Rings and Modules

Alexandre Daoud
Based on notes by Robert Evans

2015-2016

1 Basic concepts

Definition 1.1. A **ring** R is a set equipped with two binary operations $+$ and $\cdot$ satisfying the following conditions:

1. $(R, +)$ is an abelian group with identity denoted 0_R
2. $\cdot$ is associative
3. $\cdot$ distributes over $+$

If $\cdot$ is commutative then R is said to be a **commutative ring**. Furthermore, if there exists an identity element $1_R \in R$ for the operation $\cdot$ then R is said to be **unitary**.

Henceforth, all rings are assumed commutative and unitary. We shall also suppress the '$\cdot$' notation as is the standard for multiplication.

Example 1.2. $\mathbb{Z}, \mathbb{Q}$ with their standard addition and multiplication.

Example 1.3. Consider the abelian group $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. Then $\mathbb{Z}/n\mathbb{Z}$ is also a ring with multiplication modulo n.

Example 1.4. Let R be a ring. Then the ring of polynomials $R[X]$ in the indeterminate X is a ring with the usual polynomial operations.

Definition 1.5. Let R and S be rings. A mapping $\varphi : R \to S$ is called a **homomorphism** if, given $r, r' \in R$, we have

1. $\varphi(r + r') = \varphi(r) + \varphi(r')$
2. $\varphi(rr') = \varphi(r)\varphi(r')$
3. $\varphi(1_R) = 1_S$

If φ is bijective then we refer to it as an **isomorphism**. Furthermore, if φ is an isomorphism from R to itself then we call φ an **automorphism**.

Proposition 1.6. *Let $\varphi : R \to S$ be a ring homomorphism and let $s \in S$. Then there exists a unique ring homomorphism $\Phi : R[X] \to S$ such that*

- $\Phi(r) = \varphi(r)$ *for all* $r \in R$
- $\Phi(X) = s$

Proof. Let $\sum_{i=0}^{n} r_i X^i \in R[X]$. Then Φ is easily defined as follows:

$$\begin{aligned}\Phi : R[X] &\to S \\ \sum_{i=0}^{n} r_i X^i &\mapsto \sum_{i=0}^{n} \varphi(r_i) b^i\end{aligned}$$

□

Definition 1.7. Let R be a ring and $I \subseteq R$ a subset. We say that I is an **ideal** of R, denoted $I \triangleleft R$, if the following conditions are satisfied:

1. $(I, +)$ is a subgroup of $(R, +)$
2. For all $i \in I$ and $r \in R$ we have $ir \in I$

Example 1.8. *For all $n \in \mathbb{Z}$, the set $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.*

Example 1.9. *Let $R \subseteq \mathbb{C}^n$. Then*

$$\{ f \in \mathbb{C}[X_1, \ldots, X_n] \mid f(p) = 0 \; \forall \, p \in R \}$$

is an ideal of $\mathbb{C}[X_1, \ldots, X_n]$

Definition 1.10. Let R be a ring and $A \subseteq R$ a subset. We define the **ideal generated by A**, denoted (A), to be the set of all R-linear combinations of elements of A.

Definition 1.11. Let $\varphi : R \to S$ be a ring homomorphism. The **kernel** of φ is defined as

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

Proposition 1.12. *Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker \varphi$ is an ideal of R.*

Proof. This follows directly from the definitions of a ring homomorphism and an ideal. □

Definition 1.13. Let R be a ring and $I \triangleleft R$ an ideal. Suppose that $r, r' \in R$ and define the equivalence relationship $r \sim r' \iff r - r' \in I$. In this case, we say that r and r' are **congruent modulo I**. We define the **quotient ring** of R with respect to the ideal I, denoted R/I, as the set of all equivalence classes of $\sim$. The equivalence class $[r]$ is denoted $r + I$ and is the following set:

$$r + I := [r] = \{ r + i \mid i \in I \}$$

Addition is defined by

$$(r + I) + (r' + I) = (r + r') + I$$

and multiplication by

$$(r + I)(r' + I) = rr' + I$$

Proposition 1.14. *The addition and multiplication operations given in Proposition 1.13 are well-defined.*

Proof. Fix elements r, r' and s, s' in R. We shall first deal with addition. We need to show that

$$r + I = r' + I, s + I = s' + I \implies (r + s) + I = (r' + s') + I$$

Since $r + I = r' + I$, we have that $r - r' \in I$. Say $r - r' = i_1$ for $i_1 \in I$. Similarly, $s - s' = i_2$ for $i_2 \in I$. Then

$$(r + s) + I = (r' + i_1 + s' + i_2) + I = (r' + s') + i_1 + i_2 + I = (r' + s') + I$$

For multiplication, we have

$$rs + I = (r' + i_1)(s' + i_2) + I = r's' + i_1 s' + r' i_2 + i_1 i_2 + I$$

Now since I is an ideal, we must have that $i_1 s', r' i_2$ and $i_1 i_2$ are in I. The result then follows easily. $\square$

Definition 1.15. Let R be a ring and $I \triangleleft R$ an ideal. We define the **quotient map** to be the surjective ring homomorphism

$$\begin{aligned} q : R &\to R/I \\ r &\mapsto r + I \end{aligned}$$

Example 1.16. Consider the ring $\mathbb{Z}[X]$ and the ideal $(X^2 + 5) \triangleleft \mathbb{Z}[X]$ (the ideal generated by the polynomial $X^2 + 5$). We may form the quotient ring $\mathbb{Z}[X]/(X^2 + 5)$ whose elements are of the form

$$a + bX + (X^2 + 5)$$

for some $a, b \in \mathbb{Z}$. The ring $\mathbb{Z}[X]/(X^2 + 5)$ can be viewed as enforcing the constraint $X^2 - 5 = 0$ upon $\mathbb{Z}[X]$. Hence we may consider an element of $\mathbb{Z}[X]/(X^2 + 5)$ to be a polynomial $a + bX$ with the usual addition and multiplication except that $X^2 + 5 = 0$. Since $X^2 - 5 - 0$ implies that X is $\pm\sqrt{-5}$, it can be shown that $\mathbb{Z}[X]/(X^2 + 5) \cong \mathbb{Z}[\sqrt{-5}]$.

Theorem 1.17 (First Isomorphism Theorem). *Let $\varphi : R \to S$ be a ring homomorphism. Then*

$$R/\ker\varphi \cong \operatorname{im}\varphi$$

Proof. Define a map

$$\begin{aligned} \psi : R/\ker\varphi &\to \operatorname{im}\varphi \\ r + \ker\varphi &\mapsto \varphi(r) \end{aligned}$$

Then ψ is well-defined. Indeed, if $r + \ker\varphi = r' + \ker\varphi$ then $r' - r \in \ker\varphi$ and

$$\psi(r + \ker\varphi) = \varphi(r) = \varphi(r) + \varphi(r' - r) = \varphi(r') = \psi(r' + \ker\varphi)$$

ψ is clearly surjective by construction so it remains to show that ψ is injective. Suppose that $\psi(r + \ker\varphi) = \psi(r' + \ker\varphi)$. Then $\varphi(r) = \varphi(r')$. It follows that $\varphi(r - r') = 0$ whence $r - r' \in \ker\varphi$. Therefore, $r + \ker\varphi = r' + \ker\varphi$.

Finally, ψ is a ring homomorphism. Indeed, each property follows from the corresponding property of φ. $\square$

Example 1.18. Returning to Example 1.16 we have a ring homomorphism

$$\begin{aligned}\varphi : \mathbb{Z}[X] &\to \mathbb{C}\\ X &\mapsto \sqrt{-5}\end{aligned}$$

which fixes $\mathbb{Z}$. The kernel of this mapping is clearly (X^2+5) so by the previous theorem, we have that $\mathbb{Z}[X]/(X^2+5) \cong \mathbb{Z}[\sqrt{-5}]$.

Definition 1.19. Let R be a ring. We say that R is an **integral domain** if $1_R \neq 0_R$ and, given $r, r' \in R$, $rr' = 0$ implies that $r = 0$ or $r' = 0$

Definition 1.20. Let R be a ring. We say that R is a **field** if $1 \neq 0$ and every non-zero element r has a multiplicative inverse. In this case, r is called a **unit** and we denote by $R^\times$ the set of all units.

Example 1.21. $\mathbb{Z}$ is an integral domain.

Example 1.22. If R is an integral domain then so is $R[X_1, \ldots, X_n]$.

Example 1.23. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field as are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Definition 1.24. Let R be a ring and $I \triangleleft R$ a proper ideal. We say that I is **prime** if, given $r, r' \in R$, $rr' \in I$ implies $r \in I$ or $r' \in I$.

Definition 1.25. Let R be a ring and $I \triangleleft R$ a proper ideal. We say that I is **maximal** if there does not exist an ideal J such that $I \subsetneq J \subsetneq R$.

