MA377 Rings and Modules

Samir Siksek

Contents

CHAPTER 1

Introduction

These are my notes to MA377 Rings & Modules taught in 2019 and 2021. Thanks to everyone who pointed out errors in previous versions. Please let me know if you notice any errors (or see any shortcuts).

In addition to the notes, you might find it helpful to look at the following references.

- Warwick lecture notes for Introduction to Abstract Algebra, Algebra I and Algebra II.
- Dummitt & Foote, "Abstract Algebra". This is a hefty book with most things in it.
- Lecture notes by Marco Schlichting for this module (you'll find them in the UG Handbook for the year 2017). Our approach will be more hands on.

CHAPTER 2

Rings (Mostly Revision)

1. Definition

Recall the definition of a ring from MA136 and MA249:

Definition. A **ring** is a set R with two distinguished elements $0, 1 \in R$, and two binary operations

$$+ \ : \ R \times R \to R, \qquad \cdot \ : \ R \times R \to R,$$

such that

- $(R, +, 0)$ is an abelian group: thus
  - $a+0 = a = 0+a$ for all $a \in R$ (0 is the additive identity);
  - $a + (b + c) = (a + b) + c$ for all a, b, $c \in R$ (addition is associative);
  - for all $a \in R$ there is a unique $-a \in R$ such that $a + (-a) = (-a) + a = 0$ (a has an additive inverse);
  - $a + b = b + a$ for all a, $b \in R$ (addition is commutative);
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, $c \in R$ (multiplication is associative);
- $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$ (1 is the multiplicative identity);
- $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ (multiplication distributes over addition on the left and the right).

Example 1. You can check that $R = 0$ (the zero ring) is the only one for which $1 = 0$. For any other ring $1 \neq 0$.

Example 2. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ are rings with the usual addition and multiplication. For $n \geq 1$ an integer, we know that $\mathbb{Z}/n\mathbb{Z}$ is a ring.

For a ring R, the set of $n \times n$ matrices $M_n(R)$ with the usual matrix addition and multiplication forms a ring (there are some subtlties here about how to check associativity; we'll return to this later).

Definition. A ring is **commutative** if $ab = ba$ for all a, $b \in R$.

Example 3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ are all commutative rings.

If $R \neq 0$ (therefore $1 \neq 0$ inside R), then the ring $M_2(R)$ is not commutative, since

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

Definition. Let R be a ring. A subset $S \subseteq R$ is a **subring of** R if it is a ring with respect to the same operations and identity elements.

Lemma 4. *$S \subseteq R$ is a subring if and only if*

- *$0, 1 \in S$;*
- *$a + b \in S$ for all $a, b \in S$;*
- *$-a \in S$ for all $a \in S$;*
- *$ab \in S$ for all $a, b \in S$.*

Example 5. You can check that

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad : \quad a,\ b,\ d \in \mathbb{Z} \right\}$$

is a subring of $M_2(\mathbb{Z})$.

Example 6. We can make $\mathbb{R}^2$ into a ring by defining addition and multiplication componentwise

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2), \qquad (a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2).$$

The additive and multiplicative identity elements are $(0, 0)$ and $(1, 1)$ respectively. Let $S = \{(a, 0) : a \in \mathbb{R}\}$. Note this is closed under addition and multiplication, but is not a subring of $\mathbb{R}^2$ as it does not contain $(1, 1)$. It is true that S is a ring with multiplicative identity $(1, 0)$, and that it contained in $\mathbb{R}^2$, but it isn't a subring of $\mathbb{R}^2$.

2. Unit Groups and Fields

Let $R \neq 0$ be a ring. We call $u \in R$ a **unit** if there is some $v \in R$ such that $uv = vu = 1$. We write R^* for the set of units in R. In MA136 we proved that $(R^*, \cdot)$ is a group, which we called the **unit group**. In particular if $uv = vu = 1$ then v is unique and we write $v = u^{-1}$.

A **field** is a commutative ring $\neq 0$ in which every non-zero element is a unit. Thus if F is a field, then $F^* = F \setminus \{0\}$.

Example 7. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

$\mathbb{Z}$ is a commutative ring but not a field. Its unit group is $\mathbb{Z}^* = \{1, -1\}$.

Recall that $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime. For a prime p we shall write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ to stress that it is a field. This is an example of a finite field. We shall see other examples of finite fields later.

Example 8. Recall the Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \ : \ a,\ b \in \mathbb{Z}\}.$$

This is a commutative ring. In MA136 we checked this by showing that it is a subring of $\mathbb{C}$. Moreover, we computed $\mathbb{Z}[i]^*$ and found that $\mathbb{Z}[i]^* = \{1, i, -1, -i\}$ is a cyclic group of order 4 generated by i.

Exercise 9. What is $M_2(\mathbb{R})^*$? What is $M_2(\mathbb{Z})^*$?

Exercise 10. If S is a subring of R then S^* is a subgroup of R^*.

3. Integral Domains

Definition. Let R be a commutative ring. An element $x \neq 0$ is called a **zero divisor** if there is $y \neq 0$ in R such that $xy = 0$. An **integral domain** is a non-zero commutative ring that has no zero divisors.

Example 11. Any field is an integral domain. Moreover any subring of a field is an integral domain. For example, $\mathbb{Z}$ and $\mathbb{Z}[i]$ are integral domains.

$\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime (in which case $\mathbb{Z}/m\mathbb{Z}$ is a field). If m is composite then we can write $m = m_1 m_2$ where $1 < m_i < m$ and so $m_i + m\mathbb{Z} \neq 0$ but $(m_1 + m\mathbb{Z})(m_2 + m\mathbb{Z}) = 0$. Hence $m_1 + m\mathbb{Z}$, $m_2 + m\mathbb{Z}$ are zero divisors. Therefore $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain.

Lemma 12. *Every finite integral domain is a field.*

Proof. Let R be a finite integral domain and let a be a non-zero element in R. We would like to show that a is invertible. The sequence $a, a^2, a^3, \ldots$ must have repetition. Thus there are $n < m$ such that $a^m = a^n$. Thus $a^n(a^{m-n} - 1) = 0$. As $a \neq 0$ and R is an integral domain, $a^{m-n} = 1$. But $m - n \geq 1$, so a has an inverse in R, namely a^{m-n-1}. □

4. Polynomials

Let R be a commutative ring. Recall that $R[X]$ denotes the ring of polynomials in X with coefficients in R. It is important to be clear on what is and what is not a polynomial. A polynomial in X with coefficients in R has the form

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n, \qquad a_i \in R.$$

Expressions such at $1/X$ and $(X+1)/(X^2+1)$ are NOT polynomials. They are rational functions. A rational function is the ratio of two polynomials. Also the expression

$$1 + X + X^2 + X^3 + \cdots$$

is NOT a polynomial. It is an example of a powerseries in X. Polynomials have only finitely many terms.

Theorem 13. *Let R be a commutative ring. Then $R[X]$ is a commutative ring.*

Example 14. Let R be a commutative ring. Let's show that $R[X]$ is not a field. If $R = 0$ then $R[X] = 0$, so we may suppose R is the non-zero ring. Consider X. This is a non-zero element of $R[X]$. We will show that it doesn't have an multiplicative inverse in $R[X]$. Suppose it does, and let that multiplicative inverse be

$$f = a_0 + a_1 X + \cdots + a_n X^n, \qquad a_i \in R.$$

Then $Xf = 1$. This means

$$0 + a_0X + a_1X^2 + \cdots + a_nX^{n+1} = 1 + 0 \cdot X + 0 \cdot X^2 + \cdots + 0 \cdot X^{n+1}.$$

Comparing coefficients, we notice in particular that $1 = 0$, giving a contradiction. Hence X is not a unit in $R[X]$ and so $R[X]$ is not a field.

Exercise 15. Let K be a field. Show that $K[X]^* = K^*$. Before you start, let's think about what is being asked. In any ring R, the set R^* is the unit group of R; i.e. it is the set of units of R. Let $f \in K[X]$. Then f is a unit (i.e. in $K[X]^*$) if and only if there is some $g \in K[X]$ such that $fg = 1$. Start by showing that f and g both have degree 0.

Exercise 16. Show that $\overline{1}+\overline{2}X$ is a unit in $(\mathbb{Z}/4\mathbb{Z})[X]$. Why does this not contradict the previous exercise?

For a prime p, we shall write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$, when we want to stress that it is a field.

Exercise 17. Let p be a prime.

(a) How many monic polynomials of degree n are there in $\mathbb{F}_p[X]$?
(b) How many polynomials of degree at most n are there in $\mathbb{F}_p[X]$?
(c) How many polynomials of degree n are there in $\mathbb{F}_p[X]$?

The answers are p^n, p^{n+1} and $p^{n+1} - p^n$ respectively. What matters is giving your reasoning. [1]

5. Homomorphisms

Definition. Let R, S be rings. A function $\psi : R \to S$ is called a **homomorphism**, if

- $\psi(0) = 0$, $\psi(1) = 1$;
- $\psi(a + b) = \psi(a) + \psi(b)$ for all a, $b \in R$;
- $\psi(ab) = \psi(a)\psi(b)$ for all a, $b \in R$.

A bijective homomorphism is called an **isomorphism**.

Exercise 18. If ψ is a homomorphism, show that $\psi(-a) = -\psi(a)$.

Example 19. The map $\psi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by $\psi(a) = \overline{a}$ is a homomorphism. It is surjective but not injective ($\psi(m) = \psi(0)$).

Example 20. Let $a \in \mathbb{Z}$. The evaluation map $\psi : \mathbb{Z}[X] \to \mathbb{Z}$, $\psi(f(X)) = f(a)$ is a homomorphism. Note that $\psi(X) = \psi(a)$ so it is not injective. Is it surjective?

[1] If you're stuck, start with $p = 3$ and $n = 2$. A monic polynomial of degree 2 in $\mathbb{F}_3[X]$ has the form $X^2 + a_1X + a_0$ where a_0, $a_1 \in \mathbb{F}_3$. There are three possibilities for a_0 and three possibilities for a_1.

Example 21. Let R be a ring. Define

$$\psi : R \to M_2(R), \qquad \psi(a) = aI_2,$$

where I_2 is the 2×2 identity matrix. You can check that ψ is an injective homomorphism. Of course it is not surjective.

Example 22. Let $\psi : \mathbb{R}[X] \to \mathbb{R}[X]$ be given by $\psi(f(X)) = f'(X)$ (where f' denote the derivate of f). This is not a homomorphism of rings as it does not satisfy $\psi(fg) = \psi(f)\psi(g)$. However, it is homomorphism if we regard $\mathbb{R}[X]$ as an abelian group, or an $\mathbb{R}$-vector space (a homomorphism of vector spaces is the same as a linear transformation).

Exercise 23. Let R be a commutative ring. Let

$$\psi : R \to R, \qquad \psi(a) = a^2.$$

Show that ψ is a homomorphism if and only if $2 = 0$ in R. Can you give a non-commutative ring in which $2 = 0$ but ψ is not a homomorphism?

6. Ideals

Definition. Let R be a ring. A **left ideal** of R is a subset $\mathfrak{a} \subset R$ such that

- $\mathfrak{a}$ is a subgroup of $(R, +, 0)$;
- for all $r \in R$ and $a \in \mathfrak{a}$ we have $ra \in \mathfrak{a}$.

A **right ideal** of R is a subset $\mathfrak{a} \subset R$ such that

- $\mathfrak{a}$ is a subgroup of $(R, +, 0)$;
- for all $r \in R$ and $a \in \mathfrak{a}$ we have $ar \in \mathfrak{a}$.

A **2-sided ideal** of R is a subset that is both a left ideal and a right ideal.

Remarks.

- In Algebra II, the term *ideal* meant a 2-*sided ideal*.
- 0 and R are both 2-sided ideals for any ring R.
- A **proper** ideal is one which does not equal R.
- In a commutative ring, $\mathfrak{a}$ is left ideal iff it is a right ideal iff it is a 2-sided ideal. If R is a commutative ring we simply speak of ideals.

Example 24. $2\mathbb{Z}$ is **not** a subring of $\mathbb{Z}$ as $1 \notin \mathbb{Z}$, but it is an ideal.

Exercise 25. Let

$$\mathfrak{a} = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \quad : \quad a,\ c \in \mathbb{C} \right\}.$$

Show that $\mathfrak{a}$ is a left ideal of $M_2(\mathbb{C})$ but not a 2-sided ideal. Give a non-zero proper right ideal of $M_2(\mathbb{C})$. We shall show that $M_2(\mathbb{C})$ has no non-zero proper 2-sided ideals.

Exercise 26. Let I be an ideal of R (left, right or 2-sided). Show that I is proper if and only if $1 \notin I$. More generally, show that I is proper if and only if $I \cap R^* = \emptyset$.

Exercise 27. Let K be a field. Show that the only ideals of K are 0 and K itself.

Definition. Let A, B be subsets of a ring R. We define the product AB to be the set of all finite sums

$$\sum_{i=1}^{n} a_i b_i, \qquad a_i \in A,\ b_i \in B.$$

We interpret the empty sum with $n = 0$ as the 0. Thus $0 \in AB$.

Example 28. Let R be a ring and $a \in R$. Let $Ra = R\{a\}$. By definition, Ra is the set of all finite sums

$$\sum_{i=1}^{n} r_i a, \qquad r_i \in R.$$

But this can be rewritten as ra with $r = r_1 + \cdots + r_n \in R$. Thus

$$Ra = \{ra : r \in R\},$$

and likewise

$$aR = \{ar : r \in R\}.$$

It is easy to check that Ra is a left ideal and aR is a right ideal.

Note that $RaR = (Ra)R = R(aR)$ is the set of all finite sums

$$\sum_{i=1}^{n} r_i a s_i, \qquad r_i,\ s_i \in R.$$

It is easy to check that this is a 2-sided ideal of R. **It is not true that every element of RaR has the form ras, as following exercise shows**.

Exercise 29. Let

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad A' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

(i) Show that

$$M_2(\mathbb{R}) A M_2(\mathbb{R}) = M_2(\mathbb{R}).$$

(ii) Show that A' cannot be written in the form $A' = BAC$ with B, $C \in M_2(\mathbb{R})$.

Exercise 30. (i) Let I, J be left ideals of R. Show that $I \cap J$ and $I + J$ are left ideals (note $I + J = \{x + y : x \in I,\ y \in J\}$).

(ii) Suppose R is commutative. Recall that IJ is defined as the set of all finite sums

$$\sum_{i=1}^{n} x_i y_i, \qquad x_i \in I,\ y_j \in J.$$

Here we interpret the empty sum (with $n = 0$) as 0 (so $0 \in IJ$). Show that IJ is an ideal and that $IJ \subseteq I \cap J$.

(iii) Give a counterexample to show that $I \cup J$ need not be an ideal.

Definition. Let R be a commutative ring. An ideal $\mathfrak{a}$ of R is **principal** if it has the form $\mathfrak{a} = Ra = \{ra : r \in R\}$ for some $a \in R$.

Notation for ideals. If R is commutative, and $a \in R$, we write $(a) = Ra$ and call this the **(principal) ideal generated by** a. More generally, if $a_1, a_2, \ldots, a_n \in R$ we write

$$(a_1, a_2, \ldots, a_n) = Ra_1 + Ra_2 + \cdots + Ra_n$$

and call this **the ideal generated by** $a_1, \ldots, a_n$ (check that this is an ideal).

Exercise 31. Let R be a commutative ring. Let $\mathfrak{a} = (a_1, a_2, \ldots, a_m)$ and $\mathfrak{b} = (b_1, b_2, \ldots, b_m)$. Show that

$$\mathfrak{ab} = (a_i b_j \ :\ 1 \le i \le m,\ 1 \le j \le n).$$

Exercise 32. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \ :\ a,\ b \in \mathbb{Z}\}$. This ring has the property (which you can assume) that every ideal is either principal, or has two generators. The following two ideals are in fact principal. Check this and give their generators.

(i) $(1 - \sqrt{-5}, \sqrt{-5})$.
(ii) $(2, 1 + \sqrt{-5})^2$.

Example 33. Consider the ideal in $\mathbb{Z}[X]$:

$$\mathfrak{a} = (2, X) = 2 \cdot \mathbb{Z}[X] + X \cdot \mathbb{Z}[X].$$

Let's check that $\mathfrak{a}$ is not principal. So suppose it is, say $\mathfrak{a} = (f) = f \cdot \mathbb{Z}[X]$. Now $2 \in \mathfrak{a}$ so $f(X)$ is a factor of 2. Thus $2 = f(X)g(X)$ where $g(X) \in \mathbb{Z}[X]$. It follows that $f(X)$, $g(X)$ are constant polynomials, belonging to $\mathbb{Z}$. Hence $f(X) = \pm 1$ or ± 2. However $X \in \mathfrak{a}$ and therefore $f(X)$ is a factor of X; i.e. $X = f(X)h(X)$ where $h(X) \in \mathbb{Z}[X]$. Write

$$h(X) = a_0 + a_1 X + \cdots + a_n X^n, \qquad a_i \in \mathbb{Z}.$$

If $f(X) = \pm 2$, then $1 = \pm 2a_1$ (by comparing the coefficients of X in $f(X)h(X) = X$) and we get a contradiction. So $f(X) = \pm 1$. So $\mathfrak{a} = \mathbb{Z}[X]$ Hence $1 \in \mathfrak{a}$ and we can write

$$1 = 2u(X) + Xv(X), \qquad u(X),\ v(X) \in \mathbb{Z}[X].$$

Letting $X = 0$, we find that $1 = 2u(0)$ and $u(0) \in \mathbb{Z}$ giving a contradiction. Hence $\mathfrak{a}$ is not principal.

By contrast, in $\mathbb{Q}[X]$,

$$\mathfrak{b} = 2 \cdot \mathbb{Q}[X] + X \cdot \mathbb{Q}[X]$$

is principal. Indeed, $1/2 \in \mathbb{Q}[X]$ so $\mathfrak{b}$ contains $2 \cdot (1/2) = 1$ and so $\mathfrak{b} = \mathbb{Q}[X] = 1 \cdot \mathbb{Q}[X]$.

Exercise 34. Show that the ideal (X, Y) in $\mathbb{R}[X, Y]$ is not principal.

7. The Euclidean algorithm

In Foundations you saw division with remainder.

(I) Let m, $n \in \mathbb{Z}$ with $n \neq 0$. Then there are unique q, $r \in \mathbb{Z}$ such that

$$m = qn + r, \qquad 0 \leq r < |n|.$$

We call q the **quotient** and r the **remainder** obtained upon dividing m by n.

(II) Let K be a field. Let g, $f \in K[X]$ with $f \neq 0$. Then there are unique q, $r \in K[X]$ with

$$g = qf + r, \qquad r = 0 \quad \text{or} \quad \deg(r) < \deg(f).$$

We call q the **quotient** and r the **remainder** obtained upon dividing g by f. Some people define the degree of the zero polynomial to be $-\infty$. In that case they can simply write

$$g = qf + r, \qquad \deg(r) < \deg(f).$$

Example 35. Let $f = X^2 + 4X + 3$ and $g = X^4 + X^3 + 3X + 3$ in $\mathbb{F}_5[X]$. You can write $f = \overline{1}X^2 + \overline{4}X + \overline{3}$ and $g = \overline{1}X^4 + \overline{1}X^3 + \overline{3}X + \overline{3}$ if you want, but that's too pedantic for me. The important thing to remember is that we're working with the coefficients modulo 5. We do a long division to work out the quotient and remainder we obtain on dividing g by f:

$$\begin{array}{rrrrrr}
 & & & X^2 & +2X & +4 \\
\cline{3-6}
X^2+4X+3 \;) & X^4 & +X^3 & & +3X & +3 \\
 & X^4 & +4X^3 & +3X^2 & & \\
\cline{2-6}
 & & 2X^3 & +2X^2 & +3X & +3 \\
 & & 2X^3 & +3X^2 & +X & \\
\cline{3-6}
 & & & 4X^2 & +2X & +3 \\
 & & & 4X^2 & +X & +2 \\
\cline{4-6}
 & & & & X & +1
\end{array}$$

Make sure you can follow this calculation, and remember at all times that the coefficients are in $\mathbb{F}_5$. Hence the quotient is $q = X^2 + 2X + 4$ and the remainder is $r = X + 1$.

Exercise 36. Your turn! Let

$$f = X^3 + X + 1, \qquad g = X^5 + X^2 + 3$$

in $\mathbb{F}_7[X]$. Workout the quotient and remainder you obtain on dividing g by f.

Both (I) and (II) are the initial steps in Euclid's algorithm for computing the gcd (also called hcf), in $\mathbb{Z}$ and in $K[X]$. The following two theorems are among the most important consequences of Euclid's algorithm.

Theorem 37. *Let m, $n \in \mathbb{Z}$ (not both zero) and let $h = \gcd(m, n)$. Then there are u, $v \in \mathbb{Z}$ such that*

$$h = um + vn. \tag{1}$$

Theorem 38. *Let K be a field. Let f, $g \in K[X]$ (not both zero) and let $h = \gcd(f, g)$. Then there are u, $v \in K[X]$ such that*

$$h = uf + vg. \tag{2}$$

The identities (1) and (2) are often called Bezout identities. It's important to know how to determine the coefficients u, v. If you don't remember, revise Section 3.2 of your Foundations lecture notes (the extended Euclidean algorithm).

Example 39. Let f, g be as in Example 35. Let's follow the steps of the Euclidean algorithm to determine the gcd h and the coefficients u, v. We worked out that

$$X^4 + X^3 + 3X + 3 = (X^2 + 2X + 4)(X^2 + 4X + 3) + (X + 1). \tag{3}$$

Next we divide $X^2 + 4X + 3$ by $X + 1$ to obtain (you do the long division)

$$X^2 + 4X + 3 = (X + 3)(X + 1) + 0.$$

Since the last remainder is 0 we know that the gcd of f and g is the previous remainder which is $X + 1$. From (3)

$$\begin{aligned}\underbrace{X+1}_{h} &= 1 \cdot (X^4 + X^3 + 3X + 3) - (X^2 + 2X + 4)(X^2 + 4X + 3) \\ &= \underbrace{(4X^2 + 3X + 1)}_{u}\underbrace{(X^2 + 4X + 3)}_{f} + \underbrace{1}_{v} \cdot \underbrace{(X^4 + X^3 + 3X + 3)}_{g}.\end{aligned}$$

Theorem 40. *Let $m \geq 2$.*
(a) $(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{a} \ : \ a \in \mathbb{Z}$ and $\gcd(a, m) = 1\}$.
(b) $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime.

Proof. This was covered in Introduction to Abstract Algebra. But it is important to understand this, so we will revise the proof. Suppose $\gcd(a, m) = 1$. Then, by Theorem 37 there are u, $v \in \mathbb{Z}$ such that $ua + vm = 1$. Hence $\overline{u} \cdot \overline{a} = \overline{1}$ in $\mathbb{Z}/m\mathbb{Z}$. Therefore $\overline{a}$ is a unit and so belongs to $(\mathbb{Z}/m\mathbb{Z})^*$.

Suppose next that $a \in \mathbb{Z}$ such that $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. We want to show that $\gcd(a, m) = 1$. Since $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$ there $\overline{b}$ such that $\overline{a}\overline{b} = \overline{1}$. This

is the same as saying $ab-1$ is divisible by m. So $ab-1=km$ for some $k\in\mathbb{Z}$. Let $t=\gcd(a,m)$. Then t divides a and t divides m. So t divides $1=ab-km$. Hence $\gcd(a,m)=t=1$.

We now prove (b). What are we trying to show? What's a field? A field is a non-zero commutative ring where every non-zero element is a unit (i.e. has a multiplicative inverse). Suppose m is prime. Let $\overline{a}\neq\overline{0}$ in $\mathbb{Z}/m\mathbb{Z}$. Then $m\nmid a$. As m is prime, we have $\gcd(m,a)=1$. Hence by (b), $\overline{a}\in(\mathbb{Z}/m\mathbb{Z})^*$. Therefore every non-zero element of $\mathbb{Z}/m\mathbb{Z}$ is a unit and and so $\mathbb{Z}/m\mathbb{Z}$ is a field. Let's do the converse. We want to show that if m is composite then $\mathbb{Z}/m\mathbb{Z}$ is not a field. Well if m is composite then $m=m_1m_2$ where $1<m_1<m$ and $1<m_2<m$. Thus $\overline{m_1}\neq\overline{0}$ and $\gcd(m_1,m)=m_1\neq 1$ so $\overline{m_1}$ is non-zero but not a unit. Hence $\mathbb{Z}/m\mathbb{Z}$ is not a field if m is composite. □

Exercise 41. The proof of Theorem 40 in fact gives a method for computing inverses in $\mathbb{Z}/m\mathbb{Z}$. To check that $\overline{a}$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ we check that $\gcd(a,m)=1$. To compute the inverse all we do is find u, v, using Euclid's algorithm, so that $ua+vm=1$. Then $\overline{a}^{-1}=\overline{u}$. Compute $\overline{5}^{-1}$ in $\mathbb{Z}/17\mathbb{Z}$.

8. ED and PID

Definition. Let R be an integral domain. We say that R is a **Euclidean domain** (ED for short) if there is a function

$$\partial\ :\ R\setminus\{0\}\to\mathbb{N}$$

such that

(i) $\partial(ab)\geq\partial(b)$ for all a, $b\in R\setminus\{0\}$;
(ii) for all a, $b\in R$ with $b\neq 0$, there are q, $r\in R$ such that

$$a=qb+r,\qquad r=0\qquad\text{or}\qquad\partial(r)<\partial b.$$

We call q the **quotient** and r the **remainder** obtained on dividing a by b.

Example 42. $\mathbb{Z}$ is a Euclidean domain with $\partial a=|a|$. For a field K, the polynomial ring $K[X]$ is a Euclidean domain with $\partial f=\deg(f)$. In Algebra II you saw that $\mathbb{Z}[i]$ is Euclidean with $\partial(x+iy)=x^2+y^2$.

Definition. Let R be a commutative ring. Recall that an ideal $\mathfrak{a}$ of R is **principal** if it has the form $\mathfrak{a}=Ra=\{ra:r\in R\}$ for some $a\in R$.

A **principal ideal domain** (PID for short) is an integral domain in which every ideal is principal.

Example 43. In Example 33 we saw that the ideal $(2,X)$ in $\mathbb{Z}[X]$ is not principal. Hence $\mathbb{Z}[X]$ is not a PID.

In Exercise 34 you showed that the ideal (X,Y) in $\mathbb{R}[X,Y]$ is not principal. Hence $\mathbb{R}[X,Y]$ is not a PID.

Recall the following implication from Algebra II.

Theorem 44. *Any Euclidean domain is a principal ideal domain (ED $\implies$ PID).*

PROOF. Let R be a Euclidean domain, and let $\mathfrak{a}$ be an ideal of R. We want to show that $\mathfrak{a}$ is principal. If $\mathfrak{a} = 0$, then $\mathfrak{a} = (0)$ is principal. Suppose $\mathfrak{a} \neq 0$. Let $b \in \mathfrak{a}$ be the non-zero element such that $\partial(b)$ is as small as possible. We shall show that $\mathfrak{a} = (b)$. Note that $(b) = Rb$ is the set of all elements of the form cb with $c \in R$. As $b \in \mathfrak{a}$ and $\mathfrak{a}$ is an ideal we see that $cb \in \mathfrak{a}$ for all $c \in R$, and so $(b) \subseteq \mathfrak{a}$. Now let $a \in \mathfrak{a}$. Then $a = qb + r$ where q, $r \in R$, and either $r = 0$ or $\partial(r) < \partial(b)$. But, by definition, $\partial(b)$ is minimal among non-zero elements of $\mathfrak{a}$. Hence $r = 0$. Thus $a = qb \in (b)$. Therefore $\mathfrak{a} = (b)$, and so $\mathfrak{a}$ is principal. □

Example 45. Since $\mathbb{Z}$ and $K[X]$ (where K is any field) are Euclidean, they are therefore principal ideal domains. In fact, they are unique factorization domains. We won't revise what this means, but you know there is unique factorization in $\mathbb{Z}$ and $K[X]$. In particular, the concept of gcd (or hcf) makes sense in both. You should know the following recipe: if $a_1, \ldots, a_n \in R$ (where $R = \mathbb{Z}$ or $K[X]$), then

$$\underbrace{(a_1, \ldots, a_n)}_{\text{ideal generated by } a_1, \ldots, a_n} = Ra_1 + Ra_2 + \cdots + Ra_n = \underbrace{R\gcd(a_1, \ldots, a_n)}_{\text{principal ideal spanned by gcd}}.$$

Example 46. We've seen in Example 43 that $\mathbb{Z}[X]$ and $\mathbb{R}[X, Y]$ are not PIDs. We conclude from Theorem 44 that they are not Euclidean domains.

Example 47. Not every PID is a Euclidean domain. Let $w = (1 + \sqrt{-19})/2$ and let

$$R = \mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\}.$$

It is easy to show that R is an integral domain. It turns that R is a PID, but not Euclidean, although this is quite hard to show.

Example 48. You need to know the following two examples of PIDs: $\mathbb{Z}$ and $K[X]$ for any field K. These two rings are Euclidean. Recall that if R is Euclidean and $\mathfrak{a}$ is an ideal of R, then $\mathfrak{a} = Ra$ where a is the gcd of all the elements of $\mathfrak{a}$.

Exercise 49. Let K be a field. Show that $K[X, Y]$ is not a PID.

