Chapter 8 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 $(G_1, *_1), (G_2, *_2)$ be groups. The external direct product is

$$G_1 \oplus G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

under the entry-wise operations $(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$.

One can extend the definition to $G_1 \oplus \cdots \oplus G_k$.

Examples Many ...

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

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

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.

More results

Notation Let k be a factor of n; set $U_k(n) = \{x \in U(n) : x = pk + 1, p \in \mathbf{N}\}$.

Example Let $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$. Then
$U_4(20) = \{1, 9, 13, 17\} \cong U(5) = \{1, 2, 3, 4\}$,
$U_5(20) = \{1, 11\} \cong U(4) = \{1, 3\}$, and
$U(20) \cong U(4) \oplus U(5) \cong U_5(20) \oplus U_4(20)$.

Theorem 8.3 If $\gcd(s, t) = 1$, then $U(st) \cong U(s) \oplus U(t)$, $U_t(st) \cong U(s)$ and $U_s(st) \cong U(t)$.

Proof. Define $\phi : U(st) \to U(s) \times U(t)$ $\phi(x) = (x_1, x_2) \in U(s) \oplus U(t)$ such that $x_1 = x$ (mod s) and $x_2 = x$ (mod t). We will show that it is a group isomorphism.

Well defined: If $\gcd(x, st) = 1$, then $\gcd(x_1, s) = 1$ and $\gcd(x_2, t) = 1$. So, $(x_1, x_2) \in U(s) \oplus U(t)$.

One-one: If $\phi(x) = (x_1, x_2) = \phi(y)$, then $x = sp_1 + x_1 = sp_2 + x_2$ and $y = tq_1 + x_1 = sq_2 + x_2$ for some $p_1, p_2, q_1, q_2 \in \mathbf{Z}$, So, $x - y = s(p_1 - p_2) = t(q_1 - q_2)$ is divisible by s and t. Thus, $x - y = 0 \in \mathbf{Z}(st)$.

Onto: Because $\gcd(s, t) = 1$, there exist $u_1, u_2 \in \mathbf{Z}$ be such that $u_1 = sp_1 + 1 = tp_2$, i.e., $1 = tp_2 - sp_1$, and $u_2 = sq_1 = tq_2 + 1$, i.e., $1 = sq_1 - tq_2$. Regard $u_1, u_2 \in U(st)$. Then for any $(x_1, x_2) \in \mathbf{Z}_1 \oplus \mathbf{Z}_2$, $\phi(u_1x_1 + u_2x_2) = (x_1, x_2)$.

Operation preserving: Suppose $x, y \in U(st)$. Then $\phi(xy) = ([xy]_s, [xy]_t) = ([x]_s[y]_s, [x]_t[y]_t) = \phi(x)\phi(y)$.

Combining the above, we see that ϕ is an isomorphism.
The proof of $U(s) \cong U_t(st)$ is left as an homework. □

Remark For any $m = p_1^{r_1} \cdots p_k^{r_k}$, where $p_1, \ldots, p_k$ are distinct primes and $r_1, \ldots, r_k \in \mathbf{N}$, we have

$$U(m) \cong U(p_1^{r_1}) \oplus \cdots \oplus U(p_k^{r_k}).$$

For any prime p we have

(1) $U(2) = \{1\}, U(4) = \mathbf{Z}_2$, $U(2^n) \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{2^{n-2}}$ for $n \geq 3$;

(2) $U(p^n) \cong\sim \mathbf{Z}_{p^n - p^{n-1}}$ if $p > 2$.

Examples

$U(105) \sim U(3 \cdot 5 \cdot 7) \sim U(3) \oplus U(5) \oplus U(7) \sim \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_6$.

$U(720) \sim U(16 \cdot 9 \cdot 5) \sim U(19) \oplus U(9) \oplus U(5) \sim \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_4$.

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.

Additional results

Definition If H, K are normal subgroups of G such that $H \cap K = \{e\}$ and $HK = G$, then G is the internal product of H and K. For more than 2 groups, we need $G = H_1 \cdots H_k$ and $(H_1 \cdots H_j) \cap H_{j+1} = \{e\}$.

Theorem 9.6 Internal direct product $G_1 \cdots G_k$, sometimes denoted by $G_1 \times \cdots \times G_k$, is isomorphic to $G_1 \oplus \cdots \oplus G_k$.

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

ϕ is one-one: If $\phi(h_1, k_1) = \phi(h_2, k_2)$ then $h_1 k_1 = h_2 k_2$.
Thus, $h_1^{-1} h_2 = k_1 k_2^{-1} \in H \cap K = \{e\}$, and ...

ϕ is onto: If $g \in G$, then $g = hk$ for some $h \in H, k \in K$. So, ...

Finally to show that $\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2$ equals $\phi(h_1, k_1)\phi(h_2, k_2) = h_1 k_1 h_2 k_2$, we need to show that $h_2 k_1 = k_1 h_2$.

This is true because

$$k_1^{-1} h_2 k_1 h_1^{-1} h_2 = \tilde{h} h_2 = k_1^{-1} \tilde{k} \in H \cap K = \{e\}.$$

We can extend the proof to $G = H_1 \otimes \cdots \otimes H_k$. □

Remark Note that if $G \cong H_1 \times \cdots \times H_k$, then $G \cong H_1 \oplus \cdots \oplus H_k$. However, the converse is not true. For example, if $G = \mathbf{Z} \oplus \mathbf{Z}$, then $H_1 = \mathbf{Z} \oplus \{0\}$ and $H_2 = \{0\} \oplus 2\mathbf{Z}$ are normal subgroup of G such that $H_1 \oplus H_2 \cong \mathbf{Z} \oplus \mathbf{Z} = G$, but $G \ncong H_1 \times H_2$.

Theorem 9.7 A group of order p^2 for a prime p is isomorphic to $\mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \oplus \mathbf{Z}_p$. In either case, G is Abelian.

Proof. Suppose there is $a \in G$ of order p^2. Then we are done.

Assume that every nonidentity element $a \in G$ has p.

We can find $a \in G$ such that $H = \langle a \rangle$ has order p.

We show that H is normal. If not, there is $b \in G - H$ such that $bHb^{-1} \not\subseteq H$. So, $bab^{-1} \notin H$; otherwise $\langle a \rangle = \langle bab^{-1} \rangle = \tilde{H}$. Now, $b^{-1} \in \cup_{j=0}^{p-1} a^j \tilde{H} = G$. So, $b^{-1} = a^i (bab^{-1})^j$ for some i, j, and hence $e = a^i b a_j$ implying that $b = a^{-i-j}$, which is a contradiction.

Now, let $b \in G - H$ and $\tilde{H} = bHb^{-1}$. One see that $H, \tilde{H}$ are normal subgroup of G such that $H \cap \tilde{H} = \{e\}$. Hence, $G = H \times \tilde{H} \cong \mathbf{Z}_p \otimes \mathbf{Z}_p$.

Note that $bHb^{-1} = \{ba^j b^{-1} : 0 \le j \le p-1\}$ is a subgroup. If $ba^j b^{-1} \notin H$ □