Peize Liu
St. Peter's College
University of Oxford

Notes on

Rings and Modules

March, 2020

This page is intentionally left blank.

Notes on Rings and Modules

Tautochrone

November 4, 2021

Reading List

Lecture Notes

- Richard Earl, *A3: Rings and Modules* (2018-2019). **[Earl]**
  `https://courses-archive.maths.ox.ac.uk/node/view_material/44028`

  The lecture notes for 2018-2019 Oxford second year math course A3: Rings and Modules. The most elementary notes ever in this subject. Supplied with extremely abundant examples.

- Tom Sanders, *A3: Rings and Modules* (2019-2020). **[Sanders]**
  `https://courses-archive.maths.ox.ac.uk/node/view_material/47413`

  The lecture notes for 2019-2020 Oxford second year math course A3: Rings and Modules. Approximately covers the same topics as Earl's notes, but is more concise and contains slightly more material.

- Damian Rössler, *B2.2: Commutative Algebra* (2020-2021). **[Rössler]**
  `https://courses-archive.maths.ox.ac.uk/node/view_material/53657`

  The lecture notes for 2020-2021 Oxford third year math course B2.2: Commutative Algebra. Very compact and the structure resembles Atiyah's book.

Textbooks

- Thomas Hungerford, *Algebra* (GTM73). **[Hungerford]**

  My favorite introductory textbook in algebra. Covers the basic topics (groups, rings, modules and fields) and commutative algebra. The text is written in 1970s and has the reminiscent of Bourbaki style.

- Paolo Aluffi, *Algebra: Chapter 0*. **[Aluffi]**

  A novel introductory textbook in algebra. Covers the basic topics (groups, rings, modules and fields) and homological algebra. It is well-known for its early introduction of category theory which gives a higher perspective of learning algebra.

- M. Atiyah, I. MacDonald, *Introduction to Commutative Algebra*. **[Atiyah]**

  The most classical textbook in commutative algebra. It is extremely concise and many proofs are neglected or incomplete.

- Lingzhao Nie, Shisun Ding, *An Introduction to Algebra*. **[N&D]**

  Written in Chinese. An undergraduate second-year level algebra textbook. It is a very typical Chinese-style textbook designed for a one-year course in abstract algebra. Covers the basic topics (groups, rings, modules and fields) only.

- Wenwei Li, *Methods of Algebra: Volume 1*. **[LWW]**

  Written in Chinese. A graduate level algebra textbook suitable for those who have solid background in pure mathematics. It has a heavy focus on category theory and briefly introduce the basic objects of algebra from a very high perspective.

Chapter 1

Rings

1.1 Rings and Ring Homomorphisms

1.1.1 Rings and Fields

Definition 1.1.1. Rings

A ring $(R,+,\cdot)$ is an Abelian group $(R,+)$ with multiplication $\cdot$ satisfying the following axioms:

1. Associativity: $\forall\ r,s,t \in R:\quad r\cdot(s\cdot t)=(r\cdot s)\cdot t$
2. Distributivity: $\forall\ r,s,t \in R:\quad (r+s)\cdot t = r\cdot t + s\cdot t,\quad r\cdot(s+t)=r\cdot s+r\cdot t$

R is said to be a **ring with identity**, if $\quad \exists\ 1_R \in R \quad \forall\ r\in R:\quad r\cdot 1_R = 1_R\cdot r = r.$

R is said to be a **commutative ring**, if $\quad \forall\ r,s\in R:\quad r\cdot s = s\cdot r$

We will often use CRI in the notes, which stands for commutative ring with identity.

Remark. In a ring with identity, we often require that $0\neq 1$ to avoid the collapse of the whole ring. It is immediate that if $0_R = 1_R$ then $R=\{0_R\}$ is the **zero ring**.

Proposition 1.1.2. Properties of Rings

Suppose that R is a ring with identity, then:

1. The multiplicative identity 1 is unique;
2. $\forall\ r\in R:\quad r\cdot 0 = 0\cdot r = 0$;
3. $\forall\ r\in R:\quad r\cdot -1 = -1\cdot r = -r$.

Proof. Trivial. □

Remark. As in the case of groups, for $n\in\mathbb{N}$ and a in the ring R, we can define na and a^n by:

$$na := \underbrace{a+\ldots+a}_{n \text{ times}} \qquad\qquad a^n := \underbrace{a\cdot\ldots\cdot a}_{n \text{ times}}$$

In general, a^{-n} could be undefined.

Definition 1.1.3. Zero-Divisors, Integral Domains

Suppose that R is a ring. For $a\in R\setminus\{0\}$, a is said to be a left (*resp.* right) zero-divisor, if $\exists\ b\in R:\ ab=0$ (*resp.* $ba=0$). a is said to be a zero-divisor if it is both a left and a right zero-divisor.

