MATH403: Introduction to Abstract Algebra

Michael Li

Chapter 8 External Direct Products

Definition: for a finite collection of groups, the **external direct product** for $G_1, G_2, \ldots, G_n$ is $G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$

- Group operation is component wise under G_i

Example: $Z_2 \oplus Z_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

Example: Any group of order 4 is isomorphic to Z_4 or $Z_2 \oplus Z_2$. It suffices to show there is only 1 way to create the operation table for a non-cyclic group G of order 4.

By Lagrange's Theorem, elements of G (non-cyclic) only have order 1 or 2. Take distinct $a, b \in G$. Then $G = \{e, a, b, ab\}$ since

- $ab \neq a$, $ab \neq b$, $ab \neq e$, $ab = (ab)^{-1} = ba$
- Clearly $G \approx Z_2 \oplus Z_2$

Theorem: $|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$

Proof: let $s = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$ and $t = |(g_1, g_2, \ldots, |g_n|)$ Then we have

$(g_1, g_2, \ldots, g_n)^s = (e_1, e_2, \ldots, e_n) \implies t \leq s$

$(g_1, g_2, \ldots, g_n)^t = (e_1, e_2, \ldots, e_n) \implies t$ is a common multiple of $|g_1|, |g_2|, \ldots, |g_n|$ and thus $s \leq t$

Thus, we have that $s = t$

Example: Number of cyclic subgroups of order 10 in $Z_{100} \oplus Z_{25}$

- Case 1: $|a| = 10$ and $|b| = 1$ or 5. Then we have $\phi(10) * (\phi(1) + \phi(5)) = 4 * 5 = 20$
- Case 2: $|a| = 2$ and $|b| = 5$. Then we have $\phi(2) * \phi(5) = 1 * 4 = 4$
- There are 24 elements of order 10
- Since each cyclic subgroup of order 10 has 4 elements of order 10 and no 2 cyclic subgroups can share an element of order 10, there are $24/4 = 6$ cyclic subgroups of order 10

Example: For $r \mid m$ and $s \mid n$, the group $Z_m \oplus Z_n$ has a isomorphic to $\approx Z_r \oplus Z_s$

- $Z_{30} \oplus Z_{12}$ has a subgroup $\approx Z_6 \oplus Z_4$ since $\langle 5 \rangle$ is a subgroup of Z_{30} with order 6 and $\langle 3 \rangle$ is a subgroup of Z_{12} with order r. Thus $\langle 5 \rangle \oplus \langle 3 \rangle \approx Z_6 \oplus Z_4$

Theorem: Let G, H be finite cyclic groups. $G \oplus H$ is cyclic $\iff$ $|G|, |H|$ are relatively prime

Proof: Let $|G| = m$ and $|H| = n \implies |G \oplus H| = mn$

$\implies$ $\gcd(m, n) = d$ and (g, h) is a generator of $G \oplus H$. Since $(g, h)^{mn/d} = (e, e)$, we have that $nm = |(g, h)| = mn/d \implies d = 1$

$\impliedby$ Let $G = \langle g \rangle$, $H = \langle h \rangle$, $\gcd(|g|, |h|) = 1$. Then $|(g, h)| = \text{lcm}(m, n) = mn = |G \oplus H|$. Thus (g, h) is a generator of $G \oplus H$

Corollaries

- $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of finite number of finite cyclic groups $\iff$ $|G_i|, |G_j|$ are relatively prime when $i \neq j$
- Let $m = ab \cdots k$. Then $Z_m \approx Z_a \oplus Z_b \oplus \cdots \oplus Z_k$ $\iff$ $|G_i|, |G_j|$ are relatively prime when $i \neq j$

Example:

$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \approx Z_2 \oplus Z_6 \oplus Z_5 \approx Z_2 \oplus Z_{30}$

$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \approx Z_2 \oplus Z_6 \oplus Z_5 \oplus Z_2 \oplus Z_3 \oplus Z_2 \oplus Z_5 \approx Z_6 \oplus Z_{10}$

Thus $Z_2 \oplus Z_{30} \approx Z_6 \oplus Z_{10}$. HOWEVER, $Z_2 \oplus Z_{30} \not\approx Z_{60}$

Definition: $U_k(n) = \{x \in U(n) \mid x \pmod k = 1\}$. Note that $U_k(n) \leq U(n)$

Theorem: Suppose that s, t are relatively prime, then $U(st) \approx U(s) \oplus U(t)$, and $U_s(st) \approx U(t)$ and $U_t(st) \approx U(s)$

Proof: For $U(st)$ to $U(s) \oplus U(t)$, define $x \to (x \pmod s, x \pmod t)$

For $U_s(st) \to U(t)$, define $x \to x \pmod t$

For $U_t(st) \to U(s)$, define $x \to x \pmod s$

Corollary: Let $m = n_1, n_2, \cdots n_k$ where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then $U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$

