

Chapter 2

Abelian Groups

In this chapter we determine the structure of the finite Abelian groups. As a starting point we use the structure of the cyclic groups described in Section 1.4. It will turn out that every finite Abelian group is the direct product of cyclic groups. In the second section of this chapter we will show that the automorphism groups of cyclic groups are examples of Abelian groups.

Compared with groups in general the structure of Abelian groups is much easier to investigate since commutativity implies many structural properties that almost never hold in non-Abelian groups. For example, in an Abelian group every subgroup is normal and the product of subgroups is again a subgroup (1.1.5 on page 6).

From this chapter on all groups considered are finite.

2.1 The Structure of Abelian Groups

If $G = \langle x \rangle$ is a cyclic group, then $|G| = o(x)$, and Lagrange's theorem implies

$$o(y) \text{ divides } o(x) \quad \text{for all } y \in G.$$

A more general property is true for Abelian groups, as one can show using 1.6.6 on page 31:

2.1.1 *Let G be an Abelian group and U a cyclic subgroup of maximal order in G . Then*

$$o(y) \text{ divides } |U| \quad \text{for all } y \in G.$$

Proof. Let $y \in G$. We show that every prime power p^r that divides $o(y)$ also divides $|U|$. Let $|U| = p^e m$ with $(p, m) = 1$. By 1.4.3 on page 22 there exist elements $a \in \langle y \rangle$ and $b \in U$ such that

$$o(a) = p^r \quad \text{and} \quad o(b) = m,$$

and 1.6.6 on page 31 implies $o(ab) = p^r m$. Now the maximality of $|U|$ gives $p^r \mid p^e m$. \square

2.1.2 *Let G and U be as in 2.1.1. Then there exists a complement V of U in G ; in particular $G = U \times V$ and $|G| = |U||V|$.*

Proof. If $G = U$, then $V = 1$ is the desired complement. Let $G \neq U$. Among all elements in $G \setminus U$ we choose y such that $o(y)$ is minimal. Then $y \neq 1$ and $\langle y^p \rangle < \langle y \rangle$ for every prime divisor p of $o(y)$ (1.4.3 on page 22), i.e., $\langle y^p \rangle \leq U$.

Let $U = \langle u \rangle$. By 2.1.1 and 1.4.3 on page 22 $o(y)$ is a divisor of $|U|$, and U contains exactly one subgroup for every such divisor. Hence, there exists a subgroup of order $\frac{o(y)}{p}$ in $\langle u^p \rangle$, namely $\langle y^p \rangle$. Let $i \in \mathbb{N}$ such that $u^{pi} = y^p$. Then $(yu^{-i})^p = 1$, but $yu^{-i} \notin U$ since $y \notin U$. The minimality of $o(y)$ gives

$$o(y) = p.$$

Thus, $N := \langle y \rangle$ is a nontrivial subgroup of G such that

$$U \cap N = 1.$$

Let $\overline{G} := G/N$.¹ For $\langle \overline{x} \rangle \leq \overline{G}$ we obtain

$$o(\overline{x}) = |\langle \overline{x} \rangle| = \min\{n \in \mathbb{N} \mid x^n \in N\} \leq |\langle x \rangle| = o(x),$$

and since

$$UN/N \cong U/U \cap N \cong U$$

we also have $|\overline{U}| = |U|$. Hence, \overline{U} is a cyclic subgroup of maximal order in \overline{G} . By induction on $|G|$ we may assume that there exists a complement \overline{V} of \overline{U} in \overline{G} .

¹For the “bar” convention, see p. 14.

