

The Fundamental Theorem for Finite Abelian Groups

Besides the books listed in Dr. Hausen's notes, I highly recommend the following text: [DS] **Dan Sarachino**, *Abstract Algebra: A first Course*, Waveland Press, Inc. (ISBN 0-88133-665-3).

Let A_1, \dots, A_n be finitely many abelian groups. The group $A = A_1 \oplus \dots \oplus A_n$ is the *internal direct sum* of the groups A_i if every element $a \in A$ is a unique sum of elements $a_i \in A_i$. Given groups A_i , then the direct product

$A = A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) | a_i \in A_i\}$ may serve as the direct sum if we "identify" A_i with the subgroup P_i of A of all those elements where all but the i^{th} component are zero. Because of

$$a = (a_1, a_2, \dots, a_n) = (a_1, 0, \dots, 0) + (0, a_2, \dots, 0) + \dots + (0, \dots, a_n)$$

we have that

$$A = A_1 \times \dots \times A_n = P_1 \oplus \dots \oplus P_n, \text{ where } A_i \cong P_i$$

In the abelian case, the direct sum and the direct product of finitely many groups coincide. The sum of non-abelian groups is much more difficult to deal with and studied as so called *co-products* in advanced courses on algebra or group theory.

Recall that a group is *cyclic* if it is generated by one element a . In this case, $G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}$. An infinite cyclic group is isomorphic to the additive group $(\mathbb{Z}, +)$ of integers, while any finite cyclic group of cardinal n is isomorphic to the group $(\mathbb{Z}_n, +)$ of integers modulo n .

Exercise Prove that the additive group $(\mathbb{Q}, +)$ of rational numbers is not cyclic.

Exercise Prove that the multiplicative group (\mathbb{Q}^+, \cdot) of positive rational numbers is not cyclic.

Exercise We have that $(\mathbb{R}, +)$ and (\mathbb{R}^+, \cdot) are isomorphic. Are $(\mathbb{Q}, +)$ and (\mathbb{Q}^+, \cdot) isomorphic?

The following is a fundamental theorem concerning direct products (or sums) of finitely many finite cyclic groups.

Theorem Let A_1, \dots, A_n be a finite list of finite cyclic groups. Then $A = A_1 \times \dots \times A_n$ is cyclic if and only if $|A_i|$ and $|A_j|$ are relatively prime for $i \neq j$.

Example $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. On the other hand, according to the theorem, Kleins Vierer-Group $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Corollary For the cyclic group \mathbb{Z}_n of order $n = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$ we have that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \dots \times \mathbb{Z}_{p_k^{n_k}}$. That is, every cyclic group is isomorphic to product of uniquely determined cyclic groups whose orders are prime-powers.

Proof According to the Theorem, the right-hand side is a cyclic group. As a direct product, it is a group of order n . That is, the right-hand side must be isomorphic to \mathbb{Z}_n

In the representation $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ where n_i and n_j are relatively prime for $i \neq j$, the isomorphism is established by $[x]_n \mapsto ([x]_{n_1}, \dots, [x]_{n_k})$. You might have met this isomorphism before in a course on number theory as the *Chinese Remainder Theorem*.

Theorem Assume that the positive natural numbers n_1, \dots, n_k are pair-wise relatively prime, $(n_i, n_j) = 1$ for $i \neq j$, and that x_i are arbitrarily chosen integers, $i = 1, \dots, k$. Then there is some integer x such that $x \equiv x_i \pmod{n_i}, i = 1, \dots, k$. The integer x is unique modulo $n = n_1 \cdot \dots \cdot n_k$.

Proof The first part of the theorem is just a reformulation that the map $[x]_n \mapsto ([x]_{n_1}, \dots, [x]_{n_k})$ is surjective. Injectivity of this map makes any solution x unique up to congruence modulo n .

Every finite abelian group is isomorphic to a product of cyclic groups of prime-power orders. This is the content of the **Fundamental Theorem for finite Abelian Groups**:

Theorem Let A be a finite abelian group of order n . Then

$$A \cong (\mathbb{Z}_{p_1^{v_{11}}} \oplus \mathbb{Z}_{p_1^{v_{12}}} \oplus \dots \oplus \mathbb{Z}_{p_1^{v_{1l_1}}}) \oplus \dots \oplus (\mathbb{Z}_{p_k^{v_{k1}}} \oplus \mathbb{Z}_{p_k^{v_{k2}}} \oplus \dots \oplus \mathbb{Z}_{p_k^{v_{kl_k}}})$$

where

$$n = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$$

is the prime factorization of the cardinality n of A and where

$$n_1 = v_{11} + v_{12} + \dots + v_{1l_1}, \dots, n_k = v_{k1} + v_{k2} + \dots + v_{kl_k}, v_{i1} \geq v_{i2} \geq \dots \geq v_{il_i}$$

The list of prime powers p_i^{ij} is uniquely determined by the isomorphism type of A and are called the invariants of A .

Example Up to isomorphisms, there are two abelian groups of order 20. We have $20 = 2^2 \cdot 5$. Thus, $\mathbb{Z}_4 \oplus \mathbb{Z}_5$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5$ are the only possibilities for a decomposition according to the fundamental theorem. Of course, $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{20}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_2$.

Exercise Find up to isomorphism all abelian groups of order $n = 144$.

Exercise For which numbers n are all abelian groups of that order cyclic?

Theorem A finite abelian group A of cardinality n is cyclic if and only if one has that for every divisor d of n at most d –many elements $a \in A$ such that $d \cdot a = 0$.

Proof If A is \mathbb{Z}_n , then $H = \{a \mid d \cdot a = 0\}$ is a subgroup of \mathbb{Z}_n and $H = \langle [\frac{n}{d}]_n \rangle$ has exactly d –many elements. On the other hand, if A is not cyclic then one has for some i that $l_i > 1$. This gives us at least $2p_i$ –many elements in $(\mathbb{Z}_{p_i^{v_{i1}}} \oplus \mathbb{Z}_{p_i^{v_{i2}}} \oplus \dots \oplus \mathbb{Z}_{p_i^{v_{il_i}}})$ of order p_i .

In multiplicative notation, $d \cdot x = 0$ is $x^d = e$. In a field this reads as $x^d - 1 = 0$ and we can find at most d – many such x . Thus we have the following theorem of Gauss:

Theorem The multiplicative group of a finite field is cyclic.