2.4 Direct Products and Finitely Generated Abelian Groups

2.4.1 Direct Products

Def 2.43. [4] The *Cartesian product of sets* $S_1, S_2, \cdots, S_n$ is the set of all ordered n-tuples $(a_1, \cdots, a_n)$ where $a_i \in S_i$ for $i = 1, 2 \cdots, n$.

$$\begin{aligned} \prod_{i=1}^{n} S_i &= S_1 \times S_2 \times \cdots \times S_n \\ &:= \{(a_1, a_2, \cdots, a_n) \mid a_i \in S_i \text{ for } i = 1, 2, \cdots, n\}. \end{aligned}$$

Caution: The notation $(a_1, a_2, \cdots, a_n)$ here has different meaning from the cycle notation in permutation groups.

Thm 2.44. *If $G_1, G_2, \cdots, G_n$ are groups with the corresponding multiplications, then $\prod_{i=1}^{n} G_i$ is a group under the following multiplication:*

$$(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) := (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$$

for $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ in $\prod_{i=1}^{n} G_i$.

Proof.

1. **Closed:** $a_i \in G_i, b_i \in G_i \Rightarrow a_i b_i \in G_i \Rightarrow (a_1 b_1, \cdots, a_n b_n) \in \prod_{i=1}^{n} G_i$.
2. **Associativity:** By the associativity in each G_i.
3. **Identity:** Let e_i be the identity in G_i. Then $e := (e_1, e_2, \cdots, e_n)$ is the identity of G.
4. **Inverse:** The inverse of $(a_1, \cdots, a_n)$ is $(a_1^{-1}, \cdots, a_n^{-1})$.

□

Ex 2.45. $\mathbf{R}^2$, $\mathbf{R}^3$ are abelian groups.
(Every finite dimensional real vector space is an abelian group that is isomorphic to certain $\mathbf{R}^n$.)

Ex 2.46. $\mathbf{Z}^2 = \{(a, b) \mid a, b \in \mathbf{Z}\}$ is a subgroup of $\mathbf{R}^2$.
(If $H_i \leq G_i$ for $i = 1, \cdots, n$, then $\prod_{i=1}^{n} H_i \leq \prod_{i=1}^{n} G_i$).

[4] 1st HW: 1, 2, 14, 34, **46**

Ex 2.47. If e_i is the identity of G_i for $i = 1, \cdots, n$. Then

$$G_j \simeq \{e_1\} \times \{e_2\} \times \cdots \times \{e_{j-1}\} \times G_j \times \{e_{j+1}\} \times \cdots \times \{e_n\} \leq \prod_{i=1}^{n} G_i.$$

So every G_j is isomorphic to a subgroup of $\prod_{i=1}^{n} G_i$ for $j = 1, \cdots, n$.

Ex 2.48. The Klein 4-group V is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$, which is not cyclic.

Ex 2.49. $\mathbf{Z}_2 \times \mathbf{Z}_3 \simeq \mathbf{Z}_6$ is cyclic, and $(1, 1)$ is a generator.

Thm 2.50. *Let m and n be positive integers.*

1. *If $\gcd(m, n) = 1$ (i.e. m and n are relative prime), then $\mathbf{Z}_m \times \mathbf{Z}_n$ is cyclic and is isomorphic to $\mathbf{Z}_{mn}$, and $(1, 1)$ is a generator of $\mathbf{Z}_m \times \mathbf{Z}_n$.*

2. *If $\gcd(m, n) \neq 1$, then $\mathbf{Z}_m \times \mathbf{Z}_n$ is not cyclic.*

Proof. [5]

1. Suppose $\gcd(m, n) = 1$. The sum of k copies of $(1, 1)$ is equal to $(k \bmod m,\ k \bmod n)$. The smallest positive integer k that makes $(k \bmod m,\ k \bmod n) = (0, 0)$ is $k = mn$ because m and n are relative prime. So the cyclic subgroup of $(1, 1)$ in $\mathbf{Z}_m \times \mathbf{Z}_n$ has the order $mn = |\mathbf{Z}_m \times \mathbf{Z}_n|$. So $(1, 1)$ generates $\mathbf{Z}_m \times \mathbf{Z}_n$. It implies that $\mathbf{Z}_m \times \mathbf{Z}_n$ is a cyclic group isomorphic to $\mathbf{Z}_{mn}$.