Examples:

- $U(7) \approx U_{15}(105) = \{1, 16, 31, 46, 61, 76\}$
- $U(105) \approx U(7) \oplus U(15)$
- $U(105) \approx U(21) \oplus U(5)$
- $U(105) \approx U(3) \oplus U(5) \oplus U(7)$
- $U(105) = U(3 * 5 * 7) \approx U(3) \oplus U(5) \oplus (7) \approx Z_2 \oplus Z_4 \oplus Z_6$
- $U(144) = U(16) \oplus U(9) \approx Z_4 \oplus Z_2 \oplus Z_6$
- Thus $U(105) \approx U(144)$

Chapter 9 Normal Subgroups and Factor Groups

Definintion $H \leq G$ is a **normal subgroup** if $(\forall a \in G)[aH = Ha]$, denoted $H \trianglelefteq G$

Theorem: $H \trianglelefteq G \iff (\forall x \in G)[xHx^{-1} \subseteq H]$

Proof: $\implies$ for any $x \in G, h \in H$ there is an $h; \in H$ such that $xh = h'x \implies xhx^{-1} = h' \implies xHx^{-1} \subseteq H$

$\impliedby$ let $x = a$ then $aHa^{-1} \subseteq H \implies aH \subseteq Ha$. Let $x = a^{-1} then $a^{-1}H(a^{-1})^{-1} \implies Ha \subseteq aH$

Thus $aH = Ha$

Examples:

- Every Abelian group is normal since $ah = ha$ for all $a \in G$ and $h \in H \leq G$
- $Z(g)$ is always normal
- A_n is normal subgroup of S_n
- $SL(2, R)$ is normal subgroup of $GL(2, R)$ since $\det(xhx^{-1}) = 1 \implies xHx^{-1} \subseteq H$

Theorem: Let $G \trianglelefteq G$ then $G/H = \{aH \mid a \in G\}$ is a group under operation $(aH)(bH) = abH$

Proof: we first show that the operation is well defined. Take $aH = a'H, bH = b'H$ and verify $aHbH = a'Hb'H \implies abH = a'b'H$

This will show that multiplication only depends on the cosets, not the coset representatives

Note that $a' = ah_1$ and $b'bh_2 \implies a'b'H = ah_1bh_2H = ah_1bH = ah_1Hb = aHb = abH$. Now we show that it's a group

- $eH = H$ is the identity
- $a^{-1}H$ is the inverse of aH
- $(aHbH)cH = aH(bHcH)$

Example: $Z/4Z$ can be constructed as $\{0 + 4Z, 1 + 4Z, 2 + 4Z, 3 + 4Z\}$

- No other left cosets are possible since $k = 4q + r \implies k + 4Z = r + 4q + 4Z = r + 4Z$
- Also worth mentioning $Z/4Z \approx Z_4$, or more generally $Z/nZ \approx Z_n$

Example: Let $G = Z_8 \oplus Z_4$ and $H = \langle(2, 2)\rangle \leq G$ and show that G/H is isomorphic to one of $Z_8, Z_4 \oplus Z_2, Z_2 \oplus Z_2 \oplus Z_2$

- Note that Z_8 has elmt order 8, $Z_4 \oplus Z_2$ has elmt of order $1, 2, 4$, and $Z_2 \oplus Z_2 \oplus Z_2$, has elmt of order $1, 2$
- For $(a, b) + H$ we have that $((a, b) + H)^4 = \begin{cases} (4, 0) + H & a \pmod 2 = 1 \\ (0, 0) + H & a \pmod 2 = 0 \end{cases}$. Thus max order of elmt in G/H is 4
- However, $((1, 0) + H)^2 = (2, 0) + H \neq H \implies |(1, 0) + H| = 4$
- Thus G/H cannot be isomorphic to Z_8 or $Z_2 \oplus Z_2 \oplus Z_2$

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

Proof: Since G is Abelian $\implies Z(G) = G$, we show that the only element of $G/Z(G)$ is the identity coset $Z(G)$

Let $G/Z(G) = \langle gZ(G) \rangle$ and let $a \in G$. There there is an integer i such that $aZ(G) = (gZ(G))^i = g^i Z(G)$

Thus a $= g^i z$ for some $z \in Z(G)$. Since $g^i, z \in C(g)$, so does a

Since g was arbitrary, every element of G commutes with $g \implies g \in Z(G)$. Thus $gZ(G) = Z(G)$ is the only element of $G/Z(G)$

Note: usually contrapositive is used: if G is non-Abelian, then $G/Z(G)$ is not cyclic

- Using Lagrange's Theorem, a non-Abeliean group of order pq, for p, q prime, must have a trivial center

Theorem: $G/Z(G) \approx \text{Inn}(G)$

Proof: consider $T : gZ(G) \to \phi_g = gxg^{-1}$

T is well defined since $gZ(G) = hZ(G) \implies \phi_g = \phi(h)$ (image of a coset of $Z(G)$ only depends on the coset itself)