9. Cosets and Quotients

Definition. Let $\mathfrak{a}$ be an ideal of R (left, right, or 2-sided) and let $r \in R$. We call

$$r + \mathfrak{a} = \{r + a : a \in \mathfrak{a}\}$$

a **coset** of R. We let

$$R/\mathfrak{a} = \{r + \mathfrak{a} : r \in R\};$$

this is called the **quotient** of R by $\mathfrak{a}$.

Since R is an additive abelian group and $\mathfrak{a}$ is a subgroup, we know from MA136 that the quotient $R/\mathfrak{a}$ is an additive abelian group where addition is defined by

$$(r+\mathfrak{a})+(s+\mathfrak{a})=(r+s)+\mathfrak{a},$$

and the zero element is $\mathfrak{a}=0+\mathfrak{a}$. We recall also that

$$r+\mathfrak{a}=s+\mathfrak{a} \qquad \Longleftrightarrow \qquad r-s\in\mathfrak{a}. \tag{4}$$

In particular, $r+\mathfrak{a}$ is the zero coset if and only if $r\in\mathfrak{a}$.
Question: Can we define multiplication on $R/\mathfrak{a}$ in the natural way $(r+\mathfrak{a})(s+\mathfrak{a})=rs+\mathfrak{a}$? Does this make $R/\mathfrak{a}$ a ring? One problem with this definition is that the operation might not be well-defined. What does that mean? Well, the choice of representative r for the coset $r+\mathfrak{a}$ is not unique. For any $a\in\mathfrak{a}$ we know that $(r+a)+\mathfrak{a}=r+\mathfrak{a}$. We also know that for any $b\in\mathfrak{a}$ we have $(s+b)+\mathfrak{a}=s+\mathfrak{a}$. Thus we really want the following to hold: is

$$((r+a)+\mathfrak{a}))\cdot((s+b)+\mathfrak{a}))=rs+\mathfrak{a}.$$

This is equivalent to

$$(r+a)(s+b)-rs\in\mathfrak{a}.$$

We want this to be true for every r, $s\in R$ and a, $b\in\mathfrak{a}$. We claim that this is equivalent to $\mathfrak{a}$ being a 2-sided ideal. If $\mathfrak{a}$ is a 2-sided ideal then rb, as and $ab\in\mathfrak{a}$ hence

$$(r+a)(s+b)-rs=rb+as+ab\in\mathfrak{a}$$

as required. Conversely, suppose $(r+a)(s+b)-rs\in\mathfrak{a}$ for every r, $s\in R$ and a, $b\in\mathfrak{a}$. Letting $r=b=0$ we see that $as\in\mathfrak{a}$ for all $a\in\mathfrak{a}$ and $s\in R$. And letting $s=a=0$ instead, we see that $rb\in\mathfrak{a}$ for all $r\in R$ and $b\in\mathfrak{a}$. Therefore $\mathfrak{a}$ is 2-sided ideal.

Theorem 50. *Let $\mathfrak{a}$ be a 2-sided ideal of R. Then $R/\mathfrak{a}$ is a ring when addition and multiplication are defined by*

$$(r+\mathfrak{a})+(s+\mathfrak{a})=(r+s)+\mathfrak{a}, \qquad (r+\mathfrak{a}).(s+\mathfrak{a})=rs+\mathfrak{a}.$$

Moreover, the addition and multiplicative identity elements are respectively $0+\mathfrak{a}=\mathfrak{a}$ and $1+\mathfrak{a}$.

Proof. This is routine verification. For example associativity of multiplication for $R/\mathfrak{a}$ follows from associativity of multiplication for R. □

Example 51. If $\mathfrak{a}$ is a 2-sided ideal, then the map

$$R\to R/\mathfrak{a}, \qquad r\mapsto r+\mathfrak{a}$$

is a surjective homomorphism. We sometimes call this the **natural quotient map**.

Example 52. Let K be a field. Then $K[X]$ is an integral domain. Now let $I = K[X] \cdot (X^2 + X)$. This is the ideal consisting of all multiples of $X^2 + X$. Now the cosets

$$\alpha = X + I, \qquad \beta = (X + 1) + I$$

are non-zero because $X \notin I$ and $(X + 1) \notin I$. But

$$\alpha\beta = (X^2 + X) + I = 0 + I$$

as $X^2 + X \in I$. Hence α, β are zero divisors in $K[X]/I$, and $K[X]/I$ is not an integral domain.

10. Kernels, Images and the Isomorphism Theorem

Definition. Let $\psi : R \to S$ be a homomorphism of rings. We define the **kernel** of ψ to be

$$\mathrm{Ker}(\psi) = \{r \in R \ : \ \psi(r) = 0\}.$$

We define the **image** of ψ to be

$$\mathrm{Im}(\psi) = \{\psi(r) \ : \ r \in R\}.$$

Theorem 53 (The Isomorphism Theorem)**.** *Let $\psi : R \to S$ be a homomorphism of rings.*

(i) $\mathrm{Ker}(\psi)$ *is a 2-sided ideal of R.*
(ii) $\mathrm{Im}(\psi)$ *is a subring of S.*
(iii) The induced map

$$\hat{\psi} : R/\mathrm{Ker}(\psi) \to \mathrm{Im}(\psi), \qquad \hat{\psi}(r + \mathrm{Ker}(\psi)) = \psi(r)$$

is an isomorphism.

Proof. Routine verification. Or see your Algebra II lecture notes. □

Remarks.

- Some books call this "First Isomorphism Theorem", and give a Second Isomorphism Theorem and a Third Isomorphism Theorem. The other two isomorphism theorems are easy corollaries for the first one, and not worth learning.
- Some books just state that $R/\mathrm{Ker}(\psi)$ is isomorphic to $\mathrm{Im}(\psi)$ without giving the formula for the induced isomorphism $\hat{\psi}$ in terms of the original homomorphism ψ. This is really bad practice. You will need to know the formula.

Example 54. Define $\phi : \mathbb{R}[x] \to \mathbb{C}$ by $\phi(f) = f(i)$ (the elements of $\mathbb{R}[x]$ are polynomials, and to find the image of a polynomial f just substitute i in it). You can easily check that ϕ is a homomorphism.

Let's show that ϕ is surjective. Let $\alpha \in \mathbb{C}$. We can write $\alpha = a + bi$ where a, $b \in \mathbb{R}$. Now $\phi(a + bx) = a + bi = \alpha$. So ϕ is surjective.

What's the kernel? Suppose $f \in \mathrm{Ker}(\phi)$. Then $f(i) = 0$. We can write $f = a_n x^n + \cdots + a_0$ where $a_j \in \mathbb{R}$. Thus

$$a_n i^n + a_{n-1} i^{n-1} + \cdots + a_0 = 0.$$

Taking complex conjugates of both sides we have

$$\overline{a_n}\bar{i}^n + \overline{a_{n-1}}\bar{i}^{n-1} + \cdots + \overline{a_0} = 0.$$

But $\overline{a_j} = a_j$ and $\bar{i} = -i$ so

$$a_n(-i)^n + a_{n-1}(-i)^{n-1} + \cdots + a_0 = 0.$$

In otherwords, $-i$ is a root of f, just as i is a root of f. Hence $x^2+1 = (x-i)(x+i)$ is a factor of f. Conversely every multiple of x^2+1 is in the kernel. So $\mathrm{Ker}(\phi) = (x^2+1)$ (the principal ideal generated by x^2+1). The Isomorphism Theorem tells us that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ where the isomorphism is given by $f(x) + (x^2+1) \mapsto f(i)$.

Exercise 55. Often the easiest way to show that a subset of a ring is a 2-sided ideal is to find a homomorphism whose kernel is this set. Let I be the subset of $\mathbb{R}[X]$ consisting of all polynomials $a_0 + a_1 X + \cdots + a_n X^n$ with $a_0 + a_1 + \cdots + a_n = 0$.

(i) Show that I is a 2-sided ideal.
(ii) Show that $\mathbb{R}[X]/I \cong \mathbb{R}$.

11. Maximal Ideals

Definition. Let R be a commutative ring. We call a proper ideal $\mathfrak{m}$ **maximal** if there isn't any ideal $\mathfrak{a}$ satisfying

$$\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R.$$

In words, a proper ideal is maximal if and only if it is not properly contained in some other proper ideal.

Theorem 56. *Let R be a commutative ring. An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

Proof. Suppose $\mathfrak{m}$ is maximal. Let $a + \mathfrak{m} \neq 0$ (i.e. $a \notin \mathfrak{m}$). Then the ideal $aR + \mathfrak{m}$ strictly contains $\mathfrak{m}$ and so by definition of maximality equals R. In particular $1 \in aR + \mathfrak{m}$ and so $1 = ab + m$ where $b \in R$ and $m \in \mathfrak{m}$. But then $(a+\mathfrak{m})(b+\mathfrak{m}) = 1 - m + \mathfrak{m} = 1 + \mathfrak{m}$. Thus $R/\mathfrak{m}$ is a field. Conversely, suppose $R/\mathfrak{m}$ is a field. Let $\mathfrak{a}$ be a ideal properly containing $\mathfrak{m}$. Thus there is some element $a \in \mathfrak{a}$ with $a \notin \mathfrak{m}$. Hence $a + \mathfrak{m} \neq 0$ and is therefore invertible in the field $R/\mathfrak{m}$. In particular there is some $b \in R$ so that $(a+\mathfrak{m})(b+\mathfrak{m}) = 1 + \mathfrak{m}$. So $1 - ab \in \mathfrak{m} \subset \mathfrak{a}$. But $a \in \mathfrak{a}$ so $1 \in \mathfrak{a}$ so $\mathfrak{a} = R$ proving maximality of $\mathfrak{m}$. □

Exercise 57. Let m, n be non-zero elements of $\mathbb{Z}$. Show that

$$(m) \subseteq (n) \iff n \mid m.$$

Show that

$$(m) \subsetneq (n) \iff n \mid m \text{ and } m/n \neq \pm 1.$$

Example 58. Recall that $\mathbb{Z}$ is a PID (since it is Euclidean). Thus every ideal has the form $(m) = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. We want to know precisely when (m) is maximal. The zero ideal is not maximal since, for example, it is properly contained in the proper ideal $(2) = 2\mathbb{Z}$. So suppose that $m \neq 0$. Note that $(m) = (-m)$ so we suppose $m > 0$. Now from the above exercise, you can show that (m) is maximal if and only if m is prime.

This is consistent with Theorem 56 and what we know already: $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime.

Exercise 59. Let K be a field. Characterise the maximal ideals of $K[X]$ in a similar way to Example 58. If you get stuck see Theorem 65.

12. Quotients of Polynomial Rings

Let K be a field. We want to study quotients of $K[X]$. Since $K[X]$ is a PID, every ideal $\mathfrak{a}$ is principal. If $\mathfrak{a} = 0$ then $K[X]/\mathfrak{a} \cong K[X]$. Suppose $\mathfrak{a} \neq 0$. Then $\mathfrak{a} = (f)$ where $f \in K[X]$ is a non-zero polynomial. If f has degree 0, then f is a unit and $\mathfrak{a} = K[X]$ and then $K[X]/\mathfrak{a}$ is the zero ring. So we shall suppose $\mathfrak{a} = (f) = fK[X]$ where $f \in K[X]$ has positive degree. What we really would like to bring out in this section is the analogy between $K[X]/fK[X]$ and the familiar ring $\mathbb{Z}/m\mathbb{Z}$. Note that ideal $m\mathbb{Z}$ consists of all multiples of m, and the ideal $fK[X]$ consists of all the multiples of f. We can ease notation by writing $\overline{g} = g + fK[X]$. For g_1, $g_2 \in K[X]$, we say that $g_1 \equiv g_2 \pmod{f}$ if and only if $f \mid (g_1 - g_2)$. Note the meaning of equality in $K[X]/fK[X]$ (see (4)):

$$\begin{aligned} \overline{u} = \overline{v} &\iff u - v \in fK[X] \\ &\iff f \mid (u - v) \\ &\iff u \equiv v \pmod{f}. \end{aligned} \tag{5}$$

We recall also that every element of $\mathbb{Z}/m\mathbb{Z}$ has a 'canonical form'. It must be equal to a unique class $\overline{r} = r + m\mathbb{Z}$ where $r = 0, 1, \ldots, m-1$. Given $\overline{a}$ in $\mathbb{Z}/m\mathbb{Z}$ we obtain the canonical form $\overline{r} = \overline{a}$ by simply writing $a = qm + r$ (using division with remainder) where q, $r \in \mathbb{Z}$ and $0 \leq r < m$. Division with remainder works in $K[X]$ and gives us a canonical form for elements of $K[X]/fK[X]$.

Lemma 60. *Let K be a field and $f \in K[X]$ with $\deg(f) = n \geq 1$. Every element $\overline{g} \in K[X]/fK[X]$ is equal to $\overline{r} = r + fK[X]$ for some unique $r \in K[X]$ with $\deg(r) < \deg(f)$. Moreover, r is the remainder obtained on dividing g by f.*

Proof. Using division with remainder we may write $g = qf + r$ where q, $r \in K[X]$ with $\deg(r) < \deg(f)$. Note that $g - r = qf \in fK[X]$ hence $\overline{g} = \overline{r}$. We want to prove uniqueness of r. Suppose $\overline{g} = \overline{s}$ where $s \in K[X]$ and $\deg(s) < \deg(f)$. Since $\overline{r} = \overline{g} = \overline{s}$ we have

$f \mid (r-s)$. But $\deg(r-s) < \deg(f)$ since the polynomials r, s have degree $< \deg(f)$. The only polynomial divisible by f that has degree smaller than f is the zero polynomial. Thus $r - s = 0$ and so $r = s$, proving uniqueness. □

Thus when working in the quotient ring $K[X]/fK[X]$ we always simplify by taking the remainder modulo f.

Example 61. Let $f = X^2 + X + 1$, $g_1 = X + 3$ and $g_2 = X - 4$ in $\mathbb{R}[X]$. We will compute $\overline{g_1} \cdot \overline{g_2}$ in $\mathbb{R}[X]/f\mathbb{R}[X]$. By definition, this is the class of

$$g_1 g_2 = (X+3)(X-4) = X^2 - X - 12.$$

But we don't stop here. We would like to simplify by dividing $g_1 g_2$ by f and taking the remainder. Note that

$$g_1 g_2 = qf + r, \qquad q = 1, \quad r = -2X - 13$$

where q is the quotient and r is the remainder. So

$$\overline{g_1} \cdot \overline{g_2} = \overline{-2X - 13}$$

in $\mathbb{R}[X]/f\mathbb{R}[X]$.

Example 62. Let $f = X^2 + 2X + 2$, $g_1 = 2X + 3$ and $g_2 = X + 3$ in $\mathbb{F}_7[X]$. We will compute $\overline{g_1} \cdot \overline{g_2}$ in $\mathbb{F}_7[X]/f\mathbb{F}_7[X]$. By definition, this is the class of

$$g_1 g_2 = (2X+3)(X+3) = 2X^2 + 9X + 9 = 2X^2 + 2X + 2$$

as the coefficients are in $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. But we don't stop here. We would like to simplify by dividing $g_1 g_2$ by f and taking the remainder. Note that

$$g_1 g_2 = qf + r, \qquad q = 2, \quad r = 5X + 5$$

where q is the quotient and r is the remainder. So

$$\overline{g_1} \cdot \overline{g_2} = \overline{5X + 5}$$

in $\mathbb{F}_7[X]/f\mathbb{F}_7[X]$.

Exercise 63. Your turn! Let $f = X^2 + 2X + 2$, $g_1 = 2X + 3$ and $g_2 = X + 3$ in $\mathbb{F}_5[X]$. Compute $\overline{g_1} \cdot \overline{g_2}$ in $\mathbb{F}_5[X]/f\mathbb{F}_5[X]$.

Exercise 64. Let p be a prime, and let $f \in \mathbb{F}_p[X]$ have degree $n \geq 1$. Compute $\#\mathbb{F}_p[X]/f\mathbb{F}_p[X]$. You will need Lemma 60 and also your answer to Exercise 17. The answer is p^n, but what matters is your justification.

13. Quotients by Irreducible Polynomials Yield Fields

Theorem 65. *Let K be a field and $f \in K[X]$ have degree ≥ 1.*
(a) $(K[X]/fK[X])^* = \{\overline{g} \,:\, g \in K[X] \text{ and } \gcd(f,g) = 1\}$.
(b) The following are equivalent:
(i) f is irreducible
(ii) $fK[X]$ is a maximal ideal.
(iii) $K[X]/fK[X]$ is a field.

Proof. This should remind you of Theorem 40. I recommend that you read the proof of Theorem 40 again, and then try to prove this theorem on your own.

Suppose $\gcd(f,g) = 1$. By Euclid's algorithm (Theorem 38) there are $u, v \in K[X]$ such that $uf + vg = 1$. Hence $\overline{vg} = \overline{1}$ in $K[X]/fK[X]$. Therefore $\overline{g}$ is a unit and so belongs to $(K[X]/fK[X])^*$.

Suppose next that $g \in K[X]$ such that $\overline{g} \in (K[X]/fK[X])^*$. We want to show that $\gcd(f,g) = 1$. Since $\overline{g} \in (K[X]/fK[X])^*$ there exists $\overline{h}$ such that $\overline{g}\overline{h} = \overline{1}$. This is the same as saying $gh - 1$ is divisible by f. So $gh - 1 = kf$ for some $k \in K[X]$. Let $t = \gcd(f,g)$. Then t divides f and t divides g. So t divides $1 = gh - kf$. Hence $t = 1$. This proves (a). [2]

Next we prove (b). For this we'll show (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (i). Suppose f is irreducible. We want to show that $fK[X]$ is maximal. Suppose $fK[X] \subseteq \mathfrak{a}$ where $\mathfrak{a}$ is an ideal of $K[X]$. As $K[X]$ is a PID, $\mathfrak{a} = gK[X]$ for some polynomial. Note that $f \in gK[X]$ and so $g \mid f$. But f is irreducible. Thus $g = c$ or $g = cf$ where $c \in K^*$. If $g = c$ then $\mathfrak{a} = gK[X] = K[X]$. If $g = cf$ then $\mathfrak{a} = gK[X] = fK[X]$. Thus the only ideals containing $fK[X]$ are $fK[X]$ and $K[X]$, so $fK[X]$ is maximal. This shows (i) implies (ii). Note (ii) implies (iii) by Theorem 56. Finally, lets show that (iii) implies (i). Suppose f is reducible. Therefore $f = f_1 f_2$ where $0 < \deg(f_1) < \deg(f)$ and $0 < \deg(f_2) < \deg(f)$. Then $f \nmid f_1$ and so $\overline{f_1} \neq \overline{0}$. Moreover, $\gcd(f, f_1) = f_1 \neq 1$, so $\overline{f_1}$ is not a unit. Hence if f is composite, then $K[X]/fK[X]$ has a non-zero element which is not a unit and so is not a field. Thus if $K[X]/fK[X]$ is a field then f is irreducible. □

Exercise 66. The proof of Theorem 65 in fact gives a method for computing inverses in $K[X]/fK[X]$. To check that $\overline{g}$ is a unit in $K[X]/fK[X]$ we check that $\gcd(f,g) = 1$. To compute the inverse all we do is find u, v, using Euclid's algorithm, so that $uf + vg = 1$. Then $\overline{g}^{-1} = \overline{v}$. Compute $\overline{X+1}^{-1}$ in $\mathbb{F}_2[X]/(X^2 + X + 1)\mathbb{F}_2[X]$.

Exercise 67. Let $f = X^4 + X^2 + 1 \in \mathbb{F}_5[X]$.
(a) Write f as a product of monic irreducible factors.

[2] Actually $t \in K[X]$ divides 1 implies that t has degree 0. However, we follow the convention that the gcd of two polynomials is taken to be monic. Thus $t = 1$.

(b) Let $g(X) = X + b \in \mathbb{F}_5[X]$ where $b \neq 0$. Show that $g(X) + f\mathbb{F}_5[X]$ is a unit in $\mathbb{F}_5[X]/f\mathbb{F}_5[X]$.
(c) Give a zero divisor in $\mathbb{F}_5[X]/f\mathbb{F}_5[X]$.

14. Finite Fields

A finite field is (you guessed it) simply a field which has finitely many elements. An example of a finite field is $\mathbb{F}_p$ with p prime.

Is there a field with 4 elements? Note that $\mathbb{Z}/4\mathbb{Z}$ is a ring with 4 elements but it is not a field. Let $f \in \mathbb{F}_2[X]$ be a quadratic polynomial. Then $\mathbb{F}_2[X]/f\mathbb{F}_2[X]$ has $2^2 = 4$ elements. Is this a field? For this to be a field we want f to be irreducible by Theorem 65. Is there an irreducible, quadratic polynomial in $\mathbb{F}_2[X]$? This is easy to discover. A quadratic polynomial in $\mathbb{F}_2[X]$ has the form $a_2X^2 + a_1X + a_0$ where $a_i \in \mathbb{F}_2$ and $a_2 \neq 0$. Thus the only quadratic polynomials are

$$X^2, \qquad X^2 + X, \qquad X^2 + 1, \qquad X^2 + X + 1.$$

The first three are composite:

$$X^2 = X \cdot X, \qquad X^2 + X = X(X + 1), \qquad X^2 + 1 = (X + 1)^2$$

where the last one is true since $2X = 0X = 0$ in $\mathbb{F}_2[X]$. What about $X^2 + X + 1$. That is irreducible. How do we check that? If it factors then it is the product of two degree 1 polynomials (which could be the same). The only degree 1 polynomials in $\mathbb{F}_2[X]$ are X and $X + 1$. We can just do an exhaustive check and convince ourselves that X^2+X+1 is irreducible. [3] Hence $\mathbb{F}_2[X]/(X^2 + X + 1)$ is a field with 4 elements. We denote this field by $\mathbb{F}_4$.

Here are some facts about finite fields. These might be proved in Galois theory. We won't prove them in this module, but you should be aware of them.

- A finite field necessarily has p^n elements, for some prime p, and some $n \geq 1$.
- If two finite fields have the same number of elements p^n then they are isomorphic. We write $\mathbb{F}_{p^n}$ for any finite field with p^n elements.
- $\mathbb{F}_{p^n}$ is an $\mathbb{F}_p$-vector space of dimension n (more on this below).
- The unit group $\mathbb{F}_{p^n}^*$ is cyclic.

Exercise 68. A finite field with p^n elements is denoted by $\mathbb{F}_{p^n}$. Let $\alpha \in \mathbb{F}_{p^n}$. Show that $\alpha^{p^n} = \alpha$. Hint: of course this is true for $\alpha = 0$, so

[3] You could also say that a quadratic polynomial is reducible iff it has a root. The only possible roots are 0 and 1 (the elements of $\mathbb{F}_2$). Substituting 0 and 1 in $X^2 + X + 1$ we see that neither is a root. So $X^2 + X + 1$ is irreducible in $\mathbb{F}_2[X]$. Could we instead use the quadratic formula? Not here! Remember that the quadratic formula involves dividing by 2. But $2 = 0$ in $\mathbb{F}_2$, so the quadratic formula will not work.

you can suppose that $\alpha \in \mathbb{F}_{p^n}^*$, which as you know is a group of order ...

15. Computing in Finite Fields

Let p be a prime, and let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree n. We know that $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$ is a field (Theorem 65) with p^n elements (Exercise 64), and we denote this field by $\mathbb{F}_{p^n}$. We want to know how to compute in $\mathbb{F}_{p^n}$. To simplify things, let's write

$$\theta = \overline{X} = X + f\mathbb{F}_p[X].$$

Theorem 69. *Every element of $\mathbb{F}_{p^n}$ can be written uniquely as*

$$c_0 + c_1\theta + c_2\theta^2 + \cdots + c_{n-1}\theta^{n-1} \tag{6}$$

where $c_i \in \mathbb{F}_p$.

Proof. Recall Lemma 60: every element of $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$ has the form $\overline{r}$ for some unique $r \in \mathbb{F}_p[X]$ with degree $\deg(r) < n$. Thus $r = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ where $c_i \in \mathbb{F}_p$. Therefore

$$\overline{r} = c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1} = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}.$$

□

The theorem is saying that every element of $\mathbb{F}_{p^n}$ can be written as a linear combination of $1, \theta, \ldots, \theta^{n-1}$ with coefficients in $\mathbb{F}_p$, in a unique way. You can now convince yourself that $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_p$, of dimension n, with basis $1, \theta, \ldots, \theta^{n-1}$.

Exercise 70. $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)\mathbb{F}_2[X]$ has four elements 0, 1, θ, $1+\theta$. Do an addition table and a multiplication table for $\mathbb{F}_4$. I'll help you out with one multiplication. Let's compute $\theta(1+\theta)$. This is the same as $\theta + \theta^2$. We don't stop here. This must be equal to one of our four canonical representations 0, 1, θ, $1+\theta$ but we don't know which yet. We want to work that out. Recall $\theta = \overline{X}$. So $\theta + \theta^2 = \overline{X + X^2}$. We do division with remainder: $X^2 + X = 1(X^2 + X + 1) + 1$. Hence $\theta + \theta^2 = 1$.

Let's talk a little bit more about how to do computations in $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/f\mathbb{F}_p[X]$, where $f \in \mathbb{F}_p[X]$ is irreducible of degree n. For simplicity, we will assume that f is monic, and write

$$f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n.$$

Then

$$X^n \equiv -a_0 - a_1X - \cdots - a_{n-1}X^{n-1} \pmod{f}$$

which we can also write as

$$\overline{X}^n = -a_0 - a_1\overline{X} - \cdots - a_{n-1}\overline{X}^{n-1}.$$

This is the same as

$$\theta^n = -a_0 - a_1\theta - \cdots - a_{n-1}\theta^{n-1}. \tag{7}$$

The relation (7) is key to doing multiplication in $\mathbb{F}_{p^n}$. Let

$$\gamma = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}, \qquad \delta = d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1}$$

be two elements of $\mathbb{F}_{p^n}$ where the coefficients c_i, d_i belong to $\mathbb{F}_p$. Then

$$\gamma + \delta = (c_0 + d_0) + (c_1 + d_1)\theta + \cdots + (c_{n-1} + d_{n-1})\theta^{n-1}.$$

That is, if we're doing addition we simply add the coefficients which are elements of $\mathbb{F}_p$; addition is easy. Now let's think about multiplication

$$\gamma\delta = (c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1})(d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1}).$$

We expand the brackets, and collect like terms. This will give us $\gamma\delta$ as a linear combination of $1, \theta, \theta^2, \ldots, \theta^{2n-2}$ with coefficients in $\mathbb{F}_p$. We want $\gamma\delta$ as a linear combination of $1, \theta, \ldots, \theta^{n-1}$ with coefficients in $\mathbb{F}_p$. If there is a θ^n term then that's easy to eliminate, because relation (7) gives us θ^n in terms of lower powers of θ. What if we find a θ^{n+1} term? Well

$$\begin{aligned}\theta^{n+1} &= \theta(-a_0 - a_1\theta - \cdots - a_{n-1}\theta^{n-1}) \\ &= -a_0\theta - a_1\theta^2 - \cdots - a_{n-2}\theta^{n-1} - a_{n-1}\theta^n \\ &= -a_1\theta - a_1\theta^2 - \cdots - -a_{n-2}\theta^{n-1} - a_{n-1}(-a_0 - a_1\theta - \cdots - a_{n-1}\theta^{n-1}).\end{aligned}$$

Expanding brackets and collecting terms gives us θ^{n+1} as a linear combination of $1, \theta, \ldots, \theta^{n-1}$. We can just keep going. To summarize, to compute products in $\mathbb{F}_{p^n}$ what we need to work out what $\theta^n, \theta^{n+1}, \ldots, \theta^{2n-2}$ are as linear combinations $1, \theta, \ldots, \theta^{n-1}$. Once we have these, we can use them to multiply any two elements of $\mathbb{F}_{p^n}$.

Exercise 71. Let $f = X^3 + 3X + 3 \in \mathbb{F}_5[X]$. Check that f is irreducible [4].

We work in $\mathbb{F}_{5^3} = \mathbb{F}_5[X]/f\mathbb{F}_5[X]$. Here every element is a linear combination of $1, \theta, \theta^2$ with coefficients in $\mathbb{F}_5$. The field $\mathbb{F}_{5^3}$ has 125 elements, and no sane person would want to write out a multiplication table for this field. Write down θ^3 and θ^4 as linear combinations of $1, \theta, \theta^2$. Use this to compute the product

$$(1 + \theta^2)(3 + \theta + \theta^2).$$

I get θ^2, but don't take my word for it. I'm OK with making mistakes myself as I don't have to sit exams anymore.

Exercise 72. Let f be as in Exercise 71. Let

$$T : \mathbb{F}_{5^3} \to \mathbb{F}_{5^3}, \qquad T(\alpha) = (1 + \theta) \cdot \alpha.$$

[4] Hint! Let $f \in K[X]$ where K is a field, and suppose f is quadratic or cubic. Convince yourself that f is reducible in $K[X]$ if and only if f has a root in K. For infinite fields this fact is less useful as we can't run through the elements of K and check them one by one. But for a finite field such as $\mathbb{F}_5$ we can run through the elements and check if they're roots of f. While we're on the subject, if we have a quartic polynomial $f \in K[X]$, then it can be reducible but without having roots in K. Write down an example.

(a) Check that T is an $\mathbb{F}_5$-linear transformation.
(b) Show that T is an isomorphism of $\mathbb{F}_5$-vector spaces.
(c) Write down the matrix M for T with respect to the basis $1, \theta, \theta^2$.
(d) Compute the characteristic polynomial χ of M. Check that $\chi(1+\theta) = 0$. If you want an explanation for this, look up the Cayley–Hamilton theorem.