Let $N \leq V \leq G$ such that $\bar{V} = V/N$. Then V is a complement of U in G since $U \cap V \leq U \cap N = 1$. \square

The complement V in 2.1.2 can again be decomposed into a cyclic subgroup of maximal order and its complement. Hence, a repeated application of 2.1.2 gives:

2.1.3 Theorem. *Every Abelian group is the direct product of cyclic groups.* \square

Thus, for every Abelian group G :

$$G \cong C_{n_1} \times \cdots \times C_{n_r} \quad \text{and} \quad |G| = n_1 \cdots n_r.^2$$

If m is a divisor of $|G|$, then there exist divisors m_i of n_i ($i = 1, \dots, r$) such that $m = m_1 \cdots m_r$. Hence $C_{m_1} \times \cdots \times C_{m_r}$ is isomorphic to a subgroup of order m of G . This implies:

2.1.4 *Let G be an Abelian group and m a divisor of $|G|$. Then G contains a subgroup of order m .* \square

Let p be a prime. We set

$$G_p := \{x \in G \mid x \text{ is a } p\text{-element}\}.$$

2.1.5 *Let G be an Abelian group. Then G_p is a characteristic p -subgroup of order $|G|_p$.³*

Proof. For $x, y \in G_p$ also xy is a p -element; use $xy = yx$ and 1.1.2 on page 4. Thus G_p is a subgroup. Since automorphisms map p -elements to p -elements this subgroup is characteristic.

By 2.1.4 G contains a subgroup P of order $|G|_p$. Hence, P is a p -group, and thus every element of P is a p -element; in particular $P \leq G_p$.

If $P \neq G_p$, then

$$k := |G_p : P| \neq 1$$

and $(k, p) = 1$ (Lagrange's theorem). But now 2.1.4 gives a subgroup K of order k in G_p , which contradicts 1.1.8 on page 8 since every element of K is a p -element. \square

² C_{n_i} is the cyclic group of order n_i ; see 1.4.

³For $n \in \mathbb{N}$ let n_p be the largest p -power dividing n .

2.1.6 Theorem. *Let G be an Abelian group. Then*

$$G = \bigtimes_{p \in \pi(G)} G_p.$$

Proof. By 1.6.5 on page 31 the product G_1 of the subgroups G_p , $p \in \pi(G)$, is a direct product; and 2.1.5 yields

$$|G_1| = \prod_{p \in \pi(G)} |G_p| = \prod_{p \in \pi(G)} |G|_p = |G|,$$

so $G_1 = G$. □

In an Abelian group the product of two cyclic groups of coprime order is again cyclic (1.6.6 on page 31). Hence, the question whether an Abelian group is cyclic or not can already be decided in the subgroups G_p , $p \in \pi(G)$.

2.1.7 *For an Abelian group G the following statements are equivalent:*

- (i) G is cyclic.
- (ii) For all $p \in \pi(G)$ there exists exactly one subgroup of order p in G .
- (iii) G_p is cyclic for all $p \in \pi(G)$.

Proof. (i) \Rightarrow (ii) follows from 1.4.3 on page 22 and (ii) \Rightarrow (iii) from 2.1.3, both applied to G_p . Finally a repeated application of 1.6.6 on page 31 gives the implication (iii) \Rightarrow (i). □

Of course, in 2.1.3 more can be said about the factors of the decomposition. Because of the unique decomposition 2.1.6 it suffices to investigate Abelian p -groups.

An Abelian p -group is **elementary Abelian** if $x^p = 1$ for all $x \in G$.

2.1.8 *Let G be an elementary Abelian p -group of order $p^n > 1$.*

- (a) G is the direct product of n cyclic groups of order p .

(b) If G is written additively, the scalar multiplication

$$\bar{k}x := \underbrace{x + \cdots + x}_{k\text{-times}}$$

for $\bar{k} := k + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ and $x \in G$, makes G into an n -dimensional vector space V over the prime field $\mathbb{Z}/p\mathbb{Z}$. The subgroups of G correspond to the subspaces of V and the automorphisms of G to the automorphisms of V .

Proof. (a) Since every nontrivial cyclic subgroup of G has order p , G is the direct product of such subgroups (2.1.3), and since $|G| = p^n$, n factors are required.

