MATH 343 · GROUP THEORY · CHAPTER 8

External Direct Products

Definition and Examples · Properties · The Groups U(n) · Applications

Fahd M. Alshammari

Part 1 — Definition and Examples

GOAL. Build new groups from old ones by working in each coordinate separately.

- The external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$
- Examples: $U(8) \oplus U(10)$, and $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$
- Every group of order 4 is $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

Definition — External Direct Product

DEFINITION. Let $G_1, G_2, \ldots, G_n$ be groups. Their **external direct product** is the set of n-tuples

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

with the operation done componentwise:

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

- Each product $g_i g_i'$ is taken with the operation of G_i
- It is a group (Exercise 1); if every G_i is finite, its order is $|G_1||G_2| \cdots |G_n|$
- Example: $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$ under componentwise addition

Example — U(8) ⊕ U(10)

EXAMPLE. $U(8) = \{1,3,5,7\}$ and $U(10) = \{1,3,7,9\}$, so $U(8) \oplus U(10)$ has $4 \cdot 4 = 16$ elements:

$$U(8) \oplus U(10) = \{(a, b) \mid a \in \{1,3,5,7\},\ b \in \{1,3,7,9\}\}.$$

A product, coordinate by coordinate:

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

- The first coordinates multiply modulo 8, the second modulo 10

Example — $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ Is Cyclic

EXAMPLE. In $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ the operation is addition in each coordinate. The multiples of $(1,1)$ are

$$(1,1),\ \ (0,2),\ \ (1,0),\ \ (0,1),\ \ (1,2),\ \ (0,0):$$

all six elements. So $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (1,1) \rangle$ is cyclic of order 6, and by Chapter 6 it is isomorphic to $\mathbb{Z}_6$.

- The next slide writes down an isomorphism with $\mathbb{Z}_6$ by a formula

Proof That $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$

PROPOSITION. The map $\psi: \mathbb{Z}_6 \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$, $\psi(k) = (k \bmod 2,\ k \bmod 3)$, is an isomorphism.

Step 1 (well defined). For each $k \in \{0,1,\ldots,5\}$, $k \bmod 2$ and $k \bmod 3$ are single elements of $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

Step 2 (one-to-one). If $\psi(k) = \psi(l)$, then 2 and 3 divide $k - l$, so 6 divides $k - l$, and $k = l$.

Step 3 (onto). ψ is one-to-one, and both groups have 6 elements.

Step 4 (operation-preserving). As 2 and 3 divide 6, reducing mod 6 first changes nothing mod 2 or mod 3:

$$\psi(k + l) = \big((k + l) \bmod 2,\ (k + l) \bmod 3\big) = \psi(k) + \psi(l).$$

Groups of Order 4

THEOREM. Every group of order 4 is isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

PROOF. Let $|G| = 4$. If G is cyclic, then $G \cong \mathbb{Z}_4$ (Chapter 6). Suppose G is not cyclic. By Lagrange's Theorem every $x \neq e$ has order 2, so $x = x^{-1}$. Let a, b be two different elements other than e.

- $ab \neq a$ and $ab \neq b$ (cancellation), and $ab \neq e$ (else $a = b^{-1} = b$); so $G = \{e, a, b, ab\}$
- $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, so G is Abelian

Define $\varphi: G \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by

$$\varphi(e) = (0,0), \quad \varphi(a) = (1,0), \quad \varphi(b) = (0,1), \quad \varphi(ab) = (1,1).$$

Groups of Order 4 — The Isomorphism

Step 1 (well defined). e, a, b, ab are the four different elements of G, so φ gives one value at each.

Step 2 (one-to-one). The four values are different.

Step 3 (onto). Every element of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a value.

Step 4 (operation-preserving). In both groups each element is its own inverse, and two different elements other than the identity combine to the third: $a \cdot b = ab$, $a \cdot ab = b$, $b \cdot ab = a$, and $(1,0) + (0,1) = (1,1)$, $(1,0) + (1,1) = (0,1)$, $(0,1) + (1,1) = (1,0)$.

So φ is an isomorphism, and $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Part 2 — Properties

GOAL. Read off the orders of elements, and decide cyclicity, from the factors.