CHAPTER 3

More Rings

1. The Correspondence Theorem for Rings

Theorem 73. *Let $\mathfrak{a}$ be a 2-sided ideal of R, and let $\psi : R \to R/\mathfrak{a}$ be the natural quotient map.*

(i) Let J be a 2-sided ideal of $R/\mathfrak{a}$. Then $\psi^{-1}(J)$ is 2-sided ideal of R containing $\mathfrak{a}$.

*(ii) (**The Correspondence Theorem**) Let $\mathcal{I}$ be the set of 2-sided ideals of R containing $\mathfrak{a}$. Let $\mathcal{J}$ be the set of 2-sided ideals of $R/\mathfrak{a}$. Then the map*

$$\mathcal{J} \to \mathcal{I}, \qquad J \mapsto \psi^{-1}(J)$$

is a bijection.

Proof. (i) Write $I = \psi^{-1}(J)$. Want to show that I is a 2-sided ideal of R containing $\mathfrak{a}$. Note that $0 + \mathfrak{a} \in J$ and $\psi(0) = 0 + \mathfrak{a}$. Thus $0 \in \psi^{-1}(J) = I$. Suppose $a, b \in I$. Then $\psi(a) = a+\mathfrak{a}$ and $\psi(b) = b+\mathfrak{a} \in J$. As J is an ideal, $\psi(a + b) = (a + b) + \mathfrak{a} = (a + \mathfrak{a}) + (b + \mathfrak{a}) \in J$. Hence $a + b \in \psi^{-1}(J) = I$. Thus $(I, 0)$ is a subgroup of $(R, +)$.

Now let $a \in I$ and $r \in R$. Then $a+\mathfrak{a} = \psi(a) \in J$. As J is a 2-sided ideal, $(r+\mathfrak{a})(a+\mathfrak{a}) \in J$ and $(a+\mathfrak{a})(r+\mathfrak{a}) \in J$. Thus $\psi(ra) = ra+\mathfrak{a} \in J$ and $\psi(ar) = ar + \mathfrak{a} \in J$. Hence ra, $ar \in \psi^{-1}(J) = I$. Thus I is a 2-sided ideal as required.

Next we want to show that $\mathfrak{a} \subseteq I$. Let $a \in \mathfrak{a}$. Then $\psi(a) = a + \mathfrak{a} = 0 + \mathfrak{a} \in J$. Hence $a \in \psi^{-1}(J)$. Therefore $\mathfrak{a} \subseteq I$.

(ii) Before we prove (ii), let's check that $\psi(\psi^{-1}(J)) = J$. By definition of ψ^{-1}, $\psi(\psi^{-1}(J)) \subseteq J$. Let $a + \mathfrak{a} \in J$. Then $\psi(a) = a + \mathfrak{a} \in J$. So $a \in \psi^{-1}(J)$. Thus $a + \mathfrak{a} = \psi(a) \in \psi(\psi^{-1}(J))$. Hence $J \subseteq \psi(\psi^{-1}(J)$. Therefore $\psi(\psi^{-1}(J)) = J$.

Write

$$\mu : \mathcal{J} \to \mathcal{I}, \qquad \mu(J) = \psi^{-1}(J).$$

We want to check that μ is injective. Suppose J_1, $J_2 \in \mathcal{J}$ with $\mu(J_1) = \mu(J_2)$. That is, $\psi^{-1}(J_1) = \psi^{-1}(J_2)$. Then $J_1 = \psi(\psi^{-1}(J_1)) = \psi(\psi^{-1}(J_2)) = J_2$. Therefore μ is injective. Next we want to check that μ is surjective. Let $I \in \mathcal{I}$. Thus I is a 2-sided ideal of R containing $\mathfrak{a}$. Let

$$J = \psi(I) = \{\psi(a) \ : \ a \in I\} = \{a + \mathfrak{a} \ : \ a \in I\}.$$

We will show that J is a 2-sided ideal of $R/\mathfrak{a}$. Assume that for a moment. Then $J \in \mathcal{J}$ and $I = \psi^{-1}(\psi(I)) = \psi^{-1}(J) = \mu(J)$. Hence to complete the proof that μ is bijective we have to show that J is a 2-sided ideal of $R/\mathfrak{a}$. Since I is an ideal, $0 \in I$ and so $0+\mathfrak{a} = \psi(0) \in J$. Let $a+\mathfrak{a}$, $b+\mathfrak{a} \in J$. Then there are a', $b' \in I$ such that $a'+\mathfrak{a} = a+\mathfrak{a}$, $b'+\mathfrak{a} = b+\mathfrak{a}$. Hence $a-a'$ and $b-b'$ belong to $\mathfrak{a} \subseteq I$. Thus $a = (a-a')+a'$ and $b = (b-b')+b' \in I$. Thus $a+b \in I$. Hence $\psi(a+b) \in J$. Thus J is a subgroup of $(R/\mathfrak{a}, +)$. Next let $a+\mathfrak{a} \in J$ and $r+\mathfrak{a} \in R/\mathfrak{a}$. As before $a \in I$. As I is a 2-sided ideal of R we know that ra and $ar \in I$. Thus

$$(r+\mathfrak{a})(a+\mathfrak{a}) = ra+\mathfrak{a} = \psi(ra) \in J$$

and likewise $(a+\mathfrak{a})(r+\mathfrak{a}) \in J$. Hence J is a 2-sided ideal of $R/\mathfrak{a}$. □

2. Annihilators

Definition. Let R be a ring and $a \in R$. We define the **left annihilator** of a to be

$$\mathrm{Ann}_R(a) = \{r \in R : ra = 0\}.$$

Lemma 74. $\mathrm{Ann}_R(a)$ *is a left ideal of* R.

Proof. The proof is an easy exercise. □

Example 75. $\mathrm{Ann}_{\mathbb{R}}(10)$ is the set of real numbers r such that $r \cdot 10 = 0$. Thus $\mathrm{Ann}_R(10) = \{0\}$.

Example 76. $\mathrm{Ann}_{\mathbb{Z}/15\mathbb{Z}}(\overline{10})$ is the set of $r \in \mathbb{Z}/15\mathbb{Z}$ such that $r \cdot \overline{10} = \overline{0}$. Thus $\mathrm{Ann}_{\mathbb{Z}/15\mathbb{Z}} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$.

Exercise 77. Let $R = M_2(\mathbb{C})$.

(i) For which A in R is $\mathrm{Ann}_R(A) = 0$?
(ii) For which A in R is $\mathrm{Ann}_R(A) = R$?
(iii) Give $A \in M_2(\mathbb{C})$ such that $\mathrm{Ann}_R(A)$ is a non-zero proper left ideal.

3. Group Rings

Let R be a ring and G be a group. We shall use multiplicative notation for the binary operation on G. We define $R[G]$ to be the set of all formal sums

$$\sum_{g \in G} a_g \langle g \rangle$$

where $a_g \in R$, and all but finitely many a_g are zero. We shall define addition on $R[G]$ component-wise:

$$\left(\sum_{g \in G} a_g \langle g \rangle\right) + \left(\sum_{g \in G} b_g \langle g \rangle\right) = \left(\sum_{g \in G} (a_g + b_g) \langle g \rangle\right).$$

We define multiplication on $R[G]$ by $\langle g\rangle \cdot \langle h\rangle = \langle gh\rangle$ (where gh denotes multiplication in g) and then imposing distributivity:

$$\left(\sum_{g\in G} a_g\langle g\rangle\right) \cdot \left(\sum_{g\in G} b_g\langle g\rangle\right) = \sum_{g\in G} \sum_{\substack{h_1,h_2\in G,\\ h_1h_2=g}} a_{h_1}b_{h_2}\langle g\rangle.$$

Theorem 78. *$R[G]$ is a ring (called a **group ring**), where the additive identity is the formal sum where all the coefficients are 0, and the multiplicative identity is $1 = 1_R\langle 1_G\rangle$.*

Proof. This is routine verification. □

Example 79. Let's do some computations in $\mathbb{R}[S_3]$ to warm up. Let

$$\alpha \;=\; 5\cdot\langle\,\mathrm{id}\,\rangle \;+\; 3\cdot\langle\,(1,2)\,\rangle, \qquad \beta \;=\; -4\cdot\langle\,(1,3)\,\rangle \;+\; 2\cdot\langle\,(1,3,2)\,\rangle.$$

Then

$$\begin{aligned}
\alpha\beta \;&=\; (\,5\cdot\langle\,\mathrm{id}\,\rangle \;+\; 3\cdot\langle\,(1,2)\,\rangle\,)\cdot(\,-4\cdot\langle\,(1,3)\,\rangle \;+\; 2\cdot\langle\,(1,3,2)\,\rangle\,)\\
&=\; -20\cdot\langle\,\mathrm{id}\cdot(1,3)\,\rangle \;+\; 10\cdot\langle\,\mathrm{id}\cdot(1,3,2)\,\rangle\\
&\quad\; -12\cdot\langle(1,2)(1,3)\rangle + 6\cdot\langle(1,2)(1,3,2)\rangle\\
&=\; -20\cdot\langle\,(1,3)\,\rangle \;+\; 10\cdot\langle\,(1,3,2)\,\rangle - 12\cdot\langle\,(1,3,2)\,\rangle \;+\; 6\cdot\langle\,(1,3)\,\rangle\\
&=\; -14\cdot\langle\,(1,3)\,\rangle \;-\; 2\cdot\langle\,(1,3,2)\,\rangle
\end{aligned}$$

The symbol $\langle g\rangle$ **doesn't** mean the subgroup generated by g in this context. It's just a symbol that allows us to distinguish the elements of the ring R from the group G. Most of the time the angle brackets are omitted if that doesn't cause confusion. Here is the same computation in $\mathbb{R}[S_3]$ copied and pasted without explicitly writing the angle brackets.

$$\alpha \;=\; 5\cdot\mathrm{id} \;+\; 3\cdot(1,2), \qquad \beta \;=\; -4\cdot(1,3) \;+\; 2\cdot(1,3,2).$$

Then

$$\begin{aligned}
\alpha\beta \;&=\; (\,5\cdot\mathrm{id} \;+\; 3\cdot(1,2)\,)\cdot(\,-4\cdot(1,3) \;+\; 2\cdot(1,3,2)\,)\\
&=\; -20\cdot\mathrm{id}\cdot(1,3) \;+\; 10\cdot\mathrm{id}\cdot(1,3,2)\\
&\quad\; -12\cdot(1,2)(1,3) + 6\cdot(1,2)(1,3,2)\\
&=\; -20\cdot(1,3) \;+\; 10\cdot(1,3,2) - 12\cdot(1,3,2) \;+\; 6\cdot(1,3)\\
&=\; -14\cdot(1,3) \;-\; 2\cdot(1,3,2)
\end{aligned}$$

But sometimes you really need to keep the angle brackets to stop you from getting confused.

Exercise 80. In $\mathbb{R}[\mathbb{R}^*]$ let

$$\alpha \;=\; 3\cdot\langle\,1\,\rangle \;+\; 5\cdot\langle\,3\,\rangle, \qquad \beta \;=\; 2\cdot\langle\,1\,\rangle \;-\; 3\cdot\langle\,2\,\rangle.$$

Compute $\alpha+\beta$ and $\alpha\beta$. Note how confusing it would be to do this computation without the angle brackets.

Example 81. Let $C_2 = \{1, \sigma\}$ be the cyclic group of order 2 (thus $\sigma \neq 1$ but $\sigma^2 = 1$). Then any element of the group ring $\mathbb{Z}[C_2]$ has the form $a\langle 1\rangle + b\langle\sigma\rangle$. To simplify notation we write this as $a + b\sigma$. Now

$$(a + b\sigma)(c + d\sigma) = ac + bd + (ad + bc)\sigma.$$

Exercise 82. Let $C_2 = \{1, \sigma\}$ be the cyclic group of order 2 (thus $\sigma \neq 1$ but $\sigma^2 = 1$). Give a formula for $(1 + \sigma)^n$ in $\mathbb{Z}[C_2]$.

Exercise 83. Let $C_2 = \{1, \sigma\}$ be a cyclic group of order 2 (i.e. $\sigma^2 = 1$). Let R be a commutative ring. Show that $R[X]/J \cong R[C_2]$ where $J = (X^2 - 1)R[X]$ denotes the principal ideal of $R[X]$ generated by $X^2 - 1$. (**Hint:** start by defining a homomorphism $R[X] \to R[C_2]$ and then apply the Isomorphism Theorem).

Example 84. Write C_∞ for the infinite cyclic group generated by σ, thus $C_\infty = \{\sigma^n : n \in \mathbb{Z}\}$. Note that

$$1 + \sigma + \sigma^2 + \cdots$$

is **not** an element of $\mathbb{R}[C_\infty]$ as infinitely many of the coefficients are non-zero. However $3\sigma^{-1} + 2$ is an element of $\mathbb{R}[C_\infty]$. Let $\alpha = 3\sigma^{-1} + 2$ and $\beta = 1 - \sigma$. Then

$$\alpha + \beta = 3\sigma^{-1} + 3 - \sigma, \qquad \alpha\beta = 3\sigma^{-1} - 1 - 2\sigma.$$

Exercise 85. Let C_∞ be an infinite cyclic group (written multiplicatively) and let σ be a generator. Thus $C_\infty = \{\sigma^n : n \in \mathbb{Z}\}$. Let R be a commutative ring. Write $J = (XY - 1)R[X, Y]$ for the principal ideal of $R[X, Y]$ generated by $XY - 1$. A monomial in $R[X, Y]$ is an element of the form $X^r Y^s$ with $r,\ s \geq 0$. Note that the monomials form an R-basis for $R[X, Y]$.

(i) Let h be a monomial. Show that there is some $u \geq 0$ such that

$$h - X^u \in J, \qquad \text{or} \qquad h - Y^u \in J.$$

(ii) Show that $R[X, Y]/J \cong R[C_\infty]$. (**Hint:** let $\psi : R[X, Y] \to R[C_\infty]$ be the homomorphism satisfying $\psi(r) = r$ $(r \in R)$, $\psi(X) = \langle\sigma\rangle$, $\psi(Y) = \langle\sigma^{-1}\rangle$, and apply the Isomorphism Theorem. Don't bother giving the proof that ψ is a homomorphism!)

Group rings are important in representation theory, and are relevant to the *Groups and Representations* module. We shall say more about this later in the course.

4. Quaternions

Let

$$\mathbb{H} \;=\; \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \;:\; \alpha,\ \beta \in \mathbb{C} \right\},$$

where $\overline{\alpha}$ is the complex conjugate of α.

Exercise 86. Check that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$.

The ring $\mathbb{H}$ is called the **ring of quaternions**. An element of $\mathbb{H}$ is called a **quaternion**.

Now write $\alpha = a + bi$ and $\beta = c + di$ where $a, b, c, d \in \mathbb{R}$. Then we may express

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = a \cdot \mathbf{1} + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}$$

where

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Thus every quaternion maybe expressed uniquely as $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with a, b, c, $d \in \mathbb{R}$. In other words, we may consider $\mathbb{H}$ as a real vector space (instead of a ring), and then $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ is an $\mathbb{R}$-basis, so $\mathbb{H}$ is isomorphic to $\mathbb{R}^4$ *as a real vector space, not as a ring.* We shall usually write 1 for $\mathbf{1}$, and express the quaternion as $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. It is easy to check the following:

$$\begin{cases} \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \\ \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \\ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}. \end{cases} \tag{8}$$

It is very important to remember that quaternion multiplication is non-commutative! Using these rules it is now easy to compute products of quaternions. For example,

$$\begin{aligned} (1 + \mathbf{i} + \mathbf{j})(2 - \mathbf{j} + \mathbf{k}) &= 2 + 2\mathbf{i} + 2\mathbf{j} - \mathbf{j} - \mathbf{ij} - \mathbf{j}^2 + \mathbf{k} + \mathbf{ik} + \mathbf{jk} \\ &= 2 + 2\mathbf{i} + 2\mathbf{j} - \mathbf{j} - \mathbf{k} - (-1) + \mathbf{k} - \mathbf{j} + \mathbf{i} \\ &= 3 + 3\mathbf{i}. \end{aligned}$$

Quaternions are more commonly defined as expressions of the form $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ where the coefficients a, b, c, d are real and the symbols $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ satisfy the multiplication rules given in (8). This works but it becomes painful to verify that multiplication is associative. We didn't need to do this, because with our definition we didn't need to prove that $\mathbb{H}$ is a ring, but only a subring of $M_2(\mathbb{C})$, and for this we can apply Lemma 4. We note that associativity in $\mathbb{H}$ is inherited from associativity in $M_2(\mathbb{C})$ because $\mathbb{H}$ sits inside $M_2(\mathbb{C})$.

Exercise 87. Where is the mistake in the following argument? In $\mathbb{H}$, $\mathbf{i}^2 = -1 = \mathbf{j}^2$. Thus $\mathbf{i}^2 - \mathbf{j}^2 = 0$. Thus $(\mathbf{i} - \mathbf{j})(\mathbf{i} + \mathbf{j}) = 0$. As $\mathbb{H}$ is a division ring (see Chapter 5 for a definition), either $\mathbf{i} - \mathbf{j} = 0$ or $\mathbf{i} + \mathbf{j} = 0$. Hence $\mathbf{i} = \mathbf{j}$ or $\mathbf{i} = -\mathbf{j}$.

5. Centres of Rings

Definition. Let R be a ring. The **centre of** R, denoted by $Z(R)$, is

$$Z(R) = \{s \in R \ : \quad rs = sr \text{ for all } r \in R\}.$$

Thus the centre consists of elements that commute with *all* other elements. Of course, R is commutative if and only if $Z(R) = R$.

Theorem 88. *Let R be a ring. Then $Z(R)$ is a commutative ring.*

Proof. This is an easy exercise. □

Example 89. Let's compute the centre of $\mathbb{H}$ (the ring of quaternions). Any element of $\mathbb{H}$ can be written uniquely as an $\mathbb{R}$-linear combination of 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. Suppose $\alpha \in Z(\mathbb{H})$ and write

$$\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}, \qquad a,\ b,\ c,\ d \in \mathbb{R}.$$

Observe that

$$\alpha \cdot \mathbf{i} = a\mathbf{i} - b - c\mathbf{k} + d\mathbf{j}$$
$$\mathbf{i} \cdot \alpha = a\mathbf{i} - b + c\mathbf{k} - d\mathbf{j}.$$

Since $\alpha \cdot \mathbf{i} = \mathbf{i} \cdot \alpha$ we see that $c = d = 0$ and so $\alpha = a + b\mathbf{i}$. Moreover,

$$\alpha \cdot \mathbf{j} = a\mathbf{j} + b\mathbf{k}$$
$$\mathbf{j} \cdot \alpha = a\mathbf{j} - b\mathbf{k}.$$

Thus $b = 0$. Hence $\alpha = a \in \mathbb{R}$. Thus $Z(\mathbb{H}) \subseteq \mathbb{R}$. It is easy to check the reverse inclusion from the definition of multiplication in $\mathbb{H}$. Thus $Z(\mathbb{H}) = \mathbb{R}$.

Exercise 90. Show that

$$Z\left(M_2(\mathbb{R})\right) = \{a \cdot I_2 \ : \ a \in \mathbb{R}\}$$

where I_2 is the identity 2×2-matrix.

Exercise 91. Let R_1, R_2 be rings. Show that

$$Z(R_1 \times R_2) = Z(R_1) \times Z(R_2).$$

Exercise 92. Let R be a non-zero commutative ring. Let G be a group and $Z(G)$ the centre of G, defined by

$$Z(G) = \{h \in G \ : \ hg = gh \text{ for all } g \in G\}.$$

(i) Show that $Z(G)$ is a subgroup of G;
(ii) $Z(R[G]) \supseteq R[Z(G)]$.
(iii) Let $\alpha \in R[G]$. Show that $\alpha \in Z(R[G])$ if and only if

$$\alpha \cdot \langle h \rangle = \langle h \rangle \cdot \alpha.$$

for all $h \in G$.
(iv) Let $\alpha = \sum r_g \langle g \rangle \in R[G]$. Show that $\alpha \in Z(R[G])$ if and only if

$$r_{h^{-1}gh} = r_g$$

for all g, $h \in G$.

(v) Show that for any $n \geq 3$

$$Z(R[S_n]) \neq R[Z(S_n)].$$

Hint: you might find the following facts useful.

- Two elements of S_n are conjugate if and only if they have the same cycle structure.
- $Z(S_n) = \{1\}$.

CHAPTER 4

Algebras

1. Definition and Examples

Definition. Let K be a field. A **K-algebra** A is a ring such that $K \subseteq Z(A)$. Observe that every K-algebra is also a vector space over K. By the **dimension** of a K-algebra we mean its dimension as a K-vector space.

Example 93. Let L, K be fields with $K \subseteq L$. Then L is a K-algebra. In Galois Theory we write $[L : K]$ for the dimension of L as a K-vector space.

For example $\mathbb{R} \subset \mathbb{C}$ and so $\mathbb{C}$ is an $\mathbb{R}$-algebra. In fact $\mathbb{C}$ is a 2-dimensional $\mathbb{R}$-algebra.

More trivially, $\mathbb{C}$ is a 1-dimensional $\mathbb{C}$-algebra.

Example 94. If K is a field then K is a 1-dimensional K-algebra. But the polynomial ring $K[T]$ is an infinite dimensional K-algebra.

Example 95. By Example 89, $Z(\mathbb{H}) = \mathbb{R}$ where $\mathbb{H}$ is the ring of quaternions. Thus $\mathbb{H}$ is a 4-dimensional $\mathbb{R}$-algebra

Example 96. Let G be a group, with identity element 1_G. Let K be a field. We think of K as contained in $K[G]$ by indentifying $a \in K$ with $a\langle 1_G\rangle \in K[G]$. With this identification, $K \subseteq Z(K[G])$. Thus $K[G]$ is a K-algebra. Its dimension is $\#G$.

Example 97. Let K be a field and $n \geq 1$. We think of K as contained in $M_n(K)$ by identifying $a \in K$ with $aI_n \in M_n(K)$. With this identification $K \subseteq Z(M_n(K))$. Thus $M_n(K)$ is a K-algebra. Its dimension is n^2.

2. The Evaluation Map

Lemma 98. *Let K be a field and f, g, $h \in K[X]$ with $f(X) = g(X)h(X)$. Let A be a K-algebra and $\alpha \in A$. Then $f(\alpha) = g(\alpha)h(\alpha)$.*

Proof. Note the requirement that A be a K-algebra, i.e. that $K \subseteq Z(A)$. Let take a simple case where g, h are linear to try and understand why we need $K \subseteq Z(A)$.

Let $g = a_0 + a_1X$, $h = b_0 + b_1X$ with a_i, $b_i \in K$. Now

$$f(X) = a_0b_0 + (a_1b_0 + a_0b_1)X + a_1b_1X^2.$$

Hence

$$f(\alpha) = a_0b_0 + (a_1b_0 + a_0b_1)\alpha + a_1b_1\alpha^2.$$

However

$$\begin{aligned} g(\alpha)h(\alpha) &= (a_0 + a_1\alpha)(b_0 + b_1\alpha) \\ &= a_0b_0 + a_0b_1\alpha + a_1\alpha b_0 + a_1\alpha b_1\alpha. \end{aligned}$$

Does $g(\alpha)h(\alpha)$ equal $f(\alpha)$? For this to be true we would want $a_1\alpha b_0 = a_1b_0\alpha$ and $a_1\alpha b_1\alpha = a_1b_1\alpha^2$. But b_0 and b_1 belong to K which is contained in the centre $Z(A)$. So b_0, b_1 commute with all elements of A, including α, giving us $a_1\alpha b_0 = a_1b_0\alpha$ and $a_1\alpha b_1\alpha = a_1b_1\alpha^2$, and completing the proof that $g(\alpha)h(\alpha) = f(\alpha)$.

We haven't proved the lemma (or only proved it when g, h are linear). But you now understand where the hypothesis $K \subseteq Z(A)$ is needed, and you can construct your own proof. □

We will use Lemma 98 repeatedly without necessarily acknowledging it.

Theorem 99. *Let K be a field and A be a K-algebra. Let $\alpha \in A$. Then the evaluation map*

$$\mathrm{ev}_\alpha : K[X] \to A, \qquad f(X) \mapsto f(a)$$

is a homomorphism. In particular, the image $\{f(\alpha) : f \in K[X]\}$ is a commutative subalgebra of A (i.e. a commutative subring of A containing K in its centre).

Proof. This is an easy exercise. You will need Lemma 98. □

3. Minimal and Characteristic Polynomials

Lemma 100. *Let A be a K-algebra. Let $\alpha \in A$. Define*

$$\phi_\alpha : A \to A, \qquad \phi_\alpha(\beta) = \alpha \cdot \beta.$$

Then ϕ_α is a K-linear transformation.

Proof. It is clear that $\phi_\alpha(\beta + \gamma) = \phi_\alpha(\beta) + \phi_\alpha(\gamma)$. Now let $a \in K$. Then

$$\begin{aligned} \phi_\alpha(a \cdot \beta) &= \alpha a \cdot \beta \\ &= a \cdot \alpha \cdot \beta, \qquad \text{since } a \in K \subseteq Z(A) \\ &= a\phi_\alpha(\beta). \end{aligned}$$

Hence ϕ_α is a K-linear transformation. □

Observe how important the assumption $K \subseteq Z(A)$ is in the above proof. Without it, ϕ_α would be a homomorphism of abelian groups, but not a K-linear transformation.

Now suppose A has dimension n as a K-vector space. Let $\chi_\alpha(X) \in K[X]$ be the characteristic polynomial of ϕ_α and $m_\alpha(X) \in K[X]$ the minimal polynomial of ϕ_α. Recall the following

- χ_α is monic of degree n. It is defined by $\chi_\alpha(X) = \det(XI_n - \phi_\alpha)$.
- $\chi_\alpha(\phi_\alpha) = 0$ (this is the Cayley–Hamilton Theorem).
- $m_\alpha(\phi_\alpha) = 0$. Indeed m_α is the monic polynomial in $K[X]$ of least positive degree satisfying this.
- If $f \in K[X]$ satisfies $f(\phi_\alpha) = 0$ then $m_\alpha \mid f$.
- $m_\alpha \mid \chi_\alpha$. Moreover, m_α and χ_α have the same irreducible factors; the multiplicities might be different.

Lemma 101. *Let A be a K-algebra with $\dim_K(A) = n$. Let $f \in K[X]$ and $\alpha \in A$. Then $f(\alpha) = 0$ if and only if $f(\phi_\alpha) = 0$. In particular, $\chi_\alpha(\alpha) = m_\alpha(\alpha) = 0$. Moreover, m_α is the monic polynomial in $K[X]$ of smallest possible possitive degree such that $m_\alpha(\alpha) = 0$.*

Proof. Let $f = a_0 + a_1X + \cdots + a_rX^r$ be a polynomial with $a_i \in K$. Let $\beta \in A$. Then

$$\begin{aligned} f(\phi_\alpha)(\beta) &= (a_0 + a_1\phi_\alpha + \cdots + a_r\phi_\alpha^r)(\beta) \\ &= a_0 \cdot \beta + a_1\phi_\alpha(\beta) + \cdots + a_r\phi_\alpha^r(\beta) \\ &= a_0 \cdot \beta + a_1 \cdot \alpha \cdot \beta + \cdots + a_r \cdot \alpha^r \cdot \beta \\ &= f(\alpha) \cdot \beta. \end{aligned}$$

Thus if $f(\alpha) = 0$, then $f(\phi_\alpha)$ is zero as a K-linear transformation of A. Conversely if $f(\phi_\alpha)$ is zero as a K-linear transformation of A then, applying the above with $\beta = 1$ show that $f(\alpha) = 0$. The lemma follows. □

Example 102. Let's compute the characteristic polynomial for $\mathbf{i} \in \mathbb{H}$. We work with the $\mathbb{R}$-basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$. Note that

$$\begin{aligned} \mathbf{i} \cdot 1 &= \mathbf{i} = 0 \cdot 1 + 1 \cdot \mathbf{i} + 0 \cdot \mathbf{j} + 0 \cdot \mathbf{k} \\ \mathbf{i} \cdot \mathbf{i} &= -1 = -1 \cdot 1 + 0 \cdot \mathbf{i} + 0 \cdot \mathbf{j} + 0 \cdot \mathbf{k} \\ \mathbf{i} \cdot \mathbf{j} &= \mathbf{k} = 0 \cdot 1 + 0 \cdot \mathbf{i} + 0 \cdot \mathbf{j} + 1 \cdot \mathbf{k} \\ \mathbf{i} \cdot \mathbf{k} &= -\mathbf{j} = 0 \cdot 1 + 0 \cdot \mathbf{i} - 1 \cdot \mathbf{j} + 0 \cdot \mathbf{k}. \end{aligned}$$

Hence the matrix of $\mathbf{i}$ (or $\phi_{\mathbf{i}}$) with respect to this basis is

$$M_{\mathbf{i}} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

According to the convention we follow, the coefficients of the linear combinations make up the columns of the matrix (and not its rows). If you follow the opposite convention you will have the transpose of this matrix.

The characteristic polynomial is

$$\chi_\alpha(X) = \det(XI_4 - M_\alpha) = \begin{vmatrix} X & 1 & 0 & 0 \\ -1 & X & 0 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & -1 & X \end{vmatrix} = (X^2+1)^2.$$

What is $m_{\mathbf{i}}$? Recall that $m_{\mathbf{i}}$ is a divisor of $\chi_{\mathbf{i}}$ with the same irreducible factors. Thus $m_{\mathbf{i}} = X^2+1$ or $m_{\mathbf{i}} = (X^2+1)^2$. However, $\mathbf{i}^2 + 1 = 0$ so $m_{\mathbf{i}} = X^2 + 1$.