Example 1.26. Let $n \in \mathbb{Z}$. Then $n\mathbb{Z}$ is a prime ideal if and only if n is prime.

Remark. R is an integral domain if and only if $\{0\}$ is prime in R.

Theorem 1.27. *Let R be a ring and $I \triangleleft R$ an ideal. Then there is a one-to-one correspondence between the ideals J of A that contain I and the ideals of A/I.*

Proof. Fix an ideal $J \triangleleft R$ such that $I \subseteq J$. We define a map sending J to an ideal of R/I by

$$\varphi(J) = J/I = \{\, j + I \mid j \in J \,\}$$

It follows directly from the definition of J that J/I is an ideal in R/I. To show that this is a bijection. We shall construct its inverse. Let $\mathfrak{a}$ be an ideal of R/I. Define a map sending $\mathfrak{a}$ to an ideal of R by

$$\psi(\mathfrak{a}) = \{\, r \in R \mid r + I \in \mathfrak{a} \,\}$$

The fact that the right hand side of the above is an ideal follows directly from the properties of $\mathfrak{a}$. Now consider

$$\begin{aligned}\varphi(\psi(\mathfrak{a})) = \{\, j + I \mid j \in \psi(\mathfrak{a}) \,\} &= \{\, j + I \mid j \in \{\, r \in R \mid r + I \in \mathfrak{a} \,\}\,\}\\ &= \{\, r + I \mid r + I \in \mathfrak{a} \,\} = \mathfrak{a}\end{aligned}$$

The second composition $\psi \circ \varphi$ follows in a similar way. □

Proposition 1.28. *Let R be a ring and $I \triangleleft R$ an ideal. Then I is prime if and only if R/I is an integral domain.*

Proof. Suppose first that I is prime. Fix $r+I, r'+I \in R/I$ such that $(r+I)(r'+I) = 0+I$. Then $rr' + I = 0 + I$ which implies that $rr' \in I$. Now, I is prime which implies that either $r = 0$ or $r' = 0$. This then implies that either $r + I$ or $r' + I$ equals $0 + I$.

Conversely, assume that R/I is an integral domain. Fix $rr' \in I$. We need to show that either $r \in I$ or $r' \in I$. Since R/I is an integral domain, we know that $(r + I)(r' + I) = rr' + I = 0 + I$ implies that either $r + I$ or $r' + I$ equal $0 + I$. But then, either r or r' are in I. $\square$

Lemma 1.29. *Let K be a ring. Then K is a field if and only if every ideal is either zero or K.*

Proof. First suppose that K is a field and let $I \triangleleft K$ be a non-zero ideal. Fix some non-zero $x \in I$. Since I is an ideal, we must have that $xx^{-1} \in I$. But then $1 \in I$ which means I is equal to K.

Now suppose that every ideal of K is either zero or K. Fix some non-zero $x \in K$. We need to exhibit an inverse for x. Consider the ideal $(x) \triangleleft K$. By hypothesis, (x) is either the zero ideal or the whole ring K. Clearly, it cannot be the zero ideal hence $(x) = K$. It follows that there must exist some $x^{-1} \in K$ such that $xx^{-1} = 1$. $\square$

Proposition 1.30. *Let R be a ring and $I \triangleleft R$ an ideal. Then I is maximal if and only if R/I is a field.*

Proof. Suppose that R/I is a field. Then by Lemma 1.29 there cannot exist a non-trivial ideal $\mathfrak{a} \triangleleft R/I$. Since all ideals of R/I are of them form J/I for some ideal J of R containing I, we see that there cannot exist an ideal J such that $I \subsetneq J \subsetneq R$ meaning that I is maximal. Note that these conditions are all necessary and sufficient as required. $\square$

Lemma 1.31. *Any field is necessarily an integral domain.*

Proof. Let F be a field and suppose that $x, y \in F$ are such that $xy = 0$. Without loss of generality, assume that $x \neq 0$. Then $y = y(xx^{-1}) = (yx)x^{-1} = 0$ and F is an integral domain. $\square$

Proposition 1.32. *Let R be a ring and $\mathfrak{m} \triangleleft R$ a maximal ideal. Then $\mathfrak{m}$ is a prime ideal.*

Proof. By Proposition 1.30, we know that $R/\mathfrak{m}$ is a field. By Lemma 1.31 we have that $R/\mathfrak{m}$ is an integral domain. Then Proposition 1.28 implies that $\mathfrak{m}$ is prime. $\square$

2 Euclidean Domains and Principal Ideal Domains

Definition 2.1. A **Euclidean domain** is a pair (R, φ) where R is an integral domain and $\varphi : R\backslash\{0\} \to \mathbb{N}$ is a **size** function such that

1. For all $a \in R$ and $b \in A\backslash\{0\}$ there exists $q, r \in R$ such that

$$a = bq + r$$

   and either $r = 0$ or $\varphi(r) < \varphi(b)$

2. For all $a, b \in R\backslash\{0\}$ we have $\varphi(a) \leq \varphi(ab)$

Example 2.2. $\mathbb{Z}$ is a Euclidean domain with $\varphi(n) = |n|$.

Example 2.3. Let K be a field. Then $K[X]$ is a Euclidean domain with $\varphi(f) = \deg f$

Definition 2.4. Let R be a ring and $I \lhd R$ an ideal. We say that I is **principal** if there exists an $x \in R$ such that $I = (x)$. In this situation, we call x a **generator** for I.

Definition 2.5. Let R be an integral domain. We say that R is a **principal ideal domain** (PID) if every ideal is principal.

Proposition 2.6. *Let R be a Euclidean domain. Then R is a principal ideal domain.*

Proof. Let φ be the size function of R. Since the zero ideal is principle in R, we only need to consider non-zero ideals. Let $I \lhd R$ be a non-zero ideal. Choose a $b \in I \backslash \{ 0 \}$ such that $\varphi(b)$ is minimal. We claim that $I = (b)$.

It is obvious that $(b) \subseteq I$ so we just need to show that $I \subseteq (b)$. Fix some $a \in I$. Then we may write

$$a = qb + r$$

for some $q, r \in R$ such that either $r = 0$ or $\varphi(r) < \varphi(b)$. We must have $r = 0$ because if not then $r = a - qb \in I$ with $\varphi(r) < \varphi(b)$ which contradicts the minimality of $\varphi(b)$. hence $a = qb$ for some $q \in R$ whence $a \in (b)$. $\square$

Proposition 2.7. *Let R be a principal ideal domain and $I \lhd R$ a non-zero ideal. If I is prime then it is maximal.*

Proof. Let J be an ideal of R containing I. Then $I = (x)$ and $J = (y)$ for some $x, y \in R$. Now $I \subseteq J$ implies that $x \in J$ and so $x = yz$ for some $z \in R$. Hence $yz \in I$. Now I is prime meaning either $y \in I$ or $z \in I$. If $y \in I$ then $J = (y) \subseteq I$ whence $I = J$. If $z \in I$ then $z = wx$ for some $w \in R$ and thus $x = ywx$. This implies that $yw = 1$ whence y is a unit. Hence $J = (y) = R$ and I is maximal. $\square$

3 Modules: Basic Notions

Definition 3.1. Let R be a ring. An **R-module** is a set M with an addition operation $+ : M \times M \to M$ and a scalar multiplication operation $\cdot : A \times M \to M$ such that

1. $(R, +)$ is an abelian group
2. $1_R \cdot m = m$ for all $m \in M$
3. $(ab) \cdot m = a \cdot (b \cdot m)$ for all $m \in M, a, b \in R$
4. $a \cdot (m + n) = a \cdot m + a \cdot n$ for all $m, n \in M, a \in R$
5. $(a + b) \cdot m = a \cdot m + b \cdot m$ for all $m \in M, a, b \in R$

Remark. Fix $r \in R$ and define a mapping

$$\begin{aligned} \varphi_r : M &\to M \\ m &\mapsto r \cdot m \end{aligned}$$

By the 4^{th} property of a module, φ_r is an endomorphism of $(M, +)$. We denote the set of all endomorphisms of M by $\mathrm{End}(M)$. We hence have a map

$$\varphi : R \to \mathrm{End}(M)$$

which is a ring homomorphism by Properties 2, 3 and 5.

Conversely, given an abelian group $(M, +)$ and a ring homomorphism $\varphi : R \to \mathrm{End}(M)$, we can make M into an R-module by defining $\cdot : R \times M \to M$ with

$$r \cdot m = \varphi(r)m$$

Example 3.2. Let K be a field. Then a vector space over K is a K-module.

Example 3.3. Let R be a ring and $n \in \mathbb{N}$. Then the set R^n of column n-vectors with entries in R is an R-module under component wise operations.