(b) There is nothing to prove. Clearly, the existence of a basis of V with n elements is equivalent to (a). \square

In a (not necessarily Abelian) p -group G , the group

$$\Omega_i(G) := \langle x \in G \mid x^{p^i} = 1 \rangle, \quad i = 0, 1, 2, \dots$$

is a characteristic subgroup. Evidently

$$\Omega_{i-1}(G) \leq \Omega_i(G), \quad i = 1, 2, \dots$$

We set

$$\Omega(G) := \Omega_1(G).$$

If G is Abelian, then

$$\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$$

and

$$G \text{ elementary Abelian} \iff G = \Omega(G).$$

2.1.9 Let G be an Abelian p -group such that

$$(*) \quad G = A_1 \times \cdots \times A_n$$

is the direct product of n cyclic groups $A_i \neq 1$. Then

$$|\Omega(G)| = p^n.$$

More precisely: If $n_i \in \mathbb{N}$ for $i = 1, 2, \dots$ is defined by

$$|\Omega_i(G)/\Omega_{i-1}(G)| = p^{n_i},$$

then $n_i - n_{i+1}$ is the number of the factors of order p^i in $(*)$.

Proof. From

$$\Omega_i(G) = \Omega_i(A_1) \times \cdots \times \Omega_i(A_n)$$

follows $|\Omega(G)| = p^n = p^{n_1}$. Since

$$\begin{aligned} \Omega_2(G)/\Omega(G) &= \Omega(G/\Omega(G)) \stackrel{1.6.2(c)}{\cong} \Omega\left(\times_i (A_i/\Omega(A_i))\right) = \times_i \Omega(A_i/\Omega(A_i)) \\ &= \times_i \Omega_2(A_i)/\Omega(A_i), \end{aligned}$$

n_2 is the number of factors in (*) of order at least p^2 . Thus, $n_1 - n_2$ is the number of factors of order p . In the same way one calculates $n_i - n_{i+1}$ for $i \geq 2$. \square

The minimal number of generators of a group G is the **rank** $r(G)$ of G . If G is an Abelian p -group, then $r(G) = n$, where n is as in 2.1.9.

The results 2.1.3, 2.1.6, and 2.1.9 allow a complete survey over all finite Abelian groups: Such a group is a direct product of cyclic groups of prime power order, and the isomorphism type is determined by the number and the order of these factors. For example, there are exactly 9 Abelian groups of order $1000 = 2^3 \cdot 5^3$, namely

$$\begin{aligned} &C_2 \times C_2 \times C_2 \times C_5 \times C_5 \times C_5 \\ &C_2 \times C_2 \times C_2 \times C_5 \times C_{5^2} \\ &C_2 \times C_2 \times C_2 \times C_{5^3} \\ &C_2 \times C_{2^2} \times C_5 \times C_5 \times C_5 \\ &C_2 \times C_{2^2} \times C_5 \times C_{5^2} \\ &C_2 \times C_{2^2} \times C_{5^3} \\ &C_{2^3} \times C_5 \times C_5 \times C_5 \\ &C_{2^3} \times C_5 \times C_{5^2} \\ &C_{2^3} \times C_{5^3} \end{aligned}$$

Only the last of these groups is cyclic.

It should be mentioned that finitely generated Abelian groups have a structure similar to that of finite Abelian groups. They are direct products of finite Abelian groups and groups isomorphic to \mathbb{Z} (e.g., see [19], p. 82).

Exercises

Let G be a finite Abelian group.

