Abstract Algebra

Lachlan Dufort-Kennett

March 30, 2025

Contents

Preface

Chapter 1

Rings

1.1 Introduction

The objective of the field of abstract algebra is to create a general theory of algebraic structures so we can study algebraic properties of mathematical objects we are familiar with. Some examples of these are integers, real numbers, matrices, and polynomials. But what is an algebraic structure? An algebraic structure in its most basic form is a **set** of mathematical objects with some **operations** that act on the members of the set with some given constraints. In abstract algebra there are three main types of algebraic structure: **groups**, **rings**, and **fields**. These abstract structures generalise structures that we may be more familiar with such as the set of integers or matrices with addition and multiplication. Abstraction helps us investigate similarities and relationships between more familiar structures.

1.2 Binary relations

Binary relations are how we formalise relationships between elements of sets.

Definition 1.1. Let A and B be sets. Then a **binary relation** R over A and B is a subset of the Cartesian product of A with B. Let $(a, b) \in A \times B$. Then we say a is *R-related* to b and write $aRb \iff (a, b) \in R$.

Example 1.1. Let $D \subseteq \mathbb{N} \times \mathbb{P}$ be a binary relation on $\mathbb{N}$ and $\mathbb{P}$ - the set of prime numbers - given by $(n, p) \in D \iff n|p$. Clearly then, by definition the prime numbers, for any given prime p we have $(p, p) \in D$ and $(1, p) \in D$ and nothing else. So $D = \{(p, p) : p \in \mathbb{P}\} \cup \{(1, p) : p \in \mathbb{P}\}$.

Binary relations over a set and itself are called **homogeneous**. Homogeneous relations can be characterised by several different properties, of which we will now define some.

Definition 1.2. Let X be a set, $R \subseteq X^2$ a binary relation.

- R is **reflexive** $\iff \forall x \in X,\ xRx$.
- R is **symmetric** $\iff \forall x, y \in X,\ xRy \implies yRx$.

- R is **antisymmetric** $\iff \forall x, y \in X,\ xRy$ and $yRx \implies x = y$.
- R is **transitive** $\iff \forall x, y, z \in X, xRy$ and $yRz \implies xRz$.

A **function** (or **mapping**) is a type of binary relation and a **binary operation** is a type of function.

1.3 Rings

We now give the definition of a ring which is like a generalisation of the integers.

Definition 1.3. A **ring** is a set R equipped with two binary operations denoted $+$ and $\cdot$ (which we usually call "addition" and "multiplication") which have the following properties:

(i) $(a + b) + c = a + (b + c) \quad \forall a, b, c \in R$ \quad (+ is associative)

(ii) There exists an element in R denoted 0 such that $0 + a = a + 0 = a \quad \forall a \in R$ \quad (+ has an identity element)

(iii) $\forall a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$ \quad (each element in R has an additive inverse)

(iv) $a + b = b + a \quad \forall a, b \in R$ \quad (+ is commutative)

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$ \quad ($\cdot$ is associative)

(vi) There exists an element in R denoted 1 such that $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$ \quad ($\cdot$ has an identity element)

(vii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in R$ \quad ($\cdot$ distributes over +)

A note on closure: binary operations are closed by default, meaning that a ring is automatically closed under both $+$ and $\cdot$. This is the first thing we should check if we want to know if something is a ring. An observation we can make from the definition is that rings are non-empty by definition (they contain 0 and 1).

Let's now look at some consequences of the axioms. Let R be a ring and let $a_1, a_2, \dots, a_n \in R$. Then $a_1 + a_2 + \dots + a_n$ is a well-defined element in R through repeated use of the associativity axiom for addition (proof by induction). Similarly, repeated use of the commutativity axiom allows us to rearrange the terms. Brackets can also be removed in a product $a_1 \cdot a_2 \cdot \dots \cdot a_n$, although here we cannot rearrange the terms since multiplication is not necessarily commutative. Often, we don't write $\cdot$ to denote a multiplication and simply write it as a juxtaposition i.e. $ab \in R$.