Example 3.4. Let $(G, +)$ be an abelian group. Then $(G, +)$ can be viewed as a $\mathbb{Z}$-module where

$$n \cdot g = \begin{cases} g + \cdots + g & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -(g + \cdots + g) & \text{if } n < 0 \end{cases}$$

Clearly this is the only way to make $(G, +)$ into a $\mathbb{Z}$-module since $n \cdot g = (1 + \cdots + 1)g = g + \cdots + g$.

Example 3.5. Let R be a ring. Then we can consider R as a module over itself where scalar multiplication is just ring multiplication.

Example 3.6. Let R be a ring. Then $R[X_1, \ldots, X_n]$ is an R-module.

Definition 3.7. Let R be a ring and M an R-module. A **submodule** of M is a subset $N \subseteq M$ which is an R-module under the induced operations.

Example 3.8. Let M be an abelain group considered as a $\mathbb{Z}$-module. Then its submodules are the subgroups of $(M, +)$.

Example 3.9. Let K be a field and V a vector space over K. Then its K-submodules are the subspaces of V.

Example 3.10. Let R be a ring considered as a module over itself. Then the R-submodules are just the ideals of R.

Definition 3.11. Let R be a ring and M a module over R. Given a subset $X \subseteq M$ we may define the **submodule of M generated by X**

$$\langle X \rangle = \{ \text{finite } R\text{-linear combinations of } X \}$$

Definition 3.12. Let R be a ring and M an R-module. We say that M is **finitely generated** if there exists $m_1, \ldots, m_r \in M$ such that $M = \langle m_1, \ldots, m_r \rangle$. If M is generated by a single element, we say that M is **cyclic**.

Example 3.13. Let R be a ring and consider the set of all column n-vectors R^n. The elements

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T$$

for all $i = 1, \ldots n$ generate A^n as an A-module.

Example 3.14. Let K be a field and V a K-vector space. Then V is finitely generated as a K-module if and only if V is finite dimensional over K.

Example 3.15. Let G be an abelian group. Then G is cyclic as a $\mathbb{Z}$-module if and only if G is cyclic.

Example 3.16. Let R be a ring and consider it as a module over itself. Then a submodule I of R is cyclic if and only if I is principal as an ideal of R.

Remark. A submodule of a finitely generated module is not necessarily finitely generated. Indeed, consider the ring $2^{\mathbb{N}}$ with operations $X + Y = X \triangle Y = (X \backslash Y) \cup (Y \backslash X)$ and $XY = X \cap Y$ with $0 = \varnothing$ and $1 = \mathbb{N}$ as a module over itself. Then $2^{\mathbb{N}}$ is finitely generated, in particular by 1 but the submodule

$$I = \{ A \subseteq \mathbb{N} \mid A \text{ is finite} \}$$

is not.

Definition 3.17. Let R be a ring and suppose that M and N are R-modules. A **homomorphism** from M to N is a mapping $\varphi : M \to N$ that preserves R-linear combinations. In other words

1. $\varphi(m + m') = \varphi(m) + \varphi(m')$ for all $m, m' \in M$
2. $\varphi(am) = a\varphi(m)$ for all $m \in M, a \in A$

Example 3.18. Let G and H be abelian groups viewed as $\mathbb{Z}$-modules then a $\mathbb{Z}$-homomorphism is exactly a group homomorphism.

Example 3.19. Let K be a field and suppose that U and V are K-vector spaces seen as K-modules. Then a K-homomorphism $U \to V$ is a K-linear map.

Remark. Let R be a ring considered as a module over itself. Then the R-endomorphisms are not the same as the ring endomorphisms of R.

Definition 3.20. Let R be a ring and M a module over R. Suppose that N is a R-submodule of M. We define the **quotient module**, denoted M/N, to be the set of cosets of N in M:

$$M/N = \{ m + N : m \in M \}$$

with addition defined by

$$(m + N) + (m' + N) = (m + m') + N$$

and scalar multiplication by

$$a \cdot (m + N) = am + N$$

Theorem 3.21. *Let R be a ring and M, N modules over R. If $\varphi : M \to N$ is a module homomorphism then*

1. $\ker \varphi$ *is a submodule of* M
2. $\operatorname{im} \varphi$ *is a submodule of* N
3. $M/\ker \varphi \cong \operatorname{im} \varphi$

Proof. This are proved in exactly the same way as for the ideal and ring cases. □

Definition 3.22. Let R be a ring and $M_1, \dots M_k$ a collection of R-modules. We define their **direct sum** as

$$A_1 \oplus + \cdots + \oplus A_k$$

to be the R-module $A_1 \times \cdots \times A_k$ with component-wise operations. Furthermore, if $\{ M_k \}$ is a countable family of R-modules, we may define their infinite direct sum in a similar way except we require that all sequences are eventually zero:

$$\bigoplus_{i=1}^{\infty} M_i = \{ (m_1, m_2, \dots) \mid m_i \in M_i \text{ and } \exists n \in \mathbb{N}, m_j = 0 \ \forall j \geq n \}$$

Example 3.23. Let R be a ring. Then $R^n = R \oplus \cdots \oplus R$ (n times)

Definition 3.24. Let R be a ring and M a module over R. Suppose that $m_1, \dots, m_n \in M$.

1. We say that $m_1, \dots, m_r$ are **linearly independent** if

   $$r_1 m_1 + \cdots + r_n m_n = 0$$

   implies that all $r_1, \dots, r_n$ are zero
2. We say that $m_1, \dots, m_n$ **span** M if $M = \langle m_1, \dots, m_n \rangle$
3. We say that $m_1, \dots, m_n$ are a **basis** for M if they are linearly independent and span M

Remark. $\varnothing$ is a basis for 0.

Proposition 3.25. *Let R be a ring and M a module over R. Suppose that $m_1, \dots, m_n \in M$. Then the following are equivalent*

1. $m_1, \dots, m_r$ *form a basis for* M *over* R
2. *Every* $m \in M$ *can be written as a unique linear combination of the* m_i
3. $m_1, \dots, m_r$ *span* M *and given any* R*-module* N *and a mapping*

   $$f : \{ m_1, \dots, m_n \} \to N$$

   Then there exists a unique extension of f *to a homomorphism of modules*

   $$\overline{f} : M \to N$$

Proof. We first show that (1) $\implies$ (2). Suppose that $m_1, \dots, m_r$ form a basis for M over R. Then $m_1, \dots, m_r$ are linearly independent and span R. Fix some $m \in M$. Since $m_1, \dots, m_r$ span M we may write $m = a_1 m_1 + \cdots + a_n m_n$. Similarly, let $m = b_1 m_1 + \cdots + b_n m_n$ be another linear combination. Then we have

$$0 = (a_1 - b_1)m_1 + \cdots + (a_n - b_n)m_n$$

But the m_i are linearly independent so we must have that $a_i - b_i = 0$ for all i. Hence $a_i = b_i$ and such linear combinations are unique.

We now show that (2) $\implies$ (3). Consider the mapping $\overline{f} : M \to N$ which sends $a_1 m_1 + \cdots + a_n m_n \in M$ to $a_1 f(m_1) + \cdots + a_n f(m_n)$. This is indeed a unique well-defined mapping since m can be represented by a unique linear combination of the m_i. Furthermore, $\overline{f}$ satisfies the axioms of a module homomorphism by construction.

Finally, we show that (3) $\implies$ (1). Let N be an R-module and $f : \{ m_1, \dots, m_n \} \to N$ be a mapping which extends uniquely to a module homomorphism $\overline{f} : M \to N$. It suffices to show that m_i are linearly independent. Suppose that

$$r_1 m_1 + \cdots + r_n m_n = 0$$

for some $r_i \in R$. Let $f_1 : \{ m_1, \dots, m_n \} \to N$ be the function sending m_1 to 1 and the rest of the m_i to 0. Then f_1 extends to a unique function $\overline{f_1} : M \to N$. We then have

$$\begin{aligned} \overline{f_1}(r_1 m_1 + \cdots + r_n m_n) &= \overline{f_1}(0) \\ r_1 f_1(m_1) + \cdots + r_n f_1(m_n) &= 0 \\ r_1 &= 0 \end{aligned}$$

A similar argument shows that the rest of the r_i are zero. Hence the m_i are linearly independent. □

Definition 3.26. Let R be a ring and M a module over R. If there exists a basis for M over R then we say that R is **free**.

Proposition 3.27. *Let R be a ring and M a module over R. Then M is finitely generated if and only if there exists some $n \in \mathbb{N}$ and a surjective homomorphism $\varphi : R^n \to M$.*

Proof. First suppose that M is finitely generated over R. Fix some generating set $m_1, \dots m_n \in M$. Let $\varphi : R^n \to M$ be the unique homomorphism that sends e_i to m_i. Then clearly, $\operatorname{im} \varphi = M$.

