Part I

Finite Abelian groups and the DFT

1

Finite Abelian groups

This chapter contains an elementary, self-contained, but quite complete exposition of the structure theory of finite Abelian groups, including a detailed account on their endomorphisms and automorphisms. We also provide all the necessary background in number theory (only basic prerequisites are assumed).

1.1 Preliminaries in number theory

In this section we review some basic facts on elementary number theory. Most of the proofs are elementary and often left as exercises. More details can be found in the monographs by Apostol [13], Davenport [47], Herstein [71], Ireland and Rosen [79], Mac Lane and Birkhoff [113], Nagell [117], and Nathanson [118].

We denote by $\mathbb{N} = \{0, 1, 2, \ldots\}$ the set of natural numbers, and we recall that, by Peano's axioms (see [113]), every non-empty subset $A \subseteq \mathbb{N}$ admits a (unique) minimal element.

Also, a basic tool in elementary number theory is the *division (Euclidean) algorithm* (long division): let $a, b \in \mathbb{Z}$ such that $b \geq 1$, then there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that

$$a = bq + r. \tag{1.1}$$

If $r = 0$, one says that b *divides* a and we write $b|a$.

Theorem 1.1.1 (Definition of the greatest common divisor) *Let $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$. Then there exists a unique positive integer d satisfying the following conditions:*

(i) *$d|a$ and $d|b$;*
(ii) *if $d'|a$ and $d'|b$, then $d'|d$.*

Moreover, there exist (not necessarily unique) $m_0, n_0 \in \mathbb{Z}$ *such that* (Bézout identity)

$$d = m_0 a + n_0 b. \tag{1.2}$$

Definition 1.1.2 The positive integer d as in the above statement is called the *greatest common divisor* of a and b and it is denoted by $\gcd(a, b)$.

Proof of Theorem 1.1.1 Suppose that d_1 and d_2 are two positive integers satisfying conditions (i) and (ii). Then, by (ii) we have $d_1|d_2$ and $d_2|d_1$. This forces $d_1 = \pm d_2$, and therefore $d_1 = d_2$ by positivity. This proves uniqueness. In order to show existence, consider the set

$$\mathcal{I} = \{ma + nb : m, n \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Note that if $z, z' \in \mathcal{I}$ then $z + z' \in \mathcal{I}$ and $-z \in \mathcal{I}$. As a consequence, $\mathcal{I}_+ = \mathcal{I} \cap (\mathbb{N} \setminus \{0\})$ is a non-empty subset of $\mathbb{N}$. Let $d = m_0 a + n_0 b$ denote the minimal element of $\mathcal{I}_+$: we claim that $\mathcal{I} = \{hd : h \in \mathbb{Z}\}$. Indeed, the inclusion $\supseteq$ is obvious, while if $k \in \mathcal{I}$, by the division algorithm we can find $q, r \in \mathbb{Z}$ such that $k = qd + r$ with $0 \leq r < d$. Now, since $r = k - qd \in \mathcal{I}_+ \cup \{0\}$, by minimality of d we necessarily have $r = 0$, that is, $k \in \{hd : h \in \mathbb{Z}\}$. This shows the other inclusion and proves our claim. Since $a = a \cdot 1 + b \cdot 0$, $b = a \cdot 0 + b \cdot 1 \in \mathcal{I}$, there exist $h_1, h_2 \in \mathbb{Z}$ such that $a = h_1 d$ and $b = h_2 d$, so that $d|a$ and $d|b$. On the other hand, if $d'|a$ and $d'|b$, say $a = h_1' d'$ and $b = h_2' d'$, with $h_1', h_2' \in \mathbb{Z}$, then $d = m_0 a + n_0 b = m_0 h_1' d' + n_0 h_2' d' = (m_0 h_1' + n_0 h_2') d'$ so that $d'|d$. This shows that $d = \gcd(a, b)$. □

Remark 1.1.3 The set $\mathcal{I}$ is an *ideal* in the ring $\mathbb{Z}$, and $\mathbb{Z}$ is a *principal ideal domain* (see Section 6.1).

From the proof of Theorem 1.1.1 we immediately deduce the following:

Corollary 1.1.4 *Given* $a, b, c \in \mathbb{Z}$ *with* $(a, b) \neq (0, 0)$*, the linear equation*

$$na + mb = c$$

has a solution $(n, m) \in \mathbb{Z}^2$ *if and only if* $\gcd(a, b)$ *divides* c.

