Chapter 8

Rings and modular arithmetic

So far, we have been working with just one operation at a time. But standard number systems, such as $\mathbb{Z}$, have two operations $+$ and $\cdot$ which interact. It is useful to give a name to this sort of thing.

Definition 8.1. *A ring consists of a set R with elements $0, 1 \in R$, and binary operations $+$ and $\cdot$ such that: $(R, +, 0)$ is an Abelian group, $\cdot$ is associative with 1 as the identity, and $\cdot$ distributes over $+$ on the left and right:*

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(y + z) \cdot x = y \cdot x + z \cdot x$$

Definition 8.2. *A ring is commutative if in addition*

$$x \cdot y = y \cdot x$$

Here are some basic examples that everyone should already know.

Example 8.3. *Let $\mathbb{Z}$ (respectively $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) be the set of integers (respectively rational numbers, real numbers, complex numbers) with the usual operations. These are all commutative rings.*

Example 8.4. *The set $M_{nn}(\mathbb{R})$ of $n \times n$ matrices over $\mathbb{R}$ with the usual matrix operations forms a ring. It is not commutative when $n > 1$.*

We now focus on a new example. Let n be a positive integer, and write $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, where $\overline{x} = x + n\mathbb{Z}$. We already know that this has an addition given by addition of cosets:

$$\overline{a} + \overline{b} = \overline{a + b}$$

For hereon in, we'll stop writing $\oplus$. We will try to define multiplication the same way by

$$\overline{a}\overline{b} = \overline{ab}$$

However, we have to prove that this definition makes sense. In other words, we have to show that right side depends only on $\overline{a}$ and $\overline{b}$ rather than a and b.

Lemma 8.5. *If $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, then $\overline{ab} = \overline{a'b'}$*

Proof. The equality $\overline{x} = \overline{x'}$ holds if and only if $x - x'$ is divisible by n. Therefore $a' = a + nx$ and $b = b' + ny$ for some $x, y \in \mathbb{Z}$. It follows that $a'b' = ab + n(xb' + ya' + nxy)$.

□

Theorem 8.6. *$\mathbb{Z}_n$ is a commutative ring.*

Proof. The laws follow from the fact that $\mathbb{Z}$ is a commutative ring, the definition of the operations in $\mathbb{Z}_n$, and the fact that the map $\mathbb{Z} \to \mathbb{Z}_n$ is onto. For example, here is a proof of the distributive law

$$(\overline{x} + \overline{y})\overline{z} = (\overline{x + y})\overline{z} = \overline{(x + y)z}$$

□

When it's clear we're working in $\mathbb{Z}_n$, we usually just write x instead of $\bar{x}$. To get a feeling for modular multiplication, lets write down the table for $\mathbb{Z}_6$

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

One curious fact is that some nonzero numbers, such as 2, can be multiplied by other nonzero numbers to get 0. We say that such a number is a *zero divisor*.

Lemma 8.7. *An element $\overline{m} \in \mathbb{Z}_n$ is a zero divisor if $m > 1$ and m divides n.*

Proof. We have that $n = mm'$ for some $0 < m' < n$. So that $\overline{m}\overline{m'} = \overline{0}$ □

Also notice that the number 5 has a reciprocal, namely 5.

Definition 8.8. *An element $x \in R$ of a ring is invertible if there exists an element y such that $xy = yx = 1$. Let R^* denote the set of invertible elements. (When R is commutative, invertible elements are also called units.)*

Lemma 8.9. *If R is a ring R^* is a group with respect to multiplication.*

This will be proven in the exercises. The group of invertible elements are easy to determine for the previous examples. For example, $M_{nn}(\mathbb{R})^* = GL_n(\mathbb{R})$.

Given two integers a, b, a common divisor is an integer d such that $d|a$ and $d|b$. The greatest common divisor is exactly that, the common divisor greater than or equal to all others (it exists since the set of common divisors is finite). We denote this by $\gcd(a, b)$.

Lemma 8.10 (Euclid)**.** *If a, b are natural numbers then $\gcd(a, b) = \gcd(b, a\, mod\, b)$*

Proof. Let $r = a\, mod\, b$. Then the division algorithm gives $a = qb + r$ for some integer q. SInce $\gcd(b, r)$ divides b and r, it divides $qb + r = a$. Therefore $\gcd(b, r)$ is a common divisor of a and b, so that that $\gcd(b, r) \leq \gcd(a, b)$. On the other hand, $r = a - qb$ implies that $\gcd(a, b)|r$. Therefore $\gcd(a, b)$ is a common divisor of b and r, so $\gcd(a, b) \leq \gcd(b, r)$, which forces them to be equal. □

This lemma leads to a method for computing gcds. For example

$$\gcd(100, 40) = \gcd(40, 20) = \gcd(20, 0) = 20.$$

For our purposes, a *diophantine equation* is an equation with integer coefficients where the solutions are also required to be integers. The simplest examples are the linear ones: given integers a, b, c, find all integers m, n such that $am + bn = c$.

