DISCRETE MATHEMATICS

W W L CHEN

Chapter 9

GROUPS AND MODULO ARITHMETIC

9.1. Addition Groups of Integers

EXAMPLE 9.1.1. Consider the set $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, together with addition modulo 5. We have the following addition table:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

It is easy to see that the following hold:
(1) For every $x, y \in \mathbb{Z}_5$, we have $x + y \in \mathbb{Z}_5$.
(2) For every $x, y, z \in \mathbb{Z}_5$, we have $(x + y) + z = x + (y + z)$.
(3) For every $x \in \mathbb{Z}_5$, we have $x + 0 = 0 + x = x$.
(4) For every $x \in \mathbb{Z}_5$, there exists $x' \in \mathbb{Z}_5$ such that $x + x' = x' + x = 0$.

DEFINITION. A set G, together with a binary operation $*$, is said to form a group, denoted by $(G, *)$, if the following properties are satisfied:
(G1) (CLOSURE) For every $x, y \in G$, we have $x * y \in G$.
(G2) (ASSOCIATIVITY) For every $x, y, z \in G$, we have $(x * y) * z = x * (y * z)$.
(G3) (IDENTITY) There exists $e \in G$ such that $x * e = e * x = x$ for every $x \in G$.
(G4) (INVERSE) For every $x \in G$, there exists an element $x' \in G$ such that $x * x' = x' * x = e$.

Here, we are not interested in studying groups in general. Instead, we shall only concentrate on groups that arise from sets of the form $\mathbb{Z}_k = \{0, 1, \ldots, k-1\}$ and their subsets, under addition or multiplication modulo k.

It is not difficult to see that for every $k \in \mathbb{N}$, the set $\mathbb{Z}_k$ forms a group under addition modulo k. Conditions (G1) and (G2) follow from the corresponding conditions for ordinary addition and results on congruences modulo k. The identity is clearly 0. Furthermore, 0 is its own inverse, while every $x \neq 0$ clearly has inverse $k - x$.

PROPOSITION 9A. *For every $k \in \mathbb{N}$, the set $\mathbb{Z}_k$ forms a group under addition modulo k.*

We shall now concentrate on the group $\mathbb{Z}_2$ under addition modulo 2. Clearly we have

$$0 + 0 = 1 + 1 = 0 \qquad \text{and} \qquad 0 + 1 = 1 + 0 = 1.$$

In coding theory, messages will normally be sent as finite strings of 0's and 1's. It is therefore convenient to use the digit 1 to denote an error, since adding 1 modulo 2 changes the number, and adding another 1 modulo 2 has the effect of undoing this change. On the other hand, we also need to consider finitely many copies of $\mathbb{Z}_2$.

Suppose that $n \in \mathbb{N}$ is fixed. Consider the cartesian product

$$\mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n}$$

of n copies of $\mathbb{Z}_2$. We can define addition in $\mathbb{Z}_2^n$ by coordinate-wise addition modulo 2. In other words, for every $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{Z}_2^n$, we have

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

It is an easy exercise to prove the following result.

PROPOSITION 9B. *For every $n \in \mathbb{N}$, the set $\mathbb{Z}_2^n$ forms a group under coordinate-wise addition modulo 2.*

9.2. Multiplication Groups of Integers

EXAMPLE 9.2.1. Consider the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, together with multiplication modulo 4. We have the following multiplication table:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

It is clear that we cannot have a group. The number 1 is the only possible identity, but then the numbers 0 and 2 have no inverse.

EXAMPLE 9.2.2. Consider the set $\mathbb{Z}_k = \{0, 1 \ldots, k-1\}$, together with multiplication modulo k. Again it is clear that we cannot have a group. The number 1 is the only possible identity, but then the number 0 has no inverse. Also, any proper divisor of k has no inverse.

It follows that if we consider any group under multiplication modulo k, then we must at least remove every element of $\mathbb{Z}_k$ which does not have a multiplicative inverse modulo k. We then end up with the subset

$$\mathbb{Z}_k^* = \{x \in \mathbb{Z}_k : xu = 1 \text{ for some } u \in \mathbb{Z}_k\}.$$

Example 9.2.3. Consider the subset $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ of $\mathbb{Z}_{10}$. It is fairly easy to check that $\mathbb{Z}_{10}^*$, together with multiplication modulo 10, forms a group of 4 elements. In fact, we have the following group table:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

PROPOSITION 9C. *For every $k \in \mathbb{N}$, the set $\mathbb{Z}_k^*$ forms a group under multiplication modulo k.*

Proof. Condition (G2) follows from the corresponding condition for ordinary multiplication and results on congruences modulo k. The identity is clearly 1. Inverses exist by definition. It remains to prove (G1). Suppose that $x, y \in \mathbb{Z}_k^*$. Then there exist $u, v \in \mathbb{Z}_k$ such that $xu = yv = 1$. Clearly $(xy)(uv) = 1$ and $uv \in \mathbb{Z}_k$. Hence $xy \in \mathbb{Z}_k^*$. ○

