# MA3201 Algebra II Notes

Thang Pang Ern

**Reference books:**

(1). Dummit, D. S. and Foote, R. M. (2003). *Abstract Algebra 3rd Edition*. Wiley.

(2). Gallian, J. (2009). *Contemporary Abstract Algebra 7th Edition*. Cengage Learning.

## Contents

# 1. Introduction to Rings

## 1.1. *Basic Definitions and Examples*

**Definition 1.1** (ring). A ring $R$ is a set together with two binary operations $+$ and $\cdot$ (called addition and multiplication) satisfying the following axioms:

**(i)** $(R,+)$ is an Abelian group

**(ii)** $\cdot$ is associative, i.e. $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ for all $a,b,c\in R$

**(iii)** the distributive laws hold in $R$, i.e. for all $a,b,c\in R$, we have

$$(a+b)\cdot c = (a\cdot c)+(b\cdot c) \quad \text{and} \quad a\cdot(b+c) = (a\cdot b)+(a\cdot c)$$

In Definition 1.1, we usually write $ab$ in place of $a\cdot b$ or $a\times b$ for $a,b\in R$. The additive identity of $R$ will always be denoted by 0.

**Definition 1.2** (commutative ring). $R$ is commutative if $\cdot$ is commutative.

**Definition 1.3** (multiplicative identity). $R$ is said to have a multiplicative identity (or contain a 1) if there exists an element $1\in R$ such that

$$1\cdot a = a\cdot 1 = a \quad \text{for all } a\in R.$$

**Definition 1.4** (division ring). A ring $R$ with identity 1, where $1\neq 0$, is a division ring if every non-zero element $a\in R$ has a multiplicative inverse, i.e.

$$\text{for any } 0\neq a\in R \quad \text{there exists} \quad b\in R \quad \text{such that} \quad ab=ba=1.$$

**Definition 1.5** (field). A commutative division ring is a field.

**Example 1.1.** $\mathbb{Z}$ is a ring. In fact it is a commutative ring but not a division ring. Hence, $\mathbb{Z}$ is not a field.

**Example 1.2.** $\mathbb{Q},\mathbb{R},\mathbb{C}$ are fields.

**Example 1.3.** Let $n$ be a positive integer. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring, but in general, it may not have multiplicative inverses. If $n=p$ for some prime $p$, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

**Example 1.4.** $2\mathbb{Z}$ is a commutative ring without identity.

**Example 1.5.** The trivial ring $R=\{0\}$ is a commutative ring with identity $1=0$.

**Example 1.6.** The following sets can be regarded as rings:

$\mathcal{P}_n(\mathbb{R})$ which is the set of polynomials of degree at most $n$ with coefficients in $\mathbb{R}$

$\mathcal{C}^0(\mathbb{R})$ which is the set of continuous functions on $\mathbb{R}$

$\mathcal{C}^1(\mathbb{R})$ which is the set of differentiable functions on $\mathbb{R}$

**Definition 1.6** (endomorphism ring)**.** Let $V$ be a vector space over $\mathbb{R}$. Then, the endomorphism ring $\mathrm{End}_{\mathbb{R}}(V)$ is defined as follows:

$$\mathrm{End}_{\mathbb{R}}(V) = \{\varphi : \varphi \in \mathrm{Hom}(\mathbb{R},\mathbb{R})\}$$

Here, $\mathrm{Hom}(\mathbb{R},\mathbb{R})$ is the set of homomorphisms from $\mathbb{R}$ to itself.

We will formally relook at Definition 1.6 in Definition 4.7.

**Example 1.7** (endomorphism ring)**.** The endomorphism ring $\mathrm{End}_{\mathbb{R}}(V)$ of a vector space over $\mathbb{R}$ is an example of a non-commutative ring. To see why, consider

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \text{ and } \mathbf{B} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{so} \quad \mathbf{AB} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ and } \mathbf{BA} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

**Example 1.8** (quaternions)**.** Recall from MA2202 that the quaternions $Q_8$ is an example of a non-commutative ring. In fact, this is historically the first example of such a ring. To see why, we have

$$i, j, k \in Q_8 \quad \text{where} \quad ij = k \text{ but } ji = -k \neq k.$$

**Proposition 1.1.** Let $R$ be a ring. Then, the following hold:

**(i)** $0a = a0 = 0$ for all $a \in R$

**(ii)** $(-a)b = a(-b) = -ab$ for all $a, b \in R$

**(iii)** $(-a)(-b) = ab$ for all $a, b \in R$

**(iv)** If $R$ has a multiplicative identity, it is unique and $-a = (-1)a$

**Example 1.9.** Let

$$\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}.$$

It is a well-known fact that $\mathbb{Q}\left[\sqrt{2}\right]$ is a ring. We claim that $\mathbb{Q}\left[\sqrt{2}\right]$ is a field, i.e. we need to deduce that

$$\frac{1}{a + b\sqrt{2}} \quad \text{is} \quad \text{of the form } c + d\sqrt{2} \text{ where } c, d \in \mathbb{Q}.$$

This is simply the process of *rationalising the denominator* that one would recall from Secondary School. That is,

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \quad \text{so we can choose} \quad c = \frac{a}{a^2 - 2b^2} \text{ and } d = -\frac{b}{a^2 - 2b^2}.$$

**Definition 1.7** (zero divisor)**.** Let $R$ be a ring. A non-zero element $a \in R$ is a zero divisor if

$$\text{there exists a non-zero } b \in R \quad \text{such that} \quad \text{either } ab = 0 \text{ or } ba = 0.$$

**Definition 1.8** (unit). Let $R$ be a ring with a multiplicative identity. An element $u \in R$ is a unit if

$$\text{there exists some } v \in R \quad \text{such that} \quad uv = vu = 1.$$

The set of units in $R$ is denoted by $R^*$.

**Remark 1.1.** A zero divisor may not be a unit.

**Proposition 1.2.** $R^\times$ is a group under multiplication, referred to as the group of units of $R$.

**Example 1.10.** The ring $\mathbb{Z}$ has no zero divisors and its only units are $\pm 1$.

**Example 1.11.** The group of units of $\mathbb{Z}/n\mathbb{Z}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$. Recall from MA1100 or MA2202 that

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}.$$

All elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ are zero divisors. In sum, every non-zero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor.

**Definition 1.9** (integral domain). A commutative ring with multiplicative identity 1 is an integral domain if it has no zero divisors.

**Example 1.12.** Every field is an integral domain. To see why, suppose $a, b \in F$ for some field $F$ such that $a \neq 0$ and $ab = 0$. Considering $ab = 0$, multiplying both sides by $a^{-1}$, we obtain $b = 0$.

**Example 1.13.** $\mathbb{Z}$ is an integral domain.

**Example 1.14.** The ring $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$ is an integral domain.

**Definition 1.10** (Gaussian integer). Let

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C} \quad \text{denote} \quad \text{the set of Gaussian integers.}$$

**Example 1.15.** The Gaussian integers $\mathbb{Z}[i]$ is a commutative ring with identity and its unit elements are $\pm 1, \pm i$.

**Proposition 1.3** (cancellation property). Suppose $x, y, z$ are elements in an integral domain and $xy = xz$. Then, either $x = 0$ or $y = z$.

*Proof.* We have $x(y - z) = 0$ so $x = 0$ or $y - z = 0$. By definition of an integral domain (Definition 1.9), it follows that $x = 0$ or $y = z$. □

**Proposition 1.4.** Any finite integral domain is a field.

*Proof.* Let $R$ be a finite integral domain and $a \in R$ be non-zero. By the cancellation law, the map $x \mapsto ax$ is injective. Since $R$ is finite, this map is surjective, i.e.

$$\text{there exists } b \in R \quad \text{such that} \quad ab = 1, \text{ i.e. } a \text{ is a unit in } R.$$

Since $a$ was an arbitrary non-zero element, then $R$ is a field. □

**Corollary 1.1** (Sadhukhan). If $p$ is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

One can prove Corollary 1.1 using Euclid's lemma. Moreover, one can prove a stronger result (generally covered in MA3265 too) that

$$Z/n\mathbb{Z} \text{ is a field} \quad \text{if and only if} \quad n \text{ is prime.}$$

**Definition 1.11** (subring). A subring of a ring $R$ is a subgroup of $R$ that is closed under multiplication.

**Proposition 1.5** (subring criterion). A non-empty subset $S$ of a ring $R$ is a subring if $S$ is closed under subtraction and multiplication, i.e.

$$a, b \in S \quad \text{implies} \quad a - b \in S \text{ and } ab \in S.$$

**Example 1.16.** $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$.

**Example 1.17.** $n\mathbb{Z} = \{nk \in \mathbb{Z} : k \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$.

**Example 1.18.** $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

## 1.2. *Polynomial Rings, Matrix Rings, and Group Rings*

**Definition 1.12** (polynomial ring). Let $R$ be a commutative ring with multiplicative identity 1. Let $x$ be a formal variable. We define the polynomial ring $R[x]$ as follows:

$$R[x] = \{a_0 + a_1 x + \ldots + a_n x^n \in R : n \in \mathbb{Z}_{\geq 0}\}.$$

Addition and multiplication on $R[x]$ are defined in the obvious/naive way.

Each polynomial should be regarded as a formal expression instead of a function.

**Lemma 1.1.** If $R$ is an integral domain, then $R[x]$ is an integral domain.

**Definition 1.13** (matrix ring). Let $R$ be a ring with multiplicative identity 1 (or $\mathbf{I}$). Define the matrix ring $\mathcal{M}_{n\times n}(R)$ to be the set consisting of

$$\left(a_{ij}\right)_{n\times n} \quad \text{where } a_{ij} \in R.$$

Addition and multiplication on $\mathcal{M}_{n\times n}(R)$ are defined as per matrix multiplication in Linear Algebra.

**Example 1.19.** If $R=\mathbb{R}$ (recall that $\mathbb{R}$ is a field from Example 1.2) so $\mathbb{R}$ is a multiplicative identity with 1. Then, $\mathcal{M}_{n\times n}(\mathbb{R})$ is the usual matrix algebra. We have the usual subring of diagonal matrices, as well as the subring of upper triangular matrices.

**Definition 1.14** (group ring)**.** Let $R$ be a commutative ring with multiplicative identity 1. Let $G$ be a finite group. Define the group ring $R[G]$ to be the set consisting of

$$\sum_{g\in G} a_g g \quad \text{where } a_g \in R.$$

The addition on $R[G]$ is defined in the obvious way.

**Example 1.20.** We discuss multiplication in $R[G]$. We have

$$(a_g g + a_h h)\left(a_{g'} g' + a_{h'} h'\right) = a_g a_{g'} gg' + a_h a_{g'} hg' + a_g a_{h'} gh' + a_h a_{h'} hh'.$$

Here, $gg', hg', gh', hh'$ denote group multiplication in $G$.

**Example 1.21.** We shall discuss the structure of $\mathbb{R}[\mathbb{Z}/2\mathbb{Z}]$. Note that this group ring consists of formal linear combinations of the group elements with coefficients in $\mathbb{R}$. Hence,

$$\mathbb{R}[\mathbb{Z}/2\mathbb{Z}] = \{a_0 e_0 + a_1 e_1 : a_0, a_1 \in \mathbb{R}\}.$$

Here, $e_0, e_1 \in \mathbb{Z}/2\mathbb{Z}$, with $e_0$ being the identity element of $\mathbb{Z}/2\mathbb{Z}$.

**Lemma 1.2.** Let $R$ be a commutative ring with multiplicative identity 1 and $G$ be a finite group. Then, the following hold:

**(i)** Let $e \in G$ be its identity element. Then, $1e$ is the identity of the ring $R[G]$.

**(ii)** Let $e \neq g \in G$. Then, $1-g$ is a zero divisor.

**(iii)** Let $H \leq G$. Then, $R[H]$ is a subring of $R[G]$.

**(iv)** $R[G]$ is commutative if and only if $G$ is commutative

**Definition 1.15** (product of rings)**.** Let $S$ and $R$ be two rings. Define their product $S\times R$ to be the same as the product of sets. Addition and multiplication are defined component-wise, i.e.

$$(a,b)+(c,d) = (a+c, b+d) \quad \text{and} \quad (a,b)\cdot(c,d) = (ac, bd).$$

1.3. *Ring Homomorphisms and Quotient Rings*

**Definition 1.16** (ring homomorphism)**.** Let $R$ and $S$ be rings. A ring homomorphism is a map

$$\varphi : R \to S \quad \text{satisfying} \quad \varphi(a+b) = \varphi(a) + \varphi(b) \text{ and } \varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a, b \in R.$$

**Definition 1.17** (kernel)**.** The kernel of a ring homomorphism $\varphi$, denoted by $\ker\varphi$, is the following set:

$$\ker\varphi = \{r \in R : \varphi(r) = 0_S\}.$$

So, the kernel can be viewed as a homomorphism of additive groups.