- Theorem 8.1: the order of $(g_1, \ldots, g_n)$ is $\operatorname{lcm}(|g_1|, \ldots, |g_n|)$
- Counting elements and cyclic subgroups of a given order
- Theorem 8.2: when $G \oplus H$ is cyclic, and when $\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$

Theorem 8.1 — The Order of an Element

THEOREM 8.1. Let $G_1, \dots, G_n$ be finite groups and $g_i \in G_i$. Then

$$|(g_1, g_2, \dots, g_n)| = \operatorname{lcm}(|g_1|, |g_2|, \dots, |g_n|).$$

EXAMPLE. In $\mathbb{Z}_4 \oplus \mathbb{Z}_6$:

- $|(1,2)| = \operatorname{lcm}(4,3) = 12$, the largest possible order here
- $|(2,3)| = \operatorname{lcm}(2,2) = 2$: the order is the lcm, not the product

Proof of Theorem 8.1

PROOF. Let e_i be the identity of G_i, let $s = \operatorname{lcm}(|g_1|, \ldots, |g_n|)$ and $t = |(g_1, \ldots, g_n)|$. Powers are computed componentwise: $(g_1, \ldots, g_n)^k = \left(g_1^k, \ldots, g_n^k\right)$.

Step 1 (t divides s). Each $|g_i|$ divides s, so $g_i^s = e_i$ for every i, and $(g_1, \ldots, g_n)^s = (e_1, \ldots, e_n)$. By Corollary 2 of Theorem 4.1, t divides s.

Step 2 (s divides t). $\left(g_1^t, \ldots, g_n^t\right) = (e_1, \ldots, e_n)$, so $g_i^t = e_i$ and $|g_i|$ divides t for every i. So t is a common multiple of the $|g_i|$, and s divides t.

So $s = t$.

Eight Groups of Order 100?

EXAMPLE. Gallian lists eight groups of order 100 and says that no two are isomorphic. Isomorphic groups have the same largest element order and the same number of elements of order 2 (Theorem 6.1). Theorem 8.1 gives these numbers:

Group	Largest	Order 2	Group	Largest	Order 2
$\mathbb{Z}_{100}$	100	1	D_{50}	50	51
$\mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	50	3	$D_{10} \oplus \mathbb{Z}_5$	10	11
$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4$	20	1	$D_5 \oplus \mathbb{Z}_{10}$	10	11
$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	10	3	$D_5 \oplus D_5$	10	35

Two of the Eight Are Isomorphic

PROPOSITION. $D_{10} \cong D_5 \oplus \mathbb{Z}_2$. Hence $D_{10} \oplus \mathbb{Z}_5 \cong D_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong D_5 \oplus \mathbb{Z}_{10}$, and Gallian's list has only seven different groups.

PROOF. Let R and ρ be the rotations through $36°$ in D_{10} and $72°$ in D_5, and F a reflection in each. Every element of D_{10} is $R^k F^s$ for exactly one $k \in \{0, \ldots, 9\}$ and $s \in \{0,1\}$. Define $\varphi: D_{10} \to D_5 \oplus \mathbb{Z}_2$ by

$$\varphi\left(R^k F^s\right) = \left(\rho^k F^s,\ k \bmod 2\right).$$

Proof That $D_{10} \cong D_5 \oplus \mathbb{Z}_2$

Step 1 (well defined). Each element of D_{10} has exactly one name $R^k F^s$, and $\rho^k F^s \in D_5$, $k \bmod 2 \in \mathbb{Z}_2$.

Step 2 (one-to-one). If $\varphi\left(R^k F^s\right) = \varphi\left(R^l F^t\right)$, then $s = t$, and 5 and 2 divide $k - l$. So 10 divides $k - l$, and $k = l$.

Step 3 (onto). φ is one-to-one, and both groups have 20 elements.

Step 4 (operation-preserving). As $FR^b = R^{-b}F$, $(R^a F^s)\left(R^b F^t\right) = R^{a \pm b} F^{s+t}$, and the same rule holds in D_5. Since $a \pm b$ and $a + b$ have the same parity, $\varphi(xy) = \varphi(x)\varphi(y)$.

So φ is an isomorphism, and $D_{10} \cong D_5 \oplus \mathbb{Z}_2$.