1. Let $e \in \mathbb{N}$ be minimal such that $a^e = 1$ for all $a \in G$ ($\exp G := e$ is the **exponent** of G). There exists an element $b \in G$ such that $o(b) = e$.
2. Let $\exp G = e$. Then G is cyclic, if and only if $|G| = e$.
3. Let p be a prime, $C = C_{p^3} \times C_{p^3}$, $B = C_p \times C_p \times C_p$, and $G = C \times B$. Then no subgroup of G has a complement isomorphic to C_{p^2} in G .
4. Every Abelian group of order 546 is cyclic.
5. Give an example of a non-Abelian group that satisfies the statement of 2.1.4.
6. Determine $\prod_{g \in G} g$.
7. For every subgroup $U \leq G$ there exists an endomorphism φ of G such that $\text{Im } \varphi = U$.
8. If $\text{Aut } G$ is Abelian, then G is cyclic.
9. With the help of 6 show:

$$(p-1)! \equiv -1 \pmod{p} \quad (p \text{ prime}).^4$$

10. Let $a, p \in \mathbb{N}$, p a prime and $(a, p) = 1$. Then

$$a^{p-1} \equiv 1 \pmod{p}.^5$$

2.2 Automorphisms of Cyclic Groups

As examples of Abelian groups we determine in this section the automorphism groups of cyclic groups.

For an Abelian group G and every $k \in \mathbb{Z}$ the mapping

$$\alpha_k: G \rightarrow G \quad \text{such that} \quad x \mapsto x^k$$

is an endomorphism with

$$\text{Ker } \alpha_k = \{x \in G \mid x^k = 1\},$$

Thus, $\text{Ker } \alpha_k$ contains all elements of G , whose orders divide k .

2.2.1 α_k is an automorphism of the Abelian group G , if and only if $(k, |G|) = 1$.

⁴Wilson's Theorem.

⁵Fermat's Little Theorem.

Proof. If $(k, |G|) = 1$, then $\text{Ker } \alpha_k = 1$ because of 1.1.8 on page 8. Conversely, if $(k, |G|) \neq 1$, then there exists a common prime divisor p of k and $|G|$. Now by 2.1.6 the p -subgroup G_p is nontrivial, and there exists a subgroup of order p in G . This subgroup is contained in $\text{Ker } \alpha_k$. \square

Together with 1.4.3 on page 22 this gives for cyclic groups:

2.2.2 *The automorphisms of a cyclic group of order n are of the form α_k with $k \in \{1, \dots, n-1\}$ and $(k, n) = 1$.* \square

From $\alpha_k \alpha_{k'} = \alpha_{k \cdot k'} = \alpha_{k' \cdot k} = \alpha_{k'} \alpha_k$ for $k, k' \in \mathbb{Z}$ we obtain:

2.2.3 *The automorphism group of a cyclic group is Abelian.*⁶ \square

Because of the decomposition $G = \bigtimes_{p \in \pi(G)} G_p$ in 2.1.6 one has

$$\text{Aut } G \cong \bigtimes_{p \in \pi(G)} \text{Aut } G_p$$

(1.6.2 on page 29). Hence, it suffices to determine the automorphism group of cyclic p -groups.

If G is a cyclic p -group of order $p^e > 1$, then $|\text{Aut } G|$ is the number of integers k such that $1 \leq k < p^e$ and $(k, p) = 1$. Thus

$$|\text{Aut } G| = p^{e-1}(p-1).$$

In particular $|\text{Aut } G| = p-1$ if $|G| = p$. In this case:

2.2.4 *The automorphism group of a group of order p is cyclic.*⁷

*Proof.*⁸ Let G be a (cyclic) group of prime order p . Then for $g \in G$ and $\alpha \in \text{Aut } G$

$$(1) \quad g^\alpha = g \iff g = 1 \text{ or } \alpha = 1.$$

⁶One can easily extend 2.2.2 and 2.2.3 to: The endomorphism ring of a cyclic group C_n is isomorphic to the ring $\mathbb{Z}/n\mathbb{Z}$.

⁷This also follows from the well-known result that the multiplicative group of a finite field is cyclic.

⁸The argument in this proof will be used again in 8.3.1 on p. 191 in a more general context.