PROPOSITION 9D. *For every $k \in \mathbb{N}$, we have*

$$\mathbb{Z}_k^* = \{x \in \mathbb{Z}_k : (x, k) = 1\}.$$

Proof. Recall Proposition 4H. There exist $u, v \in \mathbb{Z}$ such that $(x, k) = xu + kv$. It follows that if $(x, k) = 1$, then $xu = 1$ modulo k, so that $x \in \mathbb{Z}_k^*$. On the other hand, if $(x, k) = m > 1$, then for any $u \in \mathbb{Z}_k$, we have $xu \in \{0, m, 2m, \ldots, k - m\}$, so that $xu \neq 1$ modulo k, whence $x \notin \mathbb{Z}_k^*$. ○

9.3. Group Homomorphism

In coding theory, we often consider functions of the form $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$, where $m, n \in \mathbb{N}$ and $n > m$. Here, we think of $\mathbb{Z}_2^m$ and $\mathbb{Z}_2^n$ as groups described by Proposition 9B. In particular, we are interested in the special case when the range $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$ forms a group under coordinate-wise addition modulo 2 in $\mathbb{Z}_2^n$. Instead of checking whether this is a group, we often check whether the function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is a group homomorphism. Essentially, a group homomorphism carries some of the group structure from its domain to its range, enough to show that its range is a group. To motivate this idea, we consider the following example.

Example 9.3.1. If we compare the additive group $(\mathbb{Z}_4, +)$ and the multiplicative group $(\mathbb{Z}_{10}, \cdot)$, then there does not seem to be any similarity between the group tables:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

However, if we alter the order in which we list the elements of $\mathbb{Z}_{10}^*$, then we have the following:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	7	9	3
1	1	7	9	3
7	7	9	3	1
9	9	3	1	7
3	3	1	7	9

They share the common group table (with identity e) below:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

We therefore conclude that $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_{10}^*, \cdot)$ "have a great deal in common". Indeed, we can imagine that a function $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{10}^*$, defined by

$$\phi(0) = 1, \qquad \phi(1) = 7, \qquad \phi(2) = 9, \qquad \phi(3) = 3,$$

may have some nice properties.

DEFINITION. Suppose that $(G, *)$ and $(H, \circ)$ are groups. A function $\phi : G \to H$ is said to be a group homomorphism if the following condition is satisfied:
(HOM) For every $x, y \in G$, we have $\phi(x * y) = \phi(x) \circ \phi(y)$.

DEFINITION. Suppose that $(G, *)$ and $(H, \circ)$ are groups. A function $\phi : G \to H$ is said to be a group isomorphism if the following conditions are satisfied:
(IS1) $\phi : G \to H$ is a group homomorphism.
(IS2) $\phi : G \to H$ is one-to-one.
(IS3) $\phi : G \to H$ is onto.

DEFINITION. We say that two groups G and H are isomorphic if there exists a group isomorphism $\phi : G \to H$.

EXAMPLE 9.3.2. The groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_{10}^*, \cdot)$ are isomorphic.

EXAMPLE 9.3.3. The groups $(\mathbb{Z}_2, +)$ and $(\{\pm 1\}, \cdot)$ are isomorphic. Simply define $\phi : \mathbb{Z}_2 \to \{\pm 1\}$ by $\phi(0) = 1$ and $\phi(1) = -1$.

EXAMPLE 9.3.4. Consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_4, +)$. Define $\phi : \mathbb{Z} \to \mathbb{Z}_4$ in the following way. For each $x \in \mathbb{Z}$, let $\phi(x) \in \mathbb{Z}_4$ satisfy $\phi(x) \equiv x \pmod 4$, when $\phi(x)$ is interpreted as an element of $\mathbb{Z}$. It is not difficult to check that $\phi : \mathbb{Z} \to \mathbb{Z}_4$ is a group homomorphism. This is called reduction modulo 4.

We state without proof the following result which is crucial in coding theory.

PROPOSITION 9E. *Suppose that $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is a group homomorphism. Then $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$ forms a group under coordinate-wise addition modulo 2 in $\mathbb{Z}_2^n$.*

REMARK. The general form of Proposition 9E is the following: Suppose that $(G, *)$ and $(H, \circ)$ are groups, and that $\phi : G \to H$ is a group homomorphism. Then the range $\phi(G) = \{\phi(x) : x \in G\}$ forms a group under the operation $\circ$ of H.

Problems for Chapter 9

1. Suppose that $\phi : G \to H$ and $\psi : H \to K$ are group homomorphisms. Prove that $\psi \circ \phi : G \to K$ is a group homomorphism.

2. Prove Proposition 9E.