Example 1.2. Let R be a ring and let $M_{n\times n}(R)$ be the set of $n \times n$ matrices with entries in R. Let $A \in M_{n\times n}(R)$ be denoted $[a_{ij}]$, $B \in M_{n\times n}(R) = [b_{ij}]$. Then we define two binary operations $+$ and $\cdot$ by

$$A + B = [a_{ij} + b_{ij}], \tag{1.1}$$

$$AB = [c_{ij}], \text{ where } c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}. \tag{1.2}$$

These are simply the familiar matrix addition and multiplication. We can now show that $M_{n\times n}(R)$ forms a ring with these operations.

First note that if A and B are $n \times n$ matrices over R, then $A+B$ and AB are also $n\times n$ matrices over R, so $M_{n\times n}(R)$ is closed under these operations. We can now verify each of the ring axioms:

A commutative ring is a ring R which satisfies

$$a \cdot b = b \cdot a \quad \forall a, b \in R \quad (\cdot \text{ is commutative}). \tag{1.3}$$

So a matrix ring like $M_{n\times n}(R)$ is not a commutative ring, but $\mathbb{Z}$ is.

Example 1.3. Let R be a ring. A **polynomial** over R is an expression

$$\sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{1.4}$$

where $n \geq 0$ and $a_1, a_2, \ldots, a_n \in R$. If i is the largest number such that $a_i \neq 0$, then we say that the polynomial has **degree** i. Two polynomials $\sum_{k=0}^{n} a_k x^2, \sum_{k=0}^{m} b_k x^2$ are defined to be equal if $a_i = b_i \; \forall i = 0, \ldots, \max\{n, m\}$.

We now define $R[x]$ to be the set of all polynomials over R. We can define the sum and product of two polynomials in the normal way we would expect; if $f(x) = \sum_{k=0}^{n} a_k x^k$ and $g(x) = \sum_{k=0}^{m} b_k x^k$, then

$$f(x) + g(x) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k)x^k \tag{1.5}$$

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ where } c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i}. \tag{1.6}$$

The last part comes from the distributive law. Just like matrices with entries in a ring, polynomials with coefficients in a ring also form a ring.

1.4 Subrings

Let R be a ring and let $S \in R$ such that S is a ring under the same operations on R. Then S is a **subring** of R.

Example 1.4. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is in turn a subring of $\mathbb{R}$. Similarly, $M_{n\times n}(\mathbb{Z})$ is a subring of $M_{n\times n}(\mathbb{Q})$ which is a subring of $M_{n\times n}(\mathbb{R})$ and $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$ which is a subring of $\mathbb{R}[x]$.

1.5 Fields

A field is simply an abstraction of the rational, real or complex numbers that we are used to, where we can add, substract, multiply and divide any numbers (except 0). A field can therefore be considered as a commutative ring with two additional properties.

Definition 1.4. A **field** is a commutative ring F, with operations $+$ and $\cdot$, which also satisfies two additional properties:

(i) $1 \neq 0$

(ii) $\forall a \in F$ with $a \neq 0$, there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (each nonzero element in F has a multiplicative inverse)

Chapter 2

Euclidean Domains & Factorisation

2.1 Divisors & GCD

Let a, b be integers. Then we say that a **divides** b, or a is a **divisor** of b, if $b = ac$ for some other integer c. We write $a|b$. Assuming one of a and b is not zero, then the greatest common divisor $d = \gcd(a, b)$ is defined as the largest integer that divides both a and b. If $\gcd(a, b) = 1$ then we say that a and b are coprime, meaning they have no common divisors (apart from 1).

Note that every integer divides 0, since $a \cdot 0 = 0$, so if $b \neq 0$ and $d|b$ then $|d| \leq b$. Thus if one of a and b are nonzero then there are finitely many common divisors and hence $\gcd(a, b)$ is well defined for any two integers. Also note that the set of divisors of b and $-b$ are the same since if $b = ac$, then $-b = a(-c)$. So $a|b \iff a|(-b)$. If $b \neq 0$, then $\gcd(b, 0) = |b|$. Finally note that $\gcd(a, b) = \gcd(b, a)$.

2.2 Euclidean Algorithm

We now describe a process for obtaining the greatest common divisor of two integers. This is known as the **Euclidean algorithm**. Let a, b be integers with $a \geq b > 0$.