(See also Proposition 1.2.13 below.)

Exercise 1.1.5 Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ with $(a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0)$.

(1) Show that there exists a unique positive integer d satisfying the following conditions:
   (i) $d|a_i$ for all $i = 1, 2, \ldots, n$;
   (ii) if $d'|a_i$ for all $i = 1, 2, \ldots, n$, then $d'|d$.

In particular, setting $d_2 = \gcd(a_1, a_2)$ and $d_i = \gcd(d_{i-1}, a_i)$ for $i \geq 3$, show that $d = d_n$;

(2) show that there exist $m_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$, such that (generalized Bézout identity) $d = m_1 a_1 + m_2 a_2 + \ldots + m_n a_n$.

Definition 1.1.6 Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ with $(a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0)$. The number d in Exercise 1.1.5 (1) is called the *greatest common divisor* of the a_is and it is denoted by $\gcd(a_1, a_2, \ldots, a_n)$. One says that $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ are *relatively prime* provided $\gcd(a_1, a_2, \ldots, a_n) = 1$.

An integer $p > 1$ is said to be *prime* if its positive divisors are exactly 1 and p.

Exercise 1.1.7 (Euclidean algorithm) Let $a, b \in \mathbb{N}$ and suppose that $b \geq 1$ and $b \nmid a$. Set $r_0 = a$, $r_1 = b$, and recursively define, by the division algorithm,

$$r_k = r_{k+1} q_{k+1} + r_{k+2}$$

where $0 \leq r_{k+2} < r_{k+1}$, for all $k \geq 0$. Show that $\gcd(a, b) = r_n$ where $n \in \mathbb{N}$ is the largest index for which $r_n > 0$ (so that $r_{n+1} = 0$).

Exercise 1.1.8 Let $a, b, c \in \mathbb{Z}$ and p a prime number.

(1) Prove that if $\gcd(a, b) = 1$ and $a | bc$ then $a | c$;
(2) deduce that if $p | bc$ then $p | b$ or $p | c$.

Exercise 1.1.9 (Fundamental theorem of arithmetic) Let $n \geq 2$ be an integer. Show that there exists a unique *prime factorization*

$$n = {p_1}^{m_1} {p_2}^{m_2} \cdots {p_h}^{m_h}$$

where $p_1 < p_2 < \cdots < p_h$ are prime numbers, $m_1, m_2, \ldots, m_h \geq 1$ are the *multiplicities*, and $h \geq 1$.

Hint. For uniqueness, use induction combined with Exercise 1.1.8.

Exercise 1.1.10 Let $a_1, a_2, \ldots, a_n \geq 2$ be integers. Suppose that

$$a_j = {p_1}^{m_{1j}} {p_2}^{m_{2j}} \cdots {p_h}^{m_{hj}}$$

with distinct primes p_i and multiplicities $m_{ij} \geq 0$, for all $i = 1, 2, \ldots, h$ and $j = 1, 2, \ldots, n$. Show that

$$\gcd(a_1, a_2, \ldots, a_n) = {p_1}^{m_1} {p_2}^{m_2} \cdots {p_h}^{m_h}$$

where $m_i = \min\{m_{ij} : j = 1, 2, \ldots, n\}$ for all $i = 1, 2, \ldots, h$.

Exercise 1.1.11 (Euclid's proof of the infinitude of primes)

(1) Let $p_1, p_2, \dots, p_n$, $n \geq 1$, be distinct primes. Show that the number $p_1 p_2 \cdots p_n + 1$ is not divisible by p_i for all $i = 1, 2, \dots, n$;
(2) deduce that the set of prime numbers is infinite.

There are many other proofs of the infinitude of primes. Six of them (including Euclid's proof) are in the book by Aigner and Ziegler [5]. A deep generalization of this fact will be presented in Chapter 3.

Definition 1.1.12 Let $n \geq 1$ and $a, b \in \mathbb{Z}$. One says that a is *congruent* to b *modulo* n, and one writes $a \equiv b \bmod n$, provided $n|(a-b)$.

Exercise 1.1.13 Let $n \geq 1$.

(1) Show that the congruence relation $\equiv \bmod n$ is an equivalence relation;
(2) suppose that $a = nq + r$, with $0 \leq r < n$. Show that $a \equiv r \bmod n$;
(3) deduce that there are exactly n equivalence classes and that a complete list of representatives is provided by $0, 1, \dots, n-1$.