A commutative ring R is said to be an integral domain, if R has no zero-divisors.

Proposition 1.1.4. Cancellation Law

Suppose that R is an integral domain. Then

$$\forall\ a,b\in R,\ \forall\ c\in R\setminus\{0\}:\quad ac=bc \Longrightarrow a=b$$

Proof. Trivial. □

Definition 1.1.5. Units, Fields

Suppose that R is a ring with identity. For $a \in R \setminus \{0\}$, a is said to be a left (*resp.* right) unit, if $\exists\, b \in R:\ ab = 1$ (*resp.* $ba = 1$). a is said to be a unit if it is both a left and a right unit.

If a is a unit, then there exists a unique $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. a^{-1} is called the inverse of a. A CRI R is said to be a field, if every non-zero element of R is a unit.

Definition / Proposition 1.1.6. $R^\times$

If R is a ring with identity, then the units of R form a group under multiplication, denoted by $R^\times$.

Proposition 1.1.7. Zero-Divisors and Units as Mappings.

Suppose that R is a ring.

1. $a \in R \setminus \{0\}$ is a left (*resp.* right) zero-divisor if and only if left (*resp.* right) multiplication by a is not an injective map $R \to R$;
2. $a \in R \setminus \{0\}$ is a left (*resp.* right) unit if and only if left (*resp.* right) multiplication by a is an surjective map $R \to R$;

Proof. Trivial. □

Corollary 1.1.8. Zero-Divisor $\neq$ Unit

$a \in R$ cannot be both a left (*resp.* right) zero-divisor and a right (*resp.* left) unit.

Corollary 1.1.9. Field $\Longrightarrow$ Integral Domain

Every field is an integral domain.

Proposition 1.1.10. Finite Integral Domain $\Longrightarrow$ Field

Every finite integral domain is a field.

Proof. Use Proposition 1.1.7 and the fact that injective maps $R \to R$ are surjective for the finite set R. □

Example 1.1.11. Examples of Rings

1. The set of integers $\mathbb{Z}$ forms an integral domain under addition and multiplication;
2. The rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ form fields under addition and multiplication;
3. The $n \times n$ matrices $M_{n\times n}(\mathbb{R})$ forms a non-commutative ring under matrix addition and multiplication;
4. If G is an Abelian group, then the endomorphism group $\mathrm{End}(G)$ forms a ring with indentity under map addition and composition;
5. The even integers $2\mathbb{Z}$ forms a ring without identity under addition and multiplication.
6. The group $\mathbb{Z}/n\mathbb{Z}$ forms a finite ring under addition and multiplication up to congruence. Moreover, it is a field if and only if n is a prime number.

Definition 1.1.12. Ring Homomorphisms

Suppose that R and S are rings. $f : R \to S$ is said to be a ring homomorphism, if:

$$\forall\ r, s \in R: \quad f(r+s) = f(r) + f(s)$$
$$\forall\ r, s \in R: \quad f(r \cdot s) = f(r) \cdot f(s)$$

Suppose that R and S are rings with identity. The ring homomorphism $f : R \to S$ is said to a **unital ring homomorphism**, if

$$f(1_R) = 1_S$$

Bijective (unital) ring homomorphisms are called **(unital) ring isomorphisms**.

Definition 1.1.13. Kernel and Image

Suppose that $f : R \to S$ is a ring homomorphism. We define the kernel of f to be $\ker f := f^{-1}(\{0_S\})$ and the image of f to be $\operatorname{im} f := f(R)$.

Definition 1.1.14. Subrings

Suppose that R is a ring. $S \subseteq R$ is said to be a subring of R, if the inclusion map $\iota : S \hookrightarrow R$ is a ring homomorphism.

Definition 1.1.15. The Categories Rng **and** Ring

Clearly the class of all rings forms a category, which is denoted by Rng. The morphisms in Rng are ring homomorphisms. Similarly, the class of all rings with indentity forms the category Ring, whose morphisms are unital ring homomorphisms.

Remark. In the category Ring, the monomorphisms are precisely the injective ring homomorphisms. Unlike Set and Grp, however, not all epimorphisms are surjective ring homomorphisms. For example, the inclusion $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism but is not surjective.

Remark. $\mathbb{Z}$ is the **initial object** in Ring. In order words, for any ring R with identity, there exists a unique unital ring homomorphism $f : \mathbb{Z} \to R$, which is given by

$$\forall\ n \in \mathbb{Z}: \quad f(n) = n \cdot 1_R$$

The zero ring $\{0\}$ is the **final object** in Ring.