**Example 1.22.** The quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism with kernel $n\mathbb{Z}$.

**Example 1.23.** The embedding of the subring $n\mathbb{Z} \to \mathbb{Z}$ is a ring homomorphism with a trivial kernel.

**Example 1.24.** Consider the map

$$\varphi : \mathbb{C}[x] \to \mathbb{C} \quad \text{where} \quad f(x) \mapsto f(a).$$

The kernel is given by

$$\ker\varphi = \{f(x) \in \mathbb{C}[x] : f(a) = 0\} = \{(x-a)f(x) : f(x) \in \mathbb{C}[x]\}.$$

**Lemma 1.3.** Let $\varphi : R \to S$ be a ring homomorphism. Then,

$$\operatorname{im}\varphi \text{ is a subring of } S \quad \text{and} \quad \ker\varphi \text{ is a subring of } R.$$

**Definition 1.18** (ring isomorphism)**.** A bijective ring homomorphism is an isomorphism. Two rings $R$ and $S$ are isomorphic if

$$\text{there exists an isomorphism between } R \text{ and } S \quad \text{and} \quad \text{we denote using } R \cong S.$$

**Definition 1.19** (ideal)**.** Let $R$ be a ring and $I \subseteq R$.

**(i)** $I$ is a left ideal of $R$ if $I$ is an additive subgroup of $R$ and $rI \subseteq I$ for any $r \in R$

**(ii)** $I$ is a right ideal of $R$ if $I$ is an additive subgroup of $R$ and $Ir \subseteq I$ for any $r \in R$

**(iii)** $I$ is an ideal of $R$ if $I$ is both a left ideal and a right ideal of $R$

**Example 1.25** (principal ideal)**.** $n\mathbb{Z} = (n)$ is a principal ideal in $\mathbb{Z}$. Here, $(n)$ denotes the ideal generated by $n$, i.e. the smallest ideal containing $n$. By the term 'principal', we mean that $n\mathbb{Z}$ is generated by only one element (Definition 1.25).

In general, we write $rR$ for $\{rx : x \in R\}$, which is the right ideal of $R$ generated by $r$. When $R$ is commutative, we simply write $(r)$.

**Lemma 1.4.** Let $\varphi : R \to S$ be a ring homomorphism. Then, $\ker\varphi$ is an ideal of $R$.

*Proof.* Let $x, y \in \ker \varphi$. Then,

$$\varphi(x-y) = \varphi(x) - \varphi(y) = 0 - 0 = 0$$

so $x - y \in \ker \varphi$ so $\ker \varphi$ is an additive subgroup of $R$. Then, let $r, r' \in R$ and $x \in \ker \varphi$. So,

$$\varphi\left(rxr'\right) = \varphi(r)\,\varphi(x)\,\varphi\left(r'\right) = \varphi(r) \cdot 0 \cdot \varphi\left(r'\right) = 0$$

so $rxr' \in \ker \varphi$. Here, we verified that $\ker \varphi$ is a two-sided ideal of $R$ (or in short, just an ideal) by proving **(i)** and **(ii)** in Definition 1.19 concurrently. □

**Definition 1.20** (quotient ring). Let $I \subseteq R$ be an ideal. Define the quotient ring $R/I$ as follows: we can view it as an Abelian group, where multiplication is defined as follows:

$$R/I \times R/I \to R/I \quad \text{where} \quad (a+I, b+I) \mapsto ab+I \quad \text{for all } a, b \in R.$$

The image of $a \in R$ in $R/I$ is often denoted by $\overline{a}$.

**Definition 1.21** (sum of ideals). Let $I$ and $J$ be ideals of $R$. Define

$$I + J = \{a + b : a \in I, b \in J\} \quad \text{which is an ideal of } R.$$

**Definition 1.22** (product of ideals). Let $I$ and $J$ be ideals of $R$. Define

$$IJ = \left\{\sum ab : a \in I, b \in J\right\} \quad \text{which is an ideal of } R.$$

Consequently, for any $n \in \mathbb{N}$, $I^n$ is an ideal of $R$.

**Theorem 1.1** (first isomorphism theorem). Let $\varphi : R \to S$ be a ring homomorphism. Then,

$$R/\ker \varphi \cong \varphi(R).$$

Also, for any ideal $I \subseteq R$, the quotient map

$$\pi : R \to R/I \quad \text{where} \quad a \mapsto a + I = \overline{a}$$

is a surjective ring homomorphism with kernel $I$. As such, if $I \subseteq \ker \varphi$, then $\varphi$ factors through $R/I$, i.e. we have the commutative diagram shown in Figure 1, where $\overline{\varphi}(\overline{a}) = \varphi(a)$ for $a \in R$. In fact, this is the universal property of the quotient ring.

**Example 1.26.** Let $F$ be a field. Then, $F[x]/(x) \cong F$.

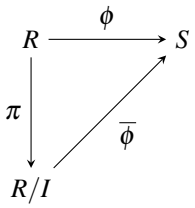


Figure 1: First isomorphism theorem for rings

**Theorem 1.2** (second isomorphism theorem)**.** Let $R$ be a ring. Let $A$ be a subring and $B$ be an ideal of $R$. Then, define

$$A+B=\{a+b : a\in A, b\in B\} \quad \text{to be a subring of } R.$$

We have the following isomorphism:

$$(A+B)/B \cong A/(A\cap B)$$

Next, let $I\subseteq J\subseteq R$ be ideals of $R$. Then, we have

$$R/J \cong (R/I)/(J/I).$$

See Figure 2 for the commutative diagram.

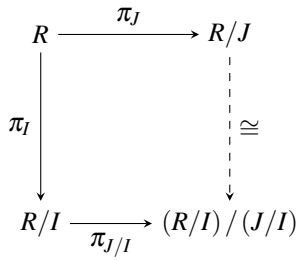


Figure 2: Second isomorphism theorem for rings

## 1.4. *Properties of Ideals*

**Definition 1.23** (smallest ideal)**.** Let $A\subseteq R$ be a subset. Let $(A)$ denote the smallest ideal in $R$ generated by $A$, so

$$(A)=\bigcap_{\substack{A\subseteq J\\ J \text{ is an ideal of } R}} \qquad J=RAR=\left\{\sum rar' : r,r'\in R, a\in A\right\}.$$

**Definition 1.24** (left and right ideals)**.** Let

$$RA = \left\{\sum ra : r \in R, a \in A\right\} \quad \text{and} \quad AR = \left\{\sum ar : r \in R, a \in A\right\}$$

to be the left ideal and right ideal generated by $A$ respectively.

**Definition 1.25** (principal ideal)**.** An ideal generated by a single element $x$ is called a principal ideal, denoted by $(x)$.

**Definition 1.26** (finitely generated ideal)**.** An ideal that is generated by a finite set is a finitely generated ideal.

**Example 1.27.** $0 = (0)$ and $R = (1)$ are trivial examples of principal ideals.

**Example 1.28.** Recall Example 1.25 where we mentioned that $(n)$ is a principal ideal.

**Example 1.29.** The ideal $(2, x) \subseteq \mathbb{Z}[x]$ is not principal.

**Example 1.30.** The ideal $\left(2x, 2x^2, 2x^3, \ldots\right) \subseteq 2\mathbb{Z}[x]$ is not finitely generated.

**Lemma 1.5.** Let $R$ be a ring. For any ideal $I \subseteq R$,

$$I = R \quad \text{if and only if} \quad I \text{ contains a unit.}$$

Furthermore, if $R$ is commutative, then

$$R \text{ is a field} \quad \text{if and only if} \quad R \text{ has only two ideals which are 0 and } R.$$

**Definition 1.27** (maximal ideal)**.** Let $I \subseteq R$ be an ideal of $R$. $I$ is said to be maximal if

$$I \neq R \quad \text{and} \quad \text{for any ideal } J \text{ containing } I \text{ we have either } J = I \text{ or } J = R.$$

**Corollary 1.2.** Let $R$ be a commutative ring. Then, the following hold:

**(i)** $R$ is a field if and only if $(0)$ is a maximal ideal

**(ii)** $I$ is a maximal ideal of $R$ if and only if $R/I$ is a field

**Example 1.31.** For any prime $p$, the ideal $(p) \subseteq \mathbb{Z}$ is maximal.

**Example 1.32.** The ideal $(x - a) \in \mathbb{C}[x]$ for any $a \in \mathbb{C}$ is a maximal ideal.

**Proposition 1.6.** Let $R$ be a ring with multiplicative identity 1. Then, any ideal $I$ is contained in a maximal ideal of $R$.

*Proof.* Use Zorn's lemma. □

**Definition 1.28** (prime ideal). Let $R$ be a commutative ring with multiplicative identity 1. An ideal $P \subseteq R$ is a prime ideal if

$$P \neq R \quad \text{and} \quad \text{for any } ab \in P \text{ either } a \in P \text{ or } b \in P.$$

**Example 1.33.** For any prime $p$, $(p) \subseteq \mathbb{Z}$ is a prime ideal.

**Example 1.34.** $(0) \subseteq \mathbb{Z}$ is a prime ideal.

**Lemma 1.6.** Let $R$ be a commutative ring with multiplicative identity 1. Let $I \subseteq R$ be an ideal. Then,

$$I \text{ is a prime ideal} \quad \text{if and only if} \quad R/I \text{ is an integral domain.}$$

So, maximal ideals are also prime ideals.

**Definition 1.29** (nilradical). Let $R$ be a commutative ring with multiplicative identity 1. Define the nilradical of $R$ to be

$$\mathfrak{N}(R) = \text{set of nilpotent elements of } R = \{x \in r : x^n = 0 \text{ for some } n \in \mathbb{Z}_{\geq 0}\}.$$

**Lemma 1.7.** Let $R$ be a commutative ring with multiplicative identity 1. Then, $\mathfrak{N}(R)$ is an ideal of $R$.

*Proof.* Let $x, y \in \mathfrak{N}(R)$. Then, there exist $n, m \in \mathbb{Z}_{\geq 0}$ such that $x^n = y^m = 0$. Note that for any $r \in R$, we have $(rx)^n = r^n x^n = 0$, where we used the fact that $R$ is commutative, so $rx \in \mathfrak{N}(R)$.

Now, let $l = 2\max\{m, n\}$, so

$$(x+y)^l = \sum_{i=0}^{l} \frac{l!}{i!\,(l-i)!} x^i y^{l-i} = 0$$

and it follows that $x + y \in \mathfrak{N}(R)$. As such, $\mathfrak{N}(R)$ is an ideal of $R$. □

## 1.5. *Rings of Fractions*

**Definition 1.30** (field of fractions). Let $R$ be an integral domain. Let $D = R \setminus \{0\}$. The field of fractions of $R$, of the quotient field of $R$, denoted by $Q$, is defined as follows:

$$\widetilde{Q} = \{(r, d) : r \in R, d \in R \setminus \{0\}\}$$

Then, define an equivalence relation on $\widetilde{Q}$ via

$$(r, d) \sim (r', d') \quad \text{if and only if} \quad rd' = r'd.$$

Then, define $Q = \widetilde{Q}/\sim$. The equivalence class $(r, d)$ is often denoted by $r/d$.

**Theorem 1.3.** Define addition on $Q$ as follows:

$$\frac{r}{d}+\frac{s}{t}=\frac{rt+ds}{dt} \quad \text{which is well-defined}$$

Define multiplication on $Q$ as follows:

$$\frac{r}{d}\times\frac{s}{t}=\frac{rs}{dt} \quad \text{which is well-defined}$$

Then, $Q$ is a field.

**Lemma 1.8.** There exists an embedding

$$\iota : R \to Q \quad \text{such that} \quad \iota(r)=\frac{r}{1}=\frac{rd}{d} \text{ for any } d\neq 0.$$

**Example 1.35.** $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

**Proposition 1.7.** Let $R$ be an integral domain with field of fractions $Q$. Let $F$ be a field containing $R$. Then,

$$F \text{ contains } Q \quad \text{so} \quad Q \text{ is the smallest field containing } R.$$

1.6. *The Chinese Remainder Theorem*

We start with a motivating fact from MA1100. Let $m,n\in\mathbb{Z}$ be coprime. By Bézout's lemma (and its converse), this is equivalent to saying that

$$\text{there exist } a,b\in\mathbb{Z} \quad \text{such that} \quad am+bn=1.$$

The new thing to take note of is that

$$\mathbb{Z}/mn\mathbb{Z}\cong\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$$

as an isomorphism of Abelian groups. This is precisely the Chinese remainder theorem. We will encounter another variant of the Chinese remainder theorem (for principal ideal domains) pretty soon in Theorem 2.4.

