e = a^jba^k$ so that $b = a^{-j-k}$. So, $bab^{-1} \in H$, which is a contradiction. Similarly, we can show that $\tilde{H}$ is normal. Thus, G is isomorphic to $H \oplus \tilde{H}$. □

Chapter 11 Fundamental Theorem of Finitely Generated Abelian Group

A groups G is finitely generated if there is a finite subset $S = \{a_1, \ldots, a_r\}$ of G such that every element in G has the form $g_1 \cdots g_m$ for some positive integer m and $g_1, \ldots, g_m \in S$.

Examples. $\mathbf{Z}_n$ is generated by $\{\bar{1}\}$, and $\mathbf{Z}_n \oplus Z$ is generated by $\{(\bar{1}, 0), (0, 1)\}$.

Theorem 11.1 Every finitely generated Abelian group is isomorphic to a direct product of $\mathbf{Z}_{m_1} \oplus \cdots \oplus \mathbf{Z}_{m_k} \oplus \mathbf{Z}^\beta$, where $m_j = p_j^{n_j}$ for some prime number p_j and positive integer n_j for each j, and a nonnegative integer β known as the Betti number.

Corollary If G is a finite Abelian group, and m divides $|G|$, then G has a subgroup of order m.

Homework 8.

(But, there may not be an element of order m.)

Isomorphic classes of Abelian groups

Suppose $|G| = 8, 10, p^2, pq$, etc.

If $|G| = 8$, then G may be isomorphic to $\mathbf{Z}_8, \mathbf{Z}_4 \oplus \mathbf{Z}_2, \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$. These groups are not isomorphic because the first one has an element of order 8, the second one has no elements of order 8 and has an element of order 4, the third group only has elements of order 1 and 2.

Not that $\mathbf{Z}_2 \oplus \mathbf{Z}_4$ is isomorphic to $\mathbf{Z}_4 \oplus \mathbf{Z}_2$ by the map $\phi(\bar{a}, \bar{b}) = (\bar{b}, \bar{a})$.

If $|G| = 10$, then it is isomorphic to $\mathbf{Z}_{10}$. Note that $\mathbf{Z}_5 \oplus \mathbf{Z}_2$ is isomorphic to $\mathbf{Z}_{10}$ because $(1, 1)$ in $\mathbf{Z}_5 \otimes \mathbf{Z}_2$ has order 10. So, $\mathbf{Z}_5 \oplus \mathbf{Z}_2$ is a cyclic group with 10 elments.

If $|G| = p^2$, then G is isomorphic to $\mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \oplus \mathbf{Z}_p$ as shown before.

If $|G| = pq$, then G is isomorphic to $\mathbf{Z}_{pq}$. Note that $\mathbf{Z}_p \oplus \mathbf{Z}_q$ is isomorphic to $\mathbf{Z}_{pq}$ because $(\bar{1}, \bar{1}) \in \mathbf{Z}_p \oplus \mathbf{Z}_q$ has order pq.