Conversely, given a homomorphism $\varphi : R^n \to M$ such that $\operatorname{im} \varphi = M$ then $\varphi(e_1), \dots, \varphi(e_n)$ is a generating set for M. □

Corollary 3.28. *Let R be a ring and M a module over R. Then M is cyclic if and only if $M = R/I$ for some ideal $I \lhd R$.*

Proof. By Proposition 3.27 we know that M is a generated by one element (cyclic) if and only if there exists some surjective homomorphism $\varphi : A \to M$. By the first isomorphism theorem for rings, this is true if and only if there exists an ideal $I = \ker \varphi$. In other words, $M \cong R/I$. □

4 Modules over a Euclidean Domain

Definition 4.1. Let R be a ring and M a module over R. We say that M is **finitely presented** if there exists $n \in \mathbb{N}$ and a finitely generated R-submodule of R^n N such that

$$M \cong R^n/N$$

In other words, M is finitely presented if the kernel of the mapping $\varphi : R^n \to M$ is finitely generated.

Remark. Let R be a ring and let $m_1, \ldots, m_r \in R^n$. Denote $N = \langle m_1, \ldots, m_n \rangle$. We may write $m_j = \sum_{i=1}^n a_{ij} e_i$ for some $a_{ij} \in R$ and for all $j = 1, \ldots, r$. Now let $f_i = e_i + N$. Then R^n/N can be viewed as the R-module generated by the f_i subject to the r relations

$$\sum_{i=1}^n a_{ij} f_i = 0$$

Conversely, suppose that M is an R-module generated by some $f_1, \ldots, f_n$ subject to the r relations

$$\sum_{i=1}^n a_{ij} f_i = 0$$

where $j = 1, \ldots, r$ and $a_{ij} \in R$. Then the homomorphism $\varphi : R^n \to M$ which maps e_i to f_i has kernel $\ker\varphi = \langle \sum a_{i1} f_i, \ldots, \sum a_{ir} f_i \rangle$. Then M is clearly finitely presented since $M \cong R^n/\ker\varphi$.

We see that finitely presented modules are exactly those modules that can be described in terms of finitely many generators subject to finitely many relations.

Definition 4.2. Let R be a ring and $\varphi : R^n \to R^m$ an R-homomorphism. Let $e_1, \ldots, e_n$ be the standard basis for R^n and $f_1, \ldots, f_m$ that of R^m. We may write $\varphi(e_j) = \sum_{i=1}^m a_{ij} g_i$. Then we define the **matrix** of φ as

$$[\![\varphi]\!] = (a_{ij})_{ij} \in \mathrm{Mat}_{m \times n}(A)$$

Remark. We can use matrices to describe the finitely presented matrix R^n/N where $N = \langle m_1, \ldots, m_r \rangle$ and $m_j = \sum_{i=1}^n a_{ij} e_i \in R^n$.

Let $h_1, \ldots, h_n$ be the standard basis for R^r. Let $\psi : R^r \to R^n$ be the R-homomorphism such that $\psi(h_j) = m_j$ for each j. Then $\mathrm{im}\,\psi = N$ and the $n \times r$ matrix $[\![\psi]\!]$ encodes each relation as a column. Hence a finitely presented module can be completey described by its **presentation matrix** $[\![\psi]\!]$

Example 4.3. Let M be the $\mathbb{Z}$-module generated by $e_1, \ldots, e_4$ subject to the the relations

$$e_1 + 2_2 + 3e_3 + 4e4 = 0$$
$$5e_1 + 6e_2 + 7e_3 + 8e_4 = 0$$

then its presentation matrix is

$$\begin{pmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 7 \\ 4 & 8 \end{pmatrix}$$

Definition 4.4. Let R be a ring and $\Phi \in \mathrm{Mat}_{n\times r}(R)$. Then the **elementary row (column) operations** on Ψ are the following:

1. swap two rows (columns)
2. multiply a row (column) by a unit in R
3. add a scalar multiple of one row (column) to another row (column)

Remark. Let R be a ring and Φ the presentation matrix of a finitely presented R-module. Then a sequence of elementary row operations results in a new set of generators and corresponding relations. A sequence of elementary column operations leaves the generators untouched and results in a new, yet equivalent, set of relations.

Definition 4.5. Let R be a ring and $\Phi, \Psi \in \mathrm{Mat}_{n\times r}(R)$ be two matrices. We say that Φ and Ψ are **equivalent** if one can be obtained from the other by a sequence of elementary row or column operations.

Remark. It follows from the above definition that if two finitely presented R-modules have equivalent presentation matrices then they are isomorphic.

Lemma 4.6. *Let R be a Euclidean domain and $\Phi \in \mathrm{Mat}_{n\times r}(R)$ a matrix. Let $d(\Phi)$ be the greatest common divisor of all the elements of Φ. If Φ' is the result of applying an elementary operation to Φ then $d(\Phi) = d(\Phi')$.*

Proof. The lemma is trivial for all elementary operations except addition of scalar multiples of rows (columns). Now let $\vec{r} = (r_1, \ldots, r_n), \vec{s} = (s_1, \ldots, s_n)$ be rows of Φ and suppose that Φ' is the result of adding $a \in R$ times $\vec{s}$ to $\vec{r}$. In other words, Φ' is the same matrix as Φ with $\vec{r}$ replaced by $(r_1 + as_1, \ldots, r_n + as_n)$. Then $\gcd(r_i + as_i, s_i) = \gcd(r_i, s_i)$ for all i whence $d(\Phi) = d(\Phi')$. The argumentation for columns follows in exactly the same way. □

Proposition 4.7. *Let (R, φ) be a Euclidean domain and $\Phi \in \mathrm{Mat}_{n\times r}(R)$ a matrix. Let d be the greatest common divisor of all the elements of Φ. Let $\varphi(\Phi)$ denote*

$$\varphi(\Phi) = \min_{i,j} \varphi(a_{ij})$$

where the $a_{ij} \in R$ are the elements of Φ. Then there exists a sequence of elementary operations that change Φ into a matrix Φ' such that the smallest element of Φ' (with respect to φ) is d.

Proof. We shall prove the proposition by induction on $\varphi(\Phi)$. It is clear that $\varphi(\Phi) \geq \varphi(d)$. If $\varphi(\Phi) = \varphi(d)$ then we are done. If not then assume, for the induction hypothesis, that the proposition is true for all matrices Φ' with elements in R such that $d(\Phi') = d$ and $\varphi(\Phi') < \varphi(\Phi)$.

Let $a_{uv} \in R$ be such that $\varphi(a_{uv}) = \varphi(\Phi)$. Now since $\varphi(a_{uv}) > \varphi(d)$, there exists an element of Φ, say $a_{lm} \in R$, such that a_{uv} does not divide a_{lm}. Indeed, if this were not the case, then a_{uv} would divide d.

First suppose that a_{lm} is in the same column or row as a_{uv}. In other words, either $u = l$ or $v = m$. By the definition of a Euclidean domain, we may write $a_{lm} = qa_{uv} + r$ for some $q, r \in R$ such that either $r = 0$ or $\varphi(r) < \varphi(a_{uv})$. Since a_{uv} does not divide a_{lm} we must have that r is non-zero. If $v = m$ so that a_{uv} and a_{lv} are in the same column, we may replace the l^{th} row of Φ by the l^{th} row minus q times the u^{th} row. This gives us a matrix Φ' whose lm^{th} element is r. Now since $\varphi(r) < \varphi(a_{uv})$, we have that $\varphi(\Phi') < \varphi(\Phi)$. By Lemma 4.6 we see that $d(\Phi') = d(\Phi) = d$. Hence by the induction hypothesis, we may transform Φ' into a matrix Ψ such that $d(\Psi) = d$ and we are done. A similar argumentation can be applied for the case where $l = u$ and a_{uv} and a_{lm} are in the same row.