CHAPTER 5

Division Rings

1. Definition and Examples

Definition. A ring D is called a **division ring** if $D \neq 0$ and every non-zero element is a unit.

Example 103.
- Recall the definition of a field: a field is a commutative ring in which every non-zero element is a unit. Hence a commutative ring is a division ring if and only if it is a field. Thus $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are division rings.
- Moreover, $\mathbb{Z}/n\mathbb{Z}$ is a division ring if and only if n is prime.
- $\mathbb{Z}$ is not a division ring. For example $2 \in \mathbb{Z}$ is not a unit.
- $\mathbb{R}[X]$ is not a division ring. For example $X \in \mathbb{R}[X]$ is not a unit.

Lemma 104. *Let D be a division ring. If $rs = 0$ with r, $s \in D$ then $r = 0$ or $s = 0$.*

PROOF. If $r \neq 0$ then it is a unit and so has an inverse r^{-1}. Thus $s = r^{-1}rs = 0$. □

Example 105. $M_2(R)$ is **not** a division ring for any ring R. For example, note that $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)^2 = 0$.

Example 106. Recall that an integral domain is a non-zero commutative ring which has no zero divisors; i.e. if $rs = 0$ then $r = 0$ or $s = 0$. A division ring which is commutative is an integral domain.

We saw above some examples of division rings but they were all commutative. The quaternions $\mathbb{H}$ are an example of a non-commutative division ring.

Theorem 107. *$\mathbb{H}$ is a division ring.*

PROOF. This is an exercise. It is easier to do this if think of quaternions as 2×2 matrices. □

Exercise 108. Let D be a division ring, $x \in D$, and $y \in Z(D)$. Show that $x^2 = y^2$ if and only if $x = \pm y$. (c.f. Exercise 87.)

Exercise 109. Define the **norm** map on quaternions by

$$\text{Norm} : \mathbb{H} \to \mathbb{R}, \qquad \text{Norm}(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}) = a^2+b^2+c^2+d^2,\ a, b, c, d \in \mathbb{R}.$$

(i) Show that $\text{Norm}(uv) = \text{Norm}(u)\,\text{Norm}(v)$, and if $u \neq 0$ then $\text{Norm}(u^{-1}) = \text{Norm}(u)^{-1}$.

(ii) Let S be a subring of $\mathbb{R}$ (e.g. $S = \mathbb{Z}$, $S = \mathbb{Z}[\sqrt{2}]$, $S = \mathbb{Q}$, etc.) Let
$$\mathbb{H}(S) = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \ : \ a, b, c, d \in S\} \subseteq \mathbb{H}.$$
Show that $\mathbb{H}(S)$ is a subring of $\mathbb{H}$.
(iii) Let K be a subfield of $\mathbb{R}$. Show that $\mathbb{H}(K)$ is a division ring.
(iv) Determine $\mathbb{H}(\mathbb{Z})^*$. Conclude that $\mathbb{H}(\mathbb{Z})$ is not a division ring.

Exercise 110. (i) Determine the elements of $\mathbb{H}^*$ of order 1, 2.
(ii) Show that the elements of $\mathbb{H}^*$ of order 4 are precisely the ones of the form $b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with b, c, $d \in \mathbb{R}$ and $b^2 + c^2 + d^2 = 1$.
(iii) Let $u \in \mathbb{H}^*$ have finite order $n \geq 3$. Show that there is some $0 < j < n/2$ such that $u^2 - 2\cos(2\pi j/n)u + 1 = 0$. (**Hint:** you know the factorization of $X^n - 1$ over $\mathbb{C}$. Use this to write down the factorization of $X^n - 1$ over $\mathbb{R}$.)

The following theorem will become important later.

Theorem 111. *Let R be a ring. The ring R is a division ring if and only if it has no non-zero proper left ideals.*

PROOF. Suppose R is a division ring and J is a non-zero left ideal. Let $a \in J$ with $a \neq 0$. As R is a division ring, a has a multiplicative inverse $a^{-1} \in R$. Thus $1 = a^{-1}a \in J$ as J is a left ideal. As $1 \in J$ we have $J = R$. Thus R has no non-zero proper left ideals.

Now let's prove the converse. Suppose that R has no non-zero proper left ideals. We want to prove that R is a division ring, meaning that every non-zero element of R is a unit. Let $a \neq 0$ be an element of R. To show that a is a unit we must prove the existence of $b \in R$ such that $ab = ba = 1$. First note that Ra is a non-zero left ideal. By our assumption $Ra = R$. Thus $1 \in Ra$, and so $1 = ba$ for some $b \in R$. We want to conclude that $ab = 1$ but we don't want to assume that R is commutative. We will use a trick! Since $1 = ba$ we have $a = a \cdot 1 = a(ba) = (ab)a$ by associativity. Hence $(ab - 1)a = 0$. Consider the left annihilator of a:
$$\mathrm{Ann}_R(a) = \{c \in R \ : \ ca = 0\}.$$
Recall that this is a left ideal (Lemma 74). If $1 \in \mathrm{Ann}_R(a)$ then $a = 1a = 0$ giving a contradiction. So $\mathrm{Ann}_R(a)$ is a proper left ideal. By assumption $\mathrm{Ann}_R(a) = 0$. But $(ab - 1) \in \mathrm{Ann}_R(a)$ since $(ab - 1)a = 0$. Thus $ab - 1 = 0$ giving $1 = ab$ as required. □

After going through the proof of Theorem 111 you're probably wondering if there is there a ring R having elements a, b where $ab = 1$ but $ba \neq 1$. The following exercise gives an affirmative answer to this question.

Exercise 112. (i) Let V be a vector space over a field K. Let $\mathrm{End}(V)$ be the set of all K-linear transformations $T : V \to V$

(these are called endomorphisms of V). Let S, $T \in \mathrm{End}(V)$. Define

$$S + T : V \to V, \qquad (S+T)(\mathbf{v}) = S(\mathbf{v}) + T(\mathbf{v}),$$

and

$$ST : V \to V, \qquad (ST)(\mathbf{v}) = (S \circ T)(\mathbf{v}) = S(T(\mathbf{v})).$$

Show that $\mathrm{End}(V)$ is a ring, specifying the additive and multiplicative identities.

(ii) Let $V = \{(a_1, a_2, \dots) : a_i \in K\}$ be the K-vector space of infinite sequences with entries in K. Let $T \in \mathrm{End}(V)$ be

$$T : V \to V, \qquad T(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots).$$

(a) Find $S \in \mathrm{End}(V)$ such that $ST = 1$.
(b) Show that $TS \neq 1$ for any $S \in \mathrm{End}(V)$.

(iii) The vector space V in (ii) is infinite dimensional. Suppose now that V is a finite dimensional vector space. Let S, $T \in \mathrm{End}(V)$ satisfy $ST = 1$. Show carefully that $TS = 1$. **Hint:** you could translate this into a question about matrices and use determinants.

2. Centres of Division Rings

Theorem 113. *If R is a division ring, then $Z(R)$ is a field. Hence R is a vector space over $Z(R)$, and so R is a $Z(R)$-algebra.*

Proof. We know that $Z(R)$ is a ring, and by definition it is commutative. A field is a commutative ring in which every non-zero element is a unit (of that ring). Let $r \in Z(R)$, with $r \neq 0$. By definition of $Z(R)$, we know that $rt = tr$ for all $t \in R$. Hence $t = r^{-1}tr$ and so $tr^{-1} = r^{-1}t$. Thus $r^{-1} \in Z(R)$ too. So $Z(R)$ is a field. □

A **division algebra** is just an algebra which is also a division ring.

Example 114. $\mathbb{H}$ is a 4-dimensional division algebra over $\mathbb{R} = Z(\mathbb{H})$.

It is natural to ask for division rings what the dimension of R over $Z(R)$ can be. Of course,

$$\dim_{Z(R)}(R) = 1 \quad \Longleftrightarrow \quad Z(R) = R \quad \Longleftrightarrow \quad R \text{ is a field.}$$

Can the dimension be 2? The following lemma say no.

Lemma 115. *Let R be a division ring and write $K = Z(R)$. Then $\dim_K(R) \neq 2$.*

Proof. Suppose $\dim_K(R) = 2$, and let $\alpha \in R \setminus K$. We easily see that the set $\{1, \alpha\}$ is K-linearly independent and so must be a K-basis.

Hence every element has the form $\lambda + \mu\alpha$ where λ, $\mu \in K$. But

$$\begin{aligned}\alpha(\lambda + \mu\alpha) &= \alpha\lambda + \alpha\mu\alpha \\ &= \lambda\alpha + \mu\alpha^2 \qquad \text{as } \lambda,\ \mu \in K = Z(R) \\ &= (\lambda + \mu\alpha)\alpha.\end{aligned}$$

Hence $\alpha \in Z(R) = K$ giving a contradiction. □

3. Minimal and Characteristic Polynomials in Division Algebras

Let A be an n-dimensional K-algebra. Let $\alpha \in A$. Recall the following:

- $\deg(\chi_\alpha) = n$.
- m_α is the monic polynomial of least possible positive degree such that $m_\alpha(\alpha) = 0$.
- $m_\alpha \mid \chi_\alpha$. Moreover, m_α, χ_α share the same irreducible factors.

Lemma 116. *Let A be an n-dimensional K-division algebra. Let $\alpha \in A$. Then*

(i) $m_\alpha \in K[X]$ *is irreducible.*
(ii) $\chi_\alpha = m_\alpha^r$ *for some positive integer* r.
(iii) $\deg(m_\alpha) \mid n$.

Proof. Suppose m_α is reducible. Thus $m_\alpha(X) = f(X)g(X)$ where f, $g \in K[X]$, and $1 \leq \deg(f) < \deg(m_\alpha)$, $1 \leq \deg(g) < \deg(m_\alpha)$. By Lemma 98

$$0 = m_\alpha(\alpha) = f(\alpha)g(\alpha).$$

As A is a division algebra, $f(\alpha) = 0$ or $g(\alpha) = 0$, contradicting the fact that m_α is the minimal polynomial. Hence m_α is irreducible.

As χ_α and m_α share the same irreducible factors, $\chi_\alpha = m_\alpha^r$ for some positive integer r. Also $n = \deg(\chi_\alpha) = r\deg(m_\alpha)$, so $\deg(m_\alpha) \mid n$. □

Exercise 117. Let K be a field, and let p be a prime. Let A be a division algebra over K of dimension p. Let $\alpha \in A \setminus K$. Write χ_α for the characteristic polynomial of α, and m_α for its minimal polynomial.

(i) Show that $\chi_\alpha = m_\alpha$.
(ii) Deduce that $1, \alpha, \cdots, \alpha^{p-1}$ are K-linearly independent.
(iii) Show that A is a field.

4. Complex Division Algebras

Theorem 118. *The only finite-dimensional $\mathbb{C}$-division algebra is $\mathbb{C}$.*

Proof. Let A be a finite-dimensional $\mathbb{C}$-division algebra. In particular, $\mathbb{C} \subseteq A$. We want to show that $A = \mathbb{C}$. Suppose $\alpha \in A$. By Lemma 116 the minimal polynomial m_α is an irreducible element of

$\mathbb{C}[X]$. However, by the fundamental theorem of algebra, the only irreducible polynomials of $\mathbb{C}[X]$ are linear. Thus $m_\alpha(X) = X - a$ with $a \in \mathbb{C}$. However, $m_\alpha(\alpha) = 0$ and so $\alpha = a \in \mathbb{C}$. Thus $A = \mathbb{C}$. □

Exercise 119. Let S be a $\mathbb{C}$-algebra, and let J be a proper 2-sided ideal of S. Suppose S satisfes the following property: for all $a \in S \setminus J$ there is some $b \in S$ such that $ab - 1 \in J$ and $ba - 1 \in J$. Show that either $S/J \cong \mathbb{C}$ or $\dim_{\mathbb{C}}(S/J) = \infty$.

Exercise 120. Let A be a finite dimensional algebra over a field K. Suppose A has no zero divisors: this means that whenever $rs = 0$ with r, $s \in A$, then $r = 0$ or $s = 0$.

(i) Let $\beta \in A$. Show that there is an irreducible polynomial $g \in K[X]$ such that $g(\beta) = 0$.
(ii) Deduce that A is a division algebra. (**Hint:** Let $\beta \in A \setminus \{0\}$. Show that there is a polynomial $h \in K[X]$ such that $\beta \cdot h(\beta) = h(\beta) \cdot \beta = 1$.)
(iii) Let $\alpha \in A$, and let

$$B = \mathrm{Im}(\mathrm{ev}_\alpha) = \{f(\alpha) \ : \ f(X) \in K[X]\}.$$

Show that B is a field.

5. Classification of Real Division Algebras

Lemma 121. *Let $f \in \mathbb{R}[X]$ be monic and irreducible. Then*

(i) either $f = X + a$
(ii) or $f = X^2 + aX + b$ with $a^2 - 4b < 0$.

Proof. Let $\lambda \in \mathbb{C}$ be a root of f. If $\lambda \in \mathbb{R}$, then $(X - \lambda) \mid f$ and so $f = X - \lambda$. i.e. $f = X + a$ where $a = -\lambda$. Thus we suppose $\lambda \in \mathbb{C} \setminus \mathbb{R}$. Then $\overline{\lambda}$ is also a root, and $\overline{\lambda} \neq \lambda$. We note that $(X - \lambda)(X - \overline{\lambda}) = X^2 + aX + b$ divides f where

$$a = -(\lambda + \overline{\lambda}) \in \mathbb{R}, \qquad b = \lambda\overline{\lambda} \in \mathbb{R}.$$

Hence $f = X^2 + aX + b$. Moreover, as the roots of f are non-real, the discriminant $a^2 - 4b$ is negative. □

We saw that the only finite-dimensional complex division algebra is $\mathbb{C}$.

Lemma 122. *The only odd-dimensional $\mathbb{R}$-division algebra is $\mathbb{R}$.*

Proof. Let A be an $\mathbb{R}$-division algebra with odd dimension n. In particular, $\mathbb{R} \subseteq A$. We want to show that $A = \mathbb{R}$. Suppose $\alpha \in A$. We want to show that $\alpha \in \mathbb{R}$. By Lemma 116, the minimal polynomial $m_\alpha(X) \in \mathbb{R}[X]$ is irreducible. By Lemma 121, m_α is either linear or quadratic. However, again by Lemma 116, the degree $\deg(m_\alpha)$ divides n which is odd. Thus $m_\alpha = X + a$ for some $a \in \mathbb{R}$. Since $m_\alpha(\alpha) = 0$ we have $\alpha = -a \in \mathbb{R}$. Thus $A = \mathbb{R}$. □

Theorem 123. *(Frobenius) Every finite-dimensional division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{H}$.*

We prove the theorem of Frobenius in steps. Let A be a real division algebra of dimension $n < \infty$. If $n = 1$ then we know that $A = \mathbb{R}$. So we suppose $n > 1$. Define the trace map

$$\text{Trace} \ : \ A \to \mathbb{R}, \qquad \text{Trace}(\alpha) = \text{Trace}(\phi_\alpha).$$

Example 124. Let $\alpha \in \mathbb{H}$ and write $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with a, b, c, $d \in \mathbb{R}$. Let us write the matrix of α (or ϕ_α) with respect to the $\mathbb{R}$-basis 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. Note that

$$\begin{aligned}
\alpha \cdot 1 &= a \cdot 1 + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k} \\
\alpha \cdot \mathbf{i} &= -b \cdot 1 + a \cdot \mathbf{i} + d \cdot \mathbf{j} - c \cdot \mathbf{k} \\
\alpha \cdot \mathbf{j} &= -c \cdot 1 - d \cdot \mathbf{i} + a \cdot \mathbf{j} + b \cdot \mathbf{k} \\
\alpha \cdot \mathbf{k} &= -d \cdot 1 + c \cdot \mathbf{i} - b \cdot \mathbf{j} + a \cdot \mathbf{k}.
\end{aligned}$$

Hence the matrix of α (or ϕ_α) with respect to this basis is

$$M_\alpha = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}.$$

Thus

$$\text{Trace}(\alpha) = \text{Trace}(\phi_\alpha) = \text{Trace}(M_\alpha) = 4a.$$

We now return to a general n-dimensional real algebra A.

Exercise 125. Show that $\text{Trace} : A \to \mathbb{R}$ is a linear transformation of real vector spaces. Moreover, if $a \in \mathbb{R} \subseteq A$ then $\text{Trace}(a) = na$.

Hence if $a \in \mathbb{R}$ then $\text{Trace}(a/n) = a$ and so $\text{Im}(\text{Trace}) = \mathbb{R}$. Let

$$V = \text{Ker}(\text{Trace}) = \{v \in A \ : \ \text{Trace}(v) = 0\}.$$

Lemma 126. *$A = \mathbb{R} \oplus V$ (as vector spaces over $\mathbb{R}$).* [1]

Proof. By the Rank–Nullity Theorem

$$\dim(V) = \dim(\text{Ker}(\text{Trace})) = n - \dim(\text{Im}(\text{Trace})) = n - 1.$$

Let $a \in \mathbb{R} \cap V$. Then $na = \text{Trace}(a) = 0$ and so $a = 0$. Hence $\mathbb{R} \cap V = \{0\}$. Therefore $\mathbb{R} \oplus V$ is a subspace of A. Moreover its dimension is $1 + (n-1) = n = \dim(A)$. Hence $\mathbb{R} \oplus V = A$. □

[1] Let us recall what direct sum means. Let V be a vector space and U, W be subspaces. We say that V is the **direct sum** of U, W, and write $V = U \oplus W$ if

(i) $V = U + W$ (here $U + W = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U, \ \mathbf{w} \in W\}$);
(ii) $U \cap W = \{\mathbf{0}\}$.

This is equivalent to the following: every $\mathbf{v} \in V$ can be written uniquely as $\mathbf{v} = \mathbf{u} + \mathbf{w}$ where $\mathbf{u} \in U$, $\mathbf{w} \in W$.

Exercise 127. Compute V for $A = \mathbb{C}$ and $A = \mathbb{H}$. Check in both cases that for $\alpha \in V$ we have α^2 is both real and ≤ 0.

Lemma 128. *Let $\alpha \in V$. Then $\alpha^2 \in \mathbb{R}$ and $\alpha^2 \leq 0$. Moreover, $\alpha^2 = 0$ if and only if $\alpha = 0$.*

PROOF. The last part of the lemma is true as $V \subseteq A$, and A is a division ring. Let $\alpha \in V$. If $\alpha \in \mathbb{R}$ then by the previous lemma, $\alpha = 0$ and the result is trivial in this case. Thus we may suppose that $\alpha \notin \mathbb{R}$. It follows from Lemma 121 that

$$m_\alpha = X^2 + aX + b$$

where $a^2 - 4b < 0$. From Algebra II we know that

$$\chi_\alpha = X^n - \operatorname{Trace}(\alpha)X^{n-1} + \cdots + (-1)^n \det(\alpha).$$

But by Lemma 116, we have $\chi_\alpha = m_\alpha^r$ for some positive integer n. We deduce that $n = 2r$ by comparing degrees. Moreover, by comparing the coefficients of $X^{n-1} = X^{2r-1}$ on both sides of the equality $\chi_\alpha = m_\alpha^r$ we have

$$ra = -\operatorname{Trace}(\alpha).$$

But $\alpha \in V$, and by definition, V is the kernel of the trace map, so $\operatorname{Trace}(\alpha) = 0$ and hence $a = 0$. It follows that $m_\alpha = X^2 + b$ with $b > 0$. As $m_\alpha(\alpha) = 0$ we see that $\alpha^2 = -b$, showing that $\alpha^2 \in \mathbb{R}$ and $\alpha^2 < 0$. □

Lemma 129. *Let*

$$\langle\ ,\ \rangle\ :\ V \times V \to \mathbb{R}, \qquad \langle \alpha, \beta \rangle = \frac{-1}{2} \cdot (\alpha\beta + \beta\alpha).$$

Then $(V, \langle\ ,\ \rangle)$ is a finite-dimensional Euclidean space.

PROOF. Recall the definition of a Euclidean space: it is a real vector space equipped with a positive-definite symmetric $\mathbb{R}$-bilinear form. It is clear that $\langle \alpha, \beta \rangle = \langle \beta, \alpha \rangle$; i.e. $\langle\ ,\ \rangle$ is symmetric. To check that it is $\mathbb{R}$-bilinear we need to check that

$$\langle \alpha_1 + \alpha_2, \beta \rangle = \langle \alpha_1, \beta \rangle + \langle \alpha_2, \beta \rangle, \qquad \alpha_1,\ \alpha_2,\ \beta \in V$$

and

$$\langle a\alpha, \beta \rangle = a\langle \alpha, \beta \rangle, \qquad a \in \mathbb{R}, \quad \alpha,\ \beta \in V.$$

These are easy exercises, but note that the proof of the second property really uses the fact that $a \in Z(A)$. Finally, we want to check that $\langle\ ,\ \rangle$ is positive definite: i.e. $\langle \alpha, \alpha \rangle > 0$ for all $\alpha \in V$ with $\alpha \neq 0$. This follows from Lemma 128 as $\langle \alpha, \alpha \rangle = -\alpha^2$. □

By Gram–Schmidt we know that the Euclidean space $(V, \langle\ ,\ \rangle)$ has an orthonormal basis. Let us denote this by $e_1, e_2, \ldots, e_{n-1}$ (recall $\dim(V) = n - 1$ where $n = \dim(A)$).

Lemma 130. *$e_i^2 = -1$ for $i = 1, \ldots, n-1$, and $e_i \cdot e_j = -e_j \cdot e_i$ for $1 \leq i \neq j \leq n - 1$.*

PROOF. As the basis is orthonormal, $\langle e_i, e_i\rangle = 1$ and $\langle e_i, e_j\rangle = 0$ for $i \neq j$. The lemma follows from the definition of $\langle\ ,\ \rangle$. □

Lemma 131. *Suppose* $1 \leq i < j < k \leq n-1$. *Then* $e_k = \pm(e_i \cdot e_j)^{-1}$.

PROOF. Let $u = e_i e_j e_k$. We're going to compute u^2 using Lemma 130:

$$\begin{aligned} u^2 &= e_i e_j e_k e_i e_j e_k \\ &= -e_j e_i e_k e_i e_j e_k \qquad (e_i e_j = -e_j e_i) \\ &= e_j e_k e_i e_i e_j e_k \qquad (e_i e_k = -e_k e_i) \\ &= -e_j e_k e_j e_k \qquad (e_i^2 = -1) \\ &= e_j e_j e_k e_k \qquad (e_j e_k = -e_k e_j) \\ &= (-1)(-1) = 1. \end{aligned}$$

Thus $(u-1)(u+1) = 0$. As A is a division algebra, $e_i e_j e_k = u = \pm 1$. Hence $e_k = \pm(e_i e_j)^{-1}$ as required. □

Lemma 132. $n = 1$, 2 *or* 4.

PROOF. By Lemma 122, $n \neq 3$. Thus we need to show that $n \leq 4$. Suppose $n \geq 5$. By the previous lemma, $e_3 = \pm(e_1 e_2)^{-1}$ and $e_4 = \pm(e_1 e_2)^{-1}$, and so $e_4 = \pm e_3$. This contradicts the fact that $e_1, \ldots, e_{n-1}$ is a basis. □

PROOF OF FROBENIUS' THEOREM. Recall that $A = \mathbb{R} \oplus V$ and $\dim(V) = n-1$. If $n = 1$, then $A = \mathbb{R}$.

Suppose $n = 2$. Then $V = \mathbb{R}e_1$ and so $A = \mathbb{R} \oplus \mathbb{R}e_1$, and moreover $e_1^2 = -1$. Thus $A \cong \mathbb{C}$.

Finally suppose $n = 4$. Then $A = \mathbb{R} \oplus \mathbb{R}e_1 \oplus \mathbb{R}e_2 \oplus \mathbb{R}e_3$. Let $\mathbf{i} = e_1$, $\mathbf{j} = e_2$, $\mathbf{k} = e_1 e_2$. We know from Lemma 130 and Lemma 131 that $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, and $\mathbf{i} \cdot \mathbf{j} = \mathbf{k}$, $\mathbf{j} \cdot \mathbf{i} = -\mathbf{k}$ etc. We simply check that the relations (8) hold. Therefore $A \cong \mathbb{H}$. □

6. An Infinite Dimensional Example

We have seen that the only finite dimensional complex division algebra is $\mathbb{C}$, and the only finite dimensional real division algebras are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$. What if we drop the restriction that the dimension is finite. Are there any others that are infinite dimensional? The answer is yes, there are plenty. Here we give two examples. A Laurent series in variable x with coefficients in $\mathbb{C}$ is an expression of the form $\sum_{n=m}^{\infty} a_n x^n$ where $m \in \mathbb{Z}$ and $a_n \in \mathbb{C}$. For example,

$$\sum_{n=-4}^{\infty} i^n x^n = x^{-4} + ix^{-3} - x^{-2} - ix^{-1} + 1 + ix + \cdots$$

is a Laurent series. But

$$\sum_{n=-\infty}^{\infty} i^n x^n$$

is not a Laurent series; in a Laurent series we can have infinitely many terms with positive exponent, but only finitely many with negative exponent. The set of Laurent series in x with coefficients in $\mathbb{C}$ is usually denoted by $\mathbb{C}((x))$. This is in fact a field if addition and multiplication are defined in an obvious way. For example

$$\begin{aligned}\frac{1}{x-ix^2} &= x^{-1}\cdot\frac{1}{1-ix} = x^{-1}(1+ix+(ix)^2+(ix)^3+\cdots\\ &= x^{-1}+i-x-ix^2+x^3+\cdots.\end{aligned}$$

Note that $\mathbb{C}((x))$ is infinite dimensional division algebra over $\mathbb{C}$ as $1, x, x^2, \ldots$ are linearly independent.

You might be wondering if there are non-commutative examples, and the answer is yes. Let $\sigma : \mathbb{C} \to \mathbb{C}$ denote complex conjugation. Instead of defining multiplication on the Laurent series in the obvious way we let

$$xb = \sigma(b)x, \qquad b \in \mathbb{C}$$

and we extend distributively. It follows that $x^n b = \sigma^n(b)x^n$ for $n \in \mathbb{Z}$. Observe that

$$\sigma^n(b) = \begin{cases} b & \text{if } n \text{ is even} \\ \overline{b} & \text{if } n \text{ is odd.}\end{cases}$$

For example,

$$\begin{aligned}(x^{-1}+ix^2)(x^{-2}+(1+i)x) &= x^{-1}\cdot x^{-2} + x^{-1}\cdot(1+i)x + ix^2\cdot x^{-2}\\ &\quad + ix^2\cdot(1+i)x\\ &= x^{-3} + \sigma^{-1}(1+i)\cdot x^{-1}\cdot x + i\\ &\quad + i\cdot\sigma^2(1+i)\cdot x^2\cdot x\\ &= x^{-3} + (1-i) + i + i(1+i)\cdot x^3\\ &= x^{-3} + 1 + (-1+i)x^3.\end{aligned}$$

Addition (defined in the obvious way) and multiplication defined as above make the set of Laurent series with coefficients in $\mathbb{C}$ into a ring denoted by $\mathbb{C}((x;\sigma))$. Note that this ring has the same elements as $\mathbb{C}((x))$ and the same addition, but different multiplication. It is clear that $\mathbb{C}((x;\sigma))$ is non-commutative (since $x\cdot i = -i\cdot x$). It can be shown that $\mathbb{C}((x;\sigma))$ is a division ring, and it is clear that $\mathbb{R}$ belongs to the centre of $\mathbb{C}((x;\sigma))$. Thus it is an infinite dimensional division algebra over $\mathbb{R}$.

Exercise 133. Determine the centre of $\mathbb{C}((x;\sigma))$.

CHAPTER 6

Wedderburn's Little Theorem

1. Main Theorem

Theorem 134 (Wedderburn's Little Theorem)**.** *Every finite division ring is a field.*

Recall that a division ring is a ring in which every non-zero element is a unit, and a field is a *commutative* ring in which every non-zero element is a unit. Thus to prove the theorem what we're required to do is to show that every finite division ring is commutative. There are infinite division rings that are not commutative and therefore not fields (for example $\mathbb{H}$), but the theorem is saying that all finite division rings are fields.

You already know examples of finite fields: $\mathbb{Z}/p\mathbb{Z}$ is a finite field for any prime p. We shall see other examples of finite fields later.

2. Centralizers

Definition. Let R be a ring and $x \in R$. We define the **centralizer** of x to be the set

$$C_x = \{r \in R \ : \ rx = xr\}.$$

In other words, it is the set of elements of R that commute multiplicatively with x.

Lemma 135. *C_x is a subring of R. Moreover,*

$$\bigcap_{x \in R} C_x = Z(R).$$

Proof. This follows easily from the definitions. □

Exercise 136. Compute the centralizer of $\mathbf{i} + \mathbf{j}$ in $\mathbb{H}$.

Lemma 137. *Let D be a division ring, and $x \in D$. Then C_x is a division subring of D.*

Proof. We know that C_x is a subring of D by Lemma 135. Let u be a non-zero element of C_x. As $D \supseteq C_s$ is a division ring, u has a multiplicative inverse u^{-1} in D. We need to show that $u^{-1} \in C_x$. But by definition of C_x

$$ux = xu.$$

Multiplying both sides on the left and on the right by u^{-1} we obtain

$$xu^{-1} = u^{-1}x.$$

Hence $u^{-1} \in C_x$ are required. □

3. Finite Division Rings and Centralizers as Vector Spaces

Recall (Theorem 113) that the centre $Z(D)$ of a division ring D is a field, and D is a vector space over $Z(D)$.