**Definition 1.31** (coprime ideals). Let $R$ be a commutative ring with multiplicative identity 1. Two ideals $A$ and $B$ of $R$ are coprime if $A+B=R$.

One should note that Definition 1.31 is consistent with the definition in $\mathbb{Z}$.

**Theorem 1.4.** Let $A_1,\ldots,A_k$ be pairwise coprime ideals of $R$. Then, we have the following isomorphism:

$$R/A_1\ldots A_k \to R/A_1\times\ldots\times R/A_k \quad \text{where} \quad r+A_1\ldots A_k\mapsto(r+A_1,\ldots,r+A_k)$$

**Example 1.36.** Let $p_i \in \mathbb{Z}$ be distinct primes for $1 \leq i \leq k$. Then, there exists $x \in \mathbb{Z}$ unique mod $p_1 \dots p_k$ such that

$$x \cong x_i \pmod{p_i} \text{ for any } x_i \in \mathbb{Z}.$$

# 2. Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

## 2.1. *Euclidean Domains*

**Definition 2.1** (norm)**.** Let $R$ be an integral domain. A norm on $R$ is a function

$$N : R \to \mathbb{Z}_{\geq 0} \quad \text{such that} \quad N(0) = 0.$$

**Definition 2.2** (Euclidean domain)**.** Let $R$ be an integral domain. We say that $R$ is a Euclidean domain (ED) if we can perform the following division algorithm with respect to some norm $N$, which is for any $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

$$a = bq + r \quad \text{with } r = 0 \text{ or } N(r) < N(b).$$

$q$ is called the quotient and $r$ is called the remainder.

**Example 2.1.** $\mathbb{Z}$ is a Euclidean domain with $N(r) = |r|$. Then, the division is exactly the division on $\mathbb{Z}$.

**Example 2.2.** Any field is a Euclidean domain with any norm, so the choice of the norm is not unique.

**Example 2.3.** The polynomial ring $R[x]$ (or over any field) is a Euclidean domain with $N(f) = \deg(f)$.

**Proposition 2.1** (Gaussian integers forms a Euclidean domain)**.** The ring of Gaussian integers $\mathbb{Z}[i] \subseteq \mathbb{C}$

$$\text{with the standard norm } N(a+bi) = a^2 + b^2 \quad \text{is a Euclidean domain.}$$

*Proof.* Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Let $\alpha/\beta = x + yi \in \mathbb{Q}[i] \subseteq \mathbb{C}$. Also, let

$$m, n \in \mathbb{Z} \quad \text{such that} \quad |x - m| \leq \frac{1}{2} \text{ and } |y - n| \leq \frac{1}{2}.$$

Then,

$$\begin{aligned} \alpha &= \beta(x + yi) \\ &= \beta[m + x - m + (n + y - n)i] \\ &= \beta(m + ni) + \beta[x - m + (y - n)i] \\ &= \beta(m + ni) + \gamma \end{aligned}$$

Then,

$$N(\gamma) = N(\beta) N(x - m + (y - n)i) \leq \frac{1}{2} N(\beta)$$

and the result follows. One notes that the quotient and remainder are not unique in this case. □

## 2.2. *Principal Ideal Domains*

**Definition 2.3** (principal ideal domain)**.** A principal ideal domain (PID) is an integral domain in which every ideal is a principal ideal.

**Example 2.4.** A field is a PID.

**Example 2.5.** The ring $\mathbb{Z}$ is a PID. It is also an ED.

**Definition 2.4.** Let $R$ be a commutative ring and $a, b \in R$ with $b \neq 0$.

**(i)** $a$ is a multiple of $b$ or $b$ is a divisor of $a$ if

$$\text{there exists } x \in R \quad \text{such that} \quad a = xb.$$

We write $b \mid a$.

**(ii)** A greatest common divisor of $a$ and $b$ is a non-zero element $d$ such that

$$d \mid a \text{ and } d \mid b \quad \text{and} \quad \text{for any } d' \text{ which divides both } a \text{ and } b \text{ we have } d' \mid d.$$

**Lemma 2.1.** Let $R$ be an integral domain. If $d, d'$ are both greatest common divisors of $a$ and $b$, then

$$d' = ud \quad \text{for some unit } u.$$

**Proposition 2.2.** Let $R$ be a PID. Let $a, b$ be non-zero such that $(a,b) = (d)$. Then, $d = \gcd(a,b)$. Hence, the gcd always exists and it is of the form $ax + by$.

**Proposition 2.3.** Every non-zero prime ideal in a PID is a maximal ideal.

**Definition 2.5** (Noetherian ring)**.** A commutative ring $R$ is said to be Noetherian if it satisfies the following ascending chain condition on ideals. That is, if

$$I_1 \subseteq I_2 \subseteq \ldots \quad \text{is} \quad \text{a chain of ideals of } R,$$

then, there exists $m \in \mathbb{N}$ such that $I_k = I_m$ for all $k \geq m$. This is equivalent to saying that

$$\bigcup_{i=1}^{\infty} I_i = I_m.$$

**Example 2.6.** Many rings that we have encountered are Noetherian. Take $\mathbb{Z}$ and $\mathbb{Z}[x]$ for example.

**Theorem 2.1.** Every PID is Noetherian.

**Proposition 2.4.** Every ED is a PID.

*Proof.* Let $R$ be an ED and $I$ be a non-zero ideal of $R$. Among the non-zero elements of $I$, let $b$ be such that $d(b)$ is minimum among all elements from $I$. Then, we shall prove that $I = \langle b \rangle$. It is clear that $\langle b \rangle \subseteq I$. For $a \in I$,

$$\text{there exist } q, r \in R \text{ such that } a = bq + r \quad \text{where} \quad r = 0 \text{ or } d(r) < d(b).$$

Note that $r = a - bq \in I$. $d(r)$ cannot be less than $d(b)$, otherwise it would contradict the minimality of $d(b)$. So, $r = 0$. This shows that $a \in \langle b \rangle$, so $I \in \langle b \rangle$. We conclude that $I = \langle b \rangle$. □

**Theorem 2.2** (Euclidean algorithm)**.** Let $R$ be a Euclidean domain and $a, b \in R$ such that both are non-zero. Then,

$$\text{one can use the Euclidean algorithm} \quad \text{to} \quad \text{compute } \gcd(a, b).$$

We will not discuss how the Euclidean algorithm works as the reader should have prior knowledge of it from MA1100.

Now, recall how factorisation works in $\mathbb{Z}$. We wish to generalise this idea to more general rings.

**Definition 2.6** (irreducibles and units)**.** Let $R$ be an integral domain. Suppose $r \in R$ is non-zero and is not a unit. Then,

$$r \text{ is irreducible over } R \quad \text{if} \quad \text{whenever } r = ab \text{ with } a, b \in R \text{ then either } a \text{ or } b \text{ is a unit.}$$

Otherwise, $r$ is reducible.

**Definition 2.7** (associate)**.** Let $R$ be an integral domain. If

$$a = ub \text{ where } u \text{ is a unit of } R \quad \text{then} \quad a \text{ and } b \text{ are associates.}$$

**Definition 2.8** (prime ideal)**.** Let $R$ be an integral domain. A non-zero element $p \in R$ is called a prime in $R$ if $(p)$ is a prime ideal. In other words,

$$p \mid ab \quad \text{implies} \quad p \mid a \text{ or } p \mid b$$

We know that $\mathbb{Z}$ is an integral domain so Definition 2.8 is in fact Euclid's lemma! Moreover, the remarkable fact here is that irreducible and prime *feels the same* but they are actually different. Without the abstractions coined in Definitions 2.6 and 2.8, this would be difficult to distinguish.

**Lemma 2.2.** In an integral domain, a prime element is always irreducible.

*Proof.* Let $p$ be a prime and suppose $p = ab$. Then, $pa' = a$ or $pb' = b$. Suppose the equation $pa' = a$ holds. Then, $a = pa' = aba'$, which implies $ba' = 1$, so $b$ is a unit. □

**Proposition 2.5.** In a PID, a non-zero element is prime if and only if it is irreducible.

**Example 2.7.** We shall verify that $1+\sqrt{-3}$ is irreducible but not prime in $\mathbb{Z}\left[\sqrt{-3}\right]$.

*Solution.* Note that $N\left(a+b\sqrt{-3}\right) = a^2+3b^2$. Suppose $1+\sqrt{-3}$ can be factorised as $xy$, where neither $x$ nor $y$ is a unit. Then,

$$N(xy) = N(x)N(y) = 4 \quad \text{which implies} \quad N(x) = N(y) = 2.$$

However, there are no integers $x$ and $y$ satisfying $a^2+3b^2 = 2$, which implies that either $x$ or $y$ is a unit and so $1+\sqrt{-3}$ is an irreducible.

Now, we prove that $1+\sqrt{-3}$ is not a prime. We see that

$$\left(1+\sqrt{-3}\right)\left(1+\sqrt{-3}\right) = 4 = 2\cdot 2$$

so $\left(1+\sqrt{-3}\right) \mid 4$. Suppose $\left(1+\sqrt{-3}\right) \mid 2$. Then, there exist $a,b \in \mathbb{Z}$ such that

$$\left(1+\sqrt{-3}\right)\left(a+b\sqrt{-3}\right) = 2 \quad \text{so} \quad a-3b+(a+b)\sqrt{-3} = 2.$$

Hence, $a-3b = 2$ and $a+b = 0$ but no integers satisfy these two equations. □

**Example 2.8.** We shall verify that 7 is irreducible over $\mathbb{Z}\left[\sqrt{5}\right]$.

*Solution.* Suppose on the contrary that $7 = xy$, where neither $x$ nor $y$ is a unit. Then, $N(7) = N(x)N(y) = 49$. As neither $x$ nor $y$ is a unit, then $N(x) = 7$. Suppose $x = a+b\sqrt{5}$. Then, there exist $a,b \in \mathbb{Z}$ such that $\left|a^2-5b^2\right| = 7$, i.e. $a^2-5b^2 = 7$ or $a^2-5b^2 = -7$. Working in modulo 7, it is easy to see that the only solution is $(a,b) = (0,0)$. However, this implies that $a$ and $b$ are divisible by 7. We write $a = 7r$ and $b = 7s$, where $r,s \in \mathbb{Z}$. Then, $x = 7\left(r+s\sqrt{5}\right)$, which implies that $N(x)$ is divisible by 49, which is a contradiction. □

## 2.3. *Unique Factorisation Domains*

**Definition 2.9** (unique factorisation domain)**.** A unique factorisation domain (UFD) is an integral domain $R$ in which every non-zero element $r \in R$ which is not a unit has the following two properties:

**(i)** $r$ can be written as a finite product of irreducibles $p_i$ of $R$, i.e.

$$r = p_1 \dots p_n$$

**(ii)** the decomposition $r = p_1 \dots p_n$ is unique up to multiplication by units and permutation, i.e. if there exist irreducibles $q_i$ such that $r = q_1 \dots q_m$, then $m = n$ and $q_i = p_i$ after relabelling

**Example 2.9.** We can uniquely decompose

$$6 = 2\cdot 3 = (-2)\cdot(-3) \quad \text{in } \mathbb{Z}.$$

**Proposition 2.6.** In a UFD, a non-zero element is prime if and only if it is irreducible.

**Proposition 2.7.** Let $a$ and $b$ be two non-zero elements of a UFD $R$. Suppose

$$a = up_1^{a_1} \dots p_n^{a_n} \text{ and } a = vp_1^{b_1} \dots p_n^{b_n} \quad \text{are the prime factorisations of } a \text{ and } b,$$

where $u$ and $v$ are units, $p_i$ are primes and the exponents $a_i, b_i \in \mathbb{Z}_{\geq 0}$. Take $p_i^0 = 1$. Then,

$$d = p_1^{d_1} \dots p_n^{d_n} \text{ where } d_i = \min\{a_i, b_i\} \quad \text{is a gcd of } a \text{ and } b.$$

**Theorem 2.3.** Every PID is a UFD.

*Proof.* Let $R$ be a PID and $a_0$ be any non-zero non-unit in $R$. We need to prove the following:

- $a_0$ is a product of irreducibles (the product might consist of only one factor)
- the factorisation is unique up to associates and the order in which the factors appear

We address the first point. If $a_0$ is an irreducible, we are done. If not, write $a_0 = b_1a_1$, where neither $b_1$ nor $a_1$ is a unit and $a_1 \neq 0$. If $a_1$ is not irreducible, write $a_1 = b_2a_2$, where neither $b_2$ nor $a_2$ is a unit and $a_2 \neq 0$. In general, $a_n = b_{n+1}a_{n+1}$ for all $n \in \mathbb{N}$ , where $b_1, b_2, \dots$ are not units in $R$ and $a_0, a_1, a_2, \dots$ are non-zero elements of $D$.