For $n \geq 1$ and $a \in \mathbb{Z}$ we denote by

$$\overline{a} = \{a + hn : h \in \mathbb{Z}\} \tag{1.3}$$

the equivalence class containing a.

We denote by $\mathbb{Z}/n\mathbb{Z} = \{\overline{a} : a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ the corresponding quotient set.

Exercise 1.1.14 Let $n \geq 1$ and $a, b \in \mathbb{Z}$. Set

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{ab}. \tag{1.4}$$

(1) Show that the operations $+$ and $\cdot$ in (1.4) are well defined;
(2) show that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a cyclic group;
(3) show that $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a unital commutative ring;
(4) show that $\overline{a}$ is invertible in $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ if and only if $\gcd(a, n) = 1$;
(5) deduce that if p is a prime, then $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field.

For (5), see also Corollary 6.1.13.

Notation 1.1.15 Let $n \geq 1$. For $k, m \in \mathbb{Z}$ we write

$$k\overline{m} = \overline{m} + \overline{m} + \cdots + \overline{m} \ (k \text{ summands})$$

if $k \geq 0$, and $k\overline{m} = -(|k|\overline{m})$ if $k < 0$, where $\overline{m}$ is as in (1.3).

The notation above is consistent with the fact that $(\mathbb{Z}/n\mathbb{Z}, +)$, as any Abelian group, is a $\mathbb{Z}$-module; see the monographs by Herstein [71], Lang [93], and Knapp [87].

Lemma 1.1.16 *Let r and s be positive integers with $\gcd(r, s) = 1$. Then for every $0 \leq k \leq rs - 1$ there exist unique $0 \leq u \leq r - 1$ and $0 \leq v \leq s - 1$ such that*

$$k \equiv us + vr \mod rs. \tag{1.5}$$

Proof. As u and v vary, with $0 \leq u \leq r - 1$ and $0 \leq v \leq s - 1$, the expression $us + vr$ yields (at most) rs integers; therefore it suffices to show that these are all distinct mod rs. Indeed, for $0 \leq u, u' \leq r - 1$ and $0 \leq v, v' \leq s - 1$ we have (keeping in mind that $\gcd(r, s) = 1$):

$$\begin{aligned} us + vr \equiv u's + v'r \mod rs &\Longrightarrow (u - u')s + (v - v')r \equiv 0 \mod rs \\ \text{(by Exercise 1.1.8.(1))} &\Longrightarrow \begin{cases} u \equiv u' \mod r \\ v \equiv v' \mod s \end{cases} \\ &\Longrightarrow u = u' \text{ and } v = v'. \end{aligned}$$

□

Notation 1.1.17 For $n \geq 1$ we denote by

- $\mathbb{Z}_n$ the *additive* group $(\mathbb{Z}/n\mathbb{Z}, +)$ *of integers* mod n;
- C_n the *multiplicative* cyclic group of order n;
- $\mathbb{Z}/n\mathbb{Z}$ the *ring* $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *of integers* mod n.

When $n = p$ is a prime, we shall denote by $\mathbb{F}_p$ the finite field $\mathbb{Z}/p\mathbb{Z}$ (cf. Exercise 1.1.14.(5)).

Note that if C_n is generated by the element $a \in C_n$, then the map $\bar{k} \mapsto a^k$, for all $k \in \mathbb{Z}$, is well defined and establishes a natural group isomorphism of $\mathbb{Z}_n$ onto C_n.

We shall examine the structure of all finite fields in Section 6.3.

Definition 1.1.18 The *Euler totient function* is the map φ defined by

$$\varphi(n) = |\{m \in \mathbb{N} : 1 \leq m \leq n, \gcd(m, n) = 1\}|$$

for all $n \geq 1$, where $|\cdot|$ denotes cardinality. In words, the value $\varphi(n)$ equals the number of positive integers less than or equal to n that are relatively prime to n.