1. Define $a_1 = a, b_1 = b$. Divide a_1 by b_1 to find quotient and remainder, $a_1 = b_1 q_1 + r_1$.
2. Repeat this step by defining $a_n = b_{n-1}, b_n = r_{n-1}$. Then once again divide a_n by b_1 to get $a_n = b_n q_n + r_n$.
3. Once we get $r_k = 0$ for some k, then $\gcd(a, b) = r_{k-1}$.

Let's verify that this algorithm actually works and finishes in a finite amount of time. First we will need a simple lemma.

> **Lemma** *Let $a = bq + r$ with $a \neq 0$. Then* $\gcd(a, b) = \gcd(b, r)$.

Proof. Since $a \neq 0$, b and r are not both zero. Hence we can define $d_1 = \gcd(a, b)$ and $d_2 = \gcd(b, r)$. Now we want to show that $d_1 = d_2$.

Note that by definition, $d_1|a$ and $d_1|b$, so $a = xd_1$ and $b = yd_1$ for some integers x and y. Then $r = a - bq = xd_1 - yd_1q = (x - yq)d_1$, so $d_1|r$ and $d_1 \leq d_2$ since $d_2 = \gcd(b, r)$. Also $d_2|b$ and $d_2|r$, so $d_2|bq + r = a$. Therefore $d_2 \leq d_1 = gcd(a, b)$. Hence $d_1 = d_2$. ■

Theorem 2.1 *The Euclidean algorithm works.*

Proof. Let a, b be integers with $a \geq b > 0$. Now apply the Euclidean algorithm. This generates a sequence of pairs of integers a_n, b_n defined by $a_1 = a$, $b_1 = b$, $a_n = b_{n-1}$, $b_n = r_{n-1}$, where $a_{n-1} = b_{n-1}q_{n-1} + r_{n-1}$ and $0 \leq r_{n-1} < b_{n-1}$. Observe that $b_n < b_{n-1}$, so the sequence of b_n is monotonically decreasing and since they are all positive, the sequence is finite. By applying the lemma to a_{n-1}, we see that

$$a_{n-1} = b_{n-1}q_{n-1} + r_{n-1} \implies \gcd(a_{n-1}, b_{n-1}) = \gcd(b_{n-1}, r_{n-1}) \tag{2.1}$$

$$= \gcd(a_n, b_n) \tag{2.2}$$

So $\gcd(a, b) = \gcd(a_1, b_1) = \cdots = \gcd(a_k, b_k)$. At step k, $r_k = 0$, so $a_k = b_kq_k$ and hence any integer dividing b_k will also divide a_k, therefore $\gcd(a_k, b_k) = b_k = r_{k-1}$. ■

2.3 Bezout's Identity

We make the following claim. Let $a, b \in \mathbb{Z}$, not both zero. Then there exists integers u, v such that $\gcd(a, b) = ua+vb$. If one of a and b is zero, say b, then $\gcd(a, b) = \gcd(a, 0) = a = 1 \cdot a + 0 \cdot b$. Also note that if $\gcd(a, b) = ua + vb$, then $\gcd(-a, b) = \gcd(a, b) = ua + vb = (-u)(-a) + vb$, and similarly for b, so we can assume without loss of generality that $a \geq b > 0$.

Lemma *The integers a_n, b_n that result from the Euclidean algorithm have the form $ua + vb$ for some integers u and v.*

Proof. We can prove this by induction on n.

Let $n = 1$. Then $a_1 = a = 1 \cdot a + 0 \cdot b$ and $b_1 = b = 0 \cdot a + 1 \cdot b$.

Now assume $a_{n-1} = ua + vb$ and $b_{n-1} = u'a + v'b$ with $u, v, u', v' \in \mathbb{Z}$. Then

$$a_n = b_{n-1} \tag{2.3}$$

$$b_n = r_{n-1} = a_{n-1} - b_{n-1}q_{n-1} \tag{2.4}$$

$$= (ua + vb) - (u'a + v'b)q_{n-1} \tag{2.5}$$

$$= (u - u'q_{n-1})a + (v - v'q_{n-1})b. \tag{2.6}$$

■

Using this lemma we can define a more powerful version of the Euclidean algorithm called the

Extended Euclidean algorithm. This algorithm not only finds the gcd, but also the integers u and v such that $\gcd(a, b) = ua + vb$.