So, $\langle a_0 \rangle \subseteq \langle a_1 \rangle \subseteq \dots$ is a strictly increasing chain of ideals. By the ascending chain condition for PIDs, this chain is finite, i.e. there exists $r \in \mathbb{N}$ such that $\langle a_r \rangle = \langle a_{r+1} \rangle = \dots$. In particular, $a_r$ is an irreducible factor of $a_0$. Thus, every non-zero non-unit in $R$ has at least one irreducible factor.

Now, write $a_0 = p_1c_1$, where $p_1$ is irreducible and $c_1$ is not a unit. If $c_1$ is not irreducible, write $c_1 = p_2c_2$, where $p_2$ is irreducible and $c_2$ is not a unit. Repeat to obtain the following strictly increasing chain of ideals: $\langle a_0 \rangle \subseteq \langle c_1 \rangle \subseteq \langle c_2 \rangle \subseteq \dots$, which terminates eventually. Suppose there exists $s \in \mathbb{N}$ such that $\langle c_s \rangle = \langle c_{s+1} \rangle$. Then, $c_s$ is irreducible and $a_0 = p_1p_2 \dots p_sc_s$, where each $p_i$ is irreducible. The first result follows.

For the second point, suppose some $a \in R$ has two different representations, i.e.

$$a = p_1p_2 \dots p_r = q_1q_2 \dots q_s,$$

where the $p$'s and $q$'s are irreducible and repetition is permitted. If $r = 1$, then $a$ is irreducible, and consequently, $s = 1$ and $p_1 = q_1$, which supports the uniqueness of factorisation claim. Assume that $a$ can be expressed as a product of fewer than $r$ irreducible factors in only one way. Since $p_1 \mid q_1q_2 \dots q_s$, then it must divide some $q_i$. Without a loss of generality, $p_1 \mid q_1$. Then, there exists $u \in R$ ($u$ is a unit) such that $q_1 = up_1$.

So, $up_1p_2\dots p_r = uq_1q_2\dots q_s$, for which by cancellation, $p_2\dots p_r = uq_2\dots q_s$. The induction hypothesis tells us that these two factorisations are identical up to associates and the order in which the factors appear. We conclude that the same is true regarding the two factorisations of $a$. □

**Corollary 2.1.** Every ED is a UFD.

**Example 2.10.** $\mathbb{Z}$ is an ED, a PID, and a UFD.

At this point, the following chain of inclusions should be quite obvious:

$$\text{fields} \subseteq \text{ED} \subseteq \text{PID} \subseteq \text{UFD} \subseteq \text{integral domains} \subseteq \text{commutative rings} \subseteq \text{rings}$$

**Example 2.11.** The ring $\mathbb{Z}[x]$ is a UFD but not a PID.

**Example 2.12** (Motzkin)**.** The ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

is a PID but not an ED. This was the first example of a PID that is not an ED, which was given by Israeli-American mathematician Theodore Motzkin.

**Example 2.13.** The ring $\mathbb{Z}\left[\sqrt{-5}\right]$ is an integral domain but not a UFD.

**Theorem 2.4** (Chinese remainder theorem)**.** Let $R$ be a PID and $r = up_1^{a_1}\dots p_n^{a_n}$ be the prime factorisation of $r$. Then,

$$R/(r) \cong R/\left(p_1^{a_1}\right) \times R/\left(p_n^{a_n}\right).$$

We consider the ring $\mathbb{Z}[i]$ of Gaussian integers as an application and summary. With the standard complex norm, we know that $\mathbb{Z}[i]$ is an ED, a PID, and aufd. Note that the norm is always $\in \mathbb{Z}_{\geq 0}$. We have the following beautiful results (Theorems 2.5 and 2.6).

**Theorem 2.5** (Fermat sum of two squares theorem)**.** Let $p \in \mathbb{Z}$ be a positive prime. Then,

$$p = a^2 + b^2 \text{ for some } a,b \in \mathbb{Z} \quad \text{if and only if} \quad p = 2 \text{ or } p \equiv 1 \pmod 4.$$

The expression is unique up to multiplication by $-1$ and interchanging $a$ and $b$.

**Theorem 2.6.** The irreducible elements in $\mathbb{Z}[i]$, up to multiplication by units, are as follows:

**(i)** $1+i$, which is of norm 2

**(ii)** $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$

**(iii)** $a \pm bi$, where

$$p = a^2 + b^2 = (a+bi)(a-bi) \text{ for } p \equiv 1 \pmod 4,$$

where $p$ is a prime in $\mathbb{Z}$

**Corollary 2.2.** The irreducible elements in $\mathbb{Z}[i]$ are either up to some unit $u \in \mathbb{Z}[i]$ and a prime $p \in \mathbb{Z}$, or $a+bi$ with $a^2+b^2 = p$ for some prime $p \in \mathbb{Z}$. In particular, a prime $p \in \mathbb{Z}$ has at most 2 irreducible factors in $\mathbb{Z}[i]$.

**Corollary 2.3.** $1 \pm i$ are irreducible over $\mathbb{Z}[i]$.

So, it remains to determine whether we can factor an odd prime $p \in \mathbb{Z}$ in the bigger ring $\mathbb{Z}[i]$.

**Lemma 2.3.** Let $p$ be a prime in $\mathbb{Z}$. If $p \equiv 3 \pmod 4$, then $p$ is irreducible over $\mathbb{Z}[i]$.

*Proof.* Consider $p = a^2+b^2$ in $\mathbb{Z}/4\mathbb{Z}$, for which $p$ cannot be 3 mod 4. □

**Lemma 2.4.** Let $p$ be a prime, where $p \equiv 1 \pmod 4$. Then,

$$p \mid \left(n^2+1\right) \quad \text{for some } n \in \mathbb{Z}.$$

*Proof.* It suffices to show that the equation $x^2+1=0$ has a root in $\mathbb{Z}/p\mathbb{Z}$. Recall from MA2202 that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$ (we will state it again in Proposition 3.4). As $4 \mid (p-1)$, there exists $r \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order 4, and the result follows. □

**Corollary 2.4.** Let $p$ be a prime, where $p \equiv 1 \pmod 4$. Then,

$$p = a^2+b^2 = (a+bi)(a-bi) \quad \text{for some } a,b \in \mathbb{Z}.$$

# 3. Polynomial Rings

## 3.1. *Definitions and Basic Properties*

In this section, we only consider commutative rings $R$ with multiplicative identity 1 for polynomial rings. Recall the polynomial ring $R[x]$ (Definition 1.12), so by repeatedly adjoining the elements $x_1, \ldots, x_n$, we define

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n].$$

**Proposition 3.1.** Let $S$ be a commutative ring with multiplicative identity 1. Let $\varphi : R \to S$ be a ring homomorphism. Then, for any $a_1, \ldots, a_n \in S$, there exists a unique ring homomorphism

$$\widetilde{\varphi} : R[x_1, \ldots, x_n] \to S \quad \text{such that} \quad \widetilde{\varphi}(r) = \varphi(r) \text{ and } \widetilde{\varphi}(x_i) = a_i.$$

**Proposition 3.2.** Let $I$ be an ideal of $R$. We consider $I$ as a subset of $R[x]$ and denote $(I) = I[x]$ to be the ideal generated by $I$ in $R[x]$. We have the following isomorphism:

$$(R/I)[x] \cong R[x]/(I).$$

So, if $I$ is prime in $R$, then $(I)$ is prime in $R[x]$.

**Proposition 3.3.** Let $F$ be a field. Then,

$$F[x] \text{ is an ED} \quad \text{with} \quad \text{the norm } N(f) = \deg(f).$$

**Corollary 3.1.** Let $F$ be a field. Then, the following hold:

**(i)** $F[x]$ is a PID, hence a UFD

**(ii)** Let $f(x) \in F[x]$. Then,

$$f(a) = 0 \text{ for } a \in F \quad \text{if and only if} \quad (x-a) \mid f(x)$$

**(iii)** Let $f(x) \in F[x]$ be of degree $n$. Then, $f(x)$ has at most $n$ roots in $F$ counting multiplicity

**(iv)** Let $f(x) \in F[x]$. Then,

$$F[x]/(f) \text{ is a field} \quad \text{if and only if} \quad f \text{ is prime.}$$

**(v)** If $p(x), q(x) \in F[x]$ are distinct irreducible polynomials, i.e. $(p(x)) \neq (q(x))$, then they are coprime

**(vi)** Let

$$f(x) = p_1^{a_1}(x) \ldots p_n^{a_n}(x) \quad \text{be} \quad \text{an irreducible factorisation of } f(x).$$

Then,

$$F[x]/(f(x)) \cong F[x]/\left(p_1^{a_1}(x)\right) \times \ldots \times F[x]/(p_n^{a_n}(x))$$

**Proposition 3.4.** Let $F$ be a field and $G \subseteq F^\times$ be a finite subgroup. Then, $G$ is cyclic. So,

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \quad \text{is} \quad \text{a cyclic group for any prime } p.$$

Proposition 3.4 was used in the proof of Lemma 2.4. Moreover, the proof of this proposition requires a well-known result known as the fundamental theorem of finitely generated Abelian groups.

**Definition 3.1** (polynomial functions)**.** Let $F$ be a field. Then, define the set of polynomial functions on $F$, denoted by $\mathcal{P}$, to be functions from $F$ to $F$ of the form

$$F \to F \quad \text{where} \quad x \mapsto f(x) = \sum_{i=0}^{n} a_i x^i.$$

Note that the set of polynomial functions on $F$, denoted by $\mathcal{P}$, is obviously a ring under pointwise addition and multiplication. As such, we have an obvious ring homomorphism $F[x] \to \mathcal{P}$ (Example 3.1).

**Example 3.1.** Consider the ring of polynomial functions on $\mathbb{Z}/2\mathbb{Z}$.

**Proposition 3.5.** The ring homomorphism

$$\varphi : F[x] \to \mathcal{P} \text{ is an isomorphism} \quad \text{if and only if} \quad F \text{ is infinite.}$$

*Proof.* Clearly, $\varphi$ is a surjective ring homomorphism. As such, it suffices to prove that

$$\ker \varphi = \{e\} \quad \text{if and only if} \quad F \text{ is infinite.}$$

We first prove the forward direction by contraposition. Suppose $F$ is a finite set. Then, $F = \{a_1, \ldots, a_n\}$. So, the image of the non-zero polynomial $(x-a_1)\ldots(x-a_n)$ is the zero function, so $\ker \varphi \neq \{e\}$.

We then prove the reverse direction. Suppose $F$ is an infinite set. Suppose

$$f(x) = \sum_{i=1}^{n} a_i x^i \in \ker \varphi.$$

Then, $f(a) = 0$ for all $a \in F$. By **(ii)** of Corollary 3.1, the result follows. □

**Theorem 3.1.** We have

$$R \text{ is a UFD} \quad \text{if and only if} \quad R[x] \text{ is a UFD.}$$

So, $F[x_1, \ldots, x_n]$ is a UFD for a field $F$.

Now, we shall consider some irreducible polynomials in $F[x]$ and construct some interesting fields.

**Lemma 3.1.** Let $F$ be a field and $f(x) \in F[x]$ be of degree 2 or 3. Then,

$$f(x) \text{ is reducible} \quad \text{if and only if} \quad f(x) \text{ has a root in } F.$$

**Example 3.2.** We have the factorisation

$$x^2+3x+4 = (x-3)(x-5) \quad \text{in } \mathbb{Z}/11\mathbb{Z}.$$

To see why, working from right to left,

$$(x-3)(x-5) = x^2-8x+15 = x^2+3x+4.$$

**Example 3.3.** Suppose $F = \mathbb{Z}/2\mathbb{Z}$ and $f(x) = x^2+x+1 \in F[x]$. Since $\deg f = 2$, by Lemma 3.1, $f$ is irreducible so $F[x]/(f(x))$ is a field. In fact, $F[x]/(f(x))$ is an $F$-vector space with basis $\{\overline{1}, \overline{x}\}$ and the vector space has cardinality 4. So, $F$ is a field with 4 elements.

