8 External Direct Products

Exercise 1. Group Properties of External Direct Products

Statement. Prove that the external direct product of any finite number of groups is a group.

Solution.

Let $G_1, \ldots, G_n$ be groups. Define

$G = G_1 \oplus \cdots \oplus G_n = \{(g_1, \ldots, g_n) : g_i \in G_i\}$

with component-wise multiplication.

1. Closure. $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n) \in G$.
2. Associativity follows from associativity in each component.
3. Identity is $(e_1, \ldots, e_n)$.
4. Inverse of $(g_1, \ldots, g_n)$ is $(g_1^{-1}, \ldots, g_n^{-1})$.

Hence G is a group. □

Exercise 2. Element of Largest Order

Statement. Prove that $(1, 1)$ is an element of largest order in $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$. State the general case.

Solution.

For $(a, b) \in \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ one has

$$|(a, b)| = \mathrm{lcm}(|a|, |b|).$$

Because $|a| \mid n_1$ and $|b| \mid n_2$,

$$|(a, b)| \leq \mathrm{lcm}(n_1, n_2) = |(1, 1)|.$$

General case: in $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ the element $(1, \ldots, 1)$ has order $\mathrm{lcm}(n_1, \ldots, n_k)$, the maximum possible. $\square$

Exercise 3. Embedding Groups in External Direct Products

Statement. Let G be a group with identity e_G and H with identity e_H. Prove $G \cong G \oplus \{e_H\}$ and $H \cong \{e_G\} \oplus H$.

Solution.

$\phi : G \to G \oplus \{e_H\}$, $\phi(g) = (g, e_H)$ is clearly an isomorphism.

By symmetry, $H \cong \{e_G\} \oplus H$. $\square$

Exercise 4. Abelian Property of External Direct Products

Statement. Show that $G \oplus H$ is abelian iff G and H are abelian. State the general case.

Solution.
$(\Rightarrow)$ If $G \oplus H$ is abelian, then for $g, g' \in G$
$(g, e)(g', e) = (g', e)(g, e) \Rightarrow gg' = g'g,$
so G is abelian; likewise H.

$(\Leftarrow)$ If both G and H are abelian, then
$(g, h)(g', h') = (gg', hh') = (g'g, h'h) = (g', h')(g, h).$

General case: $G_1 \oplus \cdots \oplus G_n$ is abelian iff every G_i is abelian. $\square$

Exercise 5. Non-Cyclic External Direct Products

Statement. Prove $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic. Does your proof work for $\mathbb{Z} \oplus G$ where G is any group with more than one element?

Solution.

Suppose $\mathbb{Z} \oplus \mathbb{Z} = \langle (a, b) \rangle$. Because the group is infinite, $a, b \neq 0$. Then $(1, 0) = n(a, b)$ implies $na = 1$ and $nb = 0$. From $na = 1$ we get $n = \pm 1$ and $a = \pm 1$, but then $nb = 0$ forces $b = 0$, contradiction.

The identical argument shows $\mathbb{Z} \oplus G$ is never cyclic when $|G| > 1$. $\square$

Exercise 6. Comparing Orders to Show Non-Isomorphism

Statement. Prove, by comparing orders of elements, that $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Solution.

In $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ the element $(1,1)$ has order $\operatorname{lcm}(8,2) = 8$.

In $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ the maximum order is $\operatorname{lcm}(4,4) = 4$.

Isomorphisms preserve element orders, so the groups are not isomorphic. $\square$

Exercise 7. Commutativity of External Direct Products

Statement. Prove that $G_1 \oplus G_2 \cong G_2 \oplus G_1$. State the general case.

Solution.
$\phi : G_1 \oplus G_2 \to G_2 \oplus G_1$, $\phi(g_1, g_2) = (g_2, g_1)$ is an isomorphism.

General case: for any permutation σ of $\{1, \ldots, n\}$,
$G_1 \oplus \cdots \oplus G_n \cong G_{\sigma(1)} \oplus \cdots \oplus G_{\sigma(n)}$. $\square$

Exercise 8. Testing Isomorphism Using Element Orders

Statement. Is $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$? Why?

