CHAPTER 8

External Direct Products

Definition and Examples

DEFINITION (External Direct Product). Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, \ldots, G_n$ is

$$G1 \oplus G2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) | g_i \in G_i\}$$

where

$$(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots g_n') = (g_1 g_1', g_2 g_2', \ldots g_n g_n')$$

and each $g_i g_i'$ is performed with the operation of G_i.

COROLLARY. *Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. Then $G1 \oplus G2 \oplus \cdots \oplus G_n$ is a group.*

PROOF.

The identity is $(e_1, e_2, \ldots, e_n)$ and $(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$. Associativity carries through componentwise. □

EXAMPLE. $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$ and $\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$ with the operation being componentwise (vector) addition.

EXAMPLE. $U(5) = \{1, 2, 3, 4\}$ and $U(12) = \{1, 5, 7, 11\}$. So

$$U(5) \oplus U(12) = \big\{(1,1), (1,5), (1,7), (1,11), (2,1), (2,5), (2,7), (2,11),$$
$$(3,1), (3,5), (3,7), (3,11), (4,1), (4,5), (4,7), (4,11)\big\}.$$

$$(2,7)(3,11) = (6 \bmod 5, 77 \bmod 12) = (1,5).$$

EXAMPLE.

$$\mathbb{Z}_2 \oplus \mathbb{Z}_5 = \big\{(0,0),(0,1),(0,2),(0,3),(0,4),(1,0),(1,1),(1,2),(1,3),(1,4)\big\}.$$

Consider $\langle(1,1)\rangle$. Since the operation is addition,

$$\langle(1,1)\rangle = \big\{(1,1), 2(1,1) = (0,2), 3(1,1) = (1,3), 4(1,1) = (0,4)$$
$$5(1,1) = (1,0), 6(1,1) = (0,1), 7(1,1) = (1,2)$$
$$8(1,1) = (0,3), 9(1,1) = (1,4), 10(1,1) = (0,0),$$

so $\mathbb{Z}_2 \oplus \mathbb{Z}_5 = \langle(1,1)\rangle$ is cyclic.

Are all groups of the form $\mathbb{Z}_n \oplus \mathbb{Z}_m$ cyclic?

EXAMPLE. Consider $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \big\{(0,0),(0,1),(1,0),(1,2)\big\}$.

Except for $(0,0)$, each element has order 2, so $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is the Klein 4-group, so is not cyclic.

Properties of External Direct Products

THEOREM (8.1 — Order of an Element in a Direct Product). *The order of an element in a direct product of a finite number of finite groups is the* lcm *of the orders of the components of the elements:*

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

PROOF.

First consider the case where the direct product has 2 factors.

Let $(g_1, g_2) \in G_1 \oplus G_2$. Let $s = \text{lcm}(|g_1|, |g_2|)$ and let $t = |(g_1, g_2)|$. *Then* $(g_1, g_2)^s = (g_1^s, g_2^s) = (e, e) \Longrightarrow$ (Theorem 4.1, Corollary 2) $t|s$. Thus $t \leq s$.

But

$$(g_1^t, g_2^t) = (g_1, g_2)^t = (e, e) \Longrightarrow |g_1| \big| t \text{ and } |g_2| \big| t.$$

Thus t is a common multiple of $|g_1|$ and $|g_2| \Longrightarrow s \leq t$ since $s = \text{lcm}(|g_1|, |g_2|)$.

Thus $s = t$ and $|(g_1, g_2)| = \text{lcm}(|g_1|, |g_2|)$.

For the general case, suppose the result holds for $G_1 \oplus G_2 \oplus \cdots \oplus G_{n-1}$. But

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \big(G_1 \oplus G_2 \oplus \cdots \oplus G_{n-1}\big) \oplus G_n,$$

so applying the previous argument, the result holds for $\big(G_1 \oplus G_2 \oplus \cdots \oplus G_n\big)$ by induction. □

EXAMPLE. Determine the number of elements of order 7 in $\mathbb{Z}_{49} \oplus \mathbb{Z}_7$.

SOLUTION.

For each such element, $7 = |(a, b)| = \text{lcm}(|a|, |b|)$ by Theorem 8.1. There are three mutually exclusive cases:

(1) $|a| = 7$ and $|b| = 7$. There are 6 choices for a $(7, 14, 21, 28, 35, 42)$ and 6 for b $(1, 2, 3, 4, 5, 6)$ for a total of 36.

(2) $|a| = 7$ and $|b| = 1$. We have 6 choices for a and 1 for b, a total of 6.

(3) $|a| = 1$ and $|b| = 7$. Another 6 choices.