## 3.2. *Irreducibility Criteria*

**Definition 3.2** (content and primitive polynomial)**.** Let

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \quad \text{be} \quad \text{a non-zero polynomial in } R[x].$$

Then, $\gcd(a_0, a_1, \ldots, a_n)$ is known as the content of $f(x)$, denoted by $\operatorname{cont} f$. We say that

$$f(x) \in R[x] \text{ is a primitive polynomial} \quad \text{if} \quad \operatorname{cont} f \text{ is a unit in } R.$$

**Lemma 3.2.** Let $R$ be a UFD. If

$$g(x) \text{ and } h(x) \text{ are primitive in } R[x] \quad \text{then} \quad f(x) = g(x)h(x) \text{ is also primitive in } R[x].$$

**Lemma 3.3** (Gauss' lemma)**.** If $R$ be a UFD with field of fractions $Q$ and let $f(x) \in R[x]$ be primitive. If

$$f(x) \text{ is reducible in } Q[x] \quad \text{then} \quad f(x) \text{ is reducible in } R[x].$$

**Corollary 3.2.** Let $R$ be a UFD with field of fractions $Q$. Then,

$$f(x) \in R[x] \text{ is reducible in } Q[x] \quad \text{if and only if} \quad f(x) \text{ is reducible in } R[x].$$

**Lemma 3.4.** Let $R$ be a UFD. Then, $R[x]$ is a UFD.

**Corollary 3.3.** If $R$ is a UFD, then $R[x_1, \ldots, x_n]$ is a UFD. In particular, $\mathbb{Z}[x]$ is a UFD.

We consider irreducible polynomials in $R[x]$ for an arbitrary integral domain $R$. We are mainly interested in $\mathbb{Z}[x]$ actually.

**Lemma 3.5.** Let $R$ be an integral domain with a proper ideal $I$. Let $p(x) \in R[x]$ be monic and non-constant. Then,

$$p(x) \text{ is irreducible over } R/I[x] \quad \text{implies} \quad p(x) \text{ is irreducible over } R[x].$$

**Example 3.4.** The polynomial $x^2+x+1$ is irreducible over $\mathbb{Z}[x]$ since it is irreducible over $\mathbb{Z}/2\mathbb{Z}[x]$.

**Example 3.5.** The polynomial $x^2+1$ is irreducible over $\mathbb{Z}[x]$ since it is irreducible over $\mathbb{Z}/3\mathbb{Z}[x]$.

**Lemma 3.6.** Let $P$ be a prime ideal in an integral domain $R$. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in R[x] \quad \text{be} \quad \text{monic and non-constant.}$$

Suppose $a_{n-1}, \ldots, a_0$ are all in $P$ but $a_0$ is not in $P^2$. Then, $f(x)$ is irreducible over $R[x]$.

**Corollary 3.4** (Eisenstein's cirterion)**.** Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x] \quad \text{be} \quad \text{monic and non-constant.}$$

Suppose $p \mid a_{n-1}, \ldots, a_0$ but $p^2$ does not divide $a_0$ for some prime $p$. Then, $f(x)$ is irreducible over $\mathbb{Z}[x]$.

**Example 3.6.** The polynomial $x^2+4x+2$ is irreducible over $\mathbb{Z}[x]$. To see why, suppose

$$\text{there exist polynomials } f(x), g(x) \in \mathbb{Z}[x] \quad \text{such that} \quad x^2+4x+2 = f(x)g(x).$$

This forces $f$ and $g$ to be monic linear polynomials. In particular, set $f(x) = x+c$ and $g(x) = x+d$ for some $c, d \in \mathbb{Z}$. Then,

$$f(x)g(x) = x^2 + (c+d)x + cd$$

which implies $c+d = 4$ and $cd = 2$. This pair of equations does not have integer solutions, resulting in a contradiction.

**Example 3.7.** Let $p \in \mathbb{Z}$ be a prime. Then,

$$x^n - p \quad \text{is} \quad \text{irreducible over } \mathbb{Z}[x].$$

**Example 3.8.** Define $R = \mathbb{R}[x][y] = \mathbb{R}[x,y]$. Then, $y^n - x$ is irreducible over $R$. As such, noting that

$$R/(x) \cong \mathbb{R}[y] \quad \text{is} \quad \text{an integral domain,}$$

it follows that $x$ is prime. Knowing that $\mathbb{R}[x,y]$ is a UFD (use Corollary 3.3, where we note that $\mathbb{R}$ is a UFD), then $y^n - x$ is a prime, so $R/(y^n - x)$ is an integral domain.

**Lemma 3.7.** Let $R$ be a commutative ring with multiplicative identity 1. Then,

$$R \text{ is Noetherian} \quad \text{if and only if} \quad \text{every ideal is finitely generated.}$$

**Theorem 3.2.** Let $R$ be a commutative ring with multiplicative identity 1. Then,

$$R \text{ is Noetherian} \quad \text{implies} \quad R[x] \text{ is Noetherian.}$$

# 4. Introduction to Module Theory

## 4.1. *Basic Definitions and Examples*

**Definition 4.1** (left $R$-module)**.** Let $R$ be a ring. A left $R$-module is an Abelian group $M$ equipped with a map (known as the action of $R$), defined by

$$R \times M \to M \quad \text{where} \quad (r,m) \mapsto rm = r \cdot m$$

such that for any $r,s \in R$ and $m,n \in M$, the following hold:

**(i)** **Distributivity:** $(r+s)\,m = rm + sm$

**(ii)** **Associativity:** $(rs) \cdot m = r \cdot (sm)$

**(iii)** **Distributivity:** $r\,(m+n) = rm + rs$

**(iv)** $1 \cdot m = m$ if $R$ has a multiplicative identity

Recall Definition 1.6. Note that an $R$-module structure on $M$ is equivalent to a ring homomorphism $R \to \mathrm{End}_{\mathrm{Ab}}(M)$, where Ab is some Abelian group — $\mathrm{End}_{\mathrm{Ab}}(M)$ denotes the ring of all group endomorphisms of $M$ (i.e. homomorphisms from $M$ to itself). We also require

$$1_R \text{ maps to the identity map on } M \quad \text{if} \quad 1_R \text{ exists.}$$

**Definition 4.2** (right $R$-module)**.** Let $R$ be a ring. A right $R$-module is an Abelian group $M$ equipped with a map (known as the action of $R$), defined by

$$M \times R \to M \quad \text{where} \quad (m,r) \mapsto mr = m \cdot r$$

such that for any $r,s \in R$ and $m,n \in M$, the following hold:

**(i)** **Distributivity:** $m\,(r+s) = mr + ms$

**(ii)** **Associativity:** $m \cdot (rs) = (mr) \cdot s$

**(iii)** **Distributivity:** $(m+n)\,r = mr + nr$

**(iv)** $m \cdot 1 = m$ if $R$ has a multiplicative identity

Although Definitions 4.1 and 4.2 hold, we often only consider left actions, or left modules over $R$ (Definition 4.1). We just refer to them as $R$-actions or $R$-modules. Note that

$$R \text{ is commutative} \quad \text{implies} \quad \text{left action is the same as right action.}$$

**Example 4.1.** We have the trivial 0 module for any ring $R$.

**Example 4.2.** For any field $F$, the $F$-modules are just the $F$-vector spaces.

**Example 4.3.** For any Abelian group $M$, we say that $M$ is a $\mathbb{Z}$-module.

**Example 4.4.** Let $R$ be a ring. Then,

$$R \text{ is a left } R\text{-module via left multiplication} \quad \text{and} \quad \text{a right } R\text{-module via right multiplication.}$$

**Example 4.5.** Let $I$ be a left ideal of $R$. Then, $I$ is a left $R$-module. Actually, $I$ is a left $R$-submodule of $R$.

**Example 4.6.** Let $I$ be a left ideal of $R$. Then, $R/I$ (the quotient Abelian group) is a left $R$-module.

**Definition 4.3** (submodule)**.** Let $M$ be an $R$-module. Then, a subgroup $N \subseteq M$ is an $R$-submodule of $M$ if $N$ is closed under the $R$-action.

**Example 4.7.** The zero module is a trivial submodule of any $R$-module.

**Example 4.8.** Let $M$ be an Abelian group or equivalently a $\mathbb{Z}$-module (Example 4.3). Then, a subgroup of $N$ is the same as a $\mathbb{Z}$-submodule of $M$.

**Example 4.9.** Let $S \subseteq R$ be a subring. Then,

$$R \text{ is an } S\text{-submodule} \quad \text{and} \quad S \text{ is an } S\text{-submodule of } R.$$

**Example 4.10.** Let $F$ be a field. An $F[x]$-module $V$ is the same as an $F$-vector space equipped with a linear map $T : V \to V$ (same as a linear transformation). An $F[x]$-submodule of $V$ is an $F$-subspace of $V$ that is stable under the $T$ action.

**Example 4.11.** Let $I$ be a left ideal of $R$. Then, $R/I$ is a left module.

**Lemma 4.1.** Let $R$ and $S$ be commutative rings with multiplicative identity 1. Let $\varphi : R \to S$ be a ring homomorphism such that $1_R \mapsto 1_S$. Let $M$ be an $S$-module. Then,

$$M \text{ is an } R\text{-module} \quad \text{via the action} \quad r \cdot m = \varphi(r) \cdot m.$$

**Proposition 4.1.** Let $R$ be a commutative ring with multiplicative identity 1. Let $M$ be an $R$-module.

**(i)** We have

$$0 \cdot m = 0 \text{ and } -1 \cdot m = -m \quad \text{for any } m \in M$$

The intersection of any non-empty collection of submodules of $M$ is also an $R$-submodule

**(ii)** The annihilator of $M$ in $R$,

$$\text{Ann}_M(R) = \{r \in R : rm = 0 \text{ for any } m \in M\} \quad \text{is an ideal of } R$$

**(iii)** Let $z \in Z(R)$ (center of $R$). Then,

$$zM = \{zm : m \in M\} \quad \text{is an } R\text{-submodule of } M.$$

**Corollary 4.1.** For any commutative ring with multiplicative identity 1, let $M$ be an $R$-module. Let $I \subseteq \text{Ann}_M(R)$ be an ideal. Then, $M$ is an $R/I$-module.

**Proposition 4.2.** Let $R$ be a commutative ring with multiplicative identity 1. Let $M$ be an $R$-module and $N \subseteq R$. Then,

the set of finite $R$-linear combinations $RN = \left\{ \sum_{\text{finite}} an : a \in R, n \in N \right\}$ is an $R$-submodule of $M$.

In particular, $RN$ is called the $R$-submodule generated by $N$.

**Proposition 4.3.** Let $R$ be a commutative ring with multiplicative identity 1. Let $M_1, \ldots, M_n$ be $R$-submodules of an $R$-module $M$. We define the $R$-submodule of $M$ as follows:

$$M_1 + \ldots + M_n = \{m_1 + \ldots + m_n \in M : m_i \in M_i, n \in M\}$$

## 4.2. *Quotient Modules and Module Homomorphisms*

**Definition 4.4** (module homomorphism)**.** Let $M$ and $N$ be $R$-modules. An $R$-module homomorphism is a map $\varphi : M \to N$ satisfying the following properties:

$$\varphi(x+y) = \varphi(x) + \varphi(y) \text{ for } x, y \in M \quad \text{and} \quad \varphi(rx) = r\varphi(x) \text{ for } r \in R, x \in M.$$

**Definition 4.5** (module isomorphism)**.** An $R$-module homomorphism $\varphi : M \to N$ is an isomorphism if it is a bijection, i.e. there also exists an $R$-module homomorphism $\psi : N \to M$ such that

$$\varphi \circ \psi = \mathrm{id}_N \quad \text{and} \quad \psi \circ \varphi = \mathrm{id}_M.$$

**Definition 4.6** (kernel and image)**.** Let $\varphi : M \to N$ be an $R$-module homomorphism. Then, define

$$\ker \varphi = \{m \in M : \varphi(m) = 0 \text{ in } N\}$$
$$\mathrm{im}\, \varphi = \varphi(M) = \{\varphi(m) \text{ in } N : m \in M\}$$

These sets are $R$-submodules of $M$ and $N$ respectively.

**Definition 4.7** (endomorphism ring)**.** Define

$$\mathrm{Hom}_R(M,N) \quad \text{to be} \quad \text{the set of } R\text{-module homomorphisms from } M \text{ to } N.$$

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

We collect some basic results about module homomorphisms.

**Proposition 4.4.** Let $M$ and $N$ be $R$-modules for a commutative ring $R$ with multiplicative identity 1. If $\varphi, \psi \in \mathrm{Hom}_R(M,N)$, then

$$\varphi + \psi : M \to N \quad \text{defined by} \quad (\varphi+\psi)(m) = \varphi(m) + \psi(m)$$

is also an $R$-module homomorphism.