We assume that $\text{Aut } G$ is noncyclic and show that this leads to a contradiction. By 2.1.7 there exists $r \in \pi(\text{Aut } G)$ and a subgroup $A \leq \text{Aut } G$ such that

$$A \cong C_r \times C_r.$$

Let \mathcal{B} be the set of all subgroups of order r of A . Then

$$(2) \quad |\mathcal{B}| = r + 1 \quad \text{and} \quad B_1 \cap B_2 = 1 \quad \text{for } B_1 \neq B_2 \text{ in } \mathcal{B}.$$

For $1 \neq B \leq A$ and $g \in G^\#$ let

$$g_B := \prod_{\beta \in B} g^\beta.$$

Then

$$(g_B)^\alpha = \prod_{\beta \in B} g^{\beta\alpha} = g_B,$$

for $\alpha \in B^\#$ and thus $g_B = 1$ because of (1). Now (2) gives

$$1 = g_A = g^{-r} \prod_{B \in \mathcal{B}} g_B = g^{-r},$$

and $o(g) = r$. This implies $p = r$ (1.1.8). On the other hand by 2.2.2

$$r \text{ divides } |\text{Aut } G| = p - 1,$$

a contradiction. □

2.2.5 *Let G be a cyclic p -group of order $p^e > 1$ and $A := \text{Aut } G$. Then*

$$A = S \times T,$$

where S is a group of order p^{e-1} and T is a cyclic group of order $p - 1$.

Proof. As we have already seen $|A| = p^{e-1}(p - 1)$. Moreover, A is Abelian (2.2.3). The direct decomposition 2.1.6 gives

$$A = S \times T \quad \text{with} \quad |S| = p^{e-1} \quad \text{and} \quad |T| = p - 1.$$

Let H be the (characteristic) subgroup of order p in G (1.4.3 on page 22) and

$$\varphi: A \rightarrow \text{Aut } H \quad \text{with} \quad \alpha \mapsto \bar{\alpha} := \alpha|_H.$$

Then φ is an epimorphism since

$$\text{Aut } H = \{\overline{\alpha_k} \mid 1 \leq k \leq p-1\}.$$

Moreover, since $|\text{Aut } H| = p-1$ and $(|S|, p-1) = 1$ we get that $S \leq \text{Ker } \varphi$ (1.1.8 on page 8). In fact $S = \text{Ker } \varphi$ since $|A| = |\text{Im } \varphi| |\text{Ker } \varphi|$. Now the Homomorphism Theorem gives

$$T \cong A / \text{Ker } \varphi \cong \text{Aut } H,$$

and T is cyclic by 2.2.4. \square

2.2.6 Let $G = \langle x \rangle$, $e \geq 2$, and A and S be as in 2.2.5.

(a) The case $p \neq 2$ or $p = 2 = e$:

$$S = \langle \alpha \rangle \quad \text{with} \quad x^\alpha = x^{1+p}.$$

In particular $\langle \alpha^{p^{e-2}} \rangle$ is the unique subgroup of order p in A , and for $\beta := \alpha^{p^{e-2}}$:

$$x^\beta = x^{1+p^{e-1}}.$$

(b) The case $p = 2 < e$:

$$S = A = \langle \gamma \rangle \times \langle \delta \rangle \quad \text{with} \quad x^\gamma = x^{-1}, \quad x^\delta = x^5.$$

In particular $\gamma, \xi := \delta^{2^{e-3}}$, and $\eta := \gamma\xi$ are the only automorphisms of order 2, and

$$x^\xi = x^{1+2^{e-1}} \quad \text{and} \quad x^\eta = x^{2^{e-1}-1}.$$

Proof. (a) Since $(p, 1+p) = 1$ the mapping α is an automorphism of G (2.2.1). If $p = 2 = e$, then $x^\alpha = x^{1+p} = x^3 = x^{-1}$ is the only nontrivial automorphism of G . Hence, in the following we may assume that $p \neq 2$. The order of α is the smallest integer $m \in \mathbb{N}$ such that

$$(1+p)^m \equiv 1 \pmod{p^e}.$$

The binomial formula applied to $(1+p)^m$ shows that

$$(1+p)^{p^{e-1}} \equiv 1 \pmod{p^e}$$

and

$$(1+p)^{p^{e-2}} \not\equiv 1 \pmod{p^e}$$

since $p \neq 2$. This gives $m = p^{e-1}$. Thus $\langle \alpha \rangle$ has the same order as S , i.e., $S = \langle \alpha \rangle$. The binomial formula also shows the statement for $\beta = \alpha^{p^{e-2}}$.