Proposition 1.1.19 *Let n be a positive integer. Then in the cyclic group $\mathbb{Z}_n$ there are exactly $\varphi(n)$ distinct generators.*

Proof. Let $1 \leq m \leq n-1$ and suppose that $\gcd(m,n) = 1$. By Bézout identity, we can find $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Let $1 \leq h \leq n-1$ be such that $\overline{h} = \overline{a}$. Then, in $\mathbb{Z}_n$ we have $\overline{m} + \overline{m} + \cdots + \overline{m} = h\overline{m} = \overline{am} = \overline{1}$. As $\overline{1}$ clearly generates $\mathbb{Z}_n$, this shows that $\overline{m}$ generates $\mathbb{Z}_n$ as well. On the other hand, if $\gcd(m,n) = q > 1$, then we can find $h, k \in \mathbb{N}$ such that $m = hq$ and $n = kq$. Note that $1 \leq k < n$. Then we have $k\overline{m} = \overline{km} = \overline{khq} = h\overline{n} = \overline{0}$ so that the (cyclic) subgroup generated by $\overline{m}$ in $\mathbb{Z}_n$ has order $\leq k$ and therefore cannot equal the whole $\mathbb{Z}_n$. This shows that $\overline{m}$ is not a generator of $\mathbb{Z}_n$.

The statement then follows from the definition of $\varphi(n)$. □

Proposition 1.1.20 (Gauss) *Let n be a positive integer. Then we have*

$$\sum_{\substack{1 \leq r \leq n \\ r|n}} \varphi(r) = n.$$

Proof. For every positive divisor r of n let us set

$$A(r) := \{k \in \mathbb{N} : 1 \leq k \leq n, \gcd(k,n) = n/r\}. \tag{1.6}$$

For $1 \leq k \leq n$ we clearly have $k \in A(r)$ with $r = n/\gcd(k,n)$, and such an r is unique, so that

$$\{1, 2, \ldots, n\} = \coprod_{\substack{1 \leq r \leq n \\ r|n}} A(r). \tag{1.7}$$

Now, for every $k \in A(r)$ there exists a unique positive integer j such that $k = j\frac{n}{r}$. It follows that $1 \leq j \leq r$ and

$$\frac{n}{r} = \gcd(k,n) = \gcd\left(j\frac{n}{r}, r\frac{n}{r}\right) = \frac{n}{r}\gcd(j,r)$$

so that $\gcd(j,r) = 1$. Conversely, if $r|n$ and $\gcd(j,r) = 1$, then $\gcd(j\frac{n}{r}, n) = \gcd(j\frac{n}{r}, r\frac{n}{r}) = \frac{n}{r}$. As a consequence, $A(r) = \{j\frac{n}{r} : \gcd(j,r) = 1\}$ so that

$$|A(r)| = \varphi(r) \tag{1.8}$$

and therefore, from (1.7) we deduce

$$n = \sum_{\substack{1 \leq r \leq n \\ r|n}} |A(r)| = \sum_{\substack{1 \leq r \leq n \\ r|n}} \varphi(r).$$

□

Theorem 1.1.21 *Let p be a prime number. The (multiplicative) group $\mathbb{F}_p^*$ of invertible elements in the field $\mathbb{F}_p$ is cyclic (of order $p-1$).*

Proof. We first observe that $|\mathbb{F}_p^*| = |\{\overline{1}, \overline{2}, \dots, \overline{p-1}\}| = p-1$.

For every positive divisor r of $p-1$ let us set

$$B(r) := \{\alpha \in \mathbb{F}_p^* : \alpha \text{ is of order } r\}.$$

Thus, if $\alpha \in B(r)$, we have $\alpha^r = 1$ and α generates a cyclic group $\langle\alpha\rangle$ of order r consisting exactly of all the solutions in $\mathbb{F}_p$ of the equation $x^r = 1$. That is, $B(r) \subseteq \langle\alpha\rangle$ (recall also that over any field, an equation of degree m has at most m solutions). By virtue of Proposition 1.1.19, $\langle\alpha\rangle$ has $\varphi(r)$ generators, namely the powers α^h with $1 \le h \le r$ and $\gcd(h, r) = 1$. As a consequence, if $B(r) \neq \varnothing$ we have $|B(r)| = \varphi(r)$. Therefore

$$p - 1 = |F_p^*| = \sum_{r|(p-1)} |B(r)| \le \sum_{r|(p-1)} \varphi(r) = p - 1,$$

where the last equality follows from Proposition 1.1.20. Since the above is indeed an equality, we deduce that $B(r) \neq \varnothing$ for every r which divides $p-1$. In particular, every element $\alpha \in B(p-1)$ is of order $p-1$ and therefore $\langle\alpha\rangle = \mathbb{F}_p^*$. □

Exercise 1.1.22 (Fermat's little theorem) Show that if p is a prime, then for all $n \in \mathbb{Z}$ we have $n^p \equiv n \mod p$ so that, if in addition $p \nmid n$, then $n^{p-1} \equiv 1 \mod p$.