**Proposition 4.5.** Let $M,N,L$ be $R$-modules for a commutative ring $R$ with multiplicative identity 1. Suppose

$$\varphi \in \mathrm{Hom}_R(M,N) \quad \text{and} \quad \psi \in \mathrm{Hom}_R(N,L).$$

Then,

$$\psi \circ \varphi \quad \text{is an } R\text{-module homomorphism from } M \text{ to } L.$$

**Proposition 4.6.** Let $M$ be an $R$-module for a commutative ring $R$ with multiplicative identity 1. Then, the map

$$\varphi : M \to M \quad \text{where} \quad m \mapsto rm \text{ for any } r \in R$$

is an $R$-module homomorphism.

**Example 4.12.** Let $M$ and $N$ be $\mathbb{Z}$-modules. Then, any homomorphism $M \to N$ is the same as a homomorphism of Abelian groups.

**Example 4.13.** For any field $F$, let $V$ and $W$ be $F$-vector spaces. Then, an $F$-module map from $V$ to $W$ is just a linear map from $V$ to $W$.

**Example 4.14.** For any $R$-modules $M$ and $N$, we can define the product module $M \oplus N = M \times N$ as the expected one (this is known as the direct sum of $M$ and $N$ which we will formally introduce in Definition 4.12).

**Definition 4.8** (quotient $R$-module)**.** Let $R$ be a ring. Let $M$ be an $R$-module with a submodule $N$. Define the quotient $R$-module $M/N$ as follows:

**(i)** $M/N = M/N$ as Abelian groups

**(ii)** the $R$-action is given by

$$r(m+N) = rm+N \quad \text{for any } m \in M, r \in R.$$

Moreover,

$$\text{the natural quotient map } \pi : M \to M/N \quad \text{is an } R\text{-module homomorphism.}$$

**Lemma 4.2** (universal property of the quotient)**.** Let $R$ be a ring. Let $M$ be an $R$-module with a submodule $N$. Let $L$ be another $R$-module. Then, for any $R$-module homomorphism $\varphi : M \to L$

such that $\varphi(N) = 0$,

there exists a unique $R$-module homomorphism $\varphi : M/N \to L$ such that Figure 3 commutes.

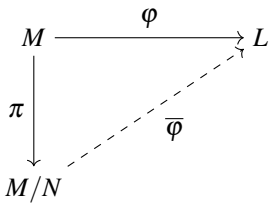


Figure 3: Universal property of the quotient

**Theorem 4.1** (isomorphism theorems)**.** Let $R$ be a ring with multiplicative identity 1. Then, the following hold:

**(1)** Let $M$ and $N$ be $R$-modules and $\varphi : M \to N$ be an $R$-module homomorphism. Then,

$$M/\ker M \cong \varphi(M).$$

**(2)** Let $M, N$ be submodules of $L$. Then,

$$(M+N)/M \cong N/(M \cap N).$$

Here,

$$M+N = \{m+n \in L : m \in M, n \in N\} \quad \text{is} \quad \text{an } R\text{-submodule of } L \text{(Proposition 4.3)}.$$

**(3)** Let $M, N$ be submodules of $L$ such that $N \subseteq M$. Then,

$$L/M \cong (L/N)/(M/N).$$

**(4)** Let $M$ and $N$ be $R$-modules such that $N \subseteq M$. Then, we have a bijection between

the set of submodules of $M$ containing $N$ and the set of submodules of $M/N$

via the quotient map $\pi : M \to M/N$.

**Definition 4.9** ($R$-algebra)**.** Let $R$ be a commutative ring with multiplicative identity 1. Then, an $R$-algebra $A$ is a ring with multiplicative identity 1 equipped with

$$\text{a ring homomorphism } f : R \to A \quad 1 \mapsto 1 \quad \text{such that } f(R) \in Z(A).$$

**Example 4.15.** A ring with multiplicative identity 1 is just a $\mathbb{Z}$-algebra.

**Definition 4.10.** Let $F$ be a field. An $F$-algebra $R$ is finite-dimensional if $R$ is a finite-dimensional $F$-vector space.

**Example 4.16.** Let $F$ be a field. The polynomial ring $F[x]$ is an $F$-algebra.

**Example 4.17.** Let $G$ be a finite group. Then, $R[G]$ is an $R$-algebra. Furthermore, if $R$ is a field, then $R[G]$ is a finite-dimensional $F$-algebra.

**Example 4.18.** Let $R$ be a commutative ring with multiplicative identity 1. Let $M$ be an $R$-module. Then, $\mathrm{End}_R(M)$ is an $R$-algebra.

**Definition 4.11** (simple module)**.** Let $R$ be a ring with multiplicative identity 1. Let $M$ be an $R$-module. Then,

$$M \text{ is simple} \quad \text{if} \quad M \neq 0 \text{ such that } 0 \text{ and } M \text{ are the only submodules of } M.$$

**Example 4.19.** All 1-dimensional vector spaces over a field $F$ are simple modules. Recall that an $F$-module is simply an $F$-vector space. We claim that

$$\text{a non-zero vector space } V \text{ over } F \text{ is simple} \quad \text{if and only if} \quad \dim(V) = 1.$$

So, if $\dim(V) = 1$, then there are no proper non-zero subspaces. Hence, $V$ is a simple $F$-module. On the other hand, if $\dim(V) > 1$, then any non-zero vector generates a 1-dimensional subspace, which is a proper non-zero submodule.

**Example 4.20.** Take $R = \mathbb{Z}$. Then, the simple $\mathbb{Z}$-modules are $\mathbb{Z}/p\mathbb{Z}$ for $p$ prime. Then, we have

$$\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} \quad \text{as rings.}$$

**Example 4.21.** Let $F$ be a field and $R = \mathcal{M}_{n\times n}(F)$ be the matrix ring. Then, $F^n$ is a simple $R$-module via matrix multiplication.

**Lemma 4.3** (Schur's lemma)**.** Let $R$ be a ring with multiplicative identity 1. Let $M$ and $N$ be simple $R$-modules. Then,

$$\text{any } R\text{-module homomorphism } \varphi : M \to N \quad \text{is} \quad \text{either 0 or an isomorphism.}$$

In particular, $\mathrm{End}_R(M)$ is a division ring.

## 4.3. *Generation of Modules, Direct Sums, and Free Modules*

**Definition 4.12** (direct sum)**.** Let $R$ be a ring with multiplicative identity 1. Let $M_1, \ldots, M_n$ be $R$-modules. Define their direct sum

$$M = M_1 \oplus \ldots \oplus M_n = \bigoplus_{i=1}^{n} M_i$$

as follows:

$$M = M_1 \times \ldots \times M_n \text{ as sets} \quad \text{and} \quad r(m_1, \ldots, m_n) = (rm_1, \ldots, rm_n) \text{ for the } R\text{-action.}$$

In relation to Definition 4.12, the more precise definition of direct sums and direct products involve categories. Finite direct sums and finite direct products are the same for $R$-modules.

**Example 4.22.** $R^n = R \oplus \ldots \oplus R$ is called the free $R$-module (simply said, a free module is one which has a basis) of rank $n$. We often write

$$\mathbf{e}_i = (0, \ldots, 1, \ldots, 0) \quad \text{where} \quad 1 \text{ is in the } i^{\text{th}} \text{ component.}$$

**Example 4.23.** By the Chinese remainder theorem (Theorem 2.4), we have

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad \text{as } \mathbb{Z}\text{-modules.}$$

**Lemma 4.4.** Let $R$ be a ring with multiplicative identity 1. Let $M$ be an $R$-module and $m_1, \ldots, m_n \in M$. Then,

$$\text{there exists a unique } R\text{-module homomorphism } \varphi : R^n \to M \quad \text{such that} \quad \mathbf{e}_i \mapsto m_i.$$

We call $R^n$ the free $R$-module of rank $n$.

**Lemma 4.5** (universal property of direct sum)**.** Let $R$ be a ring with multiplicative identity 1. Let $N, M_1, \ldots, M_n$ be $R$-modules. Then, for any $R$-module map $\varphi_i : M_i \to N$,

$$\text{there exists a unique } R\text{-module map } \varphi : \bigoplus_{i=1}^{n} M_i \to N \quad \text{such that} \quad \text{Figure 4 commutes.}$$

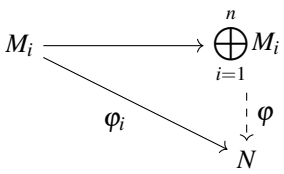


Figure 4: Universal property of direct sum

**Proposition 4.7.** Let $R$ be a ring with multiplicative identity 1. Let $M$ be an $R$-module with submodules $N_1, \ldots, N_k$. The following are equivalent:

**(i)** The natural map induced by the embeddings

$$\bigoplus_{i=1}^{k} N_i \to \sum_{i=1}^{k} N_i \quad \text{is an isomorphism}$$

**(ii)** Any $x \in N_1 + \ldots + N_k$ can be uniquely written as

$$x = a_1 + \ldots + a_k \quad \text{where } a_i \in N_i$$

**(iii)** For any $j$,

$$N_j \cap \sum_{i \neq j} N_i = 0$$

**Theorem 4.2** (universal property for free modules)**.** Let $R$ be a ring with multiplicative identity 1. Let $A = \{a_1, \ldots, a_n\}$ be a finite set. The free $R$-module over $A$ is an $R$-module $F(A)$ together with a map of sets $\iota : A \to F(A)$ such thart for any $R$-module $M$ and a map of sets $\varphi_A : A \to M$, we have

$$\text{a unique } R\text{-module homomorphism } \varphi : F(A) \to M \quad \text{such that Figure 5 commutes.}$$

The free module exists and is unique up to isomorphism. Actually,

$$F(A) \cong \bigoplus_{i=1}^{n} R.$$

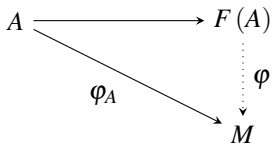


Figure 5: Universal property for free modules

**Lemma 4.6.** Let $R$ be a ring with multiplicative identity 1. Also, let

$$A_1, \ldots, A_n \text{ be } R\text{-modules} \quad \text{with} \quad \text{respective submodules } B_1, \ldots, B_n.$$

Then, we have the following isomorphism:

$$\bigoplus_{i=1}^{n} A_i / \bigoplus_{i=1}^{n} B_i \cong \bigoplus A_i / B_i$$

*Proof.* We will only prove the case where $n = 2$. We have the following commutative diagram:

$$\begin{array}{ccccc} A_1 & \longrightarrow & A_1 \oplus A_2 & \longrightarrow & A_2 \\ \downarrow & & \vdots\ \varphi & & \downarrow \\ A_1/B_1 & \longrightarrow & A_1/B_1 \oplus A_2/B_2 & \longrightarrow & A_2/B_2 \end{array}$$

Here, $\varphi$ is surjective with kernel $B_1 \oplus B_2$. The result follows by the first isomorphism theorem ((**1**) of Theorem 4.1). □

**Corollary 4.2.** Let $R$ be a ring with multiplicative identity 1 and a left ideal $I$. Then, we have the following isomorphism of $R$-modules:

$$R^n/IR^n \cong R/I \oplus \dots R/I \quad \text{which consists of } n \text{ copies.}$$

**Theorem 4.3.** Let $R$ be a commutative ring with multiplicative identity 1. Then,

$$R^n \cong R^m \quad \text{if and only if} \quad n = m.$$

**Theorem 4.4** (universal property for arbitrary direct sum of modules)**.** Let $R$ be a ring with multiplicative identity 1. Let $M_c$ be a collection of $R$-modules for, i.e. $c \in I$ for some index set $I$. Their direct sum is an $R$-module

$$\bigoplus_{c\in I} M_c \quad \text{together with} \quad \iota_c : M_c \to \bigoplus_{c\in I} M_c$$

such that for any $R$-module $N$ and $R$-module map $\varphi_c : M_c \to N$, there exists

$$\text{a unique } R\text{-module homomorphism } \varphi : \bigoplus_{c\in I} M_c \to N \quad \text{such that} \quad \text{Figure 6 commutes.}$$

The aforementioned direct sum exists and is unique up to isomorphism.

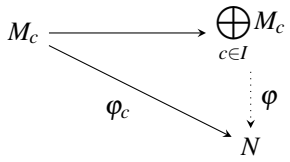


Figure 6: Universal property for arbitrary direct sum of modules

**Theorem 4.5** (universal property for arbitrary direct product of modules)**.** Let $R$ be a ring with multiplicative identity 1. Let $M_c$ be a collection of $R$-modules for, i.e. $c \in I$ for some index set $I$. Their direct product is an $R$-module

$$\pi_{c\in I} M_c \quad \text{together with} \quad \pi_c : \prod_{c\in I} M_c \to M_c$$

such that for any $R$-module $N$ and $R$-module map $\varphi_c : N \to M_c$, there exists

$$\text{a unique } R\text{-module homomorphism } \varphi : N \to \prod_{c\in I} M_c \quad \text{such that} \quad \text{Figure 7 commutes.}$$

The aforementioned direct product exists and is unique up to isomorphism.