Chapter 3

Equivalence Relations

3.1 Binary relation recap

We want some way of generalising the concept of equality for numbers as we know it. Looking at the properties for homogeneous binary relations (definition 1.2) that we defined before, we can see that equality satisfies the properties of **reflexivity**, **symmetry**, and **transitivity**.

Definition 3.1. An **equivalence relation** is a relation $\sim$ on a set A which satisfies the following properties:

(i) Reflexivity: $a \sim a \ \forall a \in A$

(ii) Symmetry: $a \sim b \implies b \sim a \ \forall a, b \in A$

(iii) Transitivity: $a \sim b$ and $b \sim c \implies a \sim c \ \forall a, b, c \in A$

Let's look at some relations and see if they satisfy the definition of equivalence.

Example 3.1. Consider the "divides" relation on $\mathbb{Z}$ that we studied in the last chapter.

- If $a \in \mathbb{Z}$, then $a = 1 \cdot a$, so $a|a$. Hence $|$ is reflexive.
- If $a|b$ and $b|c$ for $a, b, c \in \mathbb{Z}$, then for some x and y in $\mathbb{Z}$, $b = ax$ and $c = by = axy$, so $a|c$ and hence $|$ is transitive.
- However, it is easy to see that $|$ is not symmetric, for example, $1|2$ but $2\not|1$.

So $|$ is not an equivalence relation.

Example 3.2. Define a binary relation $\sim$ on $\mathbb{Z}$ by $a \sim b$ when $b - a$ is even for $a, b \in \mathbb{Z}$.

- If $a \in \mathbb{Z}$, then $a - a = 0$, which is even, so $a \sim a$ and $\sim$ is reflexive.
- Let $a, b \in \mathbb{Z}$ and suppose $a \sim b$. Then $b - a = 2x$ for some integer x, but then $a - b = -2x$ which is also even, so $b \sim a$ and $\sim$ is symmetric.

- Finally, let $a, b, c \in \mathbb{Z}$ and suppose $a \sim b$ ($b - a = 2x$) and $b \sim c$ ($c - b = 2y$) for two integers x and y. Then $c - a = (c - b) + (b - a) = 2y + 2x = 2(x + y)$, so $a \sim c$ and $\sim$ is transitive.

Therefore, $\sim$ is an equivalence relation.

Example 3.3. Let $A = \{(a, b) | a, b \in \mathbb{Z}, b \neq 0\}$. Then define a binary relation $\sim$ on $\mathbb{Z}$ by $(a, b) \sim (c, d)$ when $ad = bc$.

- Let $(a, b) \in A$, then $ab = ba$ since $\mathbb{Z}$ is a commutative ring, so $(a, b) \sim (a, b)$.
- Let $(a, b), (c, d) \in A$ with $(a, b) \sim (c, d)$. Then $ad = bc$. Hence $cb = da$ and $(c, d) \sim (a, b)$.
- Let $(a, b), (c, d), (e, f) \in A$ with $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. So $ad = bc$ and $cf = de$. Then $afd = (ad)f = (bc)f = b(cf) = b(de)$ and since $d \neq 0$, $af = bc$ so $(a, b) \sim (e, f)$.

Note that this example is equivalent to $\frac{a}{b} = \frac{c}{d}$, which is equality for rational numbers.

3.2 Equivalence classes

Definition 3.2. Let $\sim$ be an equivalence relation on a set A. If $a \in A$, then we define the **equivalence class** of a as

$$[a] = \{b \in A | a \sim b\}. \tag{3.1}$$

So $[a]$ contains all the elements of A that are related to a.

Theorem 3.1 (Properties of equivalence classes) *Let $\sim$ be an equivalence relation on a set A and let $a \in A$.*

(i) *$a \in [a]$.*

(ii) *A is the union of all the equivalence classes of $\sim$.*

(iii) *Let $b \in A$, then either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

Proof. Let $a \in A$.

(i) Since $\sim$ is an equivalence relation, it is reflexive, so $a \sim a$ and thus $a \in [a]$.

(ii) By (i), every element of A belongs to at least one equivalence class, hence (ii) is true.