Now suppose that a_{lm} is not in the same row or column as a_{uv}. Then a_{uv} divides every element a_{uj} in the same row and every element a_{iv} in the same column. We observe that we may transform Φ to a matrix Φ' where a_{uv} is fixed but all elements in the same row and column as a_{uv} become zero. Indeed, starting with the v^{th} column, we see that there exists a $z_i \in R$ such that $a_{iv} = z_i a_{uv}$. The row operation replacing the i^{th} row with the i^{th} row minus z_i times the u^{th} row makes a_{iv} equal to 0. We repeat this process for all i not equal to u. Similarly, we can perform column operations to transform all elements in the u^{th} row except a_{uv} to 0. Call this new matrix Φ'. By Lemma 4.6, we see that $d(\Phi') = d(\Phi) = d$. Furthermore, $\varphi(\Phi') \leq \varphi(\Phi)$. If $\varphi(\Phi') = d$ then we are done. If not then consider the element a_{lm} that is not divisible by a_{uv}. By assumption, $l \neq u$ and $m \neq v$ so we may replace the u^{th} row of Φ' by the u^{th} row plus the l^{th} row. By construction, $a_{lv} = 0$ so this operation does not change a_{uv}. Call this new matrix Ψ. Then $\varphi(\Psi) \leq \varphi(\Phi)$. However the u^{th} row now contains both a_{lm} and a_{uv} and we may now refer back to the previous case. ☐

Theorem 4.8. *Let R be a Euclidean domain and $\Phi \in \mathrm{Mat}_{n\times r}(R)$ a matrix. Then there exists a sequence of elementary operations that put Φ in the form*

$$\left(\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & 0 \\ & & a_k & \\ \hline & 0 & & 0 \end{array}\right)$$

where $a_1, \ldots, a_k \in R\backslash\{0\}$ and $a_1|a_2|\ldots|a_k$. This is referred to as ***Smith normal form****.*

Proof. If Φ is the zero matrix then we are done so assume that $\Phi \neq 0$. By Proposition 4.7, we can transform Φ' into a matrix with entry $a_{uv} = d = d(\Phi)$. Clearly a_{uv} divides all the elements of Φ. We may then transform this matrix into one such that $a_{11} = d$. Again by row operations, we may transform the 1^{st} row and column such that a_{11} is unaffected and all other elements in the 1^{st} row and column are zero. We thus have a matrix of the form

$$\begin{pmatrix} d & 0 \\ 0 & \Phi' \end{pmatrix}$$

where Φ' is a $n-1$ by $r-1$ matrix with elements in R, all divisible by d. We may repeat this process on Φ' and, by induction, the theorem follows. ☐

Theorem 4.9 (Structure Theorem for Finitely Presented Modules over an E.D)**.** *Let R be a Euclidean domain. Let M be a finitely presented R-module. Then*

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_k) \oplus R^m$$

for some $m \in \mathbb{N}$ and $a_1, \ldots, a_k \in R\backslash\{0\}$ such that $a_1|a_2|\ldots|a_k$.

Proof. By the definition of a finitely presented module, we have that $M \cong R^n/N$ for some $n \in \mathbb{N}$ and a finitely generated R-submodule of R^n. Consider the presentation matrix of M, say Φ. We may transform Φ into a matrix Ψ which is in Smith normal form. Then the finitely presented module corresponding to Ψ is isomorphic to M.

Now, R^n is generated by $e_1, \ldots, e_n$ and the matrix Ψ implies that N satisfies

$$N = \langle a_1 e_1, \ldots, a_k e_k \rangle$$

for some $a_1, \ldots, a_k \in R \backslash \{ 0 \}$ such that $a_1 | \ldots | a_k$. We thus have that

$$\begin{aligned} M &\cong R^n/N \\ &\cong \langle e_1, \ldots, e_n \rangle \,/\, \langle a_1 e_1, \ldots, a_k e_k \rangle \\ &\cong R/(a_1) \oplus \cdots \oplus R/(a_k) \oplus R^{n-k} \end{aligned}$$

□

Proposition 4.10. *Let R be a PID and N an R-submodule of R^n. Then N is finitely generated.*

Proof. We prove the proposition by induction on n. If $n = 1$ then the proposition is trivial since N is necessarily a principle ideal.

Now suppose that $n > 1$. Let N be an R-submodule of R^n. Let π_i denote the projection mapping of N onto its i^{th} coordinate. For example,

$$\begin{aligned} \pi_1 : N &\to R \\ (x_1, \ldots, x_n) &\mapsto x_1 \end{aligned}$$

Then $\pi_1(N)$ is clearly an ideal. Since R is a PID, we must have that $\pi_1(N) = (x)$ for some $x \in R$. Now consider

$$M = \{ (x_2, \ldots, x_n) \in R^{n-1} \mid (0, x_2, \ldots, x_n) \in N \}$$

Clearly, M is an R-submodule of R^{n-1} and, appealing to the induction hypothesis, we may choose a set of generators for M, say $y_1, \ldots, y_k$. Let $w \in N$ be such that $\pi_1(w) = x$. Then $\{ w, (0, y_1), \ldots, (0, y_k) \}$ generate N. □

Corollary 4.11. *Let R be a PID. Then any finitely generated R-module is finitely presented.*

Proof. Let M be a finitely generated R module. By definition, we have $M \cong R^n/N$ for some $n \in \mathbb{N}$ and an R-submodule of R^n, N. By Proposition 4.10, we have that N is finitely generated. By definition, this means that M is finitely presented. □

Remark. Since every ED is a PID, the structure theorem holds for finitely generated modules over a Euclidean domain.

5 Noetherian Rings/Modules

Definition 5.1. Let R be a ring. Then R is **Noetherian** if every ideal of R is finitely generated.

Lemma 5.2. *Let R be a ring. Then the following conditions are equivalent:*

1. *R is Noetherian*
2. *Every ascending chain of ideals of R is stationary*
3. *Every non-empty set of ideals of R has a maximal element.*

Proof. We first show that (1) $\implies$ (2). Suppose that R is Noetherian and let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

be an ascending chain of ideals in R. Let I be the union of the I_j for all $j \geq 1$. Then I is an ideal and, since R is Noetherian, it is finitely generated say by $a_1, \dots, a_n \in R$. Now, for all $1 \leq i \leq n$ there exists a $j \geq 1$ such that $a_i \in I_j$. Let I_k be the largest such ideal. Then I_k contains all $a_1, \dots, a_n$ whence $I \subseteq I_k$. We also have the trivial inclusion $I_k \subseteq I$ and we see that the chain is stationary.

We now show that (2) $\implies$ (3). Let $\mathcal{I}$ be a non-empty set of ideals of R. Choose an ideal $I_1 \in \mathcal{I}$. If I_1 is maximal then we are done. If not then $\mathcal{I} \backslash I_1$ is non-empty and we may choose I_2 such that $I_1 \subseteq I_2$. We may continue in this fashion, forming an ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \dots$. By assumption, this chain is stationary at some I_k. Then this I_k is the desired maximal element of $\mathcal{I}$.

Finally, we show that (3) $\implies$ (1). Suppose that every non-empty set of ideals of R has a maximal element. Let $I \lhd R$ be an ideal. Denote

$$\mathcal{I} = \{\, J \subseteq I \mid J \lhd R \text{ and } J \text{ is finitely generated} \,\}$$

Clearly $\mathcal{I}$ is non-empty since it contains the zero ideal. By assumption, we may choose a maximal element of $\mathcal{I}$, say J. If $I = J$ then we are done. If not then consider $a \in I \backslash J$. Then $(J, \{\, a \,\})$ is a finitely generated ideal contained in I which contains J. This is a contradiction to the maximality of J. Hence $I = J$ and I is Noetherian. □

Example 5.3. Let R be a PID. Then R is Noetherian.

Example 5.4. Consider $R = \mathbb{Z}[X_1, X_2, \dots]$. Then R is not Notherian since

$$(X_1) \subseteq (X_1, X_2) \dots$$

is an ascending chain of ideals that is not stationary.

Theorem 5.5 (Hilbert's Basis Theorem)**.** *Let R be Noetherian. Then $R[X]$ is Noetherian.*

Proof. Let $I \lhd R[X]$ be an ideal. If $f \in R[X]$ then $\lambda(f)$ denotes its leading coefficient. For all $m \in \mathbb{N}$ we define

$$J_m = \{\, 0 \,\} \cup \{\, r \in R \mid \exists f \in I, \deg(f) = m, \lambda(f) = r \,\}$$

It is easy to see that J_m is an ideal of R and that $J_m \subseteq J_{m+1}$ for all $m \in \mathbb{N}$. This defines an ascending chain of ideals

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$$

Now, R is Noetherian hence there must exist some $n \in \mathbb{N}$ such that $J_n = J_{n+1} = J_{n+2} = \dots$. For all $m \leq n$, the ideal J_m is finitely generated, say

$$J_m = (r_{m1}, \dots, r_{ms_m})$$

for some $r_{mj} \in R$ and $s_m \in \mathbb{N}$. Now for a fixed $m \in \mathbb{N}$, we have for each $1 \leq j \leq s_m$ some $f_{mj} \in I$ with $\deg(f_{mj}) = m$ and $\lambda(f_{mj}) = r_{mj}$. We claim that the finite set

$$S = \{ f_{mj} \in I \mid m \leq n, 1 \leq j \leq s_m \}$$

generates the ideal I. Indeed, suppose $f \in I$ with $\deg(f) = m$. We first consider the case where $m \leq n$. We have $\lambda(f) \in J_m$ and thus

$$\lambda(f) = \sum_{j=1}^{s_m} b_j r_{mj}$$

for some $b_j \in R$. Hence

$$\deg\left(f - \sum_{j=1}^{s_m} b_j f_{mj}\right) < m$$

Now if $m > n$ then $\lambda(f) \in J_m = J_n$ and thus

$$\lambda(f) = \sum_{j=1}^{s_n} b_j r_{nj}$$

for some $b_j \in R$. Hence

$$\deg\left(f - X^{m-n} \sum_{j=1}^{s_n} b_j f_{nj}\right) < m$$

Inducting on m, we see that in both cases, f may be written as an $R[X]$-linear combination of elements of S and thus $I = (S)$. □

Corollary 5.6. *Let R be Noetherian. Then $R[X_1, \dots, X_n]$ is Noetherian.*

Example 5.7. $\mathbb{Z}$ is Noetherian but not a PID.