Counting Elements of a Given Order

EXAMPLE. Let 5 divide m and n. In $\mathbb{Z}_m \oplus \mathbb{Z}_n$, $|(a,b)| = \text{lcm}(|a|,|b|) = 5$ exactly when $|a|, |b| \in \{1,5\}$, not both 1. $\mathbb{Z}_m$ and $\mathbb{Z}_n$ each have exactly one subgroup of order 5 (Theorem 4.3), so there are $5 \cdot 5 - 1 = 24$ elements of order 5.

- In general: $p^2 - 1$ elements of order p, when the prime p divides m and n

EXAMPLE. In $D_4 \oplus \mathbb{Z}_4$, $|(a,b)| = 2$ when $|a|, |b| \in \{1,2\}$, not both 1. D_4 has 6 such a and $\mathbb{Z}_4$ has 2 such b: $6 \cdot 2 - 1 = 11$ elements of order 2.

Counting Cyclic Subgroups

EXAMPLE. How many cyclic subgroups of order 10 does $\mathbb{Z}_{150} \oplus \mathbb{Z}_{50}$ have?

- $|(a, b)| = 10$ forces $|a|, |b| \in \{1,2,5,10\}$, so $a \in \langle 15 \rangle$ and $b \in \langle 5 \rangle$, the subgroups of order 10; and $\langle 15 \rangle \oplus \langle 5 \rangle \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$
- $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$ has 1 identity, 3 elements of order 2 and 24 of order 5, so $100 - 1 - 3 - 24 = 72$ of order 10
- Each cyclic subgroup of order 10 has 4 generators, and two different ones share none

So there are $72/4 = 18$ cyclic subgroups of order 10.

Naming Subgroups with Direct Products

EXAMPLE. In $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$, the subgroup $\langle 5 \rangle$ of $\mathbb{Z}_{30}$ has order 6 and $\langle 3 \rangle$ of $\mathbb{Z}_{12}$ has order 4. So $\langle 5 \rangle \oplus \langle 3 \rangle$ is a subgroup of order 24, and

$$\theta : \langle 5 \rangle \oplus \langle 3 \rangle \to \mathbb{Z}_6 \oplus \mathbb{Z}_4, \qquad \theta(a, b) = (a/5,\ b/3),$$

is an isomorphism. In the same way, for divisors r of m and s of n, $\mathbb{Z}_m \oplus \mathbb{Z}_n$ has a subgroup isomorphic to $\mathbb{Z}_r \oplus \mathbb{Z}_s$.

Theorem 8.2 — When G ⊕ H Is Cyclic

THEOREM 8.2. Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic: $\gcd(2,3) = 1$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ are not
- Both groups must be cyclic: $U(8) \oplus \mathbb{Z}_3$ is not cyclic, although $\gcd(4,3) = 1$

Proof of Theorem 8.2

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

(⇐) Let $G = \langle g \rangle$, $H = \langle h \rangle$ and $\gcd(m, n) = 1$. By Theorem 8.1, $|(g, h)| = \operatorname{lcm}(m, n) = mn$. So $\langle (g, h) \rangle$ has mn elements, and $\langle (g, h) \rangle = G \oplus H$.

(⇒) Let $G \oplus H = \langle (g, h) \rangle$ and $d = \gcd(m, n)$. By Corollary 4 of Theorem 7.1, $g^m = e$ and $h^n = e$, so

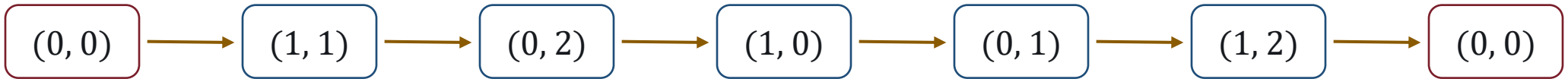
$$(g, h)^{mn/d} = \left((g^m)^{n/d},\ (h^n)^{m/d} \right) = (e, e).$$

So $mn = |(g, h)| \leq mn/d$, and $d = 1$.

