11. Integral domains

Consider the polynomial equation

$$x^2 - 5x + 6 = 0.$$

The usual way to solve this equation is to factor

$$x^2 - 5x + 6 = (x-2)(x-3).$$

Now our equation reduces to

$$(x-2)(x-3) = 0.$$

If we are trying to find the complex solutions to this equation we argue that either $x = 2$ since $x = 3$, since the only way that a product can be zero is if one of the factors is zero.

But now suppose that we work in a different ring, say the ring $\mathbb{Z}_{12}$. In this case we can still factor the polynomial equation and it is still true that $x = 2$ and $x = 3$ are both solutions to this equation. The problem is that there might be more, since

$$2 \cdot 6 = 3 \cdot 4 = 8 \cdot 3 = 4 \cdot 6 = 6 \cdot 6 = 6 \cdot 8 = 6 \cdot 10 = 8 \cdot 9 = 0.$$

In fact if $x - 2 = 4$ then $x - 3 = 3$ and so $x = 2 + 4 = 6$ is also a solution to the polynomial equation

$$x^2 - 5x + 6 = 0.$$

Similarly if $x - 2 = 9$ then $x - 3 = 8$ and so $x = 11$ is a solution.

We encode this property in a:

Definition 11.1. *Let R be a ring. We say that two non-zero elements $a \in R$, $a \neq 0$ and $b \in R$, $b \neq 0$ are* ***zero-divisors*** *if*

$$ab = 0.$$

Proposition 11.2. *The zero-divisors of $\mathbb{Z}_n$ are precisely the non-zero elements which are not coprime to n.*

Proof. Pick a non-zero $m \in \mathbb{Z}_n$. Suppose that m is not coprime to n and let $d > 1$ be the gcd. Then

$$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right) n$$

which is zero modulo n. Thus $m(n/d) = 0$ in $\mathbb{Z}_n$ whilst neither m nor n/d is zero. Thus m is a zero-divisor.

Now suppose that m is coprime to n. If $ms = 0$ in $\mathbb{Z}_n$ then n divides the product of ms in $\mathbb{Z}$. As n is coprime to m, n must divide s. But then $s = 0$ in $\mathbb{Z}_n$. It follows that m is not a zero-divisor. □

Corollary 11.3. *If p is a prime then $\mathbb{Z}_p$ has no zero divisors.*

Proof. Immediate from (11.2). □

Definition-Theorem 11.4. *Let R be a ring. Then R contains no zero-divisors if and only if the* ***cancellation laws*** *holds in R, that is,*

$$\text{if } ab = ac \text{ and } a \neq 0 \qquad \text{then} \qquad b = c,$$

and

$$\text{if } ba = ca \text{ and } a \neq 0 \qquad \text{then} \qquad b = c.$$

Proof. Suppose that a and b are zero divisors. Let $c = 0$. By assumption $b \neq c$ but

$$ab = 0 = a0 = ac$$

so that the cancellation law does not hold.

Now suppose that $a \neq 0$ is not a zero-divisor and

$$ab = ac.$$

We have

$$\begin{aligned} a(b - c) &= ab - ac \\ &= 0. \end{aligned}$$

As a is not a zero-divisor $b - c = 0$. But then $b = c$.

By symmetry if $ba = ba$ then $b = c$ as well. □

Definition 11.5. *We say that a ring R is an* ***integral domain*** *if R is commutative, with unity $1 \neq 0$, has no zero-divisors.*

Many of the examples we have seen so far are in fact not integral domains.

Example 11.6. *Both $\mathbb{Z}$ and $\mathbb{Z}_p$ are integral domains, where p is a prime. $\mathbb{Z}_n$ is not an integral domain if n is composite.*

If R and S are integral domains then surprisingly the product $R \times S$ is never an integral domain:

$$(1, 0) \cdot (0, 1) = (0, 0),$$

but neither $(1, 0)$ nor $(0, 1)$ are zero.

Example 11.7. *$M_2(\mathbb{Z}_2)$ contains zero-divisors.*

For example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Lemma 11.8. *If a is a unit then a is not a zero-divisor.*

Proof. Suppose that $ba = 0$ and that c is the multiplicative inverse of a. We compute bac, in two different ways.

$$\begin{aligned} bac &= (ba)c \\ &= 0c \\ &= 0. \end{aligned}$$

On the other hand

$$\begin{aligned} bac &= b(ac) \\ &= b1 \\ &= b. \end{aligned}$$

Thus $b = bac = 0$. Thus a is not a zero-divisor. □

Proposition 11.9. *Every field is an integral domain.*

Proof. A field is a commutative ring, with unity $1 \neq 0$ and by (11.8) there are no zero divisors. Thus every field is an integral domain. □

Unfortunately the converse is not true.

Example 11.10. $\mathbb{Z}$ *is an integral domain but not a field.*

However we do have:

Theorem 11.11. *Every finite integral domain D is a field.*

Proof. Pick a non-zero element $a \in D$. Define a function

$$f\colon D \longrightarrow D \qquad \text{by the rule} \qquad b \longrightarrow ab.$$

Suppose that $f(b_1) = f(b_2)$. Then $ab_1 = ab_2$. As D is an integral domain we can cancel, so that $b_1 = b_2$. But then f is one to one.

As D is finite and f is one to one, it follows that f is onto. As $1 \in D$ we may find $b \in D$ such that $f(b) = 1$. But then $ab = 1$. If follows that a is a unit, so that D is a field. □

Corollary 11.12. *If p is a prime then $\mathbb{Z}_p$ is a field.*

Proof. $\mathbb{Z}_p$ is a domain and it is finite, so (11.11) implies that it is a field. □

Note that we can do linear algebra over any field, not just the reals. So we can do linear algebra over a finite field.

Definition 11.13. *The **characteristic** of a ring R is the smallest non-zero integer n such that $n \cdot a = 0$ for every $a \in R$, if there is any such n; otherwise the characteristic is zero.*

Example 11.14. *$\mathbb{Z}_n$ has characteristic n; $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all have characteristic zero.*

Theorem 11.15. *If R is a ring with unity then the characteristic is the smallest n such that $n \cdot 1 = 0$ if there is any such n; otherwise the characteristic is zero.*

Proof. If $n \cdot 1$ is never zero then surely the characteristic is zero.

On the other hand if $n \cdot 1 = 0$ and there is no smaller n then surely the characteristic is at least n. If $a \in R$ then

$$\begin{aligned} n \cdot a &= a + a + \cdots + a \\ &= a1 + a1 + \cdots + a1 \\ &= a(1 + 1 + \cdots + 1) \\ &= a(n \cdot 1) \\ &= a0 \\ &= 0. \end{aligned}$$

Thus the characteristic is indeed n. $\square$