Chapter 8

Commutative Rings

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

Definition 8.1. *A commutative ring consists of a set R with 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 $+$: $x \cdot (y + z) = x \cdot y + x \cdot z$.*

Example 8.2. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with the usual operations are all commutative rings.*

Example 8.3. *$\mathbb{Z}_n$ is in fact a commutative ring. The addition has been discussed already. The product is the $mod\, n$ product*

$$x \odot y = xy \, mod \, n$$

Since the symbols $\oplus$ and $\odot$ are fairly cumbersome, we will usually use ordinary notation with the understanding that we're using $mod\, n$ rules. For example, we write $11 \cdot 9 + 11 \cdot 13$ instead of $(11 \odot 9) \oplus (11 \odot 13)$. When doing calculations by hand, the congruence symbol is very useful. For example, to see that

$$11 \cdot 9 + 11 \cdot 13 = 2 = 11 \cdot (9 + 13)$$

in $\mathbb{Z}_{15}$, we can write:

$$11 \cdot 9 + 11 \cdot 13 \equiv_{15} 99 + 143 \equiv_{15} 9 + 8 \equiv_{15} 2.$$

$$11 \cdot (9 + 13) \equiv_{15} 11 \cdot 7 \equiv_{15} 2.$$

To evaluate this in Maple, just type $11 * 9 + 11 * 13 \, mod \, 15;$.

To get a better feeling for this, we can have Maple generate the addition and multiplication tables for $\mathbb{Z}_n$ with the following code:

```
tables := proc(n::posint)
 local A,B,i,j;
 A := matrix(n+1,n+1);
 B := matrix(n+1,n+1);
 for i from 0 to n-1 do
   for j from 0 to n-1 do
    A[i+2,j+2] := i+j mod n;
    B[i+2,j+2] := i*j mod n;
   od;
  od;
 A[1,1] := `+`;
 B[1,1] := `.`;
 for i from 0 to n-1 do
   A[1,i+2] := i;
   A[i+2,1] := i;
   B[1,i+2] := i;
   B[i+2,1] := i;
 od;
 print(A,B);
 end;
```

To get the tables for $\mathbb{Z}_8$, type:

```
> tables(8);
```

$$\begin{bmatrix} + & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ 2 & 2 & 3 & 4 & 5 & 6 & 7 & 0 & 1 \\ 3 & 3 & 4 & 5 & 6 & 7 & 0 & 1 & 2 \\ 4 & 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\ 5 & 5 & 6 & 7 & 0 & 1 & 2 & 3 & 4 \\ 6 & 6 & 7 & 0 & 1 & 2 & 3 & 4 & 5 \\ 7 & 7 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}, \begin{bmatrix} . & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\ 3 & 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \\ 4 & 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 5 & 0 & 5 & 2 & 7 & 4 & 1 & 6 & 3 \\ 6 & 0 & 6 & 4 & 2 & 0 & 6 & 4 & 2 \\ 7 & 0 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

The output are matrices, which can, with a little imagination, be viewed as tables. 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:

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

$$4^2 = 4 \cdot 4 = 0$$
$$6^3 = 0$$

The construction of $\mathbb{C}$ from $\mathbb{R}$ involves adjoining $i = \sqrt{-1}$, and considering all possible expressions $a+bi$ with $a, b \in \mathbb{R}$. This construction can be generalized.

Example 8.4. *Let R be a commutative ring. Define*

$$R[i] = \{a + bi \mid a, b \in R\}$$

with rules

$$(a + bi) + (c + di) = (a + b) + (c + d)i$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

Lemma 8.5. *$R[i]$ is a commutative ring.*

For example, $\mathbb{C} = \mathbb{R}[i]$. The other examples of interest to us is the ring of Gaussian integers $\mathbb{Z}[i]$, and the Gausian field $\mathbb{Q}[i]$. We look at some other cases of this in the exercises.

A polynomial is usually regarded as an expression of the form

$$a_0 + a_1 x + \ldots a_n x^n$$

where a_i are numbers of some sort. We will actually define a polynomial to equal the sequence of its coefficients $(a_0, a_1, \ldots)$, but we will use the x to help us keep track of things.

Example 8.6. *The set of polynomials $\mathbb{C}[x]$ with complex coefficients becomes a commutative ring with*

- 0 *denoting the polynomial* $0 + 0x + \ldots$.
- $1 = 1 + 0x + \ldots$.
- $(a_0 + a_1 x + \ldots) + (b_0 + b_1 x + \ldots) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$
- $(a_0 + a_1 x + \ldots)(b_0 + b_1 x + \ldots) = (a_0 b_0) + (a_1 b_0 + a_0 b_1)x + \ldots$

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

Lemma 8.7. *Suppose that R is a commutative ring. Let $-x$ denote the inverse of x in $(R, +, 0)$. 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, by corollary 3.9, to check that $x + (-1)x = 0$. But

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

□

8.8 Exercises

1. Prove

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

   (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. Write out the addition and multiplication tables for $\mathbb{Z}_2[i] = \{0, 1, i, 1+i\}$ (the overlines are dropped for convenience). Show that $(1+i)^2 = 0$, which means that it is nilpotent.

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

$$\begin{bmatrix}
. & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
2 & 0 & 2 & 4 & 6 & 8 & 10 & 0 & 2 & 4 & 6 & 8 & 10 \\
3 & 0 & 3 & 6 & 9 & 0 & 3 & 6 & 9 & 0 & 3 & 6 & 9 \\
4 & 0 & 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 \\
5 & 0 & 5 & 10 & 3 & 8 & 1 & 6 & 11 & 4 & 9 & 2 & 7 \\
6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 \\
7 & 0 & 7 & 2 & 9 & 4 & 11 & 6 & 1 & 8 & 3 & 10 & 5 \\
8 & 0 & 8 & 4 & 0 & 8 & 4 & 0 & 8 & 4 & 0 & 8 & 4 \\
9 & 0 & 9 & 6 & 3 & 0 & 9 & 6 & 3 & 0 & 9 & 6 & 3 \\
10 & 0 & 10 & 8 & 6 & 4 & 2 & 0 & 10 & 8 & 6 & 4 & 2 \\
11 & 0 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}$$

4. Suppose that $gcd(m, n) \neq 1$. Prove that m is zero divisor in $\mathbb{Z}_n$.