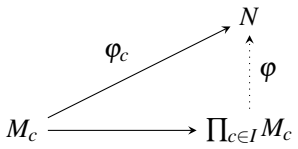


Figure 7: Universal property for arbitrary direct product of modules

## 4.4. *Tensor Product of Modules*

In this section, we assume that our rings $R$ have a multiplicative identity 1. We often consider both left modules and right modules. We start with the motivation of the tensor product $\otimes$ with two examples (Examples 4.24 and 4.25).

**Example 4.24.** Let $V = \mathbb{R}^3$ and $W = \mathbb{R}^3$ be two 3-dimensional vector spaces over $\mathbb{R}$. We shall write elements of $V$ and $W$ as row matrices, i.e. $(v_1, v_2, v_3)$ and $(w_1, w_2, w_3)$ respectively. Then, we know that $V \oplus W$ is also an $\mathbb{R}$-vector space of dimension $3+3=6$. Recall that

$$V \oplus W = \{(v,w) : v \in V, w \in W\} = \left\{(v_1, v_2, v_3, w_1, w_2, w_3) \in \mathbb{R}^6\right\}.$$

We now define a new vector space $V \otimes_{\mathbb{R}} W$ as follows:

$$V \otimes_{\mathbb{R}} W = \left\{ \sum_{\text{finite}} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} \cdot (w_1, w_2, w_3) = \sum_{\text{finite}} \begin{bmatrix} v_1w_1 & v_1w_2 & v_1w_3 \\ v_2w_1 & v_2w_2 & v_2w_3 \\ v_3w_1 & v_3w_2 & v_3w_3 \end{bmatrix} \right\}.$$

Here, $(v_1, v_2, v_3) \in V$ and $(w_1, w_2, w_3) \in W$.

As vector spaces, we have

$$V \otimes_{\mathbb{R}} W \cong \mathcal{M}_{3\times 3}(\mathbb{R}) \quad \text{which is of dimension } 3 \times 3 = 9.$$

If we write

**Example 4.25.**

# 5. Vector Spaces

## 5.1. *Definitions and Basic Theory*

We will not go through much in this chapter as they have already covered in MA2001 and MA2101.

**Theorem 5.1.** Let $F$ be a field. Then,

$$F^n \cong F^m \quad \text{if and only if} \quad n = m.$$

In other words, two finite-dimensional vector spaces are isomorphic if and only if they have the same dimension.

## 5.2. *The Matrix of a Linear Transformation*

# 6. Modules over Principal Ideal Domains

## 6.1. *The Basic Theory*

**Theorem 6.1** (submodule of free module is also free)**.** Let $R$ be a PID and $M$ be a free $R$-module of rank $n$ and $N$ be an $R$-submodule of $M$. Then,

$$N \text{ is also free} \quad \text{with} \quad \operatorname{rank}(N) \leq \operatorname{rank}(M)$$

Compare and contrast Theorem 6.1 with a known result from MA2001 — say we have a finite-dimensional vector space $V$ of rank $n$ (which means any basis of $V$ has $n$ linearly independent vectors that span the whole space). If $U$ is a subspace of $V$, then

$$U \text{ also has a basis} \quad \text{such that} \quad \operatorname{rank}(U) \leq \operatorname{rank}(V) = n.$$

Actually, the proof of the first result on $U$ having a basis is pretty much *universal* — it is merely a consequence of Zorn's lemma.

**Definition 6.1** (torsion)**.** Let $M$ be an $R$-module over an integral domain $R$. An element $m \in M$ is called torsion if

$$rm = 0 \quad \text{for some } r \in R \text{ where } r \neq 0.$$

The set of torsion elements is denoted by $\operatorname{Tor} M$.

**(i)** An $R$-module $M$ is torsion-free if $\operatorname{Tor} M = 0$

**(ii)** An $R$-module $M$ is a torsion module if $\operatorname{tor} M = M$

**Theorem 6.2.** Let $R$ be a PID and $M$ be a finitely generated $R$ module. Then,

$$M \text{ is free} \quad \text{if and only if} \quad M \text{ is torsion-free.}$$

Let $R$ be a PID. Recall from Theorem 2.3 that $R$ is also a UFD. We wish to study the diagonalisation of matrices with entries in $R$, or equivalently,

$$R\text{-module homomorphisms} \quad \varphi = (a_{ij}) \in \mathcal{M}_{n\times m}(R) : R^{\oplus m} \to R^{\oplus n}.$$

**Example 6.1.** Let $R = \mathbb{Q}$. Then, recall the usual elementary row operations (which are invertible) from MA2001. Say we have

$$\begin{bmatrix} 5 & 7 & 9 \\ 2 & 3 & 5 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 7 & 9 \\ 2/5 & 3 & 5 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 2/5 & 1/5 & 7/5 \end{bmatrix}$$
$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1/5 & 7/5 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1/5 & 0 \end{bmatrix}$$

Here, we performed scalar multiplications, elementary row operations, and elementary column operations. We need more complicated operations for a general PID $R$.

We have the following interesting fact about PIDs (Lemma 6.1).

**Lemma 6.1.** For any PID $R$, let $a_1,\dots,a_n \in R$ such that $(\alpha) = (a_1,\dots,a_n)$. Then, up to multiplication by units, we have

$$\alpha = \gcd(a_1,\dots,a_n) = \gcd(a_1,\gcd(a_2,\dots,a_n)).$$

**Lemma 6.2.** Let $R$ be a PID. Suppose $a,b \in R$ such that $\gcd(a,b) = 1$. By Bézout's identity (works for arbitrary PID), there exist $c,d \in R$ such that $ac+bd = 1$. Then,

$$\begin{bmatrix} a & b \\ -d & c \end{bmatrix}, \begin{bmatrix} a & -d \\ b & c \end{bmatrix} \in \mathcal{M}_{2\times 2}(R) \quad \text{are invertible} \quad \text{with inverses} \quad \begin{bmatrix} c & -b \\ d & a \end{bmatrix}, \begin{bmatrix} c & d \\ -b & a \end{bmatrix} \text{ respectively.}$$

**Corollary 6.1.** Let $a,b \in R$ and define $\alpha = \gcd(a,b)$. Then, there exist $\mathbf{S},\mathbf{T} \in \mathrm{GL}_2(R)$ such that

$$\begin{bmatrix} a & b \\ \star & \star \end{bmatrix} \mathbf{S} = \begin{bmatrix} \alpha & 0 \\ \star & \star \end{bmatrix} \quad \text{and} \quad \mathbf{T} \begin{bmatrix} a & \star \\ b & \star \end{bmatrix} = \begin{bmatrix} \alpha & \star \\ 0 & \star \end{bmatrix}.$$

Here, $\star$ denotes an arbitrary element in $R$.

**Lemma 6.3.** Let $R$ be a PID. Let $a,b \in R$. Then, there exist $\mathbf{S},\mathbf{T} \in \mathrm{GL}_2(R)$ such that

$$\mathbf{T} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mathbf{S} = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \quad \text{where} \quad \alpha \mid \beta.$$

Actually,

$$\alpha = \gcd(a,b) \quad \text{and} \quad \alpha\beta = ab = \det \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

uniquely up to multiplication by units.

**Theorem 6.3** (Smith normal form)**.** There exist $\mathbf{T} \in \mathcal{M}_{n\times n}(R)$ and $\mathbf{S} \in \mathcal{M}_{m\times m}(R)$ such that

$$\mathbf{TAS} = \mathrm{diag}(\alpha_1,\dots,\alpha_r,0,\dots,0) \quad \text{such that} \quad \alpha_i \mid \alpha_{i+1}.$$

The $\alpha_i$'s are the invariant factors of $\mathbf{A}$ and the RHS is the Smith normal form of $\mathbf{A}$.

**Theorem 6.4** (structure theorem for finitely generated modules over a PID)**.** Let $M$ be a finitely generated module over a PID $R$. We know that

$$M \cong \mathrm{coker}(\varphi : R^m \to R^n) \quad \text{since} \quad M \text{ is finitely generated and finitely presented.}$$

Let $S : R^n \to R^n$ and $T : R^m \to R^m$ be isomorphisms of $R$-modules. Then, we have the following isomorphism:

$$\operatorname{coker} \varphi \cong M \cong \operatorname{coker} (S \circ \varphi \circ T).$$

**Theorem 6.5.** Let $M$ be a finitely generated module over a PID $R$. Then,

$$M \cong R^k \oplus R/(\alpha_1) \oplus \ldots \oplus R(\alpha_r) \quad \text{where } \alpha_i \mid \alpha_{i+1}.$$

The elements $\alpha_i$ are the invariant factors of $M$.

**Theorem 6.6.** Let $M$ be a finitely generated module over a PID $R$. Then,

$$M \cong R^k \oplus R/\left(p_1^{a_1}\right) \oplus \ldots \oplus R/\left(p_s^{a_s}\right)$$

for not necessarily distinct prime elements $p_i$ in $R$. The elements $p_i^{a_i}$ are called the elementary factors of $M$.

**Lemma 6.4.** Let $\varphi : M \to M$ be an $R$-module homomorphism. Then,

$$\varphi(\operatorname{Tor} M) \subseteq \operatorname{Tor} N.$$

**Lemma 6.5.** Let $R$ be a PID. Let $M$ be a finitely generated $R$-module. Then,

$$M \text{ is free} \quad \text{if and only if} \quad M \text{ is torsion free.}$$

**Example 6.2.** Let $M$ be a finitely generated Abelian group. Then,

$$M \cong \mathbb{Z}^k \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z} \quad \text{where } a_i \mid a_{i+1} \text{ in } \mathbb{Z}.$$

**Example 6.3.** Let $F$ be a field. Let $G \subseteq F^\star$ be a finite subgroup. Then, $G$ is cyclic.

**Example 6.4.** The Abelian group of rational numbers $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-module. It is torsion free but not free.

**Example 6.5.** Let $M$ be an Abelian group generated by $x$ and $y$ subjected to the relation $2x+5y=0$ and $3x+7y=0$. Then, we wish to determine the structure of $M$. Consider the map

$$R^2 \to M \quad \text{where} \quad (a,b) \mapsto ax+by.$$

The kernel is generated by $(2,5)$ and $(3,7)$. We consider another map

$$\varphi : R^2 \to R^2 \quad \text{where} \quad (a,b) \mapsto a(2,5)+b(3,7) = (2a+3b, 5a+7b).$$

Then, we have $M \cong \operatorname{coker} \varphi$. The smith normal form of $\varphi$ is

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{so} \quad M \cong 0.$$

**Lemma 6.6.** Let $p$ and $q$ be distinct primes in $R$. Let $F = R/(p)$ be a field. Then, the following hold:

**(i)** Let $M = R/(q^a)$ for $a \geq 1$. As $F$-modules, we have

$$p^M/p^{t+1}M \cong 0.$$

**(ii)** Let $M = R/(p^a)$ for $a \geq 1$. Then, as $F$-modules,

$$p^t M/p^{t+1}M \cong \begin{cases} F & \text{if } t < a; \\ 0 & \text{if } t \geq a. \end{cases}$$

**(iii)** Let $M = R/(q^a) \oplus R/(p^b)$ for $a, b \geq 1$. Then, as $F$-modules,

$$p^t M/p^{t+1}M \cong \begin{cases} F & \text{if } t < a; \\ 0 & \text{if } t \geq a. \end{cases}$$

**Theorem 6.7.** Let

$$M \cong R/\left(p_1^{a_1}\right) \oplus \ldots \oplus R/\left(p_s^{a_s}\right) \cong R/\left(q_1^{b_1}\right) \oplus \ldots \oplus R/\left(q_r^{b_r}\right)$$

as modules over a PID $R$ for non-necessarily distinct primes $p_i$ and $q_i$. Then, the elementary factors are unique up to permutation and multiplication by units.

**Corollary 6.2.** Let $\varphi \in \mathcal{M}_{m\times n}(R)$ for a PID $R$. Then, the invariant factors of the Smith normal form of $\varphi$ is unique up to permutation and multiplication by units. In other words, it is independent of the invertible matrices $\mathbf{S}$ and $\mathbf{T}$ we used.