Lemma 138. *Let D be a finite division ring and write $q = \#Z(D)$. Let n be the dimension of D as a vector space over $Z(D)$.*

(i) $\#D = q^n$.
(ii) For every $x \in D$, there is some $d \mid n$ such that $\#C_x = q^d$.

Proof. Let $v_1, \ldots, v_n$ be a basis for D over $\mathbb{F} = Z(D)$. Then every element of D can be written uniquely as $\alpha_1 v_1 + \cdots + \alpha_n v_n$ where $\alpha_i \in \mathbb{F}$. The number of possibilities for any α_i is $\#F = q$. Thus the number of elements of D is q^n. This proves (i).

Let $x \in D$. Then $Z(D) \subseteq C_x$, and thus the division ring C_x is a vector space over $Z(D)$. As above $\#C_x = q^d$ where d is the dimension. We need to show that $d \mid n$. For this we will use the multiplicative structure. As D, C_x are division rings,

$$D^* = D \setminus \{0\}, \qquad C_x^* = C_x \setminus \{0\}.$$

Thus

$$\#D^* = q^n - 1, \qquad \#C_x^* = q^d - 1.$$

But C_x is a subring of D and so C_x^* is a subgroup of D^*. By Lagrange's Theorem

$$(q^d - 1) \mid (q^n - 1).$$

Using division with remainder we have $n = md + r$ where $0 \leq r < d$, and m is a positive integer. Note that

$$q^{md} - 1 = (q^d - 1)(q^{(m-1)d} + q^{(m-2)d} + \cdots + 1).$$

Hence $(q^d - 1) \mid (q^{md} - 1)$. But

$$q^n - 1 = q^{md+r} - 1 = q^r(q^{md} - 1) + (q^r - 1).$$

As $(q^d - 1) \mid (q^n - 1)$ and $(q^d - 1) \mid (q^{md} - 1)$ we have $(q^d - 1) \mid (q^r - 1)$. But $r < d$ and so $q^r - 1 < q^d - 1$. Therefore $q^r - 1 = 0$, so $r = 0$ so $n = md$, giving $d \mid n$ as required. □

4. The Orbit Stabilizer Theorem

We will need the orbit-stablizer theorem. Let G be a group acting on a set X. Recall that this means there is an operation

$$G \times X \to X, \qquad (g, x) \mapsto g * x$$

such that

- $1 * x = x$ for all $x \in X$ (here 1 is the identity element for G);
- $g * (h * x) = (gh) * x$ for all $x \in X$ and g, $h \in G$.

Recall that the **orbit** of an element $x \in X$ is the set

$$\mathrm{Orb}(x) = \{g * x \ : \ g \in G\},$$

and the **stabilizer** of $x \in X$ is

$$\mathrm{Stab}(x) = \{g \in G \ : \ g * x = x\}.$$

Note that the orbit $\mathrm{Orb}(x)$ is a subset of X, and the stabilizer $\mathrm{Stab}(x)$ is a subgroup of G.

Now suppose that G and X are finite. The orbit and stabilizer of $x \in X$ are linked by the following useful formula, which is part of the orbit-stabilizer theorem:

$$\#G = \#\,\mathrm{Stab}(x) \cdot \#\,\mathrm{Orb}(x). \tag{9}$$

Another part of the orbit-stabilizer theorem says that the orbits form a partition of X. What this means is that every element $x \in X$ belongs to an orbit (indeed $x \in \mathrm{Orb}(x)$) and if x, $y \in X$ then either $\mathrm{Orb}(x) = \mathrm{Orb}(y)$ or $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) = \emptyset$. If $x_1, x_2, \ldots, x_r$ are representatives of the disjoint orbits, then

$$\#X = \#\,\mathrm{Orb}(x_1) + \#\,\mathrm{Orb}(x_2) + \cdots + \#\,\mathrm{Orb}(x_r) \tag{10}$$

since the orbits form a partition. Using (9) we deduce that

$$\#X = \frac{\#G}{\#\,\mathrm{Stab}(x_1)} + \cdots + \frac{\#G}{\#\,\mathrm{Stab}(x_r)}.$$

5. The Class Equation

Let G be a finite group. We let G act on itself by conjugation:

$$G \times G \to G, \qquad g * x = gxg^{-1}.$$

Clearly $1 * x = x$, and for g, $h \in G$ we have

$$(gh) * x = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g * (h * x).$$

Thus we do have a group action. Note that the orbit of $x \in G$ is the set of all conjugates of x, also called the conjugacy class of x.

We define the **centre** of G to be

$$Z(G) = \{x \in G \ : \ gx = xg \text{ for all } g \in G\}.$$

Lemma 139. *$\#\,\mathrm{Orb}(x) = 1$ if and only if $x \in Z(G)$.*

Proof. Note that $x = 1 * x$. Thus $x \in \mathrm{Orb}_x$. Hence

$$\begin{aligned}
\#\,\mathrm{Orb}(x) = 1 \quad &\iff \quad \mathrm{Orb}(x) = \{x\} \\
&\iff \quad g * x = x \text{ for all } g \in G \\
&\iff \quad gxg^{-1} = x \text{ for all } g \in G \\
&\iff \quad gx = xg \text{ for all } g \in G \\
&\iff \quad x \in Z(G).
\end{aligned}$$

□

Theorem 140 (The Class Equation)**.** *Let G be a finite group. Let $y_1, \dots, y_k$ be representatives for the orbits of size at least 2 (for action of G on itself by conjugation). Then*

$$\#G = \#Z(G) + \sum_{i=1}^{k} \frac{\#G}{\#\operatorname{Stab}(y_i)}. \tag{11}$$

This identity is known as the **class equation**. [1]

Proof. Let $\{z_1\}, \{z_2\}, \dots, \{z_\ell\}$ be the orbits of size 1. Then $z_1, \dots, z_\ell, y_1, \dots, y_k$ are representatives of all the the orbits, and by (10)

$$\#G = \#\operatorname{Orb}(z_1) + \cdots + \#\operatorname{Orb}(z_\ell) + \#\operatorname{Orb}(y_1) + \cdots + \#\operatorname{Orb}(y_k).$$

But $\operatorname{Orb}(z_i) = \{z_i\}$. Moreover, by the Lemma 139, $Z(G) = \{z_1, z_2, \dots, z_\ell\}$, so $\ell = \#Z(G)$. Hence

$$\#G = \#Z(G) + \#\operatorname{Orb}(y_1) + \cdots + \#\operatorname{Orb}(y_k).$$

Finally we apply (9) to obtain $\#\operatorname{Orb}(y_i) = \#G/\#\operatorname{Stab}(y_i)$. □

Corollary 141. *Let D be a finite division ring of dimension n over its centre $Z(D)$, and write $q = \#Z(D)$. Suppose D is not a field. Then $n > 1$ and there are positive integers $d_1, d_2, \dots, d_k$ such that $d_i \mid n$, $d_i < n$ and*

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{d_i} - 1}. \tag{12}$$

Proof. The assumption that D is not a field is equivalent to saying that the division ring D is not commutative. This is equivalent to saying that $Z(D)$ is a proper subset of D. Recall that $\#D = q^n$ (Lemma 138). Thus $n > 1$.

We shall apply the class equation where $G = D^*$ (acting on itself by conjugation). Here $\#G = q^n - 1$. Moreover $Z(D^*) = Z(D) \setminus \{0\}$. Hence $\#Z(D^*) = q - 1$.

Let $y_1, \dots, y_k$ be representatives of the orbits of size at least 2. If $k = 0$ then from the class equation $q^n - 1 = q - 1$ contradicting $n > 1$. Hence $k \geq 1$. Moreover,

$$\operatorname{Stab}(y_i) = \{g \in D^* : gy_ig^{-1} = y\} = \{g \in D^* : gy_i = y_ig\}.$$

It follows that $\operatorname{Stab}(y_i) = C_{y_i}^*$ where $C_{y_i} = \{g \in D : gy_i = y_ig\}$ is the centralizer of y_i. By Lemma 138, $\#C_{y_i} = q^{d_i}$ for some $d_i \mid n$. Hence $\#\operatorname{Stab}(y_i) = \#C_{y_i}^* = q^{d_i} - 1$. Substituting into the class equation we obtain (12). To complete the proof we must show that $d_i < n$. However, if $d_i = n$ then $\#\operatorname{Stab}(y_i) = \#D^*$. By (9), $\#\operatorname{Orb}(y_i) = \#D^*/\#\operatorname{Stab}(y_i) = 1$, contradicting the choice of the y_i as representatives for the orbits of size at least 2. □

[1] As the action is given by conjugation, the orbit of y_i is the conjugacy class of y_i. This is where the name comes from.

6. Cyclotomic Polynomials

Lemma 142. *Let $d \mid n$, where d, n are positive integers. Then $X^d - 1$ divides $X^n - 1$ (as elements of the polynomial ring $\mathbb{Q}[X]$).*

PROOF. Write $n = md$. Then

$$X^n - 1 = X^{md} - 1 = (X^d - 1)(X^{(m-1)d} + X^{(m-2)d} + \cdots + X^d + 1).$$

Hence $X^d - 1$ divides $X^n - 1$. □

Definition. We define the **n-th cyclotomic polynomial**

$$\Phi_n(X) = \frac{X^n - 1}{\mathrm{LCM}\{X^d - 1 \ : \ d \mid n, \ d < n\}}. \tag{13}$$

Exercise 143. Write down $\Phi_n(X)$ for $1 \leq n \leq 6$. You should get $X - 1$, $X + 1$, $X^2 + X + 1$, $X^2 + 1$, $X^4 + X^3 + X^2 + X + 1$ and $X^2 - X + 1$.

Example 144. Let p be a prime. Then

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1.$$

Example 145. Let $r \geq 1$. Then

$$\begin{aligned} \Phi_{2^r}(X) &= \frac{X^{2^r} - 1}{\mathrm{LCM}(X - 1, X^2 - 1, X^4 - 1, \ldots, X^{2^{r-1}} - 1)} \\ &= \frac{X^{2^r} - 1}{X^{2^{r-1}} - 1} \\ &= X^{2^{r-1}} + 1. \end{aligned}$$

Exercise 146. Let m be a positive integer. Show that

$$\Phi_{3^m}(X) = \left(X^{3^{m-1}}\right)^2 + X^{3^{m-1}} + 1.$$

Theorem 147. *$\Phi_n(X)$ is a monic polynomial with coefficients in $\mathbb{Z}$.*

PROOF. We write $X^n - 1$ and each of the $X^d - 1$ as products of irreducible factors. By Gauss' Lemma, we can take all these irreducible factors as monic and with integer coefficients. As $X^d - 1 \mid X^n - 1$ for all $d \mid n$ all the irreducible factors appearing in the denominator also appear in the numerator. Cancelling these we get Φ_n as a product of irreducible factors with integer coefficients that are monic. This shows that $\Phi_n(X)$ is monic with integer coefficients. □

Now we look at the factorization of Φ_n over $\mathbb{C}$.

Theorem 148. *Let $\zeta_n = \exp(2\pi i/n)$. Then*

$$\Phi_n(X) = \prod_{\substack{1 \leq r < n, \\ \gcd(r,n) = 1}} (X - \zeta_n^r).$$

PROOF. The roots of $X^n - 1$ are the n-th roots of 1. These are

$$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}.$$

As these are distinct, and there are n of them, and $X^n - 1$ has degree n, we know that

$$X^n - 1 = \prod_{0 \le r < n} (X - \zeta_n^r).$$

As $\Phi_n(X)$ is a factor of $X^n - 1$, its roots are among $1, \zeta_n, \ldots, \zeta_n^{n-1}$. To obtain the roots of $\Phi_n(X)$ we have to remove all ζ_n^r which is a root of $X^d - 1$ for some $d \mid n$, $d < n$.

Claim: ζ_n^r is a root of $X^d - 1$ with $d \mid n$ and $d < n$ if and only if $\gcd(r, n) > 1$.

The claim immediately implies the theorem. Therefore it is enough ot prove the claim. Let $m = \gcd(r, n)$ and suppose that $m > 1$. Let $d = n/m$. Then $d \mid n$ and $d < n$. Moreover $n \mid rd$. Hence $(\zeta_n^r)^d = 1$ so ζ_n^r is a root of $X^d - 1$ ($d \mid n$, $d < n$). Coversely, suppose $\gcd(r, n) = 1$ and ζ_n^r is a root of $X^d - 1$ for some $d \mid n$. Then $\zeta_n^{rd} = 1$ and so $n \mid rd$. But $\gcd(r, n) = 1$. Hence $n \mid d$ and so $n = d$. This proves the claim and completes the proof. □

7. Proof of Wedderburn's Little Theorem

We now prove Wedderburn's Little Theorem (Theorem 134). Let D be a finite division ring of dimension n over its centre $Z(D)$, and write $q = \#Z(D)$. Suppose D is not a field. By Corollary 141, we know that $n > 1$ and there are positive integers $d_1, d_2, \ldots, d_k$ such that $d_i \mid n$, $d_i < n$ and

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{d_i} - 1}. \tag{14}$$

We will use this to derive a contradiction. As $\Phi_n(X)$ is monic with integer coefficients, $\Phi_n(q)$ is an integer. Since $q = \#Z(D)$ and $Z(D)$ is a field and so contains 0, 1, we have $q \ge 2$. The roots of $\Phi_n(X)$ are roots of unity, so $\Phi_n(q)$ is a non-zero integer. But the definition (13) of $\Phi_n(X)$, we know that $\Phi_n(X)$ is a factor of $X^n - 1$ and of $(X^n - 1)/(X^{d_i} - 1)$ for $i = 1, \ldots, k$. Thus $\Phi_n(q)$ is a factor of $q^n - 1$ and $(q^n - 1)/(q^{d_i} - 1)$ for $i = 1, \ldots, k$. From (14),

$$\Phi_n(q) \mid (q - 1). \tag{15}$$

We shall show that $|\Phi_n(q)| > q - 1$. This will contradict (15), and complete the proof. If $n = 2$ then $\Phi_2(q) = q + 1 > q - 1$ giving the required contradiciton. So suppose $n > 2$. Note that ζ_n is a root of $\Phi_n(X)$ so it has degree ≥ 1. Let λ be any root of $\Phi_n(X)$. This is a root of unity, so we can write $\lambda = a + bi$ where a, $b \in \mathbb{R}$ and $a^2 + b^2 = |\lambda|^2 = 1$. Moreover $\lambda \ne \pm 1$, since these are roots of $X - 1$,

$X^2 - 1$ and $n > 2$. Hence $b \neq 0$, and so $a^2 = 1 - b^2 < 1$ and hence $a < 1$. Now

$$\begin{aligned} |q - \lambda|^2 &= |(q - a) + bi|^2 \\ &= (q - a)^2 + b^2 \\ &= q^2 - 2aq + (a^2 + b^2) \\ &= q^2 - 2aq + 1 \\ &> q^2 - 2q + 1 \qquad a < 1 \text{ so } -2aq > -2q \\ &= (q - 1)^2. \end{aligned}$$

Hence $|q - \lambda| > q - 1$, for all roots λ of $\Phi_n(X)$. It follows that

$$|\Phi_n(q)| = \prod_{\substack{1 \leq r < n \\ \gcd(r,n)=1}} |q - \zeta_n^r| > (q - 1)^{\deg(\Phi_n(X))} \geq q - 1,$$

completing the proof.

Exercise 149. Let R be a ring, and let J be a proper 2-sided ideal of R. Suppose there are elements $a_1, a_2, \ldots, a_n \in R$ satisfying the following two properties:

- for every $a \in R$ there is some $1 \leq i \leq n$ such that $a - a_i \in J$;
- for every $1 \leq i \leq n$, either $a_i \in J$ or there is some $1 \leq j \leq n$ such that $a_i a_j - 1 \in J$ and $a_j a_i - 1 \in J$.

Show that R/J is a field.

CHAPTER 7

Modules

1. Definitions and First Examples

Definition. Let R be a ring. A **left R-module** is an additive abelian group $(M, +, 0)$ equipped with an operation

$$R \times M \to M, \qquad (r, m) \mapsto rm \qquad \text{(scalar multiplication)}$$

that satisfies the following properties:

(a) $1 \cdot m = m$ for all $m \in M$;
(b) $(r \cdot s) \cdot m = r \cdot (s \cdot m)$ for all r, $s \in R$ and $m \in M$;
(c) $(r + s) \cdot m = r \cdot m + s \cdot m$ for all r, $s \in R$ and $m \in M$;
(d) $r \cdot (m + n) = r \cdot m + r \cdot n$ for all $r \in R$ and m, $n \in M$.

There is also a notion of a right R-module, with scalar multipliction written as $M \times R \to M$, $(m, r) \mapsto mr$ and the definition is adjusted accordingly.

Example 150. Let K be a field. A K-module is exactly the same as a K-vector space.

Example 151. A $\mathbb{Z}$-module is exactly the same as an additive abelian group.

Example 152. Let R be a ring. A left ideal of R is a left R-module, and a right ideal is a right R-module.

For example, in Exercise 25, we saw that

$$\mathfrak{a} = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \quad : \quad a,\ c \in \mathbb{C} \right\}$$

is a left ideal of the matrix ring $M_2(\mathbb{C})$. It is therefore a left $M_2(\mathbb{C})$-module.

Example 153. Let R be a ring and $n \geq 1$. Then $(R^n, +, 0)$ is an abelian group. Here we think of the elements of R^n as column vectors

$$\mathbf{r} = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}.$$

Given a matrix $A \in M_n(R)$ (this is an $n \times n$ matrix with entries in R) we can form the product $A\mathbf{r}$. This is $n \times 1$ matrix with entries in R

(i.e. a column vector) and so belongs to R^n. So we have an operation

$$M_n(R) \times R^n \to R^n, \qquad (A, \mathbf{r}) \mapsto A \cdot \mathbf{r},$$

which we think of as scalar multiplication. Recall that $M_n(R)$ is a ring. From the usual properties of matrix operations we conclude that R^n is a left $M_n(R)$-module.

We can also think of R^n as a right $M_n(R)$-module if we regard the elements of R^n as row vectors. If we think of elements of R^n as column vectors then multiplication by $n \times n$ matrices on the left is not defined.

Important Remark. Usually when we speak of modules we mean left modules.

Example 154. Let K be a field and V a vector space. Let $\phi : V \to V$ be a K-linear transformation. We shall use ϕ to make V into a $K[X]$-module (where $K[X]$ is the ring of polynomials in X with coefficients in K). Let

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n, \qquad a_i \in K$$

and $\mathbf{v} \in V$. We define "scalar multiplication" $f(X) \cdot \mathbf{v}$ by

$$(a_0 + a_1 X + \cdots + a_n X^n) \cdot \mathbf{v} = a_0 \mathbf{v} + a_1 \phi(\mathbf{v}) + a_2 \phi^2(\mathbf{v}) + \cdots + a_n \phi^n(\mathbf{v}),$$

where $\phi^2 = \phi \circ \phi$, $\phi^3 = \phi \circ \phi \circ \phi$ and so on. It is an easy exercise to see that this makes V into a $K[X]$-module.

Conversely, let V be a $K[X]$-module. Then as $K \subset K[X]$ we see that V is also a K-module which is the same as a K-vector space (remember that K is a field). Define

$$\phi : V \to V, \qquad \phi(\mathbf{v}) = X \cdot \mathbf{v}$$

where $X \cdot \mathbf{v}$ simply means multiplication of $\mathbf{v} \in V$ by the scalar $X \in K[X]$. If $\lambda \in K$ and $\mathbf{v} \in V$ then

$$\begin{aligned}
\phi(\lambda \mathbf{v}) &= X \cdot (\lambda \mathbf{v}) && \text{definition of } \phi \\
&= (X\lambda) \cdot \mathbf{v} && \text{condition (b)} \\
&= (\lambda X) \cdot \mathbf{v} && K[X] \text{ is commutative} \\
&= \lambda (X \cdot \mathbf{v}) && \text{condition (b) again} \\
&= \lambda \phi(\mathbf{v}).
\end{aligned}$$

Also condition (d) of the definition of a module tells us that

$$\phi(\mathbf{v} + \mathbf{w}) = X \cdot (\mathbf{v} + \mathbf{w}) = X \cdot \mathbf{v} + X \cdot \mathbf{w} = \phi(\mathbf{v}) + \phi(\mathbf{w})$$

for all $\mathbf{v}$, $\mathbf{w} \in V$. Thus ϕ is a K-linear transformation of the K-vector space V.

We conclude the following: there is one-one correspondence between K-linear transformations of a K-vector space V, and $K[X]$-module structures on a K-vector space V.

Example 155. We can make the previous example more explicit. Recall that a finite-dimensional K-vector space is isomorphic to K^n. Now any K-linear transformation $\phi : K^n \to K^n$ is represented by a square matrix; i.e. an element $A \in M_n(K)$. Fix such a matrix $A \in M_n(K)$. Let $f(X) = a_0 + a_1X + \cdots + a_mX^m \in K[X]$ and $\mathbf{v} \in K^n$. Define

$$(16)\quad (a_0+a_1X+\cdots+a_mX^m)\cdot\mathbf{v} = a_0\mathbf{v}+a_1A\mathbf{v}+a_2A^2\mathbf{v}+\cdots+a_mA^m\mathbf{v}.$$

Note that multiplying an element of K^n by X is equivalent to multiplying that element by A; we say that X **acts as** A **on** K^n. It is easy to check that K^n becomes a $K[X]$-module with this scalar product. In fact, we don't need to check this. We can apply the previous example with $\phi : K^n \to K^n$ given by $\phi(\mathbf{v}) = A\mathbf{v}$. As usual, we are thinking of vectors $\mathbf{v}$ as being column vectors so that we can apply matrices on the left.

Exercise 156. Let G be an additive abelian group and let $n \geq 2$. Suppose $nG = 0$ (i.e. $ng = 0$ for all $g \in G$). Define

$$\mathbb{Z}/n\mathbb{Z} \times G \to G, \qquad (\overline{a}, g) \mapsto ag.$$

Show that this operation is well-defined and that, with this as scalar multiplication, G is a $\mathbb{Z}/n\mathbb{Z}$-module.

Exercise 157. Let R be a ring and $\mathfrak{a}$ a 2-sided ideal. Let M be an R-module. Suppose $\mathfrak{a}M = 0$ (i.e. $am = 0$ for all $a \in \mathfrak{a}$ and $m \in M$). Define

$$R/\mathfrak{a} \times M \to M, \qquad (r + \mathfrak{a}, m) \mapsto rm.$$

Show that this operation is well-defined and that, with this as scalar multiplication, M is an $R/\mathfrak{a}$-module.

2. Submodules, Quotients, Direct Products, Homomorphisms

Definition. Let R be a ring and M an R-module (recall our convention that R-modules mean left R-modules). An R-submodule of M is a subgroup $(N, +, 0)$ of $(M, +, 0)$ that satisfies $r \cdot n \in N$ for all $r \in R$ and $n \in N$. It is easy to see that an R-submodule is an R-module.

Example 158. Let K be a field. Recall that a K-module is the same as a K-vector space. Let V be a K-vector space. A K-submodule of V is the same as subspace of V.

Example 159. Recall that a $\mathbb{Z}$-module is the same as an additive abelian group. A submodule of a $\mathbb{Z}$-module is just a subgroup.

Example 160. Let R be a ring. We can think of R as a left R-module. Then a submodule of R is the same as a left ideal. For example $7\mathbb{Z}$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}$. The left ideal of $M_2(\mathbb{C})$ given in Example 25 is an $M_2(\mathbb{C})$-submodule of $M_2(\mathbb{C})$.

Example 161. Here is a more sophisticated example. Let K be a field, $A \in M_n(K)$. We saw in Example 155 that K^n becomes a $K[X]$-module by defining scalar multiplication by (16). Let $\lambda \in K$ be an eigenvalue for A and $\mathbf{u} \in K^n$ be a corresponding eigenvector (recall this is a non-zero vector that satisfies $A\mathbf{u} = \lambda\mathbf{u}$). Let $U = \{\alpha\mathbf{u} : \alpha \in K\}$ be the span of $\mathbf{u}$. This is a K-subspace of K^n. Now let $a_i \in K$. Then

$$(a_0 + a_1X + \cdots + a_mX^m) \cdot \underbrace{(\alpha\mathbf{u})}_{\in U} = \underbrace{(a_0\alpha + a_1\alpha\lambda + \cdots + a_m\alpha\lambda^m)}_{\in K} \cdot \mathbf{u} \in U.$$

Hence, not only is U a K-subspace of K^n. It is also a $K[X]$-submodule.

Conversely a $K[X]$-submodule U of K^n must be a K-subspace (since $K \subset K[X]$). It doesn't have to be 1-dimensional as a vector space, but let's suppose it is. So it is generated by one non-zero vector $\mathbf{u}$: $U = \{\alpha\mathbf{u} : \alpha \in K\}$. Now $X \cdot \mathbf{u} \in U$ (as $X \in K[X]$ and $\mathbf{u} \in U$ and U is a $K[X]$-submodule). Thus $A\mathbf{u} \in U$. But U is generated by $\mathbf{u}$, so $A\mathbf{u} = \lambda\mathbf{u}$. Thus $\mathbf{u}$ is an eigenvector of A.

Definition. Let M be an R-module and N be an R-submodule of M. We define the **quotient module** M/N to be the set of cosets $m + N$ with $m \in M$. Addition and scalar multiplication are given in the natural way

$$\begin{cases} (m_1 + N) + (m_2 + N) = (m_1 + m_2) + N, & m_1,\ m_2,\ m \in M, \\ r \cdot (m + N) = rm + N, & r \in R. \end{cases}$$

It is easy to check that these operations are well-defined and that M/N is an R-module. The definition of quotient module generalizes the definition of quotient group for additive abelian groups (from MA136).

Example 162. Recall that $\mathbb{R}^2$ is an $M_2(\mathbb{R})$-module. Now $\mathbb{Z}^2 \subset \mathbb{R}^2$ is a subgroup of $\mathbb{R}^2$, but not an $M_2(\mathbb{R})$-submodule. For example,

$$A = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R}), \qquad \mathbf{v} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{Z}^2, \qquad A\mathbf{v} = \begin{pmatrix} 1/2 \\ 0 \end{pmatrix} \notin \mathbb{Z}^2.$$

Thus $\mathbb{Z}^2$ is not an $M_2(\mathbb{R})$-submodule of $\mathbb{R}^2$.

However, $\mathbb{R}^2$ is also an $M_2(\mathbb{Z})$-module, and $\mathbb{Z}^2$ is an $M_2(\mathbb{Z})$-submodule. Hence the quotient $\mathbb{R}^2/\mathbb{Z}^2$ is an $M_2(\mathbb{Z})$-module.

Lemma 163. *Let M, N be R-modules. Then*

$$M \times N = \{(m, n) \ :\ m \in M,\ n \in N\}$$

is an R-module where addition and scalar multiplication is defined by

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2), \qquad r \cdot (m, n) = (rm, rn).$$

PROOF. Easy verification. □

The module $M \times N$ is called the **direct product** of the modules M, N. We can iterate this construction: if $M_1, \ldots, M_n$ are R-modules then the direct product $M_1 \times \cdots \times M_n$ is also an R module, with

the operations defined in the obvious way. In particular, if M is an R-module and $n \geq 1$ then M^n is an R-module.

Example 164. Note that $M \times 0 = \{(m, 0) : m \in M\}$ and $0 \times N = \{(0, n) : n \in N\}$ are R-submodules of $M \times N$.

Definition. Let M, N be R-modules. A map $\phi : M \to N$ is a homomorphism if

$$\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2), \qquad \phi(rm) = r\phi(m).$$

An isomorphism is a bijective homomorphism.

Example 165. Let K be a field. Recall that M, N are K-modules if and only they are K-vector spaces. Then ϕ is a homomorphism of K-modules if and only it is a linear transformation.

Example 166. Recall that a $\mathbb{Z}$-module is the same as an abelian group. A homomorphism of $\mathbb{Z}$-modules is the same as a homomorphism of abelian groups.

Given a homomorphism of R-modules $\phi : M \to N$ we define the kernel and image in the usual way

$$\mathrm{Ker}(\phi) = \{m \in M \ : \ \phi(m) = 0\}, \qquad \mathrm{Im}(\phi) = \{\phi(m) : m \in M\}.$$

Theorem 167 (The Isomorphism Theorem)**.** *Let $\phi : M \to N$ be a homomorphism of R-modules.*

(i) $\mathrm{Ker}(\phi)$ *is an R-submodule of M.*
(ii) $\mathrm{Im}(\phi)$ *is an R-submodule of N.*
(iii) The induced map

$$\hat{\phi} : M/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi), \qquad \hat{\phi}(m + \mathrm{Ker}(\phi)) = \phi(m)$$

is an isomorphism of R-modules.

Proof. Routine verification. □

Exercise 168. Let $\phi : M \to N$ be a homomorphism of R-modules. Show that ϕ is injective if and only if $\mathrm{Ker}(\phi) = 0$.

Exercise 169. (The Correspondence Theorem) Let R be a ring, M a left R-module and N a submodule of M. Let $\mathcal{A}$ be the set of submodules of M containing N. Let $\mathcal{B}$ be the set of submodules of the R-submodule M/N. Let

$$\pi \ : \ M \to M/N, \qquad \pi(m) = m + N$$

be the quotient map. Show that the map

$$\psi : \mathcal{B} \to \mathcal{A}, \qquad \psi(T) = \pi^{-1}(T)$$

gives a bijection from $\mathcal{B}$ to $\mathcal{A}$.