(b) As in (a) the binomial formula applied to $(1+2^2)^{2^k}$, $k \in \mathbb{N}$, shows that

$$(1+2^2)^{2^{e-2}} \equiv 1 \pmod{2^e}$$

and

$$(1+2^2)^{2^{e-3}} \not\equiv 1 \pmod{2^e}.$$

This implies, much as in (a), that the automorphism δ defined by

$$x^\delta = x^5 = x^{1+2^2}$$

has order 2^{e-2} . From

$$(1+2)^k \not\equiv -1 \pmod{2^e} \quad (e \geq 3),$$

for all $k \in \mathbb{N}$, we finally conclude that no power of δ is equal to the automorphism γ defined by $x^\gamma = x^{-1}$. Hence $\langle \gamma \rangle$ and $\langle \delta \rangle$ generate a subgroup of order $2^{e-2} \cdot 2 = 2^{e-1}$ in $S(= A)$. This implies $A = \langle \gamma \rangle \times \langle \delta \rangle$. The equation $x^\xi = x^{1+2^{e-1}}$ follows from

$$(1+2^2)^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}.$$

Finally $x^\eta = x^{2^{e-1}-1}$ holds since

$$x^\eta = x^{\gamma\xi} = (x^{-1})^{1+2^{e-1}} = x^{-1-2^{e-1}} \quad \text{and} \quad x^{-2^{e-1}} = x^{2^{e-1}}. \quad \square$$

It should be emphasized that in case 2.2.6 (b) the automorphism group A is not cyclic but contains a subgroup isomorphic to $Z_2 \times Z_2$.

Exercises

Let p be a prime and G a finite group.

1. Let $q \neq 1$ be a divisor of $p-1$. Use a semidirect product to construct a non-Abelian group of order pq that contains a normal subgroup of order p . Also construct a non-Abelian group of order $p^{(e-1)e}$, $e \geq 2$, that contains a cyclic normal subgroup of order p^e .

2. Let p be the smallest prime divisor of $|G|$ and N be a normal subgroup of order p . Then $N \leq Z(G)$.
3. Let $p \neq 2$ and G a cyclic p -group. Then $\text{Aut } G$ is cyclic.
4. With the idea used in the proof of 2.2.4 show: Let K be a field and U a finite subgroup of the multiplicative group of K . Then U is cyclic.

In the following let $G, \gamma, \eta, \varepsilon$ be as in 2.2.6 (b). Set

$$D := \langle \gamma \rangle \rtimes G, \quad H := \langle \eta \rangle \rtimes G,^9 \quad M := \langle \varepsilon \rangle \rtimes G.$$

5. D is a dihedral group.
6. All the involutions of M are contained in $\langle \varepsilon, x^{2^{e-1}} \rangle$.
7. Let H_1 and H_2 be subgroups of H defined by

$$H_1 := \langle x^2, \eta \rangle \quad \text{and} \quad H_2 := \langle x^2, \eta x \rangle.$$

Then

- (a) $H_1 \cap H_2 = \langle x^2 \rangle$ and $|H : H_i| = 2$, $i = 1, 2$.
- (b) H_1 is a dihedral group and contains all of the involutions of H .
- (c) H_2 contains exactly one involution.¹⁰

⁹ H is a semidihedral group; see **5.3**.

¹⁰ H_2 is called a (generalized) quaternion group; see **5.3**.



<http://www.springer.com/978-0-387-40510-0>

The Theory of Finite Groups

An Introduction

Kurzweil, H.; Stellmacher, B.

2004, XII, 388 p., Hardcover

ISBN: 978-0-387-40510-0