(iii) Let $b \in A$. Suppose $[a] \cap [b] \neq \emptyset$. Then there exists $c \in [a] \cap [b]$. So $a \sim c$ and $b \sim c$ since c is in both $[a]$ and $[b]$. Since $\sim$ is symmetric, $c \sim b$. Since $\sim$ is transitive, $a \sim c$ and $c \sim b$ implies $a \sim b$ (and $b \sim a$). Now, let $x \in [a]$, so $a \sim x$. Then by transitivity, $b \sim a$ and $a \sim x$ impliy $b \sim x$, so $x \in [b]$. Therefore, $[a] \subseteq [b]$. Similarly, it can be shown that $[b] \subseteq [a]$, so $[a] = [b]$.

■

There are two things which we learn from this proof that actually strengthen the statements in the theorem.

Corollary 3.1.1 *Let $\sim$ be an equivalence relation on a set A and let $a, b \in A$.*

(i) *A is the **disjoint** union of the equivalence classes of $\sim$.*

(ii) *$[a] = [b]$ if and only if $a \sim b$ (or equivalently, $[a] \cap [b] = \emptyset \iff a \not\sim b$).*

3.3 Partitions

Now we will look at ways of partitioning a set into disjoint subsets.

Definition 3.3. Let A and I be sets. Let $P = \{B_i | i \in I\}$ be a collection of non-empty subsets of A indexed by I. Then P is called a **partition** of A if the following properties hold:

(i) $A = \bigcup_{i \in I} B_i$ (A is the union of all the sets in P).

(ii) $B_i \cap B_j = \emptyset$ for $i \neq j$ (any two distinct members of P are disjoint).

It is clear to see that for *any* given equivalence relation $\sim$, the equivalence classes divide the set A into a partition. In fact, it works in reverse as well.

Theorem 3.2 *Let A, I be sets and let $P = \{B_i | i \in I\}$ be a partiton of A. Define a binary relation $\sim$ by $a \sim b$ if a and b lie in the same part B_i of the partition. Then $\sim$ is an equivalence relation and B_i are exactly the equivalence classes of $\sim$.*

3.4 Modular Arithmetic

Let n be an integer greater than 1. Then we say that two integers a and b are **congruent modulo** n if $n | (b - a)$. We write $a \equiv b \mod n$. For example, when $n = 2$, $a \equiv b \mod 2$ when $b - a$ is even. Note $a \equiv 0 \mod n$ if and only if $n | a$. If two positive integers are congruent mod 10, then they have the same last digit (in base 10).

Theorem 3.3 *Congruency modulo n is an equivalence relation.*

Proof. Let $a, b, c \in \mathbb{Z}$.

(i) $a - a = 0 = n \cdot 0$, so $n | (a - a)$.

(ii) Suppose $a \equiv b \mod n$, so $b - a = nq$ for some integer q. Then $a - b = -nq = n(-q)$, so $n|(a-b)$ and $b \equiv a \mod n$.

(iii) Finally, suppose $a \equiv b \mod n$ and $b \equiv c \mod n$, so $b-a=nq$ and $c-b=np$ for two integers q and p. Then $c-a=c-b+b-a=np+nq=n(p+q)$, so $n|(c-a)$ and $a \equiv c \mod n$.

■

There are a couple of nice algebraic properties of congruence modulo n. These are properties which other equivalence relations might not respect.

Theorem 3.4 *Let $a,b,c,d \in \mathbb{Z}$ with $a \equiv b \mod n$ and $c \equiv d \mod n$.*

(i) $a+c \equiv b+d \mod n$.

(ii) $ac \equiv bd \mod n$.

(iii) $a+c \equiv b+c \mod n$.

(iv) $ac \equiv bc \mod n$.

Proof. First note that $b-a=nq$ and $d-c=np$ for two integers q and p.

(i) $(b+d)-(a+c)=b-a+d-c=nq+np=n(q+p)$, so $n|((b+d)-(a+c))$.

(ii) $bd-ac=bd-bc+bc-ac=b(d-c)+c(b-a)=bnp+cnq=n(bp+cq)$, so $n|(bd-ac)$.