3. Direct Sums

Let M be an R-module and let N_1, N_2 be two submodules. The **sum** of N_1, N_2 is

$$N_1 + N_2 = \{x_1 + x_2 \ : \ x_1 \in N_1, \ x_2 \in N_2\}.$$

It is easy to check that this is an R-module. We say that this sum is **direct** if $N_1 \cap N_2 = \{0\}$.

Lemma 170. *The sum $N_1 + N_2$ is direct if and only if every element $x \in N_1 + N_2$ can be decomposted as $x = x_1 + x_2$ with $x_1 \in N_1$, $x_2 \in N_2$ in a unique way.*

Proof. Suppose the sum is direct. We already know from the definition that $x = x_1 + x_2$ with $x_i \in N_i$. Suppose $x = y_1 + y_2$ with $y_i \in N_i$. From $x_1 + x_2 = x = y_1 + y_2$ we deduce

$$\underbrace{x_1 - y_1}_{\in N_1} = \underbrace{y_2 - x_2}_{\in N_2} \in N_1 \cap N_2 = \{0\}.$$

As $N_1 \cap N_2 = 0$ we have $x_1 = y_1$ and $x_2 = y_2$ establishing uniqueness.

Now suppose the sum $N_1 + N_2$ is not direct and so $N_1 \cap N_2 \neq 0$. Let $z \in N_1 \cap N_2 - \{0\}$. Observe

$$\underbrace{z}_{\in N_1} + \underbrace{(-z)}_{\in N_2} \quad = \quad 0 \quad = \quad \underbrace{0}_{\in N_1} + \underbrace{0}_{\in N_2}.$$

Thus uniqueness fails if the sum is not direct. □

When the sum $N_1 + N_2$ is direct we write $N_1 \oplus N_2$ for the sum. We say that M is the **direct sum** of N_1, N_2 and write $M = N_1 \oplus N_2$ if $M = N_1 + N_2$ and $N_1 \cap N_2 = \{0\}$. Thus the concept of direct sums of modules is just a trivial generalization of that of direct sums of vector spaces.

More generally, if $N_1, \ldots, N_k$ are submodules of M we say that the sum $N_1 + \cdots + N_k$ is **direct** (and write $N_1 \oplus \cdots \oplus N_k$ for the sum) if

$$N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = \{0\}$$

for all j. The following is the obvious generalization of Lemma 170.

Lemma 171. *The sum $N_1 + \cdots + N_k$ is direct if and only if every element $x \in N_1 + \cdots + N_k$ can be decomposed as $x = x_1 + \cdots + x_k$ with $x_j \in N_j$ in a unique way.*

Proof. The proof is left as an easy exercise. □

Example 172. Let $V = \mathbb{R}^2$. Then $V = V_1 \oplus V_2$ where

$$V_1 = \{(x, 0) \ : \ x \in \mathbb{R}\}, \qquad V_2 = \{(0, y) \ : \ y \in \mathbb{R}\}.$$

Now let $V_3 = \{(x, x) \ : \ x \in \mathbb{R}\}$. Then $V_3 \cap (V_1 + V_2) = V_3 \neq 0$. Thus the sum $V_1 + V_2 + V_3$ is not direct.

4. Span, Linear Independence, Bases and Freeness

Definition. Let M be an R-module. Let $X = \{x_1, \ldots, x_n\}$ be a finite subset of M. We define the R**-span** of X to be

$$\mathrm{Span}_R(X) = \{r_1x_1 + \cdots + r_nx_n \ : \ r_i \in R,\ x_i \in X\}\,.$$

If X is infinite then we define

$$\mathrm{Span}_R(X) = \bigcup_{Y \text{ finite subset of } X} \mathrm{Span}_R(Y).$$

This the set of all finite linear combinations of elements of X with coefficients in R. We say a subset X of M **spans** (or **generates**) M as R-module if $M = \mathrm{Span}_R(X)$.

We say that M is **finitely generated** if it is the span of a finite subset $X \subseteq M$.

Exercise 173. Show that $\mathrm{Span}_R(X)$ is an R-submodule of M.

Note that if R is a field, and so M is an R-vector space then the span of X has the same meaning as in linear algebra.

Example 174. R^n is finitely generated as an R-module: for example it is spanned by

$$\mathbf{e}_1 = (1, 0, 0, \ldots, 0, 0), \quad \mathbf{e}_2 = (0, 1, 0, \ldots, 0, 0), \ldots, \quad \mathbf{e}_n = (0, 0, 0, \ldots, 0, 1).$$

Of course, this is not the only possible spanning set. For example,

$$\mathbf{e}_1 + \mathbf{e}_2, \quad \mathbf{e}_2, \quad \mathbf{e}_3, \ldots, \mathbf{e}_n$$

also spans R^n as an R-module.

Example 175. $M = \mathrm{Span}_R(M)$ for any M-module R.

Example 176. Let G be a group and R a ring. The group ring $R[G]$ is an R-module spanned by the set

$$\{\langle g\rangle \ : \ g \in G\}.$$

In particular, if G is finite, then $R[G]$ is a finitely generated module.

Exercise 177. Let M be an R-module. Show that M is finitely generated if and only if there is a surjective homomorphism $\phi : R^n \to M$ for some $n \geq 1$.

Definition. A subset X of M is R**-linearly independent** if whenever

$$r_1x_1 + \cdots + r_mx_m = 0$$

with $r_i \in R$, $x_i \in X$ then $r_1 = r_2 = \cdots = r_m = 0$. A subset X which both spans and is independent is called an R**-basis**. An R-module M is called **free** if it has an R-basis. Sometimes an R**-basis** is called a **free** R**-basis** to emphasise its independence.

Example 178. Recall the notation

$$G = \langle\, \mathbf{x}_1, \ldots, \mathbf{x}_r \mid \mathbf{v}_1, \ldots, \mathbf{v}_s \,\rangle$$

from Algebra I. This denotes the abelian group generated by $\mathbf{x}_1, \ldots, \mathbf{x}_r$ subject to the relations $\mathbf{v}_1, \ldots, \mathbf{v}_s$. Thus $\mathbf{x}_1, \ldots, \mathbf{x}_r$ spans G as a $\mathbb{Z}$-module. However, if $s \geq 1$, and any of the $\mathbf{v}_i$ are non-zero then this spanning set will not be free (i.e. it will not be independent), since that particular $\mathbf{v}_i$ gives a linear dependence.

For example, in the group

$$G = \langle\, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \mid \mathbf{x}_1 - \mathbf{x}_2 + 2\mathbf{x}_3 \,\rangle$$

the set $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\}$ spans but is not free, since we have the linear dependence $\mathbf{x}_1 - \mathbf{x}_2 + 2\mathbf{x}_3 = 0$. However, since $\mathbf{x}_1 = \mathbf{x}_2 - 2\mathbf{x}_3$ then we can eliminate $\mathbf{x}_1$ from our spanning set and we would still have a spanning set: $\{\mathbf{x}_2, \mathbf{x}_3\}$. This is now a basis. Thus G is free, even though our original spanning set was not free.

The word free, when applied to a set of elements of a module, means not subject to any (non-trivial linear) relations. Therefore independent.

Example 179. $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is an R-basis for R^n and so R^n is a free R-module.

Example 180. If R is a field, then an R-basis for M as a module is exactly the same as an R-basis for a M as a vector space. You know from linear algebra that every finitely generated vector space over a field has a finite basis. Therefore every finitely generated vector space over a field is free. In fact every vector space over a field has a basis and is therefore free, but this basis might be infinite.

Example 181. Let R be a ring. Then the set

$$\{1, T, T^2, \ldots\}$$

is a basis for $R[T]$ as an R-module. Therefore $R[T]$ is free as an R-module.

Example 182. If G is a group and R is a ring, then the set

$$\{\langle g \rangle \ : \ g \in G\}$$

is an R-basis for $R[G]$. Thus $R[G]$ is a free R-module.

Example 183. Recall that a module over $\mathbb{Z}$ is the same as an abelian group. Let $m \geq 2$. Consider the abelian group $(\mathbb{Z}/m\mathbb{Z}, +)$ as a $\mathbb{Z}$-module. The set $\{\overline{1}\}$ spans $\mathbb{Z}/m\mathbb{Z}$:

$$\mathrm{Span}_{\mathbb{Z}}(\overline{1}) = \{a \cdot \overline{1} \ : \ a \in \mathbb{Z}\} = \{\overline{a} \ : \ a \in \mathbb{Z}\} = \mathbb{Z}/m\mathbb{Z}.$$

However $\{\overline{1}\}$ is not $\mathbb{Z}$-linearly independent, since $m \neq 0$ but $m \cdot \overline{1} = \overline{0}$. In fact $\mathbb{Z}/m\mathbb{Z}$ does not have any non-empty $\mathbb{Z}$-linearly independent subset. If X is a non-empty subset of $\mathbb{Z}/m\mathbb{Z}$, let $\overline{x} \in X$. Then $m \cdot \overline{x} = 0$ but $m \neq 0$, so X is $\mathbb{Z}$-linearly dependent.

Now let's think about $\mathbb{Z}/m\mathbb{Z}$ as a $\mathbb{Z}/m\mathbb{Z}$-module (i.e. $R = M = \mathbb{Z}/m\mathbb{Z}$). Now

$$\text{Span}_{\mathbb{Z}/m\mathbb{Z}}(\overline{1}) = \{\overline{a} \cdot \overline{1} \ : \ \overline{a} \in \mathbb{Z}/m\mathbb{Z}\} = \mathbb{Z}/m\mathbb{Z}.$$

Let's check that the set $\{\overline{1}\}$ is $\mathbb{Z}/m\mathbb{Z}$-linearly indepdendent. Suppose $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ and $\overline{a} \cdot \overline{1} = \overline{0}$. This means that $\overline{a} = \overline{0}$. Thus $\{\overline{1}\}$ is $\mathbb{Z}/m\mathbb{Z}$-linearly independent and is therefore a $\mathbb{Z}/m\mathbb{Z}$-basis.
Important Summary: $\mathbb{Z}/m\mathbb{Z}$ is free as a $\mathbb{Z}/m\mathbb{Z}$-module. It is not free as a $\mathbb{Z}$-module.

Example 184. Let R be a ring. Then R is free when considered as an R-module. Indeed $\{1\}$ is an R-basis. This is a special case of Example 179 with $n = 1$.

Example 185. Recall from Algebra I that every finitely generated abelian group A is isomorphic to

$$\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

where n_i are positive integers and $n_1 \mid n_2 \mid \cdots \mid n_k$ and $n_i \geq 2$; moreover the integer r (called the rank) and sequence $n_1 \mid n_2 \mid \cdots \mid n_k$ is unique. This is called the **fundamental theorem of finitely generated abelian groups**.

If $k = 0$ then $A \cong \mathbb{Z}^r$ and therefore free. Let's prove the converse. Suppose A is free as a $\mathbb{Z}$-module. Then $A \cong \mathbb{Z}^m$ for some m. By the uniqueness part of the fundamental theorem, $r = m$ and $k = 0$. Hence a finitely generated abelian group is free as a $\mathbb{Z}$-module if and only if it is isomorphic to $\mathbb{Z}^r$ where r is the rank.

Example 186. Recall that $\mathbb{R}^n$ is an $M_n(\mathbb{R})$-module. Let $n \geq 2$. We show that $\mathbb{R}^n$ is not free as an $M_n(\mathbb{R})$-module. Let X be any non-empty subset of $\mathbb{R}^n$. We show that X is not independent. Let $\mathbf{v} \in X$ (which we think of as a column vector). Now let $\mathbf{w} \neq 0$ such that $\mathbf{w} \cdot \mathbf{v} = 0$ (i.e. $\mathbf{w}$ is orthogonal to $\mathbf{v}$). Let A be the $n \times n$-matrix whose rows are all equal to the transpose of $\mathbf{w}$. Then $A \neq 0$ and $A\mathbf{v} = 0$. Then X is not independent. Thus $\mathbb{R}^n$ is not free as an $M_n(\mathbb{R})$-module.

Theorem 187. *Let R be a ring and M an R-module. A set $\{x_i : i \in I\}$ is an R-basis if and only if every element $x \in M$ can be written as a sum*

$$x = \sum_{i \in I} a_i x_i$$

such that both the following hold:

(i) the a_i are unique;
(ii) all but finitely many are zero.

PROOF. This is an easy and very important exercise. □

If we start with a spanning set instead of a basis then uniqueness of the coefficients a_i is no longer true. Write down an example!

Exercise 188. Let $\mathbb{R}[X]$ be the $\mathbb{R}[T]$-module where multiplication is given by

$$(a_0+a_1T+\cdots+a_nT^n)\cdot f(X) \;=\; a_0f(X)+a_1f'(X)+a_2f''(X)+\cdots+a_nf^{(n)}(X);$$

here $f^{(n)}(X)$ denotes the n-th derivative of $f(X)$ with respect to X.

(i) Compute $(1+T-T^2-3T^5)\cdot(X+3X^2)$.
(ii) Show that $\mathrm{Span}_{\mathbb{R}[T]}(X^n)=\mathrm{Span}_{\mathbb{R}}(1,X,\ldots,X^n)$.
(iii) Show that $\mathbb{R}[X]$ is not free as an $\mathbb{R}[T]$ module.

5. Hom and End

Let M, N be R-modules. We define

$$\mathrm{Hom}_R(M,N)=\{h \;:\; h:M\to N \text{ is a homomorphism}\}.$$

We let

$$\mathrm{End}_R(M)=\mathrm{Hom}_R(M,M).$$

The elements of $\mathrm{End}_R(M)$ are **endomorphisms** of M: an endomorphism of M is nothing more than a homomorphism from M to itself.

Let f, $g\in\mathrm{Hom}_R(M,N)$, and let $r\in R$. We define $f+g$ by

$$(f+g) \;:\; M\to N, \qquad (f+g)(m)=f(m)+g(m).$$

If f, $g\in\mathrm{End}_R(M)$ then we define the product $f\cdot g$ to simply be the composition

$$(f\cdot g) \;:\; M\to M, \qquad (f\cdot g)(m)=(f\circ g)(m)=f(g(m)).$$

Theorem 189. $\mathrm{Hom}_R(M,N)$ *is an additive abelian group, where the additive identity is trivial homomorphism* $0:M\to N$, $0(m)=0$.

$\mathrm{End}_R(M)$ *is a ring, where the additive identity is as above, and the multiplicative identity is* $1:M\to M$, $1(m)=m$.

We refer to $\mathrm{End}_R(M)$ as the **endomorphism ring of** M. The unit group of $\mathrm{End}_R(M)$ is called the **automorphism group of** M and is written as $\mathrm{Aut}_R(M)=\mathrm{End}_R(M)^*$. An element of $\mathrm{Aut}_R(M)$ is called an R-automorphism of M and is simply an isomorphism $M\to M$ as an R-module (recall that only bijective maps have inverses).

Sometimes we write $\mathrm{End}(M)$ for $\mathrm{End}_R(M)$ when R is clear from the context.

Exercise 190. Let $T\in\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^2)$ be given by

$$T \;:\; \mathbb{Z}^2\to\mathbb{Z}^2, \qquad T\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}2a\\2b\end{pmatrix}.$$

Show that $ST\neq 1$ for all $S\in\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^2)$.

Exercise 191. If R is commutative, then it is possible to make $\mathrm{Hom}_R(M,N)$ into an R-module by defining

$$(rf) \;:\; M\to N, \qquad (rf)(m)=r\cdot f(m).$$

Check that $rf \in \mathrm{Hom}_R(M, M)$ if R is commutative, making clear where you have used commutativity.

Example 192. If M is isomorphic to N then $\mathrm{End}(M)$ is isomorphic to $\mathrm{End}(N)$. This is really common sense, but it is instructive to figure out the isomorphism explicitly. Let $\phi : M \to N$ be an isomorphism. Let $f \in \mathrm{End}(M)$. Thus $f : M \to M$ is a homomorphism. I want to obtain from this an element of $\mathrm{End}(N)$, that is a homomorphism $N \to N$. We look at the diagram

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{\phi} & N \end{array}$$

We want an arrow that goes from N to N. We can do this if we remember that the arrow $M \to N$ is reversible. What does that mean? It means that, as $\phi : M \to N$ is an isomorphism it has an inverse $\phi^{-1} : N \to M$. We look again at the diagram but now with the top arrow reversed

$$\begin{array}{ccc} M & \xleftarrow{\phi^{-1}} & N \\ \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{\phi} & N \end{array}$$

It should now be clear how we contruct a map $N \to N$. We follow ϕ^{-1} then f then ϕ; i.e. we simply take $\phi \circ f \circ \phi^{-1}$. This will be a homomorphism as ϕ, f, ϕ^{-1} are isomorphisms. We leave it as an exercise to check that the map

$$\mathrm{End}(M) \to \mathrm{End}(N), \qquad f \mapsto \phi \circ f \circ \phi^{-1}$$

is an isomorphism of rings.

Exercise 193. Let M, N be R-modules and suppose $\mathrm{Hom}(M, N) = 0$. Show that $\mathrm{Hom}(M^r, N^s) = 0$ for r, $s \geq 1$.

Exercise 194. Let V be a $\mathbb{Q}$-vector space. Show that $\mathrm{End}_{\mathbb{Q}}(V) = \mathrm{End}_{\mathbb{Z}}(V)$.

Exercise 195. Let

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $M = \mathbb{R}^2$ be the $\mathbb{R}[X]$-module where (see Examples 155 and 161) scalar multiplication is given by

$$(a_0 + a_1 + a_2X^2 + \cdots + a_rX^r) \cdot \mathbf{v} = a_0\mathbf{v} + a_1A\mathbf{v} + \cdots + a_rA^r\mathbf{v}.$$

Let $N = \mathbb{R}^2$ be the $\mathbb{R}[X]$-module where scalar multiplication is given by

$$(a_0 + a_1 + a_2X^2 + \cdots + a_rX^r) \cdot \mathbf{v} = a_0\mathbf{v} + a_1B\mathbf{v} + \cdots + a_rB^r\mathbf{v}.$$

(i) Compute

$$(1 - 3X + X^2) \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

in M and in N.

(ii) Let $\mathbf{w} \in \mathbb{R}^2$. Define

$$\phi_{\mathbf{w}} : M \to N, \qquad \phi_{\mathbf{w}} \begin{pmatrix} a \\ b \end{pmatrix} = (a+b)\mathbf{w}.$$

Show that $\phi_{\mathbf{w}} \in \mathrm{Hom}_{\mathbb{R}[X]}(M, N)$.

(iii) Let $\phi \in \mathrm{Hom}_{\mathbb{R}[X]}(M, N)$. Show that $\phi = \phi_{\mathbf{w}}$ for some $\mathbf{w} \in \mathbb{R}^2$.

Exercise 196. Let M, N be as in Exercise 195 but with

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Show that $\mathrm{Hom}_{\mathbb{R}[X]}(M, N) = \{0\}$.

6. Where do matrices come from?

Let M be an R-module. We know that $\mathrm{End}(M)$ is the set (ring actually) of all homomorphisms $f : M \to M$. But how do we describe the elements of this ring in terms of the M. This is a complicated question that doesn't have a complete answer. However, we can give a complete answer when M is free with finite basis. Suppose $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is an R-basis for M. Every element $\mathbf{v} \in M$ can be written **uniquely** as a linear combination

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n, \qquad a_i \in R.$$

Let f be a homomorphism. Then

$$f(\mathbf{v}) = a_1 f(\mathbf{v}_1) + \cdots + a_n f(\mathbf{v}_n).$$

Thus to specify f all we have to do (beyond know that it is a homomorphism) is to specify what $f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)$ are. But these are elements of M. So I can write each as a linear combination of the basis elements:

$$f(\mathbf{v}_j) = \alpha_{1,j}\mathbf{v}_1 + \alpha_{2,j}\mathbf{v}_2 + \cdots + \alpha_{n,j}\mathbf{v}_n, \qquad j = 1, \ldots, n. \tag{17}$$

Hence specifying a homomorphism $f : M \to M$ is equivalent to specifying the coefficients $\alpha_{i,j}$ with $i, j = 1, \ldots, n$. We associate to f the matrix $A_f = (\alpha_{i,j}) \in M_n(R)$. Here $\alpha_{i,j}$ is the element at the intersection of the i-th row and j-th column. Note that coefficients for $f(\mathbf{v}_j)$ in terms of the basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ gives us the j-th column of A_f. The choice of A_f depends on the choice of the basis. If we change the basis we conjugate the matrix, but let's not worry too much about that.

Now f, $g \in \mathrm{End}(M)$. Write $A_f = (\alpha_{i,j})$ and $A_g = (\beta_{i,j})$. What is A_{f+g}? The j-column of this matrix is simply the coefficients of

$(f+g)(\mathbf{v}_j)$ written as linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_n$. But

$$f(\mathbf{v}_j) = \alpha_{1,j}\mathbf{v}_1 + \alpha_{2,j}\mathbf{v}_2 + \cdots + \alpha_{n,j}\mathbf{v}_n,$$
$$g(\mathbf{v}_j) = \beta_{1,j}\mathbf{v}_1 + \beta_{2,j}\mathbf{v}_2 + \cdots + \beta_{n,j}\mathbf{v}_n.$$

Thus

$$(f+g)(\mathbf{v}_j) = (\alpha_{1,j}+\beta_{1,j})\mathbf{v}_1 + (\alpha_{2,j}+\beta_{2,j})\mathbf{v}_2 + \cdots + (\alpha_{n,j}+\beta_{n,j})\mathbf{v}_n.$$

Hence $A_{f+g} = A_f + A_g$ predictably enough.

What is A_{fg}. We are asking for the matrix for the composition $fg = f \circ g$. To aid our sanity let's put $n = 2$. So we can write

$$A_f = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,1} & \alpha_{2,2} \end{pmatrix}, \qquad A_g = \begin{pmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{pmatrix}.$$

Now (deep breath!)

$$\begin{aligned}(fg)(\mathbf{v}_1) &= f(g(\mathbf{v}_1)) \\ &= f(\beta_{1,1}\mathbf{v}_1 + \beta_{2,1}\mathbf{v}_2) \\ &= \beta_{1,1}f(\mathbf{v}_1) + \beta_{2,1}f(\mathbf{v}_2) \\ &= \beta_{1,1}(\alpha_{1,1}\mathbf{v}_1 + \alpha_{2,1}\mathbf{v}_2) + \beta_{2,1}(\alpha_{1,2}\mathbf{v}_1 + \alpha_{2,2}\mathbf{v}_2) \\ &= (\beta_{1,1}\alpha_{1,1} + \beta_{2,1}\alpha_{1,2})\mathbf{v}_1 + (\beta_{1,1}\alpha_{2,1} + \beta_{2,1}\alpha_{2,2})\mathbf{v}_2.\end{aligned}$$

and

$$\begin{aligned}(fg)(\mathbf{v}_2) &= f(g(\mathbf{v}_2)) \\ &= f(\beta_{1,2}\mathbf{v}_1 + \beta_{2,2}\mathbf{v}_2) \\ &= \beta_{1,2}f(\mathbf{v}_1) + \beta_{2,2}f(\mathbf{v}_2) \\ &= \beta_{1,2}(\alpha_{1,1}\mathbf{v}_1 + \alpha_{2,1}\mathbf{v}_2) + \beta_{2,2}(\alpha_{1,2}\mathbf{v}_1 + \alpha_{2,2}\mathbf{v}_2) \\ &= (\beta_{1,2}\alpha_{1,1} + \beta_{2,2}\alpha_{1,2})\mathbf{v}_1 + (\beta_{1,2}\alpha_{2,1} + \beta_{2,2}\alpha_{2,2})\mathbf{v}_2.\end{aligned}$$

Thus

$$A_{fg} = \begin{pmatrix} \beta_{1,1}\alpha_{1,1} + \beta_{2,1}\alpha_{1,2} & \beta_{1,2}\alpha_{1,1} + \beta_{2,2}\alpha_{1,2} \\ \beta_{1,1}\alpha_{2,1} + \beta_{2,1}\alpha_{2,2} & \beta_{1,2}\alpha_{2,1} + \beta_{2,2}\alpha_{2,2} \end{pmatrix}. \tag{18}$$

For the moment suppose R is commutative. Then we can swap the αs and βs to get

$$A_{fg} = \begin{pmatrix} \alpha_{1,1}\beta_{1,1} + \alpha_{1,2}\beta_{2,1} & \alpha_{1,1}\beta_{1,2} + \alpha_{1,2}\beta_{2,2} \\ \alpha_{2,1}\beta_{1,1} + \alpha_{2,2}\beta_{2,1} & \alpha_{2,1}\beta_{1,2} + \alpha_{2,2}\beta_{2,2} \end{pmatrix} = A_f A_g.$$

This is true for general n, not just $n = 2$. If you're pedantic you can have a go at writing this out. In fact this is precisely the reason why matrix multiplication is defined the way it is. Matrices are just ways of assigning coordinates to linear transformations (or R-module homomorphisms) and matrix multiplication is defined so that the product of the matrices to two homomorphism is the matrix of their composition.

In first year linear algebra you saw a horrible proof of matrix associativity that involved interchanging the order of some double summation. Let's prove matrix associativity the easy way! We want to check

$A_f(A_gA_h) = (A_fA_g)A_h$. The left hand-side is $A_{f\circ(g\circ h)}$ and the right hand-side is $A_{(f\circ g)\circ h}$. So we want to check that $f\circ(g\circ h) = (f\circ g)\circ h$. Let $\mathbf{v}\in M$. Then

$$(f\circ(g\circ h))(\mathbf{v}) = f((g\circ h)(\mathbf{v}) = f(g(h(\mathbf{v})), \qquad ((f\circ g)\circ h)(\mathbf{v}) = (f\circ g)(h(\mathbf{v})) = f(g(h(\mathbf{v}))),$$

giving $f\circ(g\circ h) = (f\circ g)\circ h$, and so matrix multiplication is associative.

The point of the above discussions is to convey where matrices come from and why matrix multiplication is defined the way it is, and also to convince of the truth of the following theorem.

Theorem 197. *Let R be a commutative ring, and M a free R-module of rank n. Then* $\mathrm{End}(M)\cong M_n(R)$ *as rings.*

Proof. We haven't done all the steps of the proof, but you can fill in the gaps if you like.

What is important is you know:

- the isomorphism $\mathrm{End}(M)\cong M_n(R)$ depends on a choice of basis for M;
- given $f\in\mathrm{End}(M)$ how do you write down the corresponding matrix;
- given a matrix how to you write down the corresponding endomorphism.

□

What happens with a general ring (i.e. one that is not commutative)? We assumed that R is commutative because the multiplications in (18) are the wrong way round and we wanted to swap them over. For general ring R the problem is fixed by defining another ring R^{opp}, called the **opposite ring** to R. The elements of R^{opp} are the same as the elements of R. Addition in R^{opp} is exactly the same as the addition of R, but the multiplication is given by

$$\alpha * \beta = \beta\cdot\alpha.$$

You can convince yourself that R^{opp} is a ring, and if R is commutative then $R^{\mathrm{opp}} = R$.

Theorem 198. *Let R be a ring, and M a free R-module of rank n. Then* $\mathrm{End}(M)\cong M_n(R^{\mathrm{opp}})$ *as rings.*

CHAPTER 8

Zorn's Lemma

1. Partial and Total Ordering

Definition. Let $\mathcal{P}$ be a set and $\preceq$ be a relation on $\mathcal{P}$. We say that $\preceq$ is a **partial ordering** on $\mathcal{P}$ if it is reflexive, antisymmetric and transitive. Recall the meaning of these terms:

- $\preceq$ is **reflexive** if $x \preceq x$ for every $x \in \mathcal{P}$.
- $\preceq$ is **antisymmetric** if for all x, $y \in \mathcal{P}$
$$x \preceq y \text{ and } y \preceq x \quad \Longrightarrow \quad x = y.$$
- $\preceq$ is **transitive** if, for all x, y, $z \in \mathcal{P}$,
$$x \preceq y \text{ and } y \preceq z \quad \Longrightarrow \quad x \preceq z.$$

A **total ordering** on $\mathcal{P}$ is a partial ordering $\preceq$ which also satisfies $x \preceq y$ or $y \preceq x$ for all x, $y \in \mathcal{P}$ (this condition is called **comparability**).

Example 199. $\leq$ is a total ordering on $\mathbb{R}$, but $<$ is not even a partial ordering (not reflexive).

Example 200. Let A be a set and $P(A)$ be the power set of A (the elements of $P(A)$ are the subsets of A). Then $\subseteq$ is a partial ordering on $P(A)$. If $\#A \geq 2$ the $\subseteq$ is not a total ordering on $P(A)$. For example, take element $a \neq b$ of A, and note that comparability fails for $\{a\}$, $\{b\} \in P(A)$.

To aid intuition we will sometimes denote partial orderings by $\leq$ regardless of the nature of $\mathcal{P}$.

Definition. Let $\preceq$ be a partial ordering on a set $\mathcal{P}$. A nonempty subset $\mathcal{C} \subseteq \mathcal{P}$ that is totally ordered is called a **chain**. An **upper bound** for a chain $\mathcal{C}$ is an element $x \in \mathcal{P}$ such that $y \preceq x$ for all $y \in \mathcal{C}$. An element $x \in \mathcal{P}$ is called **maximal** if there is no $y \in \mathcal{P}$, $y \neq x$ with $x \preceq y$.

Example 201. Take $\mathcal{P} = P(\mathbb{N})$ and order by inclusion (i.e. $A \leq B$ means $A \subseteq B$). Let

$$\mathcal{C} = \{\{1\}, \{1,2\}, \{1,2,3\}, \dots\}. \tag{19}$$

This is a chain. An upper bound for this chain $\mathcal{C}$ is $\mathbb{N}$, since $\mathbb{N} \in P(\mathbb{N})$ and every element of $\mathcal{C}$ is contained in $\mathbb{N}$. However, the set

$$\mathcal{C}' = \{\{1\}, \{2\}, \{3\}, \dots\}$$

is not a chain, since it is not totally ordered. Also $\mathbb{N}$ is a maximal element of $P(\mathbb{N})$.