Solution.

Maximum order in $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ is $\mathbf{lcm}(3, 9) = 9$;

$\mathbb{Z}_{27}$ has an element of order $\mathbf{27}$.

Hence they are not isomorphic. $\square$

Exercise 9. Multiple Subgroups of the Same Order

Statement. Give an example of an abelian group of order 12 that has two subgroups of order 6. Generalize to the case that the group has order p^2m where p is prime, m is relatively prime to p, and the subgroup has order pm.

Solution.

In $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ the cyclic subgroups

$$H_1 = \langle (1,0) \rangle \quad \text{and} \quad H_2 = \langle (1,1) \rangle$$

both have order 6 and are distinct.

General case: in $\mathbb{Z}_{pm} \oplus \mathbb{Z}_p$ the subgroups

$$\langle (1,0) \rangle \quad \text{and} \quad \langle (1,1) \rangle$$

have order pm and are distinct. $\square$

Exercise 10. Counting Elements of a Given Order

Statement. How many elements of order 9 does $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have?

Solution.

$$|(a,b)| = 9 \iff \operatorname{lcm}(|a|,|b|) = 9.$$

- $|a| = 1$, $|b| = 9$: $1 \times \phi(9) = 6$ elements.
- $|a| = 3$, $|b| = 9$: $\phi(3) \times \phi(9) = 2 \times 6 = 12$ elements.

Total: 18. $\square$

Exercise 11. Elements of Order 4 in Direct Products

Statement. How many elements of order 4 does $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ have? Explain why $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has the same number as $\mathbb{Z}_{800\,000} \oplus \mathbb{Z}_{400\,000}$. Generalize to $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Solution.
Counting the pairs (a, b) with $\mathrm{lcm}(|a|, |b|) = 4$ gives 12 elements.

The count depends only on the divisibility of m and n by 4, not on their magnitudes; hence the second pair also has 12 such elements. $\square$

Exercise 13. Non-Isomorphic Groups of Order n^2

Statement. For each integer $n > 1$, give examples of two non-isomorphic groups of order n^2
.

Solution.

$\mathbb{Z}_{n^2}$ (cyclic) and $\mathbb{Z}_n \oplus \mathbb{Z}_n$ (exponent n) have the same order n^2 but are not isomorphic. $\square$

Exercise 16. Isomorphism Preservation in Direct Products

Statement. Suppose $G_1 \cong G_2$ and $H_1 \cong H_2$. Prove that $G_1 \oplus H_1 \cong G_2 \oplus H_2$. State the general case.

Solution.
If $\alpha : G_1 \to G_2$ and $\beta : H_1 \to H_2$ are isomorphisms, then

$$\phi : G_1 \oplus H_1 \to G_2 \oplus H_2, \quad \phi(g,h) = \big(\alpha(g), \beta(h)\big)$$

is an isomorphism.

General case: if $G_i \cong G_i'$ for $i = 1, \ldots, n$, then

$$G_1 \oplus \cdots \oplus G_n \cong G_1' \oplus \cdots \oplus G_n'. \quad \square$$

Exercise 17. Cyclic Factors from Cyclic Products

Statement. If $G \oplus H$ is cyclic, prove that G and H are cyclic. State the general case.

Solution.
$G \oplus H$ cyclic $\Rightarrow$ every subgroup is cyclic.
The subgroups $G \oplus \{e_H\} \cong G$ and $\{e_G\} \oplus H \cong H$ are therefore cyclic.

General case: if $G_1 \oplus \cdots \oplus G_n$ is cyclic, then each G_i is cyclic. $\square$

Exercise 18. Cyclic and Non-Cyclic Subgroups

Statement. Find a cyclic subgroup of $\mathbb{Z}_{40} \oplus \mathbb{Z}_{30}$ of order 12 and a non-cyclic subgroup of $\mathbb{Z}_{40} \oplus \mathbb{Z}_{30}$ of order 12.

Solution.