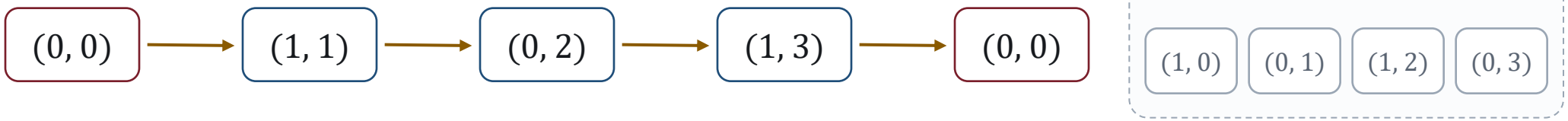
The Walk of (1, 1)

EXAMPLE. Add $(1,1)$ again and again. In $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ the walk visits every element; in $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ it is back at $(0,0)$ after 4 steps.

In $\mathbb{Z}_2 \oplus \mathbb{Z}_3$: six steps, and every element is reached



In $\mathbb{Z}_2 \oplus \mathbb{Z}_4$: back at (0, 0) after four steps



Each arrow adds (1, 1). Theorem 8.2: $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic, as gcd(2, 3) = 1; $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is not.

Corollaries 1 and 2 of Theorem 8.2

COROLLARY 1. A direct product $G_1 \oplus \cdots \oplus G_n$ of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime whenever $i \neq j$.

COROLLARY 2. Let $m = n_1 n_2 \cdots n_k$. Then $\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ if and only if n_i and n_j are relatively prime whenever $i \neq j$.

- Corollary 1: apply Theorem 8.2 to $(G_1 \oplus \cdots \oplus G_{n-1}) \oplus G_n$, and use induction on n
- Corollary 2: both groups have m elements, and a group of order m is isomorphic to $\mathbb{Z}_m$ exactly when it is cyclic (Chapter 6); then use Corollary 1

Using Corollary 2

EXAMPLE. Split cyclic factors into relatively prime pieces, or join them, and regroup:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30},$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}.$$

So $\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$. But $\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \ncong \mathbb{Z}_{60}$: since $\gcd(2,30) = 2$, it is not cyclic.

- Reordering factors, and replacing a factor by an isomorphic group, give isomorphic products (Exercises 7 and 16)

Part 3 — The Groups U(n)

GOAL. Write every group $U(n)$ as a direct product of cyclic groups.

- The subgroups $U_k(n)$
- Theorem 8.3: $U(st) \cong U(s) \oplus U(t)$ when $\gcd(s,t) = 1$
- Gauss's results on $U(2^n)$ and $U(p^n)$, and what they tell us

Definition — The Subgroups $U_k(n)$

DEFINITION. If $k > 1$ is a proper divisor of n, let

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

It is a subgroup of $U(n)$ (Chapter 3, Exercise 21).

EXAMPLE. The elements of $U(105)$ that leave remainder 1 on division by 7:

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

Theorem 8.3 — U(st) as a Direct Product

THEOREM 8.3. Let s and t be relatively prime. Then

$$U(st) \cong U(s) \oplus U(t).$$

Moreover, $U_s(st) \cong U(t)$ and $U_t(st) \cong U(s)$.

- The isomorphism is $\varphi(x) = (x \bmod s,\ x \bmod t)$ — the map of $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ again
- The hypothesis matters: $|U(20)| = 8$, but $|U(10) \oplus U(2)| = 4 \cdot 1 = 4$

Proof of Theorem 8.3 — The Map ϕ

PROOF. Define $\varphi: U(st) \to U(s) \oplus U(t)$ by $\varphi(x) = (x \bmod s,\ x \bmod t)$.

Step 1 (well defined). $\gcd(x, st) = 1$ gives $\gcd(x, s) = 1$, so $x \bmod s \in U(s)$; likewise $x \bmod t \in U(t)$.

Step 2 (one-to-one). If $\varphi(x) = \varphi(y)$, then s and t divide $x - y$. As $\gcd(s, t) = 1$, st divides $x - y$, so $x = y$.

Step 3 (onto). Let $(a, b) \in U(s) \oplus U(t)$. By the Chinese Remainder Theorem there is x with $0 \le x < st$, $x \equiv a \pmod{s}$ and $x \equiv b \pmod{t}$. Then $\gcd(x, s) = \gcd(a, s) = 1$ and $\gcd(x, t) = 1$, so $x \in U(st)$ and $\varphi(x) = (a, b)$.