(iii) and (iv) follow from the (i) and (ii) by setting $d=c$. ■

3.5 Quotient Structures

A powerful technique in abstract algebra is to use what we have been studying in this chapter to create smaller algebraic structures from larger ones while preserving some of the original structure. We start with some set X which is endowed with some mathematical structure (for example, X could be a ring, vector space, group, etc.). We then consider an equivalence relation on X which preserves this structure in the same way as in the above theorem (it respects the operations). Then we construct the same structure on the set of equivalence classes. This is called the **quotient structure**.

For example, we have the integers $\mathbb{Z}$ which form a commutative ring under normal addition and multiplication. Congruence modulo n is an equivalence relation which we have shown respects the operations. Can we define a ring structure on the set of equivalence classes of congruence modulo n? First we need to know what the equivalence classes actually are.

Theorem 3.5 *Congruence modulo n partitions $\mathbb{Z}$ into precisely n equivalence classes which are given by*

$$[r]=\{kn+r|k \in \mathbb{Z}\} \quad \textit{for } r=0,1,\ldots,n-1. \tag{3.2}$$

*We call these sets **congruence classes mod** n.*

Proof. Let $0 \leq r \leq n-1$, $a \in \mathbb{Z}$. Then

$$\begin{aligned} a \in [r] &\iff r \equiv a \mod n & (3.3)\\ &\iff n|(a-r) & (3.4)\\ &\iff a-r = nk \quad \text{for some integer } k & (3.5)\\ &\iff a = nk + r, & (3.6)\end{aligned}$$

hence $[r] = \{nk + r | k \in \mathbb{Z}\}$. Now we need to show that *all* integers belong to one of these equivalence classes.

Let $a \in \mathbb{Z}$. Divide a by n to get a quotient and remainder $a = nq + r$ for some $q, r \in \mathbb{Z}$ (remember that $0 \leq r \leq n-1$). Hence $a \in [r]$. So every integer belongs to one of the equivalence classes $[0], [1], \ldots, [n-1]$, so there are *at most* n equivalence classes. In order to show that there are *exactly* n, we need to show that they are distinct.

Let $0 \leq r, s \leq n-1$ and suppose $[r] = [s]$. Then $r \equiv s \mod n$, so $n|(s-r)$. But $-n < s - r < n$, so $s - r$ must be 0 and $s = r$. This shows that the equivalence classes are distinct and there are therefore exactly n of them. ■

Now that we have our equivalence classes we can work on defining addition and multiplication for the congruence classes. The easiest way to do this is to define them in terms of the representative element of the class, for example

$$\begin{aligned} [a] + [b] &= [a+b] & (3.7)\\ [a] \cdot [b] &= [ab]. & (3.8)\end{aligned}$$

However, these may not be well defined because the result of the operations depend on what the representative element of each class is. For example, in the case of $n = 3$, we want to show that $[1] + [2]$ and $[7] + [5]$ result in the same equivalence class.

Lemma *The operations defined above are well defined.*

Proof. Let a, c be two representatives of the same congruence class (so $[a] = [c]$ and $a \equiv c \mod n$). Let b, d be two representatives of another congruence class. Then by theorem 3.4:

$$\begin{aligned} a + b &\equiv c + d \mod n & (3.9)\\ ab &\equiv cd \mod n. & (3.10)\end{aligned}$$

So $[a+b] = [c+d]$ and $[ab] = [cd]$ and thus the operations are well defined. ■

We can now show that the set of congruence classes with these operations also forms a ring structure which is the same as the original set.

Theorem 3.6 *Let $n > 1 \in \mathbb{Z}$ The set $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ of congruence classes is a commutative ring under the operations of addition and multiplication defined above.*

Proof. We go step-by-step through the ring axioms. They are very simple to verify as they all follow from the fact that $\mathbb{Z}$ is itself a commutative ring.

(i) $([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] = [a]+[b+c] = [a]+([b]+[c]) \quad \forall a,b,c \in \mathbb{Z}$.

(ii) $[a]+[0] = [a+0] = [a] = [0+a] = [0]+[a] \quad \forall a \in \mathbb{Z}$.

(iii) $[a]+[-a] = [a+(-a)] = [0] \quad \forall a \in \mathbb{Z}$.

(iv) $[a]+[b] = [a+b] = [b+a] = [b]+[a] \quad \forall a,b \in \mathbb{Z}$.

