Chapter 6

Commutative Rings and Fields

The set of integers $\mathbb{Z}$ has two interesting operations: addition and multiplication, which interact in a nice way.

Definition 6.1. *A commutative ring consists of a set R with distinct elements $0, 1 \in R$, and binary operations $+$ and $\cdot$ such that:*

1. *$(R, +, 0)$ is an Abelian group*
2. *$\cdot$ is commutative and associative with 1 as the identity: $x \cdot y = y \cdot x$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $x \cdot 1 = x$.*
3. *$\cdot$ distributes over $+$: $x \cdot (y + z) = x \cdot y + x \cdot z$.*

Definition 6.2. *A commutative ring R is a field if in addition, every nonzero $x \in R$ possesses a multiplicative inverse, i.e. an element $y \in R$ with $xy = 1$.*

As a homework problem, you will show that the multiplicative inverse of x is unique if it exists. We will denote it by x^{-1}.

Example 6.3. *$\mathbb{Z}$, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in Z, b \neq 0\}$, $\mathbb{R}$ and $\mathbb{C}$ with the usual operations are all commutative rings. All but the $\mathbb{Z}$ are fields.*

The main new examples are the following:

Theorem 6.4. *The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a commutative ring with addition and multiplication given by*

$$x \oplus y = x + y \bmod n$$

$$x \odot y = xy \bmod n$$

Theorem 6.5. *$\mathbb{Z}_n$ is a field if and only if n is prime.*

We will prove the second theorem, after we have developed a bit more theory. Since the symbols $\oplus$ and $\odot$ are fairly cumbersome, we will often use ordinary notation with the understanding that we're using $mod\, n$ rules.

I generated the following tables for $\mathbb{Z}_8$ using a computer:

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

.	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Looking at the second table, we can see quite a few zeros which don't come from multiplication by 0. A nonzero element a such $ab = 0$, with $b \neq 0$, is called a zero divisor. The elements $2, 4, 6$ are zero divisors. Zero divisors exibit some strange properties, for example $4 \cdot 1 = 4 \cdot 3$, so one can't cancel the 4. These elements have a more extreme property that they become 0 after multiplying them with themselves enough times:

$$2^3 = 2 \cdot 2 \cdot 2 = 0$$

$$4^2 = 4 \cdot 4 = 0$$

$$6^3 = 0$$

Most standard identities from high school algebra can be carried out for commutative rings. For example:

Lemma 6.6. *Suppose that R is a commutative ring. Let $-x$ denote the additive inverse of x, which means the unique element so that $x + (-x) = 0$. Then*

(a) $0 \cdot x = 0$.

(b) $(-1) \cdot x = -x$

Proof. Therefore

$$0 \cdot x + x = 0 \cdot x + 1 \cdot x = x \cdot 0 + x \cdot 1 = x(1 + 0) = x$$

Adding $-x$ to both sides proves (a).

For (b), it is enough to check that $x + (-1)x = 0$. But

$$x + (-1)x = (1 - 1)x = 0 \cdot x = 0$$

□

6.7 Exercises

1. Prove

   (a) $(x + y)^2 = x^2 + 2xy + y^2$.

   (b) $(x - y)(x + y) = x^2 - y^2$

   hold in any commutative ring R, where we define $x^2 = xx$, $2x = x + x$, and $x - y = x + (-y)$. (Check all the steps.)

2. Prove that an element $x \in R$ can have at most one multplicative inverse (which why we can give it a name x^{-1}). In the definition of multplicative inverse we insisted the element be nonzero. Why is that? Suppose that we a commutative ring R with an element 0^{-1} which gave an inverse to 0, then what would go wrong?

3. Find all the zero divisors and nilpotent elements in $\mathbb{Z}_{12}$. If you need it, here's the multiplication table

.	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

4. Recall that the greatest common divisor $gcd(m, n)$ is the largest integer dividing both m and n. Suppose that $m \in \mathbb{Z}_n$ has $gcd(m, n) \neq 1$. Prove that m is zero divisor in $\mathbb{Z}_n$. Conclude that m does not have a multiplicative inverse in $\mathbb{Z}_n$.

5. Sequences of "random" numbers are often generated on a computer by the following method: Choose integers $n \geq 2, a, b, x_0$, and consider the sequence

$$x_{i+1} = (ax_i + b) \, mod \, n.$$

This sequence will eventually repeat itself. The period is the smallest k such that $x_{i+k} = x_i$ for all i large enough. Obviously, short periods are less useful, since the pattern shouldn't be too predictable.

(a) Prove that the period is at most n.

(b) Explain why picking a nilpotent in $\mathbb{Z}_n$ would be a really bad choice.

6. Guess a formula for 2^{-1} in $\mathbb{Z}_p$ where p is an odd prime by trying $p = 3, 5, 7$ etc. Now prove it.