Example 202. Now take $\mathcal{P} = \{A \in P(\mathbb{N}) \ : \ \#A < \infty\}$, again ordered by inclusion. Let $\mathcal{C}$ be as in (19). Then $\mathcal{C}$ is again a chain in $\mathcal{P}$. It doesn't however have an upper bound in $\mathcal{P}$. Any upper bound must contain all of the elements of $\mathcal{C}$ and so must be infinite.

The partially ordered set $\mathcal{P}$ has no maximal elements, since if A is in $\mathcal{P}$ we can find $n \in \mathbb{N} \setminus A$, and we can take $A \cup \{n\} \in \mathcal{P}$ which satisfies $A \preceq A \cup \{n\}$ (i.e. $A \subseteq A \cup \{n\}$) and $A \neq A \cup \{n\}$.

Theorem 203. *(Zorn's Lemma) Let $\mathcal{P}$ be a non-empty partially ordered set. Suppose that every chain $\mathcal{C}$ of $\mathcal{P}$ has an upper bound belonging to $\mathcal{P}$. Then $\mathcal{P}$ has at least one maximal element.*

Zorn's Lemma is equivalent to the Axiom of Choice, and so does not have a proof. It is one of the axioms (basic assumptions) of mathematics that most mathematicians are willing to assume.

Here is a lemma that is often useful when applying Zorn's Lemma.

Lemma 204. *Let $\mathcal{P}$ be a partially ordered set, and let $\{x_1, \ldots, x_n\}$ be a finite chain in $\mathcal{P}$. Then there is some $1 \leq j \leq n$ such that $x_i \preceq x_j$ for all $1 \leq i \leq n$.*

Proof. We can do this by induction. If $n = 1$ we just take $j = 1$. Suppose it is true for $n = k$. Let $\{x_1, \ldots, x_{k+1}\}$ be a finite chain. Then $\{x_1, \ldots, x_k\}$ is a finite chain. By the inductive hypothesis there is some $1 \leq j' \leq k$ such that $x_i \preceq x_{j'}$ for all $1 \leq i \leq k$. If $x_{k+1} \preceq x_{j'}$ then let $j = j'$, otherwise let $j = k + 1$. In either case we have $x_i \preceq x_j$ for $1 \leq i \leq k + 1$, completing the proof of the inductive step. □

Note that any finite subset of a chain is a finite chain.

2. Maximal Ideals

Let R be a commutative ring. Recall that a **maximal ideal** $\mathfrak{m}$ is a proper ideal that is not contained in any other proper ideal.

Theorem 205. *Let R be a non-zero commutative ring. Then R has a maximal ideal.*

Proof. Let $\mathcal{P}$ be the set of all proper ideals $\mathfrak{b}$ of R. Since R is non-zero, the ideal (0) is proper and so belongs to $\mathcal{P}$. Hence $\mathcal{P} \neq \emptyset$. We order $\mathcal{P}$ by inclusion. The statement that R has a maximal ideal is equivalent to the statement that $\mathcal{P}$ has a maximal element. We will use Zorn's Lemma to show this.

Let $\mathcal{C} = \{\mathfrak{b}_i : i \in I\}$ be a chain in $\mathcal{P}$. This means that the $\mathfrak{b}_i$ are proper ideals of R, and that for every $i, j \in I$ either $\mathfrak{b}_i \subseteq \mathfrak{b}_j$ or $\mathfrak{b}_j \subseteq \mathfrak{b}_i$. We let

$$\mathfrak{b} = \bigcup_{i \in I} \mathfrak{b}_i.$$

We claim that $\mathfrak{b}$ is an ideal of R. Clearly $0 \in \mathfrak{b}$ as it is contained in any $\mathfrak{b}_i$. Let $\alpha \in \mathfrak{b}$ and $r \in R$. Then $\alpha \in \mathfrak{b}_i$ for some i and as $\mathfrak{b}_i$ is an

ideal, $r\alpha \in \mathfrak{b}_i \subseteq \mathfrak{b}$. Now let $\alpha, \beta \in \mathfrak{b}$. We need to show that $\alpha + \beta \in \mathfrak{b}$. It is here that we must use the fact that $\mathcal{C}$ is a chain. By definition of $\mathfrak{b}$, $\alpha \in \mathfrak{b}_i$, $\beta \in \mathfrak{b}_j$ for some $i, j \in I$. As $\mathcal{C}$ is a chain, we may suppose without loss of generality that $\mathfrak{b}_i \subseteq \mathfrak{b}_j$. Thus α, β are both in the ideal $\mathfrak{b}_j$ and so $\alpha + \beta \in \mathfrak{b}_j \subseteq \mathfrak{b}$. This proves that $\mathfrak{b}$ is an ideal. Also all $\mathfrak{b}_i$ are proper, and so $1 \notin \mathfrak{b}_i$ and so $1 \notin \mathfrak{b}$ and so $\mathfrak{b}$ is proper. We have shown that $\mathfrak{b} \in \mathcal{P}$. Since $\mathfrak{b}_i \subseteq \mathfrak{b}$ for all $i \in I$, the element $\mathfrak{b} \in \mathcal{P}$ is an upper bound for $\mathcal{C}$.

By Zorn's Lemma, $\mathcal{P}$ has a maximal element $\mathfrak{m}$. This completes the proof. □

Important Remark. It is not true that a union of ideals has to be an ideal. Most of the time it isn't. Consider for example $2\mathbb{Z} \cup 3\mathbb{Z}$. This is a union of two ideals of $\mathbb{Z}$, but it isn't an ideal, since it contains 2, 3 but not $5 = 2 + 3$. However, **the union of a chain of ideals is an ideal** as we saw in the proof.

Exercise 206. Let R be a ring (not necessarily commutative). A **maximal left ideal** $\mathfrak{m}$ of R is a proper left ideal that is not contained in any other proper left ideal. Use Zorn's Lemma to show that R must have a maximal left ideal.

Exercise 207. Let R be a commutative ring and $\mathfrak{a}$ a proper ideal of R.

(i) Use Zorn's Lemma to show that $\mathfrak{a}$ is contained in a maximal ideal.
(ii) Instead of using Zorn's Lemma directly, deduce that $\mathfrak{a}$ is contained in a maximal ideal immediately from Theorem 205 and the Correspondence Theorem (Theorem 73).

Exercise 208. Let R be a ring and M an R-module. Let N_0 be a submodule of M. Let $\mathcal{P}$ be the set of submodule N of M satisfying $N \cap N_0 = \{0\}$, and order $\mathcal{P}$ by inclusion. Show that $\mathcal{P}$ has a maximal element.

Exercise 209. Let G be a group with identity element 1_G, and let $k \in G \setminus \{1_G\}$. Let $\mathcal{P}$ be the set of normal subgroups H of G not containining k, and order $\mathcal{P}$ by inclusion. Show that $\mathcal{P}$ has a maximal element.

Exercise 210. Let R be a ring and M a left R-module. A **maximal submodule of** M is a proper submodule that is not contained in any other proper submodule. In this exercise you will show that the $\mathbb{Z}$-module $\mathbb{Q}$ has no maximal submodules. Let N be a non-trivial proper submodule of $\mathbb{Q}$.

(i) Show that there is some integer $c \geq 1$ such that $c \in N$.
(ii) Show that there is some integer $b > 1$ such that $\frac{1}{b} \in \mathbb{Q} \setminus N$.
(iii) Let $N' = N + \mathbb{Z}\left(\frac{1}{b}\right)$. Show that N' is a $\mathbb{Z}$-submodule of $\mathbb{Q}$ properly containing N.

(iv) Show that $\frac{1}{cb^2} \notin N'$.
(v) Deduce that that $\mathbb{Q}$ has no maximal $\mathbb{Z}$-submodules.
(vi) Let $\mathcal{P}$ be the set of all proper $\mathbb{Z}$-submodules of $\mathbb{Q}$, ordered by inclusion. The above says that $\mathcal{P}$ has no maximal element. If you try to use Zorn's Lemma to show that $\mathcal{P}$ has a maximal element where does the argument break down?

3. Existence of Bases

Theorem 211. *Let D be a division ring. Let M be an D-module.*
(i) M has an D-basis.
(ii) Every D-linearly independent subset $S \subseteq M$ can be extended to a basis.
(iii) Every spanning set $S \subseteq M$ contains a basis.

Recall that fields are commutative division rings. Thus the theorem immediately implies the following corollary.

Corollary 212. *Let K be a field. Let V be a K-vector space.*
(i) V has an K-basis.
(ii) Every K-linearly independent subset $S \subseteq V$ can be extended to a basis.
(iii) Every spanning set $S \subseteq V$ contains a basis.

You already know these results for **finitely generated** vector spaces. The point now is that Zorn's Lemma allows us to deal with infinitely generated settings.

Proof of Theorem 211. Let's prove (ii) first. So let S be an D-linearly independent set. Let $\mathcal{P}$ be the set whose elements are subsets $T \subseteq M$ satisfying

- $S \subseteq T$;
- T is D-linearly independent.

The set $\mathcal{P}$ is non-empty as $S \in \mathcal{P}$. We order $\mathcal{P}$ by inclusion. Let $\mathcal{C} = \{T_i : i \in I\}$ be a non-empty chain in $\mathcal{P}$. Let

$$T = \bigcup_{i \in I} T_i.$$

Clearly $S \subseteq T$. We want to show that T is D-linearly independent. Suppose $\mathbf{v}_1, \ldots, \mathbf{v}_m \in T$ and $\alpha_1, \ldots, \alpha_m \in D$ satisfy

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_m \mathbf{v}_m = 0.$$

Since T is the union of the T_i, each $\mathbf{v}_j$ belongs to some T_{i_j} with $i_j \in I$. As $\mathcal{C}$ is a chain, the subset $\{T_{i_1}, \ldots, T_{i_m}\}$ is a finite chain. By Lemma 204 one of $T_{i_1}, \ldots, T_{i_m}$ contains all the others. Without loss of generality, suppose that this is T_{i_1}. Thus $\mathbf{v}_1, \ldots, \mathbf{v}_m \in T_{i_1}$. As $T_{i_1} \in \mathcal{P}$, it is linearly independent, thus $\alpha_1, \ldots, \alpha_m = 0$. It follows that T is linearly independent. Hence $T \in \mathcal{P}$ and T is an upper bound for $\mathcal{C}$. By

Zorn's Lemma $\mathcal{P}$ has a maximal element. Let's write T for this maximal element. This is linearly independent and contains S. We will complete the proof of (ii) by showing that T spans M and so is a basis. Let $\mathbf{v} \in M$. We want to write $\mathbf{v}$ as a finite linear combination combination of elements of T with coefficients in D. Since T is maximal, $T \cup \{\mathbf{v}\}$ does not belong to $\mathcal{P}$ and hence is linearly dependent. Thus there are $\mathbf{v}_1, \ldots, \mathbf{v}_m \in T$ and $\alpha_1, \ldots, \alpha_m, \alpha \in D$, not all zero, such that

$$\alpha_1\mathbf{v}_1 + \cdots + \alpha_m\mathbf{v}_m + \alpha\mathbf{v} = 0.$$

If $\alpha = 0$ then we have linear dependence among $\mathbf{v}_1, \ldots, \mathbf{v}_m \in T$ which is a contradiction. Thus $\alpha \neq 0$. As D is a division ring, α has an inverse α^{-1}. Hence

$$\mathbf{v} = -\alpha^{-1}\alpha_1\mathbf{v}_1 - \cdots - \alpha^{-1}\alpha_m\mathbf{v}_m \in \mathrm{Span}(T).$$

It follows that T is a basis. This completes the proof of (ii).

To prove (i) apply (ii) with $S = \emptyset$.

Let's prove (iii). We now let $\mathcal{P}$ be the set whose elements are subsets $T \subseteq M$ satisfying

- $T \subseteq S$;
- T is linearly independent.

Note $\emptyset \in \mathcal{P}$ so $\mathcal{P} \neq \emptyset$. Following almost the same steps as before, we can prove that every chain in $\mathcal{P}$ has an upper bound belonging to $\mathcal{P}$. By Zorn's Lemma, $\mathcal{P}$ has a maximal element T. This is linearly independent and is contained in S. We want to show that $\mathrm{Span}(T) = M$. We know that $\mathrm{Span}(S) = M$. Hence it is sufficient to show that $S \subseteq \mathrm{Span}(T)$. Let $\mathbf{v} \in S$. If $\mathbf{v} \in T$ then $\mathbf{v} \in \mathrm{Span}(T)$ and we're done. So suppose $\mathbf{v} \notin T$. Note $T \subsetneq T \cup \{\mathbf{v}\} \subseteq S$. By maximality of T in $\mathcal{P}$ we see that $T \cup \{\mathbf{v}\}$ must be linearly dependent. Hence there are $\mathbf{v}_1, \ldots, \mathbf{v}_m \in T$, and $\alpha_1, \ldots, \alpha_m, \alpha \in D$, not all zero, such that

$$\alpha_1\mathbf{v}_1 + \cdots + \alpha_m\mathbf{v}_m + \alpha\mathbf{v} = 0.$$

If $\alpha = 0$ then we have linear dependence among $\mathbf{v}_1, \ldots, \mathbf{v}_m \in T$ which is a contradiction. Thus $\alpha \neq 0$. As D is a division ring, α has an inverse α^{-1}. Hence

$$\mathbf{v} = -\alpha^{-1}\alpha_1\mathbf{v}_1 - \cdots - \alpha^{-1}\alpha_m\mathbf{v}_m \in \mathrm{Span}(T).$$

Hence $S \subseteq \mathrm{Span}(T)$ and so $M = \mathrm{Span}(S) \subseteq \mathrm{Span}(T)$. So $\mathrm{Span}(T) = M$. This completes the proof. □

Important Remark. The union of linearly independent sets need not be linearly independent. For example $\{\mathbf{i}, \mathbf{j}\}$ and $\{\mathbf{i}+\mathbf{j}\}$ are two linearly independent sets in $\mathbb{R}^2$ but their union $\{\mathbf{i}, \mathbf{j}, \mathbf{i}+\mathbf{j}\}$ is linearly dependent. However, **the union of a chain of linearly independent sets is linearly independent**, as we saw in the above proof.

Exercise 213. A function $f : \mathbb{R} \to \mathbb{R}$ is called **additive** if

$$f(x + y) = f(x) + f(y)$$

for all x, $y \in \mathbb{R}$.

(i) Let f be additive. Show that $f(nx) = nf(x)$ for all $x \in \mathbb{R}$ and $n \in \mathbb{Z}$.
(ii) Show that $f(qx) = qf(x)$ for all $x \in \mathbb{R}$ and $q \in \mathbb{Q}$. Thus f is a linear transformation when considered as a $\mathbb{Q}$-vector space.
(iii) Suppose f is a continuous additive function. Show that $f(x) = \alpha x$ where $\alpha = f(1)$.
(iv) We now drop the continuity assumption on f. Show that there exists an additive function $f : \mathbb{R} \to \mathbb{R}$ such that $f(1) = 1$, $f(\sqrt{2}) = 0$, $f(\pi) = \log 2$. You may suppose that 1, $\sqrt{2}$, π are $\mathbb{Q}$-linearly independent.

Exercise 214. Let M, N be R-modules. Let $\mathcal{P}$ be the set of pairs (L, f) where L is an R-submodule of M and $f : L \to N$ is a homomorphism. We write $(L_1, f_1) \preceq (L_2, f_2)$ if $L_1 \subseteq L_2$ and $f_2|_{L_1} = f_1$.

(i) Take $R = M = N = \mathbb{Z}$, and $L_1 = 2\mathbb{Z}$. Let $f_1 : L_1 \to \mathbb{Z}$ be given by $f_1(2x) = x$ for $x \in \mathbb{Z}$. Show that (L_1, f_1) is a maximal element of $\mathcal{P}$.
(ii) Take $R = M = N = \mathbb{Z}$, and $L_1 = 2\mathbb{Z}$. Let $f_1 : L_1 \to \mathbb{Z}$ be given by $f_1(2x) = 4x$ for $x \in \mathbb{Z}$. Show that (L_1, f_1) is not a maximal element of $\mathcal{P}$.
(iii) Show that every chain $\mathcal{C}$ of $\mathcal{P}$ has an upper bound.

CHAPTER 9

Simple Modules

1. Definitions and First Examples

Definition. An R-module M is **simple** (or **irreducible**) if $M \neq 0$ and the only submodules of M are 0 and M.

Example 215. If M, N are non-zero R-modules then $M \times N$ is not a simple R-module (e.g. $M \times \{0\}$ is a proper non-zero R-submodule).

Example 216. Let K be a field. Recall that K-module is the same as a K-vector space. Note that a K-vector space V is simple as a K-module if and only if $\dim_K(V) = 1$.

Example 217. $\mathbb{Z}$ is not simple as a $\mathbb{Z}$-module. For example, $2\mathbb{Z}$ is a submodule which is equal to neither 0 nor $\mathbb{Z}$.

Example 218. Let $m \geq 2$. We shall show that $\mathbb{Z}/m\mathbb{Z}$ is simple as a $\mathbb{Z}$-module if and only if m is prime. Thus $\mathbb{Z}/m\mathbb{Z}$ is simple if and only if it is a field.

By the correspondence theorem, the submodules of the $\mathbb{Z}/m\mathbb{Z}$ are of the form $I/m\mathbb{Z}$ where I is a $\mathbb{Z}$-submodule of $\mathbb{Z}$ (i.e. I is an ideal) containing $m\mathbb{Z}$. As $\mathbb{Z}$ is a PID, $I = n\mathbb{Z}$ for some positive integer n. However, $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $m \in n\mathbb{Z}$ which is equivalent to $n \mid m$. Hence the $\mathbb{Z}$-submodules of $\mathbb{Z}/m\mathbb{Z}$ have the form $n\mathbb{Z}/m\mathbb{Z}$ where $n \mid m$. If $n = 1$ then $n\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$. If $n = m$ then $m\mathbb{Z}/m\mathbb{Z} = 0$. If $n \neq 1$, m then $n\mathbb{Z} \neq \mathbb{Z}$, $m\mathbb{Z}$, and so $n\mathbb{Z}/m\mathbb{Z} \neq \mathbb{Z}/m\mathbb{Z}$, $m\mathbb{Z}/m\mathbb{Z}$.

We conclude that $\mathbb{Z}/m\mathbb{Z}$ is simple as a $\mathbb{Z}$-module if and only m is prime.

Exercise 219. Let K be a field and $f \in K[X]$ have degree ≥ 1. Show that $K[X]/fK[X]$ is simple if and only if f is irreducible. i.e. $K[X]/fK[X]$ is simple if and only if it is a field.

Lemma 220. *Let $M \neq 0$ be an R-module. Then M is simple if and only if $M = Rv = \mathrm{Span}_R(v)$ for every non-zero $v \in M$.*

Proof. Suppose M is simple. Let $v \in M$ be non-zero. Then Rv is a non-trivial submodule of M and so $Rv = M$.

Let's prove the converse. Let N be a non-zero submodule of M. Let $v \in N$ be a non-zero element. By assumption, $M = Rv$. However $Rv \subseteq N$ and so $N = M$. Thus M is simple. $\square$

Example 221. Here is a much more interesting example. Let K be a field and $n \geq 1$. Recall that K^n is an $M_n(K)$-module. Let $v \in K^n$ be a non-zero vector. Write $v = v_1$. By first year linear algebra, v_1 can be extended to a K-basis $v_1, v_2, \ldots, v_n$ for K. Now let w be any other non-zero vector in K^n, and extend that to a K-basis $w_1 = w, w_2, \ldots, w_n$. We know that there is a matrix $B \in M_n(K)$ (called a change of basis matrix) such that $Bv_i = w_i$. In particular, $w = Bv$ and so $w \in M_n(K) \cdot v$. As this is true for any non-zero w, we have $K^n = M_n(K) \cdot v$. By Lemma 220, K^n is a simple $M_n(K)$-module.

The following theorem generalizes the example.

Theorem 222. *Let D be a division ring. Then D^n is a simple as an $M_n(D)$-module.*

Proof. We use Lemma 220. The proof is actually simpler than the one we gave in the example. Let $\mathbf{v} \in D^n \setminus \{\mathbf{0}\}$. We want to show that $D^n = M_n(D) \cdot \mathbf{v}$. Let $\mathbf{w} \in D^n$. Write

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \qquad \mathbf{w} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}, \qquad v_i,\ w_i \in D.$$

As $\mathbf{v} \neq \mathbf{0}$, there is some j such that $v_j \neq 0$. As D is a division ring, this v_j has a multiplicative inverse v_j^{-1}. Let $A \in M_n(K)$ be the matrix whose j-th column has entries $w_1 v_j^{-1}, w_2 v_j^{-1}, \ldots, w_n v_j^{-1}$, and whose other entries are 0. Then $A\mathbf{v} = \mathbf{w}$. This completes the proof. □

2. Schur's Lemma

Theorem 223 (Schur's Lemma I)**.** *Let $f : M \to N$ be a homomorphism of simple R-modules M, N. Then either $f = 0$ or f is an isomorphism.*

Proof. Recall that $\mathrm{Ker}(f)$ is a submodule of M and $\mathrm{Im}(f)$ is a submodule of N. Observe that

$$f = 0 \quad \Longleftrightarrow \quad \mathrm{Ker}(f) = M \quad \text{and} \quad \mathrm{Im}(f) = 0.$$

Suppose $f \neq 0$. Thus $\mathrm{Ker}(f)$ is a proper submodule of the simple module M. Therefore $\mathrm{Ker}(f) = 0$. Hence f is injective. Moreover, $\mathrm{Im}(f)$ is a non-zero submodule of the simple module N, therefore $\mathrm{Im}(f) = N$. Hence f is surjective. Thus f is an isomorphism. □

Theorem 224 (Schur's Lemma II)**.** *Let M be a simple R-module. Then $\mathrm{End}_R(M)$ is a division ring.*

Proof. Let $f \in \mathrm{End}_R(M) \setminus \{0\}$. We want to show that f is a unit of $\mathrm{End}_R(M)$. As M is simple, Schur's Lemma (Theorem 223) tells us that f is an isomorphism. Thus there some isomorphism $g = f^{-1} : M \to M$

such that $g \circ f = f \circ g = I_M$ (which is the identity element of $\mathrm{End}_R(M)$). Hence f is a unit in $\mathrm{End}_R(M)$. □

Exercise 225. Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Let $M = \mathbb{R}^2$ be the $\mathbb{R}[X]$-module where X acts as A. Show $\mathrm{End}_{\mathbb{R}[X]}(M)$ is a division ring.

Exercise 226. Let

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Let $M = \mathbb{R}^2$ be the $\mathbb{R}[X]$-module where X acts as A.

(i) Determine the $\mathbb{R}[X]$-submodules of M.
(ii) Let

$$\phi : M \to M, \qquad \phi \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} u \\ 0 \end{pmatrix}.$$

Show that $\phi \in \mathrm{End}_{\mathbb{R}[X]}(M)$.
(iii) Deduce that $\mathrm{End}_{\mathbb{R}[X]}(M)$ is not a division ring. Why does this not contradict Schur's Lemma?

3. Characterisation of Division Rings

Theorem 227. *Let R be a non-zero ring. The following are equivalent.*

(i) Every R-module has a basis.
(ii) R is a division ring.

Lemma 228. *Let R be a non-zero ring. Suppose there exists a non-zero left R-module which is both simple and free. Then R is a division ring.*

Proof. Let $M \neq 0$ be a left R-module which is simple and free. As M is free it has an R-basis $\{v_i : i \in I\}$. This basis is non-empty as $M \neq 0$. Let v be any element of this basis. Then $\{v\}$ will be R-linearly independent; thus if $a \in R$ and $av = 0$ then $a = 0$. In particular $v \neq 0$ (as $1 \in R$). By Lemma 220, $M = Rv$. Let

$$\phi : R \to M, \qquad r \mapsto rv.$$

Then ϕ is a homomorphism of left R-modules. As $\{v\}$ is linearly independent, $\ker(\phi) = 0$ and so ϕ is injective. Moreover, ϕ is surjective as $\mathrm{Im}(\phi) = Rv = M$. Hence ϕ is an isomorphism of left R-modules. Now M is simple, therefore R is simple as an R-module; i.e. R does not have any left R-submodules. But a left R-submodule of R is the same as left ideal of R. Thus R has no left ideals. By Theorem 111, R is a division ring. □

PROOF OF THEOREM 227. We know that (ii) implies (i) by Theorem 211. Let's do the reverse implication. So suppose (i); i.e. suppose that every R-module is free. By Zorn's Lemma, R has a maximal left ideal $\mathfrak{m}$. Consider the module $R/\mathfrak{m}$. Note that this does not have to be a ring since $\mathfrak{m}$ is not assumed to be a 2-sided ideal. However it is the quotient of the left R-module R by the left R-module $\mathfrak{m}$ and hence a left R-module. By the correspondence theorem (Theorem 73), the left submodules of $R/\mathfrak{m}$ are in $1-1$ correspondence with the left submodules of R containing $\mathfrak{m}$. As $\mathfrak{m}$ is a maximal left submodule of R, the only submodules of R containing it are R itself and $\mathfrak{m}$. Thus the only left submodules of $R/\mathfrak{m}$ are $R/\mathfrak{m}$ itself and $\mathfrak{m}/\mathfrak{m} = 0$. Hence $R/\mathfrak{m}$ is a simple R-module. We are supposing that every R-module is free. Thus $R/\mathfrak{m}$ is an R-module that is both simple and free. By Lemma 228, the ring R is a division ring. This completes the proof. □

CHAPTER 10

Semisimple Modules

1. Definition and Examples

Definition. Let R be a ring. An R-module is called **semisimple** if, for every submodule U, there is a submodule W such that $M = U \oplus W$. Sometimes we say that W is **complementary** to U.

A ring R is called **a semisimple ring** if it is semisimple when regarded as a left R-module.

Example 229. Let K be a field. Then every K-module is semisimple. To see this let M be K-module and U be a submodule. Note here that M is really just a vector space over K and U is a subspace. Let $\{\mathbf{u}_i : i \in I\}$ be a basis for U. We can extend this to a basis

$$\mathcal{B} = \{\mathbf{u}_i : i \in I\} \cup \{\mathbf{w}_j : j \in J\}$$

for M. We let $W = \text{Span}(\{\mathbf{w}_j : j \in J\})$. It is easy to see that $U + V = \text{Span}(\mathcal{B}) = M$, and from the linear independence of $\mathcal{B}$ that $U \cap V = \{\mathbf{0}\}$. Thus $M = U \oplus V$. Hence M is semisimple.

In fact, the same argument works if you replace K by a division ring.

Example 230. Let's convince ourselves that $\mathbb{Z}$ is not a semisimple ring. Here we are viewing $\mathbb{Z}$ as a $\mathbb{Z}$-module. A submodule is just an ideal. Let $U = 2\mathbb{Z}$. We want to see that U does not have a complementary ideal. Let V be some other ideal. The ideals of $\mathbb{Z}$ are just 0 and $n\mathbb{Z}$ with $n = 1, 2, \ldots$. But $0 \oplus 2\mathbb{Z} = 2\mathbb{Z}$ so 0 is not complementary to $2\mathbb{Z}$. Also $2\mathbb{Z} \cap n\mathbb{Z} \supseteq 2n\mathbb{Z}$, and so non-zero for all $n = 1, 2, \ldots$. Hence $2\mathbb{Z}$ has not complementary ideal. Therefore $\mathbb{Z}$ is not a semisimple ring.

Exercise 231. Show $\mathbb{R}[X]$ is not a semisimple ring.

Example 232. Let $M = \mathbb{R}[X]/(X^2)$. This is an $\mathbb{R}[X]$-module. By the correspondence theorem (Exercise 169) its submodules are in $1-1$-correspondence with the ideals $\mathfrak{a}$ of $\mathbb{R}[X]$ containing (X^2). As $\mathbb{R}[X]$ is a PID, any ideal is principal, so we can write $\mathfrak{a} = (f(X))$ where we may suppose that the polynomial f is monic. Now $(X^2) \subseteq (f(X))$ if and only if $f(X) \mid X^2$ which is equivalent to $f(X) = 1$ or X or X^2. Thus $\mathfrak{a} = \mathbb{R}[X]$ or (X) or (X^2). Hence, by the correspondence theorem, the submodules of M are of the form $\mathfrak{a}/(X^2)$ where $\mathfrak{a}$ is one of these possibilities; i.e. these are

$$0 = (X^2)/(X^2), \qquad U = (X)/(X^2), \qquad M = \mathbb{R}[X]/(X^2).$$

Note that the submodule U does not have a complementary submodule. Hence $M = \mathbb{R}[X]/(X^2)$ is not semisimple as an $\mathbb{R}[X]$-module.

Exercise 233. Let K be a field, and let $M = K[X]/(X^2+1)$, considered as a $K[X]$-module.

(i) If $K = \mathbb{R}$, show that M is simple.
(ii) If $K = \mathbb{C}$, show that M is not simple, but is semisimple.
(iii) If $K = \mathbb{F}_2$, show that M is neither simple nor semisimple.

