External Direct Products

Main Goals:

- Learn how to construct larger groups from smaller ones using external direct products
- Understand when direct products of cyclic groups are cyclic
- Apply direct products to U-groups and cryptography
- Preview: Chapter 9 will show how to decompose large groups into products of smaller ones (analogous to prime factorization)

Key Application: Constructing all finite Abelian groups

Definition: External Direct Product

Definition 8.1 (External Direct Product): Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The **external direct product** of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the i-th component is an element of G_i and the operation is componentwise.

In symbols: $G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$, where:

- $(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n')$ is defined to be $(g_1 g_1', g_2 g_2', \ldots, g_n g_n')$.

Note: Each product $g_i g_i'$ is performed with the operation of G_i.

Properties of External Direct Products

Order Property: When each G_i is finite: $|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1| \cdot |G_2| \cdots |G_n|$.

Group Structure: The external direct product of groups is itself a group (Exercise 1).

Familiar Examples:

- $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$ (componentwise addition)
- $\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$ (componentwise addition)

Note: We ignore scalar multiplication for now, focusing only on the group structure.

Example: $U(8) \oplus U(10)$

The Group:

$$U(8) \oplus U(10) = \{(1,1),(1,3),(1,7),(1,9),(3,1),(3,3),(3,7),(3,9),(5,1),(5,3),(5,7),(5,9),(7,1),(7,3),(7,7),(7,9)\}$$

Order: $|U(8) \oplus U(10)| = |U(8)| \cdot |U(10)| = 4 \cdot 4 = 16$

Sample Calculation:

$$(3,7)(7,9) = (3 \cdot 7 \bmod 8, 7 \cdot 9 \bmod 10) = (21 \bmod 8, 63 \bmod 10) = (5,3)$$

Key Point:

- First components combine by multiplication modulo 8
- Second components combine by multiplication modulo 10
- Each component operates independently in its respective group

Example: $\mathbb{Z}_2 \oplus \mathbb{Z}_3$

The Group: $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$

Properties:

- This is an Abelian group of order 6
- Operations are componentwise addition modulo 2 and modulo 3

Question: How does this relate to $\mathbb{Z}_6$, another Abelian group of order 6?

Example: Classification of Groups of Order 4

Theorem: A group of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Proof Strategy: We show that for any non-cyclic group G of order 4, the operation table is uniquely determined.

Step 1: By Lagrange's Theorem, elements of G have order 1 or 2.

Step 2: Let a and b be distinct non-identity elements of G.

Step 3: By cancellation, $ab \neq a$ and $ab \neq b$.

Step 4: Moreover, $ab \neq e$, for otherwise $a = b^{-1} = b$ (contradiction).

Step 5: Thus $G = \{e, a, b, ab\}$.

Step 6: The operation is uniquely determined by: $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

Key Observation from Examples 2 and 3

When is $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$? From our examples:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$ ✓ (Example 2)
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \ncong \mathbb{Z}_4$ ✗ (Example 3)

Pattern:

- $\gcd(2, 3) = 1$ and we get isomorphism
- $\gcd(2, 2) = 2 \neq 1$ and we don't get isomorphism

Theorem 8.2 will provide the complete characterization!

Theorem 8.1 The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols:
$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$

Proof: Let identity of G_i be e_i, $s = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$, and $t = |(g_1, g_2, \ldots, g_n)|$

Proof that $t \leq s$: Since s is a multiple of each $|g_i|$, we have $g_i^s = e_i$ for all i. Therefore:
$(g_1, g_2, \ldots, g_n)^s = (g_1^s, g_2^s, \ldots, g_n^s) = (e_1, e_2, \ldots, e_n)$. This shows that $t \leq s$.

Proof that $s \leq t$: From $(g_1, g_2, \ldots, g_n)^t = (e_1, e_2, \ldots, e_n)$, we have:
$(g_1^t, g_2^t, \ldots, g_n^t) = (e_1, e_2, \ldots, e_n)$. This means $g_i^t = e_i$ for all i. So $|g_i|$ divides t for each i. Since t is a common multiple of all $|g_i|$, and s is the *least* common multiple, we have $s \leq t$.