Theorem 8.11. *Given integers a, b, c, $am+bn = c$ has a solution with $m, n \in \mathbb{Z}$ if and only if $\gcd(a, b)|c$.*

Proof. Since $(m', n') = (\pm m, \pm n)$ is a solution of $\pm an' + \pm bm' = c$, we may as well assume that $a, b \geq 0$. We now prove the theorem for natural numbers a, b by induction on the minimum $min(a, b)$.

If $min(a, b) = 0$, then one of them, say $b = 0$. Since $a = \gcd(a, b)$ divides c by assumption, $(c/a, 0)$ gives a solution of $am + bn = c$. Now assume that $a'm + b'n = c'$ has a solution whenever $min(a', b') < min(a, b)$ and the other conditions are fulfilled. Suppose $b \leq a$, and let $r = r(a, b) = a\, mod\, b$ and $q = q(a, b)$ be given as in theorem 4.5. Then $rm' + bn' = c$ has a solution since $min(r, b) = r < b = min(a, b)$ and $\gcd(b, r) = \gcd(a, b)$ divides c. Let $m = n'$ and $n = m' - qn'$, then

$$am + bn = an' + b(m' - qn') = bm' + rn' = c.$$

□

From the last proof, we can deduce:

Corollary 8.12. *Given $a, b \in \mathbb{Z}$, there exists $m, n \in \mathbb{Z}$ such that $am + bn = \gcd(a, b)$.*

We can now determine the invertible elements

Theorem 8.13. *$m \in \mathbb{Z}_n$ is invertible if and only if* $\gcd(m,n) = 1$ *(we also say that m and n are* relatively prime *or* coprime*).*

Proof. If $gcd(m,n) = 1$, then $mm' + nn' = 1$ or $mm' = -n'n + 1$ for some integers by corollary 8.12. After replacing (m', n') by $(m' + m''n, n' - m'')$ for some suitable m'', we can assume that $0 \leq m' \leq n$. Since have $r(mm', n) = 1$, $mm' = 1$.

The converse follows by reversing these steps. □

Definition 8.14. *A ring is called a division ring if $R^* = R - \{0\}$. A commutative division ring is called a field.*

For example $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields. We will see a noncommutative division ring later on. The previous theorem implies the following:

Theorem 8.15. *The ring $\mathbb{Z}_n$ is a field if and only if n is prime.*

Corollary 8.16 (Fermat's little theorem)**.** *When p is a prime and n and integer, then p divides $n^p - n$.*

Proof. If p divides n, then clearly it divides $n^p - n$. Now suppose that p does not divide n, then $\overline{n} \in \mathbb{Z}_p^*$. This is a group of order $p - 1$. So by Lagrange's theorem, $\overline{n}$ has order dividing $p - 1$. This implies that $\overline{n}^{p-1} = \overline{1}$, or that $\overline{n}^{p-1} - \overline{1} = \overline{0}$. This implies that p divides $n^{p-1} - 1$ (which is usually taken as the statement of Fermat's little theorem) and therefore $n^p - n$. □

8.17 Exercises

1. Let R be a commutative ring. Prove that $0 \cdot x = 0$. (This might appear to be a completely obvious statement, but it isn't – the only things you know about R are what follows from the axioms.)

2. Let R be a commutative ring. Prove that $(-1) \cdot x = -x$, where $-x$ is the additive inverse of x, that is $(-x) + x = 0$.

3. The Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$.

   (a) Check that is closed under addition and multiplication, and is therefore a ring.

   (b) Determine the group $\mathbb{Z}[i]^*$ of invertible elements.

4. Check that the Gaussian field $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a field when equipped with the usual operations.

5. Prove that there are no zero divisors in a field, i.e. if $xy = 0$ then $x = 0$ or $y = 0$.

6. If R_1 and R_2 are commutative rings, define $R = R_1 \times R_2$ with operations $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$ and $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_1 b_2)$. Check that this is a commutative ring with appropriate choice of constants. Show that this has zero divisors.

7. An element x of a commutative ring is nilpotent if $x^N = 0$ for some integer $N \geq 0$. Determine the nilpotent elements of $\mathbb{Z}_n$.

8. Prove that the sum and product of nilpotent elements in a commutative ring are also nilpotent.

9. 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.