Example 5.8. Let K be a field. Then $K[X_1, \dots, X_n]$ is Noetherian.

Example 5.9. If R is any PID then $R[X_1, \dots, X_n]$ is Noetherian.

Definition 5.10. Let R be a ring and M an R-module. Then M is said to be **Noetherian** if every submodule of M is finitely generated.

Lemma 5.11. *Let R be a ring and M an R-module. Then the following conditions are equivalent:*

1. *M is Noetherian*
2. *Every ascending chain of R-submodules of M is stationary*
3. *Every non-empty collection of R-submodules of M has a maximal element*

Proof. This follows the exact same argumentation as the case for ideals. □

Proposition 5.12. *Let R be a ring and*

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if both L and N are.

Proof. First suppose that M is Noetherian. Then any ascending chain of submodules of L or N corresponds to an ascending chain of submodules of M and they are thus stationary.

Conversely, suppose that L and N are Noetherian modules. Let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of submodules of M. Then the ascending chains

$$\alpha^{-1}(M_1) \subseteq \alpha^{-1}(M_2) \subseteq \dots$$

of L and

$$\beta(M_1) \subseteq \beta(M_2) \subseteq \dots$$

of N are stationary. Suppose that $\alpha^{-1}(M_k) = \alpha^{-1}(M_K)$ and $\beta(M_k) = \beta(M_K)$ for all $k \geq K$. We claim that $M_k = M_K$ for all $k \geq K$. Indeed, fix $k \geq K$ and choose $x \in M_k$. Then $\beta(x) \in \beta(M_k) = \beta(M_K)$ and thus there exists a $y \in M_K$ with $\beta(x) = \beta(y)$. This is equivalent to $x - y \in \ker \beta$. But the sequence is exact at M and $\ker(\beta) = \operatorname{im}(\alpha)$ and thus there exists $z \in L$ with $\alpha(z) = x - y \in M_k$. Therefore, $z \in \alpha^{-1}(M_k) = \alpha^{-1}(M_K)$ and we see that $\alpha(z) = x - y \in M_K$. This shows that $x \in M_K$ and thus $M_k = M_K$ for all $k \geq K$. □

Corollary 5.13. *Let R be a ring and $M_1, \dots, M_n$ Noetherian R-modules. Then*

$$M_1 \oplus \dots \oplus M_n$$

is Noetherian.

Proof. We prove the corollary by induction on n. If $n = 1$ then there is nothing to prove so suppose $n = 2$ for the basis case. We have a short exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_1 \oplus M_2 \xrightarrow{\beta} M_2 \longrightarrow 0$$

with the morphisms given by

$$\begin{aligned} \alpha : M_1 &\to M_1 \oplus M_2 \\ m_1 &\mapsto (m_1, 0) \end{aligned}$$

and

$$\begin{aligned} \beta : M_1 \oplus M_2 &\to M_2 \\ (m_1, m_2) &\mapsto m_2 \end{aligned}$$

Hence by the previous proposition, $M_1 \oplus M_2$ is Noetherian. The corollary then follows by induction on n. □

Proposition 5.14. *Let R be a Noetherian ring and M a finitely generated R-module. Then M is Noetherian.*

Proof. Since M is finitely generated, there exists an $n \in \mathbb{N}$ and a R-submodule of R^n, say N, such that $M \cong R^n/N$. The previous corollary implies that R^n is a Noetherian R-module and we have the exact sequence

$$R^n \longrightarrow M \longrightarrow 0$$

The proposition then implies that M is Noetherian. □

Corollary 5.15. *Let R be a Notherian ring and M a Noetherian R-module. Then every R-submodule of M is Noetherian.*

Proof. Let N be an R-submodule of M. Then, since M is Noetherian, N is finitely generated over R. Since R is a Noetherian module over itself, the previous proposition implies that N is Noetherian. □

6 Factorisation

Definition 6.1. Let R be an integral domain. We say that $r \in R$ is **irreducible** if it is not a unit and $r = xy$ for some $x, y \in R$ implies that either x or y are units.

Definition 6.2. Let R be an integral domain. We say that $r \in R$ is **prime** if $r|xy$ for some $x, y \in R$ implies that either $r|x$ or $r|y$.

Lemma 6.3. *Let R be an integral domain. Any prime element of R is necessarily irreducible.*

Proof. Let $r \in R$ be prime and suppose that $r = xy$ for some $x, y \in R$. Then by definition of primality, $r|x$ or $r|y$. Suppose, without loss of generality, that $r|x$. Then $x = rb$ for some $b \in R$. Then $r = rby$. Since R is an integral domain, we must have that $1 = by$ and y is thus a unit. Similarly, if $r|y$ then x is a unit. □

Proposition 6.4. *Let R be a PID. Then $r \in R$ is prime if and only if it is irreducible.*

Proof. The forward case is covered by the previous lemma. It suffices to prove the backwards implication. To this end, let $r \in R$ be irreducible. Since in a PID, any non-zero ideal is prime if and only if it is maximal, it suffices to show that (r) is a maximal ideal. Suppose there exists an ideal $J \triangleleft R$ such that

$$(r) \subseteq J \subseteq R$$

Since R is a PID, we have $J = (s)$ for some $s \in R$. Now, $(r) \subseteq (s)$ so $r = sa$ for some $a \in R$. r is irreducible so either s is a unit or a is the unit. In the former case, $(s) = R$ and in the latter, $(s) = (r)$ and thus (r) is maximal. □

Corollary 6.5. *Let R be a PID and $r \in R \setminus \{0\}$. Then the following are equivalent*

1. *(r) is maximal*
2. *r is prime*
3. *r is irreducible*

Definition 6.6. Let R be an integral domain. We say that R is a **unique factorisation domain** (UFD) if every non-zero $r \in R$ satisfies the following conditions:

UFD1 There exists a natural number n, irreducibles $p_1, \ldots, p_n \in R$ and a unit $u \in R$ such that

$$r = up_1 \ldots p_n$$

UFD2 Such a representation is unique up to units. In other words, if $r = vq_1, \ldots, q_m$ is another representation of r then $m = n$ and $p_i = w_i q_i$ for some units $w_i \in R$.

Proposition 6.7. *Let R be a UFD. Then $r \in R$ is prime if and only if it is irreducible.*

Proof. The forward case is again proven by the lemma. It suffices to show the backwards implication. Let $r \in R$ be irreducible and suppose $r|xy$ for some $x, y \in R$. Then $xy = rz$ for some $z \in R$. If either $x = 0$ or $y = 0$ then the result is trivial so assume they are both non-zero. Writing x, y and z as products of irreducibles, we have

$$(up_1 \ldots p_l)(vq_1 \ldots q_m) = wrs_1 \ldots s_n$$

for some units $u, v, w \in R$ and irreducibles $p_i, q_j, s_k \in R$. By UFD2, either r is a product of a unit with a p_i or the product of a unit with a q_j. In the former case, $r|x$. In the latter case $r|y$. □

Proposition 6.8. *Let R be a Noetherian integral domain. Then R satisfies UFD1.*

Proof. We shall refer to $r \in R$ as **undecomposable** if it is non-zero, non-unitary and cannot be written as a product of irreducibles. Suppose that $r \in R$ is undecomposable. Then if $r = x_1 y_1$ we must have that both x_1 and y_1 are non-units in R and one of them is undecomposable. Say x_1. We can play the same game with x_1 and write $x_1 = x_2 y_2$ for some non-zero, non-unitary $x_2, y_2 \in R$. Say that x_2 is again undecomposable. We then have the ascending chain of ideals

$$(r) \subseteq (x_1) \subseteq (x_2) \subseteq \ldots$$

which is non-stationary. This is a contradiction to R being Noetherian so this process must stop and at one stage, we must be able to retrieve a decomposition into irreducibles. □

Proposition 6.9. *Let R be an integral domain. Then R is a UFD if and only if it satisfies UFD1 and every irreducible in R is prime.*

Proof. The forward implication has been covered by previous results. It suffices to show the backwards implication. To this end, suppose that R satisfies UFD1 and every irreducible in R is prime. We must prove that R satisifies UFD2. Let $r \in R$ be non-zero, non-unitary and suppose that

$$r = p_1 \ldots p_m = q_1 \ldots q_n$$

for some irreducibles $p_i, q_j \in R$ and $, \leq n$. By assumption, each p_i is prime so $p_1|q_1 \ldots q_n$ implies that $p_1|q_j$ for some $1 \leq j \leq n$. After renumbering, we may assume that $p_1|q_1$ so that $q_1 = u_1 p_1$. But q_1 and p_1 are irreducible so u_1 must be a unit. Now, cancelling common terms on both sides of the equatuon, we have

$$p_2 \ldots p_m = u_1 q_2 \ldots q_n$$

Continuining in this way, we obtain

$$1 = u_1 \ldots u_m q_{m+1 \ldots q_n}$$

for some units $u_i \in R$ such that $q_i = u_i p_i$ (after renumbering). Now if $m < n$ then necessarily q_{m+1} is a unit which is a contradiction. Hence $n = m$ and UFD2 is satisfied. □

Corollary 6.10. *Any Noetherian integral domain in which every irreducible is prime is a UFD. In particular, every PID is a UFD.*

Remark. *This implies that the following holds:*

$$\text{ED} \implies \text{PID} \implies \text{UFD}$$

Example 6.11. $\mathbb{Z}$ is a UFD.