Cyclic: $\langle(10, 10)\rangle$ has order $\mathbf{lcm}(4, 3) = 12$.

Non-cyclic: $\langle(20, 0)\rangle \oplus \langle(0, 5)\rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$ has order 12 but is not cyclic. $\square$

Exercise 36. Finding Subgroups of Specified Order

Statement. Find a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ that has order 9.

Solution.

The subgroup

$$\langle(4,0,0)\rangle \oplus \langle(0,0,5)\rangle \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

has order 9. $\square$

Exercise 38. Matrix Group Isomorphism

Statement. Let

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}_3 \right\}$$

under matrix multiplication. Show H is an abelian group of order 9. Is H isomorphic to $\mathbb{Z}_9$ or to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$?

Solution.

$|H| = 9$ and every non-identity element has order 3; hence $H \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$. $\square$

Exercise 40. Infinite Order in Direct Products

Statement. Let $(a_1, \ldots, a_n) \in G_1 \oplus \cdots \oplus G_n$. Give a necessary and sufficient condition for $|(a_1, \ldots, a_n)| = \infty$.

Solution.

$$|(a_1, \ldots, a_n)| = \infty \iff |a_i| = \infty \text{ for at least one } i. \quad \square$$

Exercise 46. Infinite Group with Specific Subgroups

Statement. Give an example of an infinite group that has both a subgroup isomorphic to D_4 and a subgroup isomorphic to A_4.

Solution.
$\mathbb{Z} \oplus D_4 \oplus A_4$ is infinite and contains copies of both D_4 and A_4. $\square$

Exercise 51a. Counting Isomorphisms

Statement. How many isomorphisms are there from $\mathbb{Z}_{18}$ to $\mathbb{Z}_2 \oplus \mathbb{Z}_9$? Give formulas for two of the isomorphisms.

Solution.
Because $\gcd(2, 9) = 1$, $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{18}$ is cyclic of order 18. The number of isomorphisms equals the number of generators of $\mathbb{Z}_{18}$, namely $\phi(18) = 6$.

Two explicit isomorphisms:

$$\phi_1(x) = (x \bmod 2, x \bmod 9), \qquad \phi_2(x) = (x \bmod 2, 2x \bmod 9). \quad \square$$

Exercise 56. Polynomial Group Isomorphism

Statement. Let $G = \{ax^2 + bx + c : a, b, c \in \mathbb{Z}_3\}$ with polynomial addition mod 3. Prove $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Generalize.

Solution.
The coefficient map $\phi(ax^2 + bx + c) = (a, b, c)$ is an isomorphism of additive groups. For any prime p and degree bound n, polynomials of degree at most n over $\mathbb{Z}_p$ form a group isomorphic to $(n + 1)$ copies of $\mathbb{Z}_p$. $\square$

Exercise 57. Cyclic Groups with Exactly Two Generators

Statement. Determine all cyclic groups that have exactly two generators.

Solution.

A cyclic group of order n has $\phi(n)$ generators. $\phi(n) = 2$ iff $n \in \{3, 4, 6\}$. The infinite cyclic group $\mathbb{Z}$ has exactly two generators (± 1). Thus the complete list is

$$\mathbb{Z}, \quad \mathbb{Z}_3, \quad \mathbb{Z}_4, \quad \mathbb{Z}_6. \quad \square$$

Exercise 80. Exponent of a Group

Statement. Find the smallest positive integer n such that $x^n = 1$ for all $x \in U(100)$. Show your reasoning.

Solution.
$U(100) \cong U(2^2) \oplus U(5^2) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{20}$; its exponent is $\mathbf{lcm}(2, 20) = 20$. $\square$

Exercise 81. Determining Cyclic Subgroups

Statement. Which of the following groups are cyclic?

a. $U(35)$

b. $U_5(40)$

c. $U_8(40)$

Solution.

a. $U(35) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_6$ is not cyclic.

b. $U_5(40) \cong U(8) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic.

c. $U_8(40) \cong U(5) \cong \mathbb{Z}_4$ is cyclic. $\square$