2. Suppose $\gcd(m, n) = d \neq 1$. Given $(a, b) \in \mathbf{Z}_m \times \mathbf{Z}_n$, the sum of k copies of (a, b) is $(ka \bmod m,\ kb \bmod n)$. Notice that both m and n divide $\frac{mn}{d} = m \cdot \frac{n}{d} = \frac{m}{d} \cdot n$. Then

$$(\frac{mn}{d}a \bmod m,\ \frac{mn}{d}b \bmod n) = (0, 0).$$

   So the cyclic subgroup generated by (a, b) has an order no more than $\frac{mn}{d} < mn = |\mathbf{Z}_m \times \mathbf{Z}_n|$. Thus $\mathbf{Z}_m \times \mathbf{Z}_n$ can not be generated by any one of its elements, which implies that $\mathbf{Z}_m \times \mathbf{Z}_n$ is not cyclic.

□

Cor 2.51. The group $\prod_{i=1}^{n} \mathbf{Z}_{m_i}$ is cyclic and is isomorphic to $\mathbf{Z}_{m_1 m_2 \cdots m_n}$ if and only if the numbers m_i for $i = 1, \cdots, n$ are pairwise relative prime, that is, the gcd of any two of them is 1.

[5] 1st HW: 1, 2, 14, 34, **46**

Proof. (For reference only) If m_i for $i = 1, \cdots, n$ are pairwise relative prime, then

$$\prod_{i=1}^{n} \mathbf{Z}_{m_i} \simeq \mathbf{Z}_{m_1 m_2} \left(\prod_{i=3}^{n} \mathbf{Z}_{m_i} \right) \simeq \mathbf{Z}_{m_1 m_2 m_3} \left(\prod_{i=4}^{n} \mathbf{Z}_{m_i} \right) \simeq \cdots \simeq \mathbf{Z}_{m_1 m_2 \cdots m_n}.$$

Conversely, if $\prod_{i=1}^{n} \mathbf{Z}_{m_i} \simeq \mathbf{Z}_{m_1 m_2 \cdots m_n}$, then $\prod_{i=1}^{n} \mathbf{Z}_{m_i}$ contains a subgroup isomorphic to $\mathbf{Z}_{m_i} \times \mathbf{Z}_{m_j}$ for $1 \leq i < j \leq n$. Every subgroup of the cyclic group $\prod_{i=1}^{n} \mathbf{Z}_{m_i} \simeq \mathbf{Z}_{m_1 m_2 \cdots m_n}$ is cyclic. Hence $\mathbf{Z}_{m_i} \times \mathbf{Z}_{m_j}$ is cyclic. So $\gcd(m_i, m_j) = 1$ for $1 \leq i < j \leq n$. □

Cor 2.52. [6] If a positive integer n is factorized as a product of powers of distinct prime numbers:

$$n = (p_1)^{n_1} (p_2)^{n_2} \cdots (p_r)^{n_r},$$

then

$$\mathbf{Z}_n \simeq \mathbf{Z}_{(p_1)^{n_1}} \times \mathbf{Z}_{(p_2)^{n_2}} \times \cdots \times \mathbf{Z}_{(p_r)^{n_r}}.$$

Note: Each $\mathbf{Z}_{(p_i)^{n_i}}$ can <u>not</u> be further decomposed into a product of proper nontrivial subgroups.

Ex 2.53. $(\mathbf{Z}_5)^2 \ncong \mathbf{Z}_{5^2}$. The group $(\mathbf{Z}_5)^2$ is not cyclic, but $\mathbf{Z}_{5^2} = \mathbf{Z}_{25}$ is cyclic.

Def 2.54. The *least common multiple* (abbreviated lcm) of positive integers $r_1, r_2, \cdots, r_n$ is the smallest positive integer that is a multiple of each r_i for $i = 1, 2, \cdots, n$.

If M is a multiple of r_i for $i = 1, \cdots, n$, then M is a multiple of $\text{lcm}(r_1, \cdots, r_n)$.