1.1.2 Characteristics

Definition 1.1.16. Characteristics

Suppose that R is a ring with identity. The least positive integer n such that $n1_R = 0_R$ is called the characteristic of R, denoted by $\operatorname{char} R = n$. If no such n exists, then we say that $\operatorname{char} R = 0$.

Remark. If $n1_R = 0_R$, then $na = 0_R$ for all $a \in R$.

Proposition 1.1.17. Characteristic of an Integral Domain

Suppose that R is an integral domain. Then $\operatorname{char} R$ is either 0 or a prime number p.

Proof. If $\operatorname{char} R = mn$, for some $m, n \in \mathbb{Z}_+$, then

$$mn1_R = m1_R \cdot n1_R = 0$$

By definition of characteristic, $m1_R,\ n1_R \neq 0$, which implies that R has zero-divisors. □

Definition 1.1.18. Field Homomorphisms, Subfields

Suppose that F, K are fields. A unital ring homomorphism $f : F \to K$ is automatically a field homomorphism. It is immediate that all field homomorphisms are injective.

If $E \subseteq F$, then E is said to be a subfield of F, if the inclusion map $\iota : S \hookrightarrow R$ is a field homomorphism. F is called an **extension field** of E.

Proposition 1.1.19. Characteristics and Subfields

Suppose that F is a field.

1. if $\operatorname{char} F = 0$, then F has a subfield isomorphic to $\mathbb{Q}$;
2. if $\operatorname{char} F = p$, then F has a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Moreover, the subfield in 1 and 2 are minimal with respect to inclusion. Such subfield is called the **prime subfield** of F.

Proof. Suppose that E is a subfield of F. Clearly, $n1_F \in E$ for any $n \in \mathbb{Z}$. If $\operatorname{char} F = p$, then

$$\{0_F, 1_F, 1_F + 1_F, \cdots, (p-1)1_F\} = \mathbb{Z}/p\mathbb{Z} \subseteq E$$

If $\operatorname{char} F = 0$, then $m1_F \neq (n1_F)^{-1}$ for $m, n \in \mathbb{Z} \setminus \{0\}$. It follows that

$$\{(m1_F)(n1_F)^{-1} \in F : \ m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}\} = \mathbb{Q} \subseteq E$$

The minimality then follows trivially. □

Remark. For p prime, the finite field $\mathbb{Z}/p\mathbb{Z}$ is also denoted by $\mathbb{F}_p$.

Corollary 1.1.20. Cardinality of Finite Fields

Suppose that F is a finite field. Then $\operatorname{card} F = p^n$ for some prime number p and $n \in \mathbb{N}$.

Proof. If F is a finite field, it must have a non-zero characteristic p. By Proposition 1.1.19, F contains $\mathbb{F}_p$ as a subfield. In particular, F is a (finite-dimensional) vector space over $\mathbb{F}_p$. Suppose that $\dim_{\mathbb{F}_p} F = n$. Then $F \cong (\mathbb{F}_p)^n$ as vector spaces and we have $\operatorname{card} F = p^n$. □

Proposition 1.1.21. Embedding into a Ring with Identity

Every ring R can be embedding into a ring S which has an identity. S can be chosen such that $\operatorname{char} S = \operatorname{char} R$ or $\operatorname{char} S = 0$.

Proof. Suppose that we want $\operatorname{char} S = 0$. Let S be the additive Abelian group $R \oplus \mathbb{Z}$ with multiplication defined by

$$\forall\ r_1, r_2 \in R\ \ \forall\ n_1, n_2 \in \mathbb{Z} : \quad (r_1, n_1) \cdot (r_2, n_2) := (r_1 r_2 + n_2 r_1 + n_1 r_2, n_1 n_2)$$

One can verify that the multiplication defined above satisfies associativity and distributivity so that S is indeed a ring. S has characteristic 0 because $\mathbb{Z}$ has characteristic 0. Observe that $(0,1) \in S$ is the identity and $r \mapsto (r, 0)$ is a ring monomorphism (i.e. embedding) from R to S.

If we want $\operatorname{char} S = \operatorname{char} R$, then set $S = R \oplus \mathbb{Z}/n\mathbb{Z}$ where $n = \operatorname{char} R$ and everything is the same as above. □

1.1.3 Product Rings

Definition 1.1.22. Product of Rings: Set-Theoretic Definition

Suppose that R, S are rings. Then we define a ring structure on the Cartesian product of sets $R \times S$ by

$$\forall\ r_1, r_2 \in R\ \forall\ s_1, s_2 \in S : \quad (r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2)$$
$$\forall\ r_1, r_2 \in R\ \forall\ s_1, s_2 \in S : \quad (r_1, s_1) \cdot (r_2, s_2) := (r_1 \cdot r_2, s_1 \cdot s_2)$$

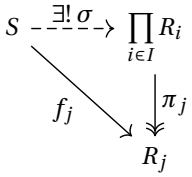
$R \times S$ is called the **(external) direct product** of ring R and S. Inductively, we can define the direct product of any finite number of rings.