Thus $\mathbb{Z}_{49} \oplus \mathbb{Z}_7$ has 48 elements of order 7. □

EXAMPLE. Find the number of cyclic subgroups of order 14 in $\mathbb{Z}_{196} \oplus \mathbb{Z}_{49}$.

SOLUTION.

We count the elements (a, b) of order 14:

(1) $|a| = 14$ and $|b| = 7$ or 1. $\mathbb{Z}_{196}$ has a unique cyclic subroup of order 14 and this has $\phi(14) = 6$ generators (Theorem 4.4), so we have 6 choices for a and 7 for b, a total of 42 for (a, b).

(2) $|a| = 2$ and $|b| = 7$. By Theorem 4.4, since $2|196$, there is $\phi(2) = 1$ subgroup of order 2, and thus element of order 2. There are 6 choices for b, so 6 overall.

Thus we have 48 elements of order 14.

Because each cyclic group has 6 elements of order 14, and no two of the cyclic groups can have an element of order 14 in common, there are $48/6 = 8$ cyclic subgroups of order 14. □

EXAMPLE. Since $|8| = 6$ in $\mathbb{Z}_{48}$ and $|4| = 4$ in $\mathbb{Z}_{16}$, $\langle 8 \rangle \oplus \langle 4 \rangle$ is a subgroup of order 24 in $\mathbb{Z}_{48} \oplus \mathbb{Z}_{16}$.

THEOREM (8.2 — Criterion for $G \oplus H$ to be Cyclic). *Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic $\iff$ $|G|$ and $|H|$ are relatively prime.*

PROOF.

Let $|G| = m$ and $|H| = n$, so $|G \oplus H| = mn$.

($\Longrightarrow$) Assume $G \oplus H$ is cyclic. Suppose $\gcd(m, n) = d$ and (g, h) is a generator of $G \oplus H$. Now

$$(g, h)^{\frac{mn}{d}} = \left((g^m)^{\frac{n}{d}}, (h^n)^{\frac{m}{d}}\right) = (e, e) \Longrightarrow mn = |(g, h)| \leq \frac{mn}{d} \Longrightarrow d = 1.$$

Thus $|G|$ and $|H|$ are relatively prime.

($\Longleftarrow$) Suppose $G = \langle g \rangle$ and $H = \langle h \rangle$, and $\gcd(m, n) = 1$. Then

$$|(g, h)| = \operatorname{lcm}(m, n) = mn = |G \oplus H|,$$

so (g, h) is a generator of $G \oplus H \Longrightarrow G \oplus H$ is cyclic. □

COROLLARY (1 — Criterion for $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ to be Cyclic). *An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic $\iff$ $|G_i| and |G_j|$ are relatively prime when $i \neq j$.*

PROOF.

Theorem 8.2 and induction. □

COROLLARY (Criterion for $\mathbb{Z}_{n_1 n_2 \cdots n_k} \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$).

Let $m = n_1 n_2 \cdots n_k$. Then $\mathbb{Z}_m \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ $\iff$ n_i and n_j are relatively prime when $i \neq j$.

EXAMPLE.

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_7 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{70},$$

and

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_7 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \approx \mathbb{Z}_{10} \oplus \mathbb{Z}_{14}.$$

Thus

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{70} \approx \mathbb{Z}_{10} \oplus \mathbb{Z}_{14}, \text{ but } \mathbb{Z}_2 \oplus \mathbb{Z}_{70} \not\approx \mathbb{Z}_{140}$$

<u>$U(n)$ as an External Direct Product</u>

If $k|n$, let

$$U_k(n) = \{x \in U(n) | x \bmod k = 1\}.$$

EXAMPLE.

$U(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, so

$U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and

$U_7(21) = \{1, 8\}$.

LEMMA. *If $k|n$, $U_k(n) \leq U(n)$.*

PROOF.

For $a, b \in U_k(n)$, $a \bmod k = 1$ and $b \bmod k = 1 \Longrightarrow$

$$(ab) \bmod k = (a \bmod k)(b \bmod k) = 1 \cdot 1 = 1,$$

so $U_k(n)$ is closed under multiplication mod k.

Since $1 \in U_k(n)$, $U_k(n) \neq \emptyset$, $U_k(n) \leq U(n)$ by the Finite Subgroup test. $\square$

The next theorem requires two preliminary results:

LEMMA (1 — Page 24 #17). *Let* $a, b, s, t \in \mathbb{Z}$. *If* $a \mod st = b \mod st$, $a \mod s = b \mod s$ *and* $a \mod t = b \mod t$. *The converse is true if* $\gcd(s,t) = 1$.

PROOF.

($\Longrightarrow$) Since $st|a-b$, $s|a-b$ and $t|a-b \Longrightarrow$

$a \mod s = b \mod s$ and $a \mod t = b \mod t$.