Thm 2.55. *Let $(a_1, a_2, \cdots, a_n) \in \prod_{i=1}^{n} G_i$. If a_i is of finite order r_i in G_i, then the order of $(a_1, a_2, \cdots, a_n)$ in $\prod_{i=1}^{n} G_i$ is lcm$(r_1, r_2, \cdots, r_n)$.*

Proof.

$$(a_1, a_2, \cdots, a_n)^k = (a_1^k,\ a_2^k,\ \cdots,\ a_n^k).$$

So

$$(a_1^m,\ a_2^m,\ \cdots,\ a_n^m) = (e_1, e_2, \cdots, e_n)$$

if and only if m is a multiple of r_i for $i = 1, 2, \cdots, n$, if and only if m is a multiple of $\text{lcm}(r_1, r_2, \cdots, r_n)$. The smallest such positive integer is $\text{lcm}(r_1, r_2, \cdots, r_n)$. So the order of $(a_1, a_2, \cdots, a_n)$ is $\text{lcm}(r_1, r_2, \cdots, r_n)$. □

Ex 2.56. The order of $(8, 4, 10)$ in $\mathbf{Z}_{12} \times \mathbf{Z}_{60} \times \mathbf{Z}_{24}$.

[6] 2nd HW: 13, 15, 32, 47, **50**

2.4.2 The Structure of Finitely Generated Abelian Groups

Thm 2.57 (Fundamental Theorem of Finitely Generated Abelian Groups). *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form*

$$\mathbf{Z}_{(p_1)^{r_1}} \times \mathbf{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbf{Z}_{(p_n)^{r_n}} \times \mathbf{Z} \times \mathbf{Z} \times \cdots \times \mathbf{Z}$$

*where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number (***Betti number** *of G) of factor $\mathbf{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.*

The proof (omitted) is challenging.

In particular, every finite abelian group is isomorphic to a product of finite cyclic groups. (**Caution:** finite group $\neq$ finitely generated group)

Ex 2.58. Decompose the following three groups:

$$\begin{aligned}
\mathbf{Z}_4 \times \mathbf{Z}_{12} \times \mathbf{Z}_{15} &\simeq \mathbf{Z}_{2^2} \times (\mathbf{Z}_{2^2} \times \mathbf{Z}_3) \times (\mathbf{Z}_3 \times \mathbf{Z}_5) \simeq (\mathbf{Z}_{2^2})^2 \times (\mathbf{Z}_3)^2 \times \mathbf{Z}_5, \\
\mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_{60} &\simeq \mathbf{Z}_3 \times \mathbf{Z}_{2^2} \times (\mathbf{Z}_{2^2} \times \mathbf{Z}_3 \times \mathbf{Z}_5) \simeq (\mathbf{Z}_{2^2})^2 \times (\mathbf{Z}_3)^2 \times \mathbf{Z}_5, \\
\mathbf{Z}_{20} \times \mathbf{Z}_{36} &\simeq (\mathbf{Z}_{2^2} \times \mathbf{Z}_5) \times (\mathbf{Z}_{2^2} \times \mathbf{Z}_{3^2}) \simeq (\mathbf{Z}_{2^2})^2 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5.
\end{aligned}$$

Therefore, $\mathbf{Z}_4 \times \mathbf{Z}_{12} \times \mathbf{Z}_{15} \cong \mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_{60} \ncong \mathbf{Z}_{20} \times \mathbf{Z}_{36}$.

Ex 2.59 (Ex 11.13, p.109). Find all abelian groups, up to isomorphism, of order 360.

2.4.3 Applications

Def 2.60. A group G is *decomposable* if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is indecomposable.

Thm 2.61. *The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.*

Thm 2.62. *If G is a finite abelian group, then G has a subgroup of order m for every m that divides $|G|$.*

Ex 2.63. If m is a square-free integer, then every abelian group of order m is isomorphic to $\mathbf{Z}_m$ and is cyclic.

2.4.4 Homework, II-11, p.110-p.113

1st 1, 2, 14, 34, **46**

2nd 13, 15, 32, 47, **50**

3rd 18, **26**, 36, 53

(opt) 29, 37, 38, 39, 52, 54