(v) $([a]\cdot[b])\cdot[c] = [ab]\cdot[c] = [(ab)c] = [a(bc)] = [a]\cdot[bc] = [a]\cdot([b]\cdot[c]) \quad \forall a,b,c \in \mathbb{Z}$.

(vi) $[a]\cdot[1] = [a\cdot 1] = [a] = [1\cdot a] = [1]\cdot[a] \quad \forall a \in \mathbb{Z}$.

(vii) $[a]\cdot[b] = [ab] = [ba] = [b]\cdot[a] \quad \forall a,b \in \mathbb{Z}$.

(viii) $[a]\cdot([b]+[c]) = [a]\cdot[b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a]\cdot[b]+[a]\cdot[c] \quad \forall a,b,c \in \mathbb{Z}$ (and similarly for the right-distributivity).

■

Notice that what we have done is quite amazing. We have taken a commutative ring $\mathbb{Z}$ with infinitely many elements and "reduced" it down to a commutative ring $\mathbb{Z}/n\mathbb{Z}$ with only n elements! When we are working with this ring, we sometimes omit the brackets for the congruence classes and simply write them as numbers. For example, we write the elements of $\mathbb{Z}/3\mathbb{Z}$ as $\{0,1,2\}$ and $\mathbb{Z}/6\mathbb{Z}$ and $\{0,1,2,3,4,5\}$.

3.6 Multiplication Tables

One way to examine the structure of these finite rings is by looking at the addition and multiplication tables. Note that in $\mathbb{Z}/4\mathbb{Z}$, some elements don't have multiplicative inverses. For example, the equation $2a \equiv 1 \mod 4$ has no solutions in $\mathbb{Z}/4\mathbb{Z}$, so 2 has no multiplicative inverse. However, in $\mathbb{Z}/5\mathbb{Z}$, all elements have multiplicative inverses.

$$1^{-1} = 1, \quad 2^{-1} = 3, \quad 3^{-1} = 2, \quad 4^{-1} = 4. \tag{3.11}$$

Hence $\mathbb{Z}/5\mathbb{Z}$ is a field. It turns out that whenever n is a prime number, $\mathbb{Z}/n\mathbb{Z}$ is a field.

Theorem 3.7 *Let p be a prime number. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Proof. We know that $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring, so all that remains it to prove the final two field axioms.

(i) $1 \neq 0 \mod p$, so 1 is a valid multiplicative identity.

(ii) Let $a \in \mathbb{Z}$ such that $a \not\equiv 0 \mod p$. Since p is prime, $\gcd(a,p) = 1$. By Bezout's identity, there exists two integers u, v such that $ua + vp = 1$. Reducing mod p, we get $ua \equiv 1 \mod p$, hence $[u]$ is a multiplicative inverse of $[a]$ in $\mathbb{Z}/p\mathbb{Z}$.

■

Let's do an example of solving some modular arithmetic equations.

Example 3.4. Determine all solutions (if any) in the ring $\mathbb{Z}/49\mathbb{Z}$ of the following equations.

(i) $4x \equiv 9 \mod 49$. Observe that $\gcd(4, 49) = 1$. Using the extended Euclidean algorithm, we can see that $37(4) \equiv 1 \mod 49$. Hence 37 is a multiplicative inverse for 4 in $\mathbb{Z}/49\mathbb{Z}$, so if we multiply the equation on the left by 37 we will cancel out the 4.

$$37 \cdot 4x \equiv 37 \cdot 9 \mod 49 \tag{3.12}$$

$$x \equiv 39 \mod 49. \tag{3.13}$$

(ii) $7x \equiv 0 \mod 49$. Observe that $7x \equiv 0 \mod 49 \iff 49|7x \iff 7x = 49q$ for some integer q. Hence the solutions in $\mathbb{Z}/49\mathbb{Z}$ are 0, 7, 14, 21, 28, 35, and 42.

(iii) $7x \equiv 9 \mod 49$. Suppose x is a solution of the equation. Then multiplying on the left by 7 we get

$$7 \cdot 7x \equiv 49x \equiv 9 \mod 49 \tag{3.14}$$

$$\implies 0 \equiv 14 \mod 49. \tag{3.15}$$

This last implication is impossible, so the equation has no solutions in $\mathbb{Z}/49\mathbb{Z}$.

Chapter 4

Groups

4.1 What is a group?