## 6.2. *The Rational Canonical Form*

We first recall some concepts from Linear Algebra. Let $F$ be a field and let $V$ be a finite-dimensional $F[x]$-module. Suppose $x$ acts on $V$ via a linear transformation $T$. Assume that $\dim_F V = n$ and fix an $F$-basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of $V$. We then have $T = (a_{ij}) \in \mathcal{M}_{n\times n}(F)$. We write $\mathbf{I} \in \mathcal{M}_{n\times n}(F)$ for the identity matrix.

Note that the set $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ forms a basis for the $F$-module $V$. However, it is only a set of generators for the $F[x]$-module $V$. Hence, we have the following isomorphism of $F[x]$-modules:

$$V \cong F[x]/(f_1(x)) \oplus \ldots \oplus F[x]/(f_r(x)) \quad \text{where } f_i \mid f_{i+1}$$

Let

$$V \cong F[x]/(f(x)) \quad \text{where} \quad f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0.$$

We consider the basis $\{1, x, x^2, \ldots, x^{n-1}\}$ under the isomorphism. With respect to this basis, $x$ acts via the matrix

$$\mathbf{T} = \begin{bmatrix} 0 & 0 & \ldots & \ldots & -a_0 \\ 1 & 0 & \ldots & \ldots & -a_1 \\ 0 & 1 & \ldots & \ldots & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}.$$

By direct computation, we have $\det(x\mathbf{I} - \mathbf{T}) = f(x)$.

**Definition 6.2** (rational canonical form)**.** The rational canonical form (RCF) of a matrix $\mathbf{T}$ is the matrix

$$\begin{bmatrix} T_1 & & \\ & T_2 & \\ & & \ddots \end{bmatrix}$$

where each $T_i$ is of the form as mentioned earlier with respect to the $F[x]$-submodule $F[x]/(f_i(x))$.

**Proposition 6.1.** Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{n\times n}(F)$.

**(i)** The RCF of $\mathbf{A}$ is unique

**(ii)** $\mathbf{A}$ is similar to its RCF

**(iii)** $\mathbf{A}$ is similar to $\mathbf{B}$ if and only if they have the same RCF

**Example 6.6.** We shall compute the RCF of the matirx

$$\mathcal{A} = \begin{bmatrix} 2 & -2 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{bmatrix} \quad \text{in } \mathcal{M}_{3\times 3}(\mathbb{Q}).$$

*Solution.* We have

$$x\mathbf{I} - \mathbf{A} = \begin{bmatrix} x-2 & 2 & -14 \\ 0 & x-3 & 7 \\ 0 & 0 & x-2 \end{bmatrix}.$$

Let $T_1$ denote the gcd of all $1\times 1$ minors, $T_1T_2$ denote the gcd of all $2\times 2$ minors and $T_1T_2T_3$ denote $\det(x\mathbf{I} - \mathbf{A})$.

We first compute $T_1$. Note that all entries of $x\mathbf{I} - \mathbf{A}$ are

$$x-2, 2, -14, x-3, 7, x-2 \quad \text{whose gcd is } 1.$$

So, $T_1 = 1$. We then look at all $2\times 2$ sub-determinants. One is able to determine that $T_1T_2 = x-2$, so $T_2 = x-2$. Lastly, $T_3 = (x-2)(x-3)$.

The Smith normal form of $x\mathbf{I}-\mathbf{A}$ is the diagonal matrix $\operatorname{diag}(1, x-2, (x-2)(x-3))$. The RCF of $\mathbf{A}$ is a block-diagonal matrix whose blocks are the companion matrices of the invariant factors. As our invariant factors are $1, x-2, (x-2)(x-3)$, the companion blocks we need in the RCF are for the polynomials $x-2$ and $(x-2)(x-3)$.

Hence, the RCF is a direct sum of

$$\text{a } 1\times 1 \text{ companion block for } x-2 \quad \text{and} \quad \text{a } 2\times 2 \text{ companion block for } x^2-5x+6.$$

Note that

$$\text{for a quadratic polynomial } x^2+ax+b \quad \text{its companion matrix is} \quad \begin{bmatrix} 0 & -b \\ 1 & -a \end{bmatrix}.$$

As such, the RCF of $\mathbf{A}$ is

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & -6 \\ 0 & 1 & 5 \end{bmatrix}.$$

□

## 6.3. *The Jordan Canonical Form*

Now, we talk about the characteristic polynomial and minimal polynomial of a square matrix.

**Definition 6.3** (minimal polynomial)**.** Let $T \in \mathcal{M}_{n\times n}(F)$. We consider the $F[x]$-module $V = F^n$, where $x$ acts as $T$. Let $\operatorname{Ann}_{F[x]}(V) = (p(x))$. Then, $p(x)$ is the minimal polynomial (often assumed to be monic) of $T$.

In fact, a number of properties of the characteristic polynomial and minimal polynomial have already been covered in MA2101.

**Definition 6.4** (algberaically closed field)**.** Let $F$ be a field. $F$ is algebraically closed if every non-constant polynomial in $F[x]$ has a root in $F$.

**Example 6.7.** $\mathbb{C}$ is algebraically closed, while $\mathbb{Q}$ and $\mathbb{R}$ are not.

**Lemma 6.7.** Let $F$ be an algebraically closed field. Then, the following hold:

**(i)** $F$ is infinite

**(ii)** If $f(x) \in F[x]$ is irreducible, then

$$f(x) = k(x-a) \quad \text{for some } a \in F \text{ and } k \in F^\times.$$

**Lemma 6.8.** Let $F$ be an algebraically closed field. Let $T \in \mathcal{M}_{n\times n}(F)$. Then, $T$ has an eigenvalue.

**Example 6.8.** The matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \quad \text{has no eigenvalue in } \mathbb{R}.$$

**Example 6.9.** Let $V \cong F[x]/(x-a)^n$ for some $a \in F$. Then, we consider the following $F$-basis of $V$ via the isomorphism:

$$1, x-\lambda, (x-\lambda)^2, \ldots, (x-\lambda)^{n-1}$$

Then, $x$ acts on the matrix

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & \lambda \end{bmatrix}$$

Let $T \in \mathcal{M}_{n\times n}(F)$ for some algebraically closed field $F$. We consider $V = F^n$ as an $F[x]$-module where $x$ acts on $T$. Then, we have

$$V \cong F[x]/((x-\lambda_1)^{a_1}) \oplus \ldots \oplus F[x]/((x-\lambda_r)^{a_r})$$

**Definition 6.5** (Jordan canonical form)**.** The Jordan canonical form (JCF) of a matrix is

$$\mathbf{J} = \begin{bmatrix} T_1 & & \\ & T_2 & \\ & & \ddots \end{bmatrix}$$

where each $T_i$ is of the form in the example with respect to the $F[x]$-submodule $F[x]/((-\lambda_i)^{a_i})$.

**Proposition 6.2.** Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{n\times n}(F)$ for an algebraically closed field $F$.

**(i)** The JCF of $\mathbf{A}$ is unique up to permutation

**(ii)** $\mathbf{A}$ is similar to its JCF

**(iii)** $\mathbf{A}$ is similar to $\mathbf{B}$ if and only if they have the same JCF up to permutation

**Example 6.10.** One can compute the JCF of the matrix

$$\mathcal{A} = \begin{bmatrix} 2 & -2 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{bmatrix} \quad \text{in } \mathcal{M}_{3\times 3}(\mathbb{C}).$$

The JCF is

$$\mathbf{J} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

Since each Jordan block is of size 1, $\mathbf{A}$ is said to be diagonalisable over $\mathbb{C}$.

**Example 6.11.** The JCF of

$$\mathbf{A} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathbf{M}_{2\times 2}(\mathbb{C}) \quad \text{is} \quad \mathbf{J} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

which is diagonalisable over $\mathbb{C}$ as each Jordan block is of size 1.

**Example 6.12.** The JCF of

$$\mathbf{A} = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix} \in \mathbf{M}_{2\times 2}(\mathbb{C}) \quad \text{is} \quad \mathbf{J} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

which contains one Jordan block of size 2. Hence, $\mathbf{A}$ is not diagonalisable over $\mathbb{C}$.

**Corollary 6.3.** Let $F$ be an algebraically closed field. Let $T \in \mathcal{M}_{n\times n}(F)$ with a Jordan canonical form $\mathbf{J}$.

**(i)** $T$ is diagonalisable over $F$ if and only if $\mathbf{J}$ is a diagonal matrix

**(ii)** $T$ is diagonalizable over $F$ if and only if its minimal polynomial does not have multiple roots

**Proposition 6.3.** Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{n\times n}(F)$. Let $V$ and $W$ be $F[x]$-modules, where $x$ acts on $\mathbf{A}$ and $\mathbf{B}$, respectively. Then, the following are equivalent:

**(i)** $\mathbf{A}$ and $\mathbf{B}$ are similar

**(ii)** $\mathbf{A}$ and $\mathbf{B}$ have the same RCF

**(iii)** $V \cong W$

**(iv)** $V$ and $W$ have the same invariant factors

**(v)** $V$ and $W$ have the same elementary factors

**(vi)** If $F$ is algebraically closed, then $\mathbf{A}$ and $\mathbf{B}$ have the same JCF

**Definition 6.6** (nilpotent matrix)**.** Let $F$ be a field. A matrix $\mathbf{A} \in \mathcal{M}_{n\times n}(F)$ is nilpotent if

$$\text{there exists } k \in \mathbb{N} \quad \text{such that} \quad \mathbf{A}^k = \mathbf{0}.$$

We wish to classify the *nilpotent orbits*, i.e. orbits consisting of nilpotent matrices.

**Lemma 6.9.** Let $\mathbf{A} \in \mathcal{M}_{n\times n}(F)$ be nilpotent. The minimal polynomial $m_{\mathbf{A}}(x) = x^k$ for some $k \in \mathbb{N}$ and the characteristic polynomial is $c_{\mathbf{A}}(x) = x^n$.

**Corollary 6.4.** The set of nilpotent orbits on $M_{n\times n}(F)$ is in bijection with the set of partitions of $n$.

We then consider the conjugacy classes in $\mathrm{GL}_2(F_2)$, where $F_2$ is the finite field with 2 elements. We wish to determine the number of conjugacy classes and find a representative of each class.

**Proposition 6.4.** There are 3 conjugacy classes in $\mathrm{GL}_2(F_2)$. Their elementary factors are

$$\left\{(x-1)^2\right\},\{x-1,x-1\},\left\{x^2+x+1\right\}.$$

We can find the representative using either the JCF or the RCF.

Next, we consider orbits of $\mathrm{GL}_3(\mathbb{Q})$ on the set

$$S=\left\{\mathbf{A}\in\mathrm{GL}_3(\mathbb{Q}):\mathbf{A}^6=\mathbf{I}\right\}.$$

The elements in this set are of order $2,3,6$. We consider the factorisation

$$\begin{aligned}x^6-1&=\left(x^3+1\right)\left(x^3-1\right)\\&=(x+1)\left(x^2-x+1\right)(x-1)\left(x^2+x+1\right)\\&=(x-1)(x+1)\left(x^2-x+1\right)\left(x^2+x+1\right)\end{aligned}$$

Let $\mathbf{A}\in S$. Then, the minimal polynomial $m_{\mathbf{A}}(x)$ of $\mathbf{A}$ must divide $x^6-1$. We also know that $\deg m_{\mathbf{A}}(x)\leq 3$. As such, we have the following possibilities (at first glance) for $m_{\mathbf{A}}(x)$:

**(1)** $x-1$
**(2)** $x+1$
**(3)** $x^2-x+1$
**(4)** $x^2+x+1$
**(5)** $(x-1)(x+1)$
**(6)** $(x-1)\left(x^2-x+1\right)$
**(7)** $(x-1)\left(x^2+x+1\right)$
**(8)** $(x+1)\left(X^2-x+1\right)$
**(9)** $(x+1)\left(x^2+x+1\right)$

By Proposition 6.4, we shall classify the $F[x]$-modules of $F$-dimension 3 with the largest invariant factors being $m_{\mathbf{A}}(x)$. They are classified by the invariant factors. Consequently, the invariant factors corresponding to each case are as follows:

**(1)** $x-1,x-1,x-1$
**(2)** $x+1,x+1,x+1$
**(3)** Impossible
**(4)** Impossible
**(5)** $x-1,(x-1)(x+1)$ or $x+1,(x-1)(x+1)$
**(6)** $(x-1)\left(x^2-x+1\right)$
**(7)** $(x-1)\left(x^2+x+1\right)$
**(8)** $(x+1)\left(x^2-x+1\right)$
**(9)** $(x+1)\left(x^2+x+1\right)$

We know that the orbits of $\mathbf{A}$ are uniquely determined by the invariant factors. So, there are 7 orbits.