($\Longleftarrow$) Assume $\gcd(s,t) = 1$, $s|a-b$ and $t|a-b$. Then $\text{lcm}(s,t)|a-b$. But

$$st = \text{lcm}(s,t) \cdot \gcd(st) = \text{lcm}(st) \cdot 1 = \text{lcm}(st),$$

so

$$st|a-b \Longrightarrow a \mod st = b \mod st.$$

□

LEMMA (2 — Page 24 # 19). $\gcd(a,bc) = 1 \iff \gcd(a,b) = 1$ *and* $\gcd(a,c) = 1$.

PROOF.

By the Fundamental Theorem of Arithmetic,

$$a = p_1 p_2 \cdots p_k,\ b = q_1 q_2 \cdots q_l,\ c = r_1 r_2 \cdots r_m$$

where the p_i, q_i, r_i are primes.

$\gcd(a,bc) = 1 \iff p_i \neq q_j$ and $p_i \neq r_h$ for any i, j, h.

$\gcd(a,b) = 1 \iff p_i \neq q_j$ for any i, j.

$\gcd(a,c) = 1 \iff p_i \neq r_h$ for any i, h.

The result clearly follows. □

THEOREM (8.3 — $U(n)$ as an Exterior Direct Product). *Suppose s and t are relatively prime. Then $U(st) \approx U(s) \oplus U(t)$. Also, $U_s(st) \approx U(t)$ and $U_t(st) \approx U(s)$.*

PROOF.

We are given $\gcd(s,t) = 1$. If $x \in U(st)$, $\gcd(x, st) = 1 \Longrightarrow$ (Lemma 2) $\gcd(x,s) = 1$ and $\gcd(x,t) = 1$, so define

$$\phi : U(st) \to U(s) \oplus U(t) \text{ by } \phi(x) = (x \bmod s, x \bmod t).$$

[Since elements in $U(st)$, $U(s)$, and $U(t)$ have multiple representations, we need to show ϕ is well-defined.]

Suppose $x = y \bmod st$. By Lemma 1, $x = y \bmod s$ and $x = y \bmod t$, so

$$\phi(x) = (x \bmod s, x \bmod t) = (y \bmod s, y \bmod t) = \phi(y),$$

so ϕ is well-defined.

[To show ϕ is 1–1.] Suppose $x, y \in U(st)$ and $\phi(x) = \phi(y)$. Then

$$\begin{aligned}(x \bmod s, x \bmod t) = (y \bmod s, y \bmod t) &\Longrightarrow \\ x = y \bmod s \text{ and } x = y \bmod t &\Longrightarrow \\ (\text{by Lemma 1 since } \gcd(s,t) = 1)\ x = y \bmod st.&\end{aligned}$$

Thus ϕ is 1–1.

[To show ϕ is onto.] Let $(a,b) \in U(s) \oplus U(t)$. Then $\gcd(a,s) = 1$ and $\gcd(b,t) = 1$. Since $\gcd(s,t) = 1$, $\exists\ q_1, q_2 \in \mathbb{Z} \ni sq_1 + tq_2 = 1 \Longrightarrow$ $\gcd(t, q_1) = 1$ and $\gcd(s, q_2) = 1$. Consider $z = bsq_1 + atq_2$.

[To show $z \in U(st)$ and $\phi(z) = (a \bmod s, b \bmod t)$.] Suppose $p | st$, p a prime. Then $p|s$ or $p|t$. If $p|s$, $p|bsq_1$, but $p \not| atq_2$ since, by Lemma 2, s is relativelty prime to atq_2 since it is relatively prime to each factor. So $p \not| z$. If $p|t$, a symmetric argument also gives $p \not| z$. Thus $\gcd(z, st) = 1 \Longrightarrow z \in U(s,t)$.

[To show $z = a \bmod s$ and $z = b \bmod t$.]

$$z - a = bsq_1 + atq_2 - a = bsq_1 + a(tq_2 - 1) = bsq_1 + a(-sq_1) \Longrightarrow$$
$$s|z - a \Longrightarrow z = a \bmod s.$$

Another symmeric argument yields $z = b \bmod t$. Thus

$$\phi(z) = (a \bmod s, b \bmod t)$$

and ϕ is onto.

[Show preservation of operation.]

Suppose $x, y \in U(st)$. Then $\gcd(x, st) = 1$ and $\gcd(y, st) = 1$. Recalling Lemma 2,

$$\gcd(x, s) = \gcd(x, t) = \gcd(ys) = \gcd(y, t) = 1$$

Then

$$\phi(xy) = (xy \bmod s, xy \bmod t) =$$
$$(x \bmod s, x \bmod t) \cdot (y \bmod s, y \bmod t) = \phi(x)\phi(y).$$

We conclude $U(st) \approx U(s) \oplus U(t)$.

For $U_s(st) \approx U(t)$, use $\alpha : U_s(st) \to U(t)$ defined by $\alpha(x) = x \bmod t$.

For $U_t(st) \approx U(s)$, use $\beta : U_t(st) \to U(s)$ defined by $\beta(x) = x \bmod s$. □

COROLLARY. *Let* $m = n_1 n_2 \cdots n_k$ *where* $\gcd(n_i, n_j) = 1$ *for* $i \neq j$. *Then*

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k).$$

PROOF.

Follows from Theorem 8.3 by induction. □

EXAMPLE. $U(315) = U(5 \cdot 7 \cdot 9)$ with $5, 7, 9$ pairwise relatively prime. Thus $U(315) \approx U(5) \oplus U(63) \approx U(7) \oplus U(45) \approx U(9) \oplus U(35) \approx U(5) \oplus U(7) \oplus U(9)$. The order of any of the factors in the above can be interchanged. Also,

$$U(9) \approx U_{35}(315) = \{1, 71, 106, 176, 211, 281\}.$$

$$U(35) \approx U_9(315) = \{1, 19, 37, 46, 64, 73, 82, 109, 118, 127, 136, 163, 172, 181, 199, 208, 226, 244, 253, 262, 271, 289, 298, 307\}.$$

$$U(5) \approx U_{63}(315) = \{1, 64, 127, 253\}.$$

$$U(7) \approx U_{45}(315) = \{1, 46, 136, 181, 226, 271\}.$$

<u>U-groups</u>

Proved by Carl Gauss:

(1) $U(2) \approx 0$.

(2) $U(4) \approx \mathbb{Z}_2$.

(3) $U(2^n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-1}}$ for $n \geq 3$.

(4) $U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}$ for p an odd prime.

With these 4 results and Theorem 8.3, we can write any U-group as an external direct product of cyclic groups. We will eventually show that any finite Abelian group can be written as such a direct product.

EXAMPLE.

$$U(385) \approx U(5 \cdot 7 \cdot 11) \approx U(5) \oplus U(7) \oplus U(11) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{10}.$$

EXAMPLE.

$$U(2800) \approx U(25 \cdot 16 \cdot 7) \approx U(5^2) \oplus U(2^4) \oplus U(7) \approx \mathbb{Z}_{20} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_6.$$

Why is this important?

(1) Possible orders of elements:

$\underline{\mathbb{Z}_{20}}$	$\underline{\mathbb{Z}_2}$	$\underline{\mathbb{Z}_8}$	$\underline{\mathbb{Z}_6}$
1	1	1	1
2	2	2	2
4		4	3
5		8	6
10			
20			

For the order of an element, we take the lcm of the possible choices. Thus possible orders in

$$\mathbb{Z}_{20} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_6$$

are

$$1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120.$$

This would be hard to determine without direct product decomposition.

(2) Assuming $(a, b, c, d) \in \mathbb{Z}_{20} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_6$, how many of these elements are of order 12?

$$|(a, b, c, d)| = 12 \iff \text{lcm}\big(|a|, |b|, |c|, |d|\big) = 12.$$

For the moment, since $|b| = 1$ or $|b| = 2$, consider just $\mathbb{Z}_{20} \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_6$.

For each such element, $|d| = 3$ or $|d| = 6$, and at least one of $|a| = 4$ or $|c| = 4$ must occur. From Theorem 4.4, $\mathbb{Z}_6$ has two elements each of orders 3 and 6, so we have 4 choices for d.

Case 1: $|a| = 4$. There are $\phi(4) = 2$ elements of order 4 in $\mathbb{Z}_{20}$. Then $|c| = 4$ or $|c| = 2$ or $|c| = 1$, so we have $\phi(4) + \phi(2) + \phi(1) = 2 + 1 + 1 = 4$ choices for c, giving $2 \cdot 4 \cdot 4 = 32$ choices for a, c, d.

Case 2: $|c| = 4$. Then $|a| = 1$ or $|(|a) = 2$ (we have already counted $|a| = |c| = 4$). So we have, like in Case 1, $2 \cdot 2 \cdot 4 = 16$ choices for a, c, d.

Then, for each of this total of $32 + 16 = 48$ choices, we have 2 choices for b, neither of which affects the lcm.

Thus there are 96 elements of order 12.

Again, this is hard to count without direct product decomposition.

(3) $\mathrm{Aut}(\mathbb{Z}_{2800}) \approx U(2800)$, so $\mathrm{Aut}(\mathbb{Z}_{2800})$ has 96 isomorphisms of order 12.

Question: The $U(n)$ are all Abelian groups. Are all Abelian groups external direct products of cyclic groups?