Proof of Theorem 8.3 — Step 4 and $U_s(st)$

Step 4 (operation-preserving). Reducing mod s before or after multiplying gives the same result (Chapter 0, Exercise 11). So, with xy computed mod st,

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

The second part. Define $\psi\colon U_s(st) \to U(t)$ by $\psi(x) = x \bmod t$. For $x \in U_s(st)$, $\varphi(x) = \big(1, \psi(x)\big)$, so Steps 1, 2 and 4 for ψ follow from those for φ. For Step 3, let $b \in U(t)$. Step 3 for φ gives $x \in U(st)$ with $\varphi(x) = (1, b)$; then $x \bmod s = 1$, so $x \in U_s(st)$, and $\psi(x) = b$.

So $U_s(st) \cong U(t)$, and, exchanging s and t, $U_t(st) \cong U(s)$.

The Corollary — Splitting U(n) Completely

COROLLARY. If $m = n_1 n_2 \cdots n_k$ with $\gcd(n_i, n_j) = 1$ for $i \neq j$, then

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

EXAMPLE. For $105 = 3 \cdot 5 \cdot 7$:

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

- By Theorem 8.3, $U(15) \cong U_7(105) = \{1,8,22,29,43,64,71,92\}$ and $U(5) \cong U_{21}(105) = \{1,22,43,64\}$

Gauss's Theorem on U(2ⁿ) and U(pⁿ)

THEOREM (GAUSS, 1801). For $n \geq 1$ and every odd prime p:

$$U(2) \cong \{0\}, \qquad U(4) \cong \mathbb{Z}_2, \qquad U(2^n) \cong \mathbb{Z}_{2^{n-2}} \oplus \mathbb{Z}_2 \ \ (n \geq 3),$$

$$U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}}.$$

- With the Corollary, every $U(n)$ is a direct product of cyclic groups
- $|U(p^n)| = p^n - p^{n-1}$: of $1, 2, \ldots, p^n$, exactly p^{n-1} are multiples of p

The proof is beyond this course.

U(105) and U(144)

EXAMPLE. By the Corollary and Gauss's theorem,

$$U(105) \cong U(3) \oplus U(5) \oplus U(7) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6,$$

$$U(144) \cong U(16) \oplus U(9) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

- $|U(105)| = 2 \cdot 4 \cdot 6 = 48$, and $U(105) \cong U(144)$
- By Theorem 8.1, the elements of $U(105)$ have orders 1, 2, 3, 4, 6 and 12; exactly 16 have order 12
- As $\mathrm{Aut}(\mathbb{Z}_{105}) \cong U(105)$ (Theorem 6.4), $\mathbb{Z}_{105}$ has exactly 16 automorphisms of order 12

Automorphisms of Automorphisms

EXAMPLE. By Theorem 6.4, the Corollary of Theorem 8.3, Gauss's theorem, and the fact that isomorphic groups have isomorphic automorphism groups:

$$\mathrm{Aut}\left(\mathrm{Aut}\left(\mathrm{Aut}(\mathbb{Z}_{27})\right)\right) \cong \mathrm{Aut}\left(\mathrm{Aut}\left(U(27)\right)\right) \cong \mathrm{Aut}\left(\mathrm{Aut}(\mathbb{Z}_{18})\right)$$

$$\cong \mathrm{Aut}\left(U(18)\right) \cong \mathrm{Aut}(\mathbb{Z}_6) \cong U(6) \cong \mathbb{Z}_2.$$

So $\left|\mathrm{Aut}\left(\mathrm{Aut}\left(\mathrm{Aut}(\mathbb{Z}_{27})\right)\right)\right| = 2.$

What to Take Away

- $G_1 \oplus \cdots \oplus G_n$: tuples, componentwise operation, order $|G_1| \cdots |G_n|$
- $|(g_1, \ldots, g_n)| = \operatorname{lcm}(|g_1|, \ldots, |g_n|)$ (Theorem 8.1)
- $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ exactly when $\gcd(m, n) = 1$ (Theorem 8.2)
- $U(st) \cong U(s) \oplus U(t)$ when $\gcd(s, t) = 1$, by $x \mapsto (x \bmod s,\ x \bmod t)$; with Gauss's theorem, every $U(n)$ is a product of cyclic groups