We end this section with the following well-known results (see also Remark 5.2.15), which we deduce from Theorem 1.1.1.

Corollary 1.1.23 (Chinese remainder theorem I) *Let r, s be two positive integers such that $\gcd(r, s) = 1$. Then for all $(a, b) \in \mathbb{Z}$ there exists $x = x(a, b) \in \mathbb{Z}$ solution to the system*

$$\begin{cases} x \equiv a \mod r \\ x \equiv b \mod s. \end{cases} \tag{1.9}$$

Proof. By Bézout identity, we can find $u, v \in \mathbb{Z}$ such that $1 = ur + vs$. We leave it to the reader to check that the quantities $a + (b-a)ur$ and $b + (a-b)vs$ are equal and constitute a solution to (1.9). □

Exercise 1.1.24 With the notation from Corollary 1.1.23, set $\delta_1 = x(1, 0)$ and $\delta_2 = x(0, 1)$. Show that $x(a, b) = a\delta_1 + b\delta_2$.

Exercise 1.1.25 (Chinese remainder theorem II) Let $r_1, r_2, \dots, r_n$ be positive integers such that $\gcd(r_i, r_j) = 1$ for all $1 \le i < j \le n$.

(a) Show that for all $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$ there exists a solution $x = x(a_1, a_2, \dots, a_n) \in \mathbb{Z}$ of the system

$$\begin{cases} x \equiv a_1 & \mod r_1 \\ x \equiv a_2 & \mod r_2 \\ \dots & \dots \\ x \equiv a_n & \mod r_n; \end{cases} \tag{1.10}$$

(b) set $R = r_1 r_2 \cdots r_n$. Show that $y \in \mathbb{Z}$ is another solution to (1.10) if and only if $x \equiv y \mod R$.

Hint. For every $i = 1, 2, \dots, n$ denote by $\delta_i \in \mathbb{Z}$ a solution to (1.9) with $a = 1, b = 0, r = r_i$, and $s = R/r_i$. Show that δ_i is a solution to (1.9) with $a = 1, b = 0, r = r_i$, and $s = r_j$, for all $j \neq i$. Then show that $x(a_1, a_2, \dots, a_n) = a_1\delta_1 + a_2\delta_2 + \cdots + a_n\delta_n$.

Proposition 1.1.26 *Let $n \geq 1$, $m \in \mathbb{Z}$, and set $d = \gcd(m, n)$. Then, in the cyclic group $\mathbb{Z}_n$ the element $\overline{m}$ has order $\frac{n}{d}$.*

Proof. For $k \in \mathbb{Z}$ we have

$$\begin{aligned} km \equiv 0 \mod n \quad &\Leftrightarrow n \mid km \\ &\Leftrightarrow \frac{n}{d} \mid k\frac{m}{d} \\ &\Leftrightarrow \frac{n}{d} \mid k, \end{aligned}$$

since $\frac{n}{d}$ and $\frac{m}{d}$ are relatively prime. □

Exercise 1.1.27 Deduce Proposition 1.1.19 from Proposition 1.1.26.

1.2 Structure theory of finite Abelian groups: preliminary results

In this section we review some basic facts on finite Abelian groups and their structure. Our exposition is based on the following monographs: by Machì [102], Zappa [170], Kurzweil and Stellmacher [90], Kurosh [89], Rotman [132], Herstein [71], Nathanson [118], and on the papers [18, 72, 120].

We use additive notation. In particular, for $a \in \mathbb{Z}_n$ and $r \in \mathbb{N}$ we set $ra = a + a + \cdots + a$ (r summands). Moreover, for an element a (respectively a subset B) of an Abelian group A, we denote by $\langle a \rangle = \{ra : r \in \mathbb{N}\}$ (respectively $\langle B \rangle$) the subgroup of A generated by a (respectively B) and by $\mathrm{o}(a) = |\langle a \rangle| \in \mathbb{N} \cup \{\infty\}$ the *order* of a.

Let A be a finite Abelian group and let $A_1, A_2, \dots, A_k \leq A$, $k \geq 1$ be subgroups of A.