Remark. Commonly, $\underbrace{R \times \cdots \times R}_{n \text{ times}}$ is denoted by R^n.

Proposition 1.1.23. Product of Rings: Universal Property

Suppose the $\{R_i\}_{i\in I}$ is a family of rings. The product ring is the ring $\prod_{i\in I} R_i$ with the canonical projections $\pi_j : \prod_{i\in I} R_i \twoheadrightarrow R_j$ satisfying the following universal property:

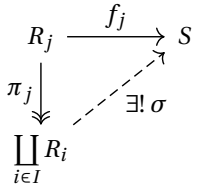
For any ring S and ring homomorphisms $f_j : S \to R_j$, there exists a unique ring homomorphism $\sigma : S \to \prod_{i\in I} R_i$ such that $f_j = \pi_j \circ \sigma$.



Moreover, any ring satisfying the universal property is uniquely determined up to ring isomorphism.

Remark. Readers should check that the set-theoretical definition of the product ring satisfies the universal property.

Remark. It is tempting to think about the coproduct of rings. That is, the product of rings with all arrows reversed:



In the category of Abelian groups Ab, the coproduct is the direct sum of groups. One may think if we can define the "direct sum" of commutative rings as coproduct, which coincides with product for a finite indexing set I. Unfortunately the answer is no. The correct structure in the case of CRI is the **tensor product of rings as $\mathbb{Z}$-modules**:

$$R \amalg S = R \otimes_{\mathbb{Z}} S$$

We shall discuss the tensor product in detail in Section 5.3.

1.2 Ideals

We want to construct a structure analogous to quotient sets in Set or quotient groups in Grp. In particular we need special substructure of rings that plays the role of normal subgroups for groups. The things we are looking for are ideals.

1.2.1 Ideals

Motivation. Consider a ring R with identity and an equivalence relation $\sim$ on R which is compatible with addition and multiplication. That is,

$$r_1 \sim r_1' \ \wedge \ r_2 \sim r_2' \quad \Longrightarrow \quad r_1 r_2 \sim r_1' r_2', \ r_1 + r_2 \sim r_1' + r_2'$$

Consider an additive subgroup $I \subseteq R$ that determines the equivalence relation. We have

$$r \sim r' \quad \Longleftrightarrow \quad r - r' \sim 0 \quad \Longleftrightarrow \quad r - r' \in I$$

and

$$r_1 r_2 \sim r_1' r_2' \quad \Longleftrightarrow \quad r_1 r_2 - r_1' r_2' \in I \quad \Longleftrightarrow \quad r_1(r_2 - r_2') + (r_1 - r_1') r_2' \in I$$

suggesting that I should be closed under left and right multiplication by any ring element $r \in R$:

$$rI \subseteq I, \ Ir \subseteq I \quad \Longrightarrow \quad rI = Ir = I$$

It motivates us to define the ideals of a ring:

Definition 1.2.1. Ideals

Suppose that R is a ring with identity and $I \subseteq R$ is a (not necessarily unital) subring of R. I is said to be a left (*resp.* right) ideal of R, if $rI = I$ (*resp.* $Ir = I$) for any $r \in R$.

I is said to be a **(two-sided) ideal** of R, if it is both a left and a right ideal. We denote it by $I \trianglelefteq R$.

If the ideal $I = \{0\}$ or R, we say that I is a **trivial ideal**. If $I \neq R$, we say that I is a **proper ideal** of R.

Remark. By definition, if $I \trianglelefteq R$, then $1 \in I \iff I = R$.

Proposition 1.2.2. Ideals in a Field

Suppose that F is a field. Then the only ideals in F are $\{0\}$ and F itself.

Proof. Suppose that $I \trianglelefteq F$. If $a \in I$ and $a \neq 0$, then $1 = aa^{-1} \in I$ and hence $I = F$. □

Proposition 1.2.3. Intersection of Ideals

Suppose that $\{I_j\}_{j\in J}$ is a family of ideals in R. Then $\bigcap_{j\in J} I_j$ is an ideal of R.

Proof. Trivial. □

Definition / Proposition 1.2.4. Ideal generated by a subset

Suppose that A is a subset of R. The following statements are equivalent:

1. I is the intersection of all ideals