- $gZ(G) = hZ(G) \implies h^{-1}g \in Z(G) \implies h^{-1}gx = xh^{-1}g \implies gx^{-1} = hxh^{-1}$ thus on to one
- Clearly, T is onto
- $\phi_g \phi_h = \phi(gh)$ thus T is operation preserving

Cauchy Theorem for Abelian Groups: Let G be finite, Abeliean, and let p be prime that divides the order of G. Then G has an element of order p

Proof by strong induction

- Clearly base case holds for $|G| = 2$
- IH: assume that the statement is true for all Abelian groups of order less than $|G|$
- IS: Certainly G has elements of prime order, so if $|x| = m = qn$ for prime q, then $|x^n| = q$
  - If $q = p$ we are done
  - Otherwise every subgroup of an Abeliean group is normal, so construct $\bar{G} = G/\langle x \rangle$. Then p divides $|\bar{G}| = |G|/q$
  - Thus by induction, $\bar{G}$ has an element $y\langle x \rangle$ of order p. Then $(y\langle x \rangle)^p = y^p \langle x \rangle = \langle x \rangle \implies y^p \in \langle x \rangle$
    * If $y^p = e$ then done
    * Otherwise $|y^p| = q$ and $|y^q| = p$

Definition: G is the **internal direct product** of H, K (denoted $G = H \times K$) if $H, K \trianglelefteq G$, $G = HK$, and $H \cap K = \{\epsilon\}$

- Can be expanded to a finite collection of normal subgroups of G where $G = H_1 \times H_2 \times \cdots \times H_n$ if
  - $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n \mid h_i \in H_i\}$
  - $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for $I \in \{1, 2, \ldots, n-1\}$
- Intuition behind internal direct product is to take a group G and find 2 subgroups H, K such that $G \approx H \oplus K$
- Intuition behind external direct product is to take 2 unrelated groups H, K are produce a larger group $H \oplus K$

Example: if s, t are relatively prime then $U(st) = U_s(st) \times U_t(st)$

Non-Example: take $G = S_3, H = \langle (123) \rangle, K = \langle (12) \rangle$

- $G = HK$, $H \cap K = \epsilon$, but $G \not\approx H \oplus K$ since $H \oplus K$ is cyclic but S_3 isn't. Also, K isn't normal

Theorem: $H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$

Proof: first need to show that normality of H guarantees h in all H_i commute. For distinct $h_i \in H_i$ and $h_j \in H_j$

$(h_i h_j h_i^{-1}) h_j^{-1} \in H_j h_j^{-1} = H_j$ and $h_i (h_j h_i^{-1}) h_j^{-1} \in h_i H_i = H_i$

Thus we have $h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_i = \{e\} \implies h_i h_j = h_j h_i$

Next we show that there is a unique representation of g. Take $g = h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$, which can be represented as

$h_n' h_2^{-1} = (h_1')^{-1} h_1 \cdots (h_{n-1}')^{-1} h_{n-1} \implies h_n' h_n^{-1} \in H_1 \cdots H_{n-1} \cap H_n = \{e\}$

Thus $h_n' h_n^{-1} = e \implies h_n' = h_n$. This step can be recursively applied to show $h_i' = h_i$

Thus we can define $\phi : G \to H_1 \oplus H_2 \oplus \cdots \oplus H_n, \phi(h_1 h_2 \cdots h_n) = (h_1, h_2, \ldots, h_n)$

UPSHOT: $H \oplus K$ is the product $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$ is the same as $h_1 h_2 k_1 k_2 \in H \times K$

Theorem: $|G| = 2p \implies G \approx Z_{p^2}$ or $G \approx Z_p \oplus Z_p$

Proof: let $|G| = p^2$. Then if G has an element of order p^2, then $G \approx Z_{p^2}$

Otherwise every nonidentity element of G has order p. We need to show that for any element a, $\langle a \rangle \trianglelefteq G$

If not, then there is $b \in G$ such that $bab^{-1} \notin \langle a \rangle \implies \langle a \rangle \cap \langle bab^{-1} \rangle = \{e\}$

Taking left cosets of $\langle bab^{-1} \rangle$ of the form $a^i \langle bab^{-1} \rangle$, we know that b^{-1} must lie in one of these

Thus $b^{-1} = a^i (bab^{-1})^j = a^i ba^j b^{-1}$ for some i, j

This gives $e = a^i ba^j \implies b \in \langle a \rangle$. Contradiction since we said $b \notin \langle a \rangle$

Thus every subgroup $\langle a \rangle$ is normal in G

Finally we take nonidentity x and an element $y \notin \langle x \rangle$. Then by comparing orders, we have that $G = \langle x \rangle \times \langle y \rangle \approx Z_p \oplus Z_p$