Example 6.12. Let K be a field. Then $K[X]$ is a UFD.

Definition 6.13. Let R be a UFD. If $r, s \in R$ are non-zero and have prime factorisations

$$r = up_1^{e_1} \dots p_n^{e_n}$$
$$s = vp_1^{f_1} \dots p_m^{f_m}$$

for some units $u, v \in R$, primes $p_i \in R$, natural numbers e_i, f_j and $n \leq m$ then we define their **greatest common divisor** to be

$$\gcd(r, s) = p_1^{\min\{e_1, f_1\}} \dots p_n^{\min\{e_n, f_n\}}$$

Definition 6.14. Let R be a UFD and $f = \sum_{i=0}^{n} r_i X^i \in R[X]$ a non-zero polynomial. We define the **content** of f to be

$$c(f) = \gcd_{0 \leq i \leq n, r_i \neq 0}(r_i)$$

Definition 6.15. Let R be a UFD and $f \in R[X]$ a non-zero polynomial. Then R is said to be **primitive** if $c(f) = 1$.

Lemma 6.16. *Let R be a UFD and $f \in R[X]$ a non-zero polynomial. Then there exists a primitive polynomial $f_0 \in R[X]$ such that $f = c(f)f_0$.*

Proof. This follows immediately upon dividing f through by its content. The resulting polynomial is then primitive. □

Proposition 6.17. *Let R be a UFD and $f, g \in R[X]$ primitive polynomials. Then fg is primitive.*

Proof. Suppose that fg is not primitive. Then $c(fg)$ has a prime factor, say $p \in R$. Consider the homomorphism

$$\pi : R[X] \to (R/(p))[X]$$

Then $\pi(f)\pi(g) = \pi(fg) = 0$. Now, $(R/(p))[X]$ is an integral domain so either $\pi(f) = 0$ or $\pi(g) = 0$. This is equivalent to saying that $p|c(f)$ or $p|c(g)$. But f and g are primitive so this is a contradiction and we must have that fg is primitive. □

Corollary 6.18. *Let R be a UFD and $f, g \in R[X]$ non-zero polynomials. Then $c(fg) = c(f)c(g)$.*

Proof. We may write $f = c(f)f_0$ and $g = c(g)g_0$ for some primitive polynomials f_0 and g_0. Then $fg = c(f)c(g)f_0g_0$. By the previous proposition, f_0g_0 is primitive and the corollary follows. □

Proposition 6.19 (Gauss' Lemma). *Let R be a UFD and $K = \mathrm{Frac}(R)$. If $f \in R[X]$ is non-constant and irreducible in $R[X]$ then f is irreducible in $K[X]$.*

Proof. f is clearly primitive since otherwise, we would be able to factor out its non-unit content. Now suppose that $f = gh$ for some non-units (and thus non-constants) $g, h \in K[X]$. Clearing denominators we may write

$$g = \frac{G}{r}, h = \frac{H}{s}$$

for some $G, H \in R[X]$ and $r, s \in R$ such that r is coprime to $c(G)$ and s is coprime to $c(H)$. Then

$$rs = c(rsf) = c(G)c(H)$$

hence $r|c(H)$ and $s|c(G)$. We may then write

$$f = \frac{G}{a}\frac{H}{b} = \frac{G}{b}\frac{H}{a}$$

but the latter is a product of two polynomials in $R[X]$ and such a decomposition is not possible since f is irredudicble in R by hypothesis. Hence f is irreducible in $K[X]$. □

Lemma 6.20. *Let R be a UFD and $K = \mathrm{Frac}(R)$. If $f \in R[X]$ is a non-constant and irreducible polynomial then*

$$R[X] \cap fK[X] = fR[X]$$

Proof. First suppose that $g = fh$ for some $h \in R[X]$, Then $g \in R[X]$ and $g \in fK[X]$.

Conversely, suppose that $g \in R[X] \cap fK[X]$ so that $g = fh$ for some $h \in K[X]$. We first note that f must be primitive since it is irreducible. Now write

$$h = \frac{H}{b}$$

with $H \in R[X]$ and $b \in R$ such that b is coprime to $c(H)$. Then $bg = fH$ and $bc(g) = c(H)$. We therefore have that $b|c(H)$. This implies that b is a unit in R whence $h \in R[X]$. Hence $g \in fR[X]$. □

Theorem 6.21. *Let R be a Noetherian UFD. Then $R[X]$ is a Noetherian UFD.*

Proof. Hilbert's Basis Theorem implies that $R[X]$ is a Noetherian integral domain and, by Proposition 6.8, $R[X]$ satisfies UFD1. Hence by Proposition 6.9, it suffices to show that every irreducible in $R[X]$ is prime. To this end, suppose that $f \in R[X]$ is irreducible. We consider two cases, first suppose that $f \in R$. Then f is irreducible in R. Now R is a UFD and every irreducible is prime in R so f is prime in R. We thus have

$$R[X]/(f) \cong (R/(f))[X]$$

is an integral domain and thus f is prime in $R[X]$.

Now suppose that f is not constant. By the previous lemma, $R[X] \cap fK[X] = fR[X]$ and so

$$R[X]/fR[X] = R[X]/(R[X] \cap fK[X])$$

This implies the existence of an injective ring homomorphism

$$R[X]/fR[X] \hookrightarrow K[X]/fK[X]$$

Now, Gauss' Lemma implies that f is irreducible in $K[X]$ and, since $K[X]$ is a PID, is thus prime in $K[X]$. We then have that $K[X]/fK[X]$ is an integral domain that contains $R[X]/fR[X]$ as a subring. The latter is therefore also an integral domain whence f is prime in $R[X]$. □

Corollary 6.22. *Let R be a Noetherian UFD. Then $R[X_1, \ldots, X_n]$ is a Noetherian UFD.*

Example 6.23. *$\mathbb{Z}[X_1, \ldots, X_n]$ is a UFD.*

Example 6.24. *If K is a field then $K[X_1, \ldots, X_n]$ is a UFD.*

Proposition 6.25. *Let R be an integral domain and $f \in R[X]$ a non-constant monic polynomial. Let $\mathfrak{p} \lhd R$ be a prime ideal of R such that the reduction $\overline{f} = f \pmod{\mathfrak{p}}$ is irreducible in $(R/\mathfrak{p})[X]$. Then f is irreducible in $R[X]$.*

Proof. Suppose that $f \in R[X]$ is irreducible. Then we can write $f = gh$ for some $g, h \in R[X]$ also monic and non-constant. Then $\overline{f} = \overline{g}\overline{h}$. But this contradicts the hypothesis that $\overline{f}$ does not factor in $(R/\mathfrak{p})[X]$. □

Proposition 6.26 (Eisenstein's Irreducibility Criterion)**.** *Let R be an integral domain and $f(X) = \sum_{i=0}^{n} r_i X^i \in R[X]$ be a non-constant monic polynomial in $R[X]$. Suppose there exists a prime ideal $\mathfrak{p} \lhd R$ such that*

1. *$r_i \in \mathfrak{p}$ for all $0 \leq i \leq n-1$*

2. *$r_0 \notin \mathfrak{p}^2$*

then f is irreducible in $R[X]$.