Conclusion: $s \leq t$ and $t \leq s$, so $s = t$. ∎

Example 4: Groups of Order 100

- $\mathbb{Z}_{25} \oplus \mathbb{Z}_4$
- $\mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4$
- $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- D_{50}
- $D_{10} \oplus \mathbb{Z}_5$
- $D_5 \oplus D_5$

How do we know these are not isomorphic?

Problem: Let m and n be positive integers divisible by 5. Find the number of elements of order 5 in $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Solution: By Theorem 8.1, we need (a, b) where $5 = |(a, b)| = \mathrm{lcm}(|a|, |b|)$.

Analysis: This requires $|a| \in \{1, 5\}$ and $|b| \in \{1, 5\}$, but not both equal to 1. **Counting:**

- Both $\mathbb{Z}_m$ and $\mathbb{Z}_n$ have unique subgroups of order 5
- Each subgroup contains exactly 5 elements
- So there are 5 choices for a and 5 choices for b
- This gives $5 \times 5 = 25$ total pairs (a, b)
- Excluding $(0, 0)$, we have **24 elements of order 5**

General Result: If m and n are positive integers divisible by a prime p, then the number of elements of order p in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is $p^2 - 1$.

Proof: Identical to the argument for $p = 5$:

- Each of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ has a unique subgroup of order p
- Each such subgroup has p elements
- Total pairs: $p \times p = p^2$
- Excluding identity: $p^2 - 1$ elements of order p

Problem: Determine the number of cyclic subgroups of order 10 in $\mathbb{Z}_{150} \oplus \mathbb{Z}_{50}$.

Strategy:

1. Count elements of order 10
2. Use the fact that each cyclic subgroup of order 10 contains exactly $\phi(10) = 4$ elements of order 10
3. Divide the count by 4

Step 1: For $10 = |(a, b)| = \text{lcm}(|a|, |b|)$, we need $|a|, |b| \in \{1, 2, 5, 10\}$.

- a must belong to the unique subgroup $\langle 15 \rangle$ of order 10 in $\mathbb{Z}_{150}$
- b must belong to the unique subgroup $\langle 5 \rangle$ of order 10 in $\mathbb{Z}_{50}$
- So $(a, b) \in \langle 15 \rangle \oplus \langle 5 \rangle \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$

Step 2: Count elements of each order in $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$. Total elements: $|\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}| = 100$.
Elements to subtract:

- Order 1: Just $(0, 0)$, so **1 element**
- Order 2: From Example 5 pattern, **3 elements**
- Order 5: From Example 5, **24 elements**

Elements of order 10: $100 - 1 - 3 - 24 = 72$

Step 3: Count cyclic subgroups: Number of cyclic subgroups: $72 \div 4 = \boxed{18}$

Problem: Determine the number of elements of order 2 in $D_4 \oplus \mathbb{Z}_3$.

Solution: For $|(a, b)| = 2$, we need $|a| \in \{1, 2\}$ and $|b| \in \{1, 2\}$, but not both order 1.
Recall: $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

- Order 1: R_0 (1 element)
- Order 2: R_{180}, H, V, D, D' (5 elements)
- Total including identity: 6 elements of order dividing 2

In $\mathbb{Z}_3$**:**

- Order 1: 0 (1 element)
- Order 2: none (0 elements)
- Total including identity: 1 element of order dividing 2

Counting (a, b): $6 \times 2 - 1 = 12 - 1 = \boxed{11}$ elements of order 2

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 if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.

Proof: By induction using Theorem 8.2.

Example Applications:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ is cyclic (all orders pairwise relatively prime)
- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$ is NOT cyclic ($\gcd(2,4) = 2 \neq 1$)

Corollary 2 (Criterion for $\mathbb{Z}_{n_1 n_2 \cdots n_k} \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$): Let $m = n_1 n_2 \cdots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

Proof: Both groups are cyclic of the same order. The result follows from Corollary 1.