Exercise 234. Let

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

Let $M = \mathbb{R}^2$ be the $\mathbb{R}[X]$-module were

$$(a_0 + a_1X + \cdots + a_nX^n)\mathbf{v} = a_0\mathbf{v} + a_1A\mathbf{v} + \cdots + a_nA^n\mathbf{v}.$$

(i) Determine the $\mathbb{R}[X]$-submodules of M (there are 3 of them).
(ii) Deduce that M is not semisimple as an $\mathbb{R}[X]$-module.

Lemma 235. *Let M be a simple module. Then M is semisimple.*

Proof. The only submodules of M are 0 and M. If we take $U = 0$ we can take $W = M$, and if we take $U = M$ then we let $W = 0$. In either case $M = U \oplus W$. □

Example 236. Let D be a division ring. Then D has no non-zero proper left ideals. Therefore D is simple as a left D-module. Therefore D is semisimple as a left D-module. Hence D is a semisimple ring.

Exercise 237. Let K_1, K_2 be fields. Let $R = K_1 \times K_2$. Determine the ideals of R. Show that R is a semisimple ring.

Lemma 238. *Let M be semisimple. Let N be a submodule of M. Then N is semisimple.*

Proof. Let U be a submodule of N. Then U is a submodule of M. As M is semisimple, there is a submodule V of M so that $M = U \oplus V$. Let $W = V \cap N$. Then W is a submodule of N. We claim that $N = U \oplus W$. Note that $U \cap W \subset U \cap V = \{0\}$ as $U \oplus V$ is a direct sum. Hence $U \cap W = \{0\}$. Let $\mathbf{n} \in N$. Then $\mathbf{n} \in M = U \oplus V$. So we can write $\mathbf{n} = \mathbf{u} + \mathbf{v}$ where $\mathbf{u} \in U$ and $\mathbf{v} \in V$. However, $\mathbf{v} = \mathbf{n} - \mathbf{u}$. As $\mathbf{n} \in N$ and $\mathbf{u} \in U \subseteq N$ then $\mathbf{v} \in N$. Hence $\mathbf{v} \in N \cap V = W$. Thus every element $\mathbf{n} \in N$ can be written as $\mathbf{u}+\mathbf{v}$ where $\mathbf{u} \in U$ and $\mathbf{v} \in W$. Thus $N = U \oplus W$. It follows that N is semisimple. □

Exercise 239. Let $\mathbb{R}[X]$ be the $\mathbb{R}[T]$-module where multiplication is given by

$$(b_0+b_1T+\cdots+b_nT^n)\cdot f(X) \;=\; b_0f(X)+b_1f(X+1)+\cdots+b_nf(X+n).$$

(a) Show that $\mathbb{R}$ is an $\mathbb{R}[T]$-submodule of $\mathbb{R}[X]$.
(b) Compute $(-1+T)\cdot(X+3X^2)$.

(c) Let $f(X) \in \mathbb{R}[X]$ have degree $m \geq 1$. Show that $(-1+T) \cdot f(X)$ has degree $m-1$.
(d) Show that $\mathbb{R}[X]$ is not free as an $\mathbb{R}[T]$-module.
(e) Show that $\mathbb{R}[X]$ is not semisimple as an $\mathbb{R}[T]$-module.
(f) Let $f(X) \in \mathbb{R}[X] \setminus \{0\}$ have degree $m \geq 0$. Show that

$$\mathrm{Span}_{\mathbb{R}[T]}(f(X)) = \mathrm{Span}_{\mathbb{R}}(1, X, \ldots, X^m).$$

Exercise 240. Let R be a commutative ring, and let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are pairwise distinct proper ideals satisfying $\mathfrak{b} \cap \mathfrak{c} = \mathfrak{a}$ and $\mathfrak{b} + \mathfrak{c} = R$. Suppose that the only ideals containing $\mathfrak{a}$ are $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ and R.

(i) Show that $R/\mathfrak{a}$ is not simple.
(ii) Show that $R/\mathfrak{a}$ is semisimple.
(iii) Let K be a field, and let g, $h \in K[X]$ be irreducible and monic, with $g \neq h$. Show that $K[X]/(gh)$ is semisimple.

2. Semisimple implies direct sum of simple modules

Now we will take K to be a field and A a K-algebra. Recall that this is simply a ring whose centre contains K. Since $K \subseteq Z(A) \subseteq A$, an A-module V is also a K-module and thus a K-vector space.

Theorem 241. *Let V be an A-module which is finite dimensional when considered as a K-vector space. Suppose V is semisimple as an A-module. Then V is the direct sum of finitely many simple A-modules.*

Proof. Let V be a semisimple A-module which is finite dimensional as a K-vector space. The proof is by induction on $\dim_K(V)$. Suppose first that $\dim_K(V) = 1$. Any A-submodule of V is also a K-subspace and so has dimension 0 or 1 over K. Thus the only A-submodules of V are 0 and V so V is simple, so already a direct sum of one simple A-module.

Now for the inductive step. Again if V is simple then we're finished. So suppose V is not simple. Then there is a A-submodule $0 \subsetneq U \subsetneq V$. Hence $1 \leq \dim_K(U) \leq \dim_K(V) - 1$. As V is semisimple, we have $V = U \oplus W$ where W is an A-submodule. Moreover $\dim_K(W) = \dim_K(V) - \dim_K(U)$, so $1 \leq \dim_K(W) \leq \dim_K(V) - 1$. By Lemma 238, U and W are semisimple. By the inductive hypothesis, $U = U_1 \oplus \cdots \oplus U_r$ and $W = W_1 \oplus \cdots \oplus W_s$ where the U_i and V_j are simple. Thus $V = U \oplus W = U_1 \oplus \cdots \oplus U_r \oplus W_1 \oplus \cdots \oplus W_s$ is the direct sum of simple submodules. □

3. Artin–Wedderburn

Theorem 242 (Artin–Wedderburn)**.** *Let K be a field. Let A be a finite dimensional semisimple K-algebra. Then*

$$A \cong \prod_{i=1}^{m} M_{n_i}(D_i)$$

for some positive integers $n_1, \dots, n_m$ and K-division algebras $D_1, \dots, D_m$. Moreover, the factors $M_{n_i}(D_i)$ are unique up to reordering.

We omit the proof.

4. The Centre of a Group Ring

Recall that for a ring R, the **centre of** R, denoted by $Z(R)$, is

$$Z(R) = \{s \in R \ : \quad rs = sr \text{ for all } r \in R\}.$$

For now K is a field and G is a finite group. We would like to understand $Z(K[G])$.

Lemma 243. *Let ψ be an element of $K[G]$. Then $\psi \in Z(K[G])$ if and only if $h\psi h^{-1} = \psi h$ for all $h \in G$.*

Proof. If $\psi \in Z(K[G])$ then $h\psi h^{-1} = hh^{-1}\psi = \psi$ for all $h \in G$. We want to prove the converse.

Suppose $h\psi h^{-1} = \psi$ for all $h \in G$. This is equivalent to $h\psi = \psi h$ for all $h \in G$. We want to show that $\phi\psi = \psi\phi$ for all $\phi \in K[G]$. But

$$\phi = \sum_{h \in G} b_h \cdot h, \qquad b_h \in K.$$

So

$$\begin{aligned} \psi \cdot \phi = \psi \cdot \left(\sum_{h \in G} b_h \cdot h \right) &= \left(\sum_{h \in G} b_h \cdot \psi \cdot h \right) \\ = \left(\sum_{h \in G} b_h \cdot h \cdot \psi \right) &= \left(\sum_{h \in G} b_h \cdot h \right) \cdot \psi = \phi \cdot \psi. \end{aligned}$$

□

Lemma 244. *Let ψ be an element of $K[G]$, and write*

$$\psi = \sum_{g \in G} a_g \cdot g.$$

Then $\psi \in Z(K[G])$ if and only if $a_g = a_{h^{-1}gh}$ for all g, $h \in G$.

Proof. By Lemma 243 we know that $\psi \in Z(K[G])$ iff $h\psi h^{-1} = \psi$ for all $h \in G$, i.e.

$$\sum_{g \in G} a_g \cdot g = \sum_{g \in G} a_g \cdot hgh^{-1}.$$

Let $k \in G$ and let's compare the coefficient of k on both sides of this equality:

- On the left, the coefficient of k is a_k.
- On the right, the coefficient of k is a_g where $hgh^{-1} = k$. This is the same as $g = h^{-1}kh$. Thus, on the right, the coefficient of k is $a_{h^{-1}kh}$.

Hence $\psi \in Z(K[G])$ iff $a_k = a_{h^{-1}kh}$ for all k, $h \in G$. □

Lemma 245. *Let $C_1, C_2, \ldots, C_r$ be the conjugacy classes of G. For $i = 1, 2, \ldots, r$ we let*

$$\phi_i = \left(\sum_{g \in C_i} g \right) \quad \in K[G].$$

Then $\phi_1, \phi_2, \ldots, \phi_r$ is a K-basis for $Z(K[G])$.

PROOF. Recall the following facts from Algebra II.

- Two elements g, $g' \in G$ belong to the same conjugacy class C_i if and only if $g = h^{-1}g'h$ for some $h \in G$.
- The conjugacy classes $C_1, C_2, \cdots, C_r$ form a partition of G. Thus
$$G = C_1 \cup C_2 \cup \cdots \cup C_r,$$
and
$$C_i \cap C_j = \emptyset \qquad \text{whenever } i \neq j.$$

Let $\psi \in K[G]$. Can write

$$\psi = \sum_{g \in G} a_g \cdot g = \sum_{i=1}^{r} \sum_{g \in C_i} a_g \cdot g, \qquad a_g \in K.$$

By Lemma 244, $\psi \in Z(K[G])$ if and only if $a_g = a_{g'}$ whenever g, g' belong to same C_i. Thus $\psi \in Z(K[G])$ if and only if

$$\psi = \sum_{i=1}^{r} a_i \cdot \left(\sum_{g \in C_i} g \right) = \sum_{i=1}^{r} a_i \cdot \phi_i.$$

Hence $Z(K[G]) = \mathrm{Span}(\phi_1, \ldots, \phi_r)$. It remains to show that $\phi_1, \ldots, \phi_r$ are linearly independent. If $\sum a_i \phi_i = 0$ then

$$0 = \sum_{i=1}^{r} a_i \cdot \left(\sum_{g \in C_i} g \right).$$

Note that each $g \in G$ occurs exactly once in the double sum, with coefficient a_i where i is the unique index such that $g \in C_i$. So $a_i = 0$. □

Example 246. From Algebra II we know that two elements in S_n are conjugate if and only if they have the same cycle structure. Therefore the conjugacy classes in S_3 are

$$C_1 = \{\mathrm{id}\}, \quad C_2 = \{(1,2), (1,3), (2,3)\}, \quad C_3 = \{(1,2,3), (1,3,2)\}.$$

Let $\phi_1 = \langle \mathrm{id} \rangle$, $\phi_2 = \langle (1,2) \rangle + \langle (1,3) \rangle + \langle (2,3) \rangle$, $\phi_3 = \langle (1,2,3) \rangle + \langle (1,3,2) \rangle$.

By Lemma 245, ϕ_1, ϕ_2, ϕ_3 is a basis for $Z(K[S_3])$.

5. Centres of Matrix Rings

Let R be a ring and $n \geq 1$. The purpose of this section is to understand the centre of the matrix ring $M_n(R)$. Let $e_{i,j} \in M_n(R)$ be the matrix with the entry 1 in the (i,j)-th position, and 0 everywhere else. Note that these n^2 elements $e_{i,j}$ with $1 \leq i,\ j \leq n$ are a basis for $M_n(R)$ as an R-module. Thus every matrix $A \in M_n(R)$ can be written uniquely as

$$A = \sum_{1 \leq i,\ j \leq n} a_{i,j} \cdot e_{i,j}, \qquad a_{i,j} \in R. \tag{20}$$

Indeed, the coefficients $a_{i,j}$ are just the entries of this matrix. We note the following property of these matrices:

$$e_{i,j} \cdot e_{r,s} = \delta_{j,r} \cdot e_{i,s}, \qquad \delta_{j,r} = \begin{cases} 1 & j = r \\ 0 & j \neq r. \end{cases} \tag{21}$$

Here $\delta_{j,r}$ is called the **Kronecker delta**. Formula (21) is easy to check. In fact we shall need the following more general formula

$$(\alpha \cdot e_{i,j}) \cdot (\beta \cdot e_{r,s}) = (\delta_{j,r} \cdot \alpha \cdot \beta) \cdot e_{i,s}, \tag{22}$$

for any $\alpha,\ \beta \in R$.

Lemma 247. *Let $A \in M_n(R)$ be as in (20). For any $1 \leq u,\ v \leq n$*

$$a_{u,v} \cdot I_n = \sum_{k=1}^{n} e_{k,u} \cdot A \cdot e_{v,k}.$$

Proof. The proof is really easy. We start with the formula (20). From this we have

$$A \cdot e_{v,k} = \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{i,j} \cdot e_{i,j} \cdot e_{v,k}.$$

Note that $e_{i,j} \cdot e_{v,k} = 0$ if $j \neq v$ by (21). Thus in the inner sum we can restrict to $j = v$. We get

$$A \cdot e_{v,k} = \sum_{1 \leq i \leq n} a_{i,v} \cdot e_{i,v} \cdot e_{v,k} = \sum_{1 \leq i \leq n} a_{i,v} \cdot e_{i,k}$$

again using formula (21). Hence

$$e_{k,u} \cdot A \cdot e_{v,k} = \sum_{1 \leq i \leq n} e_{k,u} \cdot (a_{i,v} \cdot e_{i,k}).$$

Here the summand is zero except when $i = u$. Thus

$$e_{k,u} \cdot A \cdot e_{v,k} = a_{u,v} \cdot e_{k,k}$$

by (22). Now

$$\sum_{k=1}^{n} e_{k,u} \cdot A \cdot e_{v,k} = a_{u,v} \cdot \underbrace{(e_{1,1} + e_{2,2} + \cdots + e_{n,n})}_{I_n}$$

completing the proof. □

Lemma 248. *Let R be a ring. Suppose $A = (a_{i,j}) \in Z(M_n(R))$. Then $a_{u,v} = 0$ whenever $u \neq v$.*

PROOF. Suppose $A \in Z(M_n(R))$ and $u \neq v$. Then

$$\begin{aligned} a_{u,v} \cdot I_n &= \sum_{k=1}^{n} e_{k,u} \cdot A \cdot e_{v,k} && \text{by Lemma 247} \\ &= \sum_{k=1}^{n} e_{k,u} \cdot e_{v,k} \cdot A && \text{as } A \in Z(M_n(R)) \\ &= 0 && \text{by (21) since } u \neq v. \end{aligned}$$

□

Lemma 249. *Let R be a ring. Let $A \in Z(M_n(R))$. Then $A = a \cdot I_n$ for some $a \in R$.*

PROOF. Suppose $A = (a_{i,j}) \in Z(M_n(R))$. By Lemma 248 we know that $a_{u,v} = 0$ whenever $u \neq v$. Thus

$$A = \sum_{i=1}^{n} a_{i,i} \cdot e_{i,i}.$$

We compute $Ae_{u,v}$ and $Ae_{v,u}$ and compare. Note

$$\begin{aligned} Ae_{u,v} &= \sum_{i=1}^{n} a_{i,i} \cdot e_{i,i} \cdot e_{u,v} \\ &= a_{u,u} \cdot e_{u,u} \cdot e_{u,v} && \text{using (21)} \\ &= a_{u,u} \cdot e_{u,v} && \text{using (21)} \end{aligned}$$

and

$$\begin{aligned} e_{u,v}A &= \sum_{i=1}^{n} e_{u,v} \cdot a_{i,i} \cdot e_{i,i} \\ &= e_{u,v} \cdot a_{v,v} \cdot e_{v,v} && \text{using (22)} \\ &= a_{v,v} \cdot e_{u,v} && \text{using (21).} \end{aligned}$$

But $A \in Z(M_n(R))$, so $Ae_{u,v} = e_{u,v}A$. Hence, by the above calculations, $a_{u,u} \cdot e_{u,v} = a_{v,v} \cdot e_{u,v}$, so $a_{u,u} = a_{v,v}$ for all u, v. Write $a_{u,u} = a$. Then

$$A = a \sum_{i=1}^{n} e_{i,i} = a \cdot I_n.$$

□

Lemma 250. *Let R be a ring. Then*

$$Z\left(M_n(R)\right) = Z(R) \cdot I_n = \left\{ \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & a \end{pmatrix} \ : \ a \in Z(R) \right\}.$$

PROOF. Let $A \in Z(M_n(R))$. By Lemma 249 we have $A = aI_n$ for some $a \in R$. Let $b \in R$. Since $A \in Z(M_n(R))$, the matrix $A = aI_n$ commutes with the matrix $B = bI_n$. This is equivalent to $ab = ba$. Thus $a \in Z(R)$, and so $A \in Z(R) \cdot I_n$. We have proved that $Z(M_n(R)) \subseteq Z(R) \cdot I_n$. The reverse inclusion is an easy exercise. □

6. Maschke's Theorem

Let K be a field and G a group. Since $K \subseteq K[G]$, a $K[G]$-module is also a K-module, or in otherwords a vector space over K. Maschke's Theorem is one of the two big theorems of representation theory that we see in the course; the other one is Schur's Lemma.

Theorem 251 (Maschke's Theorem)**.** *Let K be a field and G a finite group. Suppose that $\#G \cdot 1_K \neq 0_K$. Let V be a $K[G]$-module. Then V is a semisimple $K[G]$ module. In particular $K[G]$ is a semisimple K-algebra.*

Example 252. Let G be a finite group, and K a field. If $K = \mathbb{C}$ or $\mathbb{R}$, then $\#G \cdot 1_K = \#G \neq 0$, so can apply Maschke's theorem to deduce that $K[G]$ is semisimple.

Example 253. Let $G = S_5$. Then $\#G = 120$. Note that $\#G \cdot \overline{1} = \overline{0}$ in $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, so we cannot apply Maschke's theorem to the group rings $\mathbb{F}_2[S_5]$, $\mathbb{F}_3[S_5]$, $\mathbb{F}_5[S_5]$. But $\#G \cdot \overline{1} \neq \overline{0}$ in $\mathbb{F}_p$ for all primes $p \geq 7$, so can apply Maschke's theorem to deduce that $\mathbb{F}_p[G]$ is semisimple for $p \geq 7$.

Exercise 254. Let V be an R-module and let $\pi : V \to V$ be an R-module homomorphism satisfying $\pi^2 = \pi$ (i.e. $\pi \circ \pi = \pi$). Show that $V = \ker(\pi) \oplus \mathrm{Im}(\pi)$. **Hint:** Show that $\mathbf{v} - \pi(\mathbf{v}) \in \ker(\pi)$ for all $\mathbf{v} \in V$.

Exercise 255. Let K be a field and G a group. Let V be a $K[G]$-module. Let $\pi : V \to V$ satisfy the following:

- π is K-linear;
- $\pi(h\mathbf{v}) = h\pi(\mathbf{v})$ for all $\mathbf{v} \in V$ and $h \in G$.

Show that π is $K[G]$-linear.

PROOF OF MASCHKE'S THEOREM. Let U be a $K[G]$-submodule of V. Then U is a K-subspace of V. By Example 229, there is a K-subspace W' such that $V = U \oplus W'$. Note that we're not finished by any means. If W' is a $K[G]$-submodule then we would be finished, but in general it does not have to be. However every $\mathbf{v} \in V$ can be decomposed uniquely as $\mathbf{v} = \mathbf{u} + \mathbf{w}'$ with $\mathbf{u} \in U$ and $\mathbf{w}' \in W'$. We let ϕ be the projection:

$$\phi : V \to V, \qquad \phi(\mathbf{u} + \mathbf{w}') = \mathbf{u}, \qquad (\mathbf{u} \in U,\ \mathbf{w}' \in W').$$

This ϕ is a K-linear transformation which satisfies $\phi(\mathbf{u}) = \mathbf{u}$ for any $\mathbf{u} \in U$, and $\mathrm{Im}(\phi) = U$.

Let

$$\pi : V \to V, \qquad \pi(\mathbf{v}) = \frac{1}{\#G} \sum_{g \in G} g^{-1}\phi(g\mathbf{v}).$$

Note that this does not make sense if $\#G$ is zero when regarded as an element of the field K, which is why we imposed the condition $\#G \cdot 1_K \neq 0_K$.

We **claim** the following:

(i) π is a $K[G]$-homomorphism.
(ii) $\pi^2 = \pi$;
(iii) $\mathrm{Im}(\pi) = U$;

Let's assume these claims for now. Let $W = \ker(\pi)$. By (i), π is a $K[G]$-homomorphism and so W is a $K[G]$-module. Also by (ii), $\pi^2 = \pi$ and so by Exercise 254, $V = \mathrm{Im}(\pi) \oplus \ker(\pi) = U \oplus W$ by (iii). Thus we found a complementary submodule to U and so V is semisimple as a $K[G]$-module. All that remains is to prove claim (i), (ii) and (iii).

Let $\mathbf{u} \in U$. Since U is a $K[G]$-submodule, we know that $g\mathbf{u} \in U$ for all $g \in G$. Hence $\phi(g\mathbf{u}) = g\mathbf{u}$ by the definition of ϕ. Now

$$\pi(\mathbf{u}) = \frac{1}{\#G} \sum_{g \in G} g^{-1}g\mathbf{u} = \frac{1}{\#G} \sum_{g \in G} \mathbf{u} = \mathbf{u}.$$

In particular $U \subseteq \mathrm{Im}(\pi)$. Let $\mathbf{v} \in V$. By definition of ϕ we know that $\phi(g\mathbf{v}) \in U$. Since U is a $K[G]$-module, $\pi(\mathbf{v}) \in U$. Hence $\mathrm{Im}(\pi) = U$. This proves claim (iii).

For claim (ii), let $\mathbf{v} \in V$. We said that $\pi(\mathbf{v}) \in U$, and that $\pi(\mathbf{u}) = \mathbf{u}$ for all $\mathbf{u} \in U$. Hence $\pi^2(\mathbf{v}) = \pi(\pi(\mathbf{v})) = \pi(\mathbf{v})$.

It remains to check (i). Since ϕ is K-linear, is is easy to see that π is K-linear. By Exercise 255, to show that π is $K[G]$-linear it is enough to show that $\pi(h\mathbf{v}) = h\pi(\mathbf{v})$ for all $\mathbf{v} \in V$ and $h \in G$. From the definition of π,

$$\pi(h\mathbf{v}) = \frac{1}{\#G} \sum_{g \in G} g^{-1}\phi(gh\mathbf{v}).$$

Write $k = gh$. Note that as g runs through the elements of G so does $k = gh$. Moreover $g^{-1} = hk^{-1}$. Thus

$$\pi(h\mathbf{v}) = \frac{1}{\#G} \sum_{k \in G} hk^{-1}\phi(k\mathbf{v}) = h\pi(\mathbf{v}).$$

This completes the proof. □

7. Examples of Artin–Wedderburn and Maschke in Action

Theorem 256. *Let G be a finite group. Let m be the number of conjugacy classes of G. Then there are positive integers $n_1, n_2, \ldots, n_m$ such*

that

$$\mathbb{C}[G] \cong \prod_{i=1}^{m} M_{n_i}(\mathbb{C}). \tag{23}$$

Moreover,

$$\#G = n_1^2 + n_2^2 + \cdots + n_m^2.$$

PROOF. By Maschke's theorem, $\mathbb{C}[G]$ is a semisimple $\mathbb{C}$-algebra, and so by Artin–Wedderburn,

$$\mathbb{C}[G] \cong \prod_{i=1}^{m} M_{n_i}(D_i)$$

where D_i are finite dimensional $\mathbb{C}$-division algebras. But, by Theorem 123 the only finite dimensional $\mathbb{C}$-division algebra is $\mathbb{C}$. Thus (23) holds, for some value of m and some positive integers $n_1, \ldots, n_m$. Computing dimensions on either side of (23) gives

$$\#G = \dim_{\mathbb{C}}(\mathbb{C}[G]) = \sum_{i=1}^{m} \dim_{\mathbb{C}}(M_{n_i}(\mathbb{C})) = n_1^2 + \cdots + n_m^2.$$

It remains to check that m is the number of conjugacy classes. By Exercise 91,

$$Z(\mathbb{C}[G]) \cong \prod_{i=1}^{m} Z(M_{n_i}(\mathbb{C})).$$

However, from Lemma 250, $Z(M_{n_i}(\mathbb{C})) \cong \mathbb{C}$. Thus

$$Z(\mathbb{C}[G]) \cong \mathbb{C}^m.$$

Hence $m = \dim_{\mathbb{C}}(Z(\mathbb{C}[G]))$. By Lemma 245, this dimension is the number of conjugacy classes of G. □

Example 257. Let us apply Theorem 256 to $G = S_3$. Note that $\#S_3 = 6$, and (see Example 246) the group S_3 has 3 conjugacy classes. Thus we are looking for positive integers n_1, n_2, n_3 such that $n_1^2+n_2^2+n_3^2 = 6$. The only possibility (up to reordering) is $n_1 = n_2 = 1$ and $n_3 = 2$. Thus

$$\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}).$$

Exercise 258. Write down the corresponding theorem to Theorem 256 where $\mathbb{C}$ is replaced with $\mathbb{R}$. **Hint:** you will need Frobenius' Theorem.

Exercise 259. Write down the corresponding theorem to Theorem 256 where $\mathbb{C}$ is replaced with $\mathbb{F}_p$. **Hint:** you will need Wedderburn's Little Theorem.

Exercise 260. Let G be a finite group, and suppose

$$\mathbb{R}[G] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}.$$

(i) Determine the order of G.
(ii) Determine the number of conjugacy classes of G.

(iii) Explain why G is non-abelian.
(iv) Write $\mathbb{C}[G]$ as a product of matrix rings.

CHAPTER 11

Simple Rings

1. Definition and First Examples

Definition. A ring R is **simple** if its only 2-sided ideals are 0 and R.

Example 261. $\mathbb{Z}$ is not simple. e.g. $2\mathbb{Z}$ is a proper non-zero 2-sided ideal.

Example 262. Recall that the only ideals of a field K are 0 and K. Thus every field is a simple ring.

Theorem 263. *Division rings are simple.*

PROOF. By Theorem 111, a division ring has no non-zero proper left ideal. Any 2-sided ideal is a left ideal. Thus division rings are simple. □

Example 264. Recall that fields are division rings. Thus Theorem 263 is a generalization of Example 262. In particular, the quaternions are a division ring and thus simple.

Exercise 265. Let

$$J = \left\{ \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}.$$

Show that J is a 2-sided ideal of $M_2(\mathbb{Z})$.

Exercise 266. Let R be a non-zero ring. Suppose R is non-simple. Show that $M_2(R)$ is non-simple.

Exercise 267. Let R be a non-zero commutative ring. Show that R is simple if and only if R is a field.

2. Matrix Rings of Simple Rings are Simple

Theorem 268. *Let R be a simple ring. Then $M_n(R)$ is simple.*

Example 269. Theorem 268 gives us lots of examples of simple rings. For example, $\mathbb{R}$ is a simple ring (we said fields are simple), thus $M_2(\mathbb{R})$ is a simple ring. But we can iterate the process to deduce that $M_2(M_2(\mathbb{R}))$ is a simple ring. What's $M_2(M_2(\mathbb{R}))$? It's the ring of 2×2 matrices whose entries are 2×2 real matrices. But also $\mathbb{H}$ is a simple ring (we said division rings are simple) and so $M_2(\mathbb{H})$ is a simple ring and so $M_7(M_2(\mathbb{H}))$ is a simple ring ...

Let's start thinking about proving Theorem 268. Recall what it means for a ring R to be simple. It means that the only 2-sided ideals are 0 and R itself.

PROOF OF THEOREM 268. Let J be an 2-sided ideal of $M_n(R)$. Suppose $J \neq 0$. We want to show that $J = M_n(R)$, and for this it is enough to show that $I_n \in J$. As $J \neq 0$, there is a matrix $A \in J$ with $A \neq 0$. Thus one of the entries $a_{u,v}$ of A is non-zero. From Lemma 247 and the fact that J is a 2-sided ideal, we have $a_{u,v} \cdot I_n \in J$. We haven't yet shown that I_n belongs to J, but we've shown that a non-zero multiple of it belongs to J. We need to use the fact that R is simple to show that $I_n \in J$.

Consider the maps

$$\phi : R \to M_n(R), \quad \phi(r) = r \cdot I_n, \qquad \psi : M_n(R) \to M_n(R)/J, \quad B \mapsto B + J.$$

It's easy to see that ϕ is a homomorphism, and ψ is just the natural quotient homomorphism. Thus $\psi \circ \phi$ is a homomorphism, and its kernel is a 2-sided ideal of R. Moreover, $(\psi \circ \phi)(a_{u,v}) = \psi(a_{u,v} \cdot I_n) = 0$ as $a_{u,v} \cdot I_n \in J$. Thus the 2-sided ideal $\ker(\psi \circ \phi)$ contain the non-zero element $a_{u,v}$. As R is simple, $\ker(\psi \circ \phi) = R$. Thus

$$I_n + J = \psi(I_n) = (\psi \circ \phi)(1) = 0$$

giving $I_n \in J$ and completing the proof. □

Exercise 270. Let K be a field and V be a countably infinite dimensional K-vector space (this means that V has a countably infinite K-basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \dots$). Let $R = \mathrm{End}_K(V)$ (this is the endormphism ring of V, but recall that an endomorphism of a K-vector space is the same as K-linear transformation $V \to V$).

(i) Let I be the set of endomorphism $T \in \mathrm{End}_K(V)$ with finite rank. Show that I is a 2-sided ideal of R. (Recall that the rank of a linear transformation T is the dimension of the image.)
(ii) Show that R/I is a simple ring.