Proof. Suppose that $f \in R[X]$ is irreducible. Then we can write $f = gh$ for some $g, h \in R[X]$ monic and non-constant. Reducing modulo $\mathfrak{p}$ we have

$$\overline{g}\overline{h} = \overline{f} = X^n$$

By definition of $\mathfrak{p}$, $R/\mathfrak{p}$ is an integral domain and so both $\overline{g}$ and $\overline{h}$ have zero constant term. This implies that the constant terms of g and h are elements of $\mathfrak{p}$. But this would imply that the constant term of f is in $\mathfrak{p}^2$ which is a contradiction. □

7 The Vandermonde Identity

Proposition 7.1. *Consider the matrix*

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_n \\ \vdots & \vdots & \cdots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \end{pmatrix}$$

with entries in $\mathbb{Z}[X_1, \ldots, X_n]$. Then $\det V = \prod_{i<j}(X_j - X_i)$

Proof. Let $\Delta(X_1, \ldots, X_n)$ denote $\det V \in \mathbb{Z}[X_1, \ldots, X_n]$. Fix some $i \neq j$ and set $X_i = X_j$. Then $\Delta = 0$ since V has two equal columns. Hence Δ is divisible by $X_j - X_i$. Since $\mathbb{Z}[X_1, \ldots, X_n]$ is a UFD and the polynomials $X_j - X_i$ for $i < j$ are all coprime to each other, we see that Δ is divisible by $\prod_{i<j}(X_j - X_i)$. Now, $\deg \Delta = \binom{n}{2} = \deg \prod_{i<j}(X_j - X_i)$ hence they must differ only by a constant. To determine this constant, we need look only at the the diagonal term $X_2 X_3^2 \ldots X_n^{n-1}$. This has coefficient 1 in both expressions so the overall constant must be 1. □

8 The Cayley-Hamilton Theorem

Theorem 8.1. *Let R be a ring and M a finitely generated R-module. Suppose that $\varphi : M \to M$ is an R-linear endomorphism of M. Then φ satisfies a polynomial equation of the form*

$$\varphi^n + r_{n-1}\varphi^{n-1} + \cdots + r_0 = 0$$

for some $r_i \in R$

Proof. Let $x_1, \ldots, x_n$ be generators for M over R. Then

$$\varphi(x_i) = \sum_{j=1}^{n} r_{ij} x_j$$

for all $1 \leq i \leq n$ where $r_{ij} \in R$. Denote $\Phi = (r_{ij}) \in M_n(R)$. Given $m \in M$, we may consider M to be an $R[\varphi]$-module by taking scalar multiplication to be

$$\varphi \cdot m = \varphi(m)$$

Now define the matrix

$$C = \varphi I - \Phi$$

which is an element of $M_n(R[\varphi])$. Then, by construction,

$$C(x_1, \ldots, x_n)^T = \vec{0} \in M^n$$

Left multiplying by the adjugate of C and using the definition of the determinant, we have

$$\det C(x_1, \ldots, x_n)^T = (\operatorname{adj} C)C(x_1, \ldots, x_n)^T = \vec{0} \in M^n$$

But $x_1, \ldots, x_n$ generate M so we must have that $\det C = 0$. The result then follows upon expanding the definition of $\det C$. $\square$

Remark. The above theorem can be reformulated to state that any matrix with entries in a commutative ring satisfies its own characteristic polynomial - a more general version of the well-known theorem of linear algebra.

9 Chinese Remainder Theorem

Lemma 9.1. *Let R be a ring and $I, J \lhd R$ ideals. Then the following sets are also ideals of R:*

$$I + J := \{\, x + y \mid x \in I, y \in J \,\}$$
$$IJ := \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; x_i \in I, y_i \in J, n \in \mathbb{N} \right\}$$

furthermore, we have the following relations:

1. *$I + J = I \cup J$*
2. *$IJ \subseteq I \cap J$*

3. $(x)(y) = (xy)$ *for all* $x, y \in R$

Proof. It is clear that $I + J$ is a subgroup of $(R, +)$ so suppose that $r \in R$ and $i \in I + J$. By definition, $i = x + y$ for some $x \in I, y \in J$. Then $ir = (x + y)r = xr + yr$. But I and J are both ideals so $xr \in I, yr \in J$ whence $ir \in R$ and $I + J$ is an ideal.

It is also clear that IJ is a subgroup of $(R, +)$ so suppose that $r \in R$ and $i \in IJ$. By definition we have $i = \sum_{i=1}^{n} x_i y_i$ for some $x_i \in I, y_i \in J$ and $n \in \mathbb{N}$. Then

$$ir = \sum_{i=1}^{n} x_i y_i r$$

Now, $y_i r \in J$ for all $1 \leq i \leq n$ so, clearly the above is also an element of IJ. This shows that IJ is an ideal of R.

To prove the relations, first let $i \in I + J$. Then, by definition, $i = x + y$ for some $x \in I, y \in J$. Since $I \cup J$ is an ideal and, in particular, an additive group, we must therefore have that $x + y \in I + J$ if and only if $x + y \in I \cup J$.

Now suppose that $i \in IJ$. Then $i = \sum_{i=1}^{n} x_i y_i$ for some $x_i \in I, y_i \in J$ and $n \in \mathbb{N}$. Now, for i to be an element of $I \cap J$, we would require that $i \in I$ and $i \in J$. Fix some $1 \leq i \leq n$ and consider the corresponding term in the expansion of i: $x_i y_i$. x_i is an element of I and y_i is an element of R so, by definition, $x_i y_i \in I$. Similarly, $x_i y_i \in J$. Now by the additive subgroup property of IJ, we see that the entire summation is an element of $I \cap J$ and we are done.

Finally, suppose that $i \in (x)(y)$. Then $i = \sum_{i=1}^{n} x_i y_i$ for some $x_i \in (x), y_i \in (y)$ and $n \in \mathbb{N}$. Clearly each term in the summation is an element of (xy) whence the entire summation is an element of (xy). Conversely, suppose that $i \in (xy)$. Then $i = rxy$ for some $r \in R$. We may consider rx to be an element of (x) itself so that rxy is indeed an element of $(x)(y)$ and the lemma is proved. $\square$

Definition 9.2. Let R be a ring and $I, J \triangleleft R$ ideals. Then I and J are said to be comaximal if $I + J = R$.

Remark. The condition that two ideals I and J are comaximal is equivalent to the condition that there exists, $x \in I, y \in J$ such that $x + y = 1$.

Example 9.3. Consider the ideals $(2), (3)$ in $\mathbb{Z}$. Then these ideals are comaximal.

Lemma 9.4. *Let* R *be a ring and* $I, J \triangleleft R$ *comaximal ideals. Then* $IJ = I \cap J$.

Proof. By the previous lemma, it suffices to show that $I \cap J \subseteq IJ$. Since I and J are comaximal, we may choose $x \in I, y \in J$ such that $x + y = 1$. Then, given any $i \in I \cap J$, we have $ix + iy = i \in IJ$. $\square$

Theorem 9.5. *Let* R *be a ring and* $I, J \triangleleft R$ *comaximal ideals. Then*

$$R/IJ \cong R/I \times R/J$$

Proof. Consider the homomorphism of rings

$$\begin{aligned} \varphi : R &\to R/I \times R/J \\ \varphi(r) &\mapsto (r + I, r + J) \end{aligned}$$

Clearly, $\ker \varphi = I \cap J$. By the previous lemma, the kernel is therefore equal to IJ. Now it suffices to prove that φ is surjective whence the theorem will follow by application of the first isomorphism theorem. To this end, suppose that $(r_1 + I, r_2 + J) \in R/I \times R/J$. Note that

$$\begin{aligned} \varphi(x) &= (x + I, 1 - y + J) = (0 + I, 1 + J) \\ \varphi(y) &= (1 - x + I, y + J) = (1 + I, 0 + J) \end{aligned}$$

so that

$$\varphi(r_1 y + r_2 x) = (r_1 + I, r_2 + I)$$

and thus φ is surjective. □

Corollary 9.6. *Let R be a ring and $I_1, \dots, I_n \triangleleft R$ a collection of pairwise comaximal ideals. Then*

$$R/I_1 \dots I_n \cong R/I_1 \oplus \cdots \oplus R/I_n$$

Proof. We prove the corollary by induction on n. The case where $n = 2$ is covered by the previous theorem. It thus suffices to show that I_1 and $I_2 \dots I_n$ are comaximal. Indeed, for all $i = 2, \dots, n$ there exists $x_i \in I_1$ and $y_i \in I_i$ such that

$$x_i + y_i = 1$$

This implies that $y_2 \dots y_n \cong 1 \pmod{I_1}$. In other words, there exists $\tilde{x} \in I_1$ such that

$$\tilde{x} + y_2 \dots y_n = 1$$

and thus I_1 and $I_2 \dots I_n$ are comaximal. Hence

$$R/I_1 \dots I_n \cong R/I_1 \oplus R/I_2 \dots I_n$$

and the corollary follows by induction on n. □

Corollary 9.7 (Chinese Remainder Theorem)**.** *Let R be a ring and suppose that $r_1, \dots, r_k \in R$ generate pairwise comaximal ideals. Then*

$$R/(r_1 \dots r_k) \cong R/(r_1) \oplus \cdots \oplus R/(r_k)$$

Example 9.8. Let n be a natural number and let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be its unique factorisation into distinct primes p_i. Then

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{\alpha_1}) \oplus \cdots \oplus \mathbb{Z}(p_k^{\alpha_k})$$