Example 1: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$

Example 2: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$

However: $\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \ncong \mathbb{Z}_{60}$ (since $\gcd(2, 30) = 2 \neq 1$)

The Group of Units Modulo n

New Notation: For a proper divisor $k > 1$ of a positive integer n, define:
$U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$

Example: $U_7(105) = \{1, 8, 22, 29, 43, 64, 71, 92\}$

Fact: $U_k(n)$ is a subgroup of $U(n)$ (Exercise 21, Chapter 3)

Theorem ($U(n)$ as an External Direct Product): Suppose s and t are relatively prime. Then $U(st) \cong U(s) \oplus U(t)$. Moreover: $U_s(st) \cong U(t)$ and $U_t(st) \cong U(s)$.

Proof: Define the following mappings:

1. $\phi : U(st) \to U(s) \oplus U(t)$ by $\phi(x) = (x \bmod s, x \bmod t)$
2. $\psi : U_s(st) \to U(t)$ by $\psi(x) = x \bmod t$
3. $\rho : U_t(st) \to U(s)$ by $\rho(x) = x \bmod s$

To complete the proof, we must verify:

- Each mapping is operation-preserving
- Each mapping is one-to-one
- Each mapping is onto

These verifications are left to Exercises 11, 19, and 21 in Chapter 0. ∎

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

$$U(m) \cong U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$$

Proof: Apply Theorem 8.3 iteratively.

Example ($U(105)$): Applying Theorem in different ways:

$$U(105) \cong U(7) \oplus U(15)$$
$$U(105) \cong U(21) \oplus U(5)$$
$$U(105) \cong U(3) \oplus U(5) \oplus U(7)$$

Gauss's Results on U-Groups

1. $U(2) \cong \{0\}$ (trivial group)
2. $U(4) \cong \mathbb{Z}_2$
3. $U(2^n) \cong \mathbb{Z}_{2^{n-2}} \oplus \mathbb{Z}_2$ for $n \geq 3$
4. $U(p^n) \cong \mathbb{Z}_{p^{n-1}(p-1)}$ for p an odd prime

Why these matter: Every U-group can be written as an external direct product of cyclic groups using:

- The corollary to Theorem 8.3 (to factor by prime powers)
- Gauss's results (to express each $U(p^n)$ as $\oplus$ of cyclic groups)

Example: $U(105)$ as $\oplus$ of Cyclic Groups

Using Gauss's results: $U(105) = U(3 \cdot 5 \cdot 7) \cong U(3) \oplus U(5) \oplus U(7)$

For each prime power:

- $U(3) = U(3^1) \cong \mathbb{Z}_{3^0(3-1)} = \mathbb{Z}_2$
- $U(5) = U(5^1) \cong \mathbb{Z}_{5^0(5-1)} = \mathbb{Z}_4$
- $U(7) = U(7^1) \cong \mathbb{Z}_{7^0(7-1)} = \mathbb{Z}_6$

Therefore: $U(105) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$

Example: $U(144)$

Factoring 144: $144 = 16 \cdot 9 = 2^4 \cdot 3^2$

Applying the corollary to Theorem 8.3: $U(144) \cong U(16) \oplus U(9)$

Using Gauss's results:

- $U(16) = U(2^4) \cong \mathbb{Z}_{2^{4-2}} \oplus \mathbb{Z}_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_2$
- $U(9) = U(3^2) \cong \mathbb{Z}_{3^{2-1}(3-1)} = \mathbb{Z}_{3\cdot 2} = \mathbb{Z}_6$

Therefore: $U(144) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$

Observation: $U(105) \cong U(144)$ since both equal $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$!

Advantages of Direct Product Representation

What we immediately know about $U(105) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$:

1. **Order:** $|U(105)| = 2 \cdot 4 \cdot 6 = 48$
2. **Element orders:** By Theorem 8.1, possible orders are divisors of $\mathbf{lcm}(2, 4, 6) = \mathbf{12}$. So, possible orders: 1, 2, 3, 4, 6, 12.
3. **Counting elements of specific order:** We can determine that $U(105)$ has exactly **16 elements of order 12.**
4. **Isomorphic groups:** We instantly see $U(105) \cong U(144)$
5. **Connection to automorphisms:** Since $\mathrm{Aut}(\mathbb{Z}_{105}) \cong U(105)$, we know $\mathrm{Aut}(\mathbb{Z}_{105})$ has exactly 16 automorphisms of order 12

Compare: Try computing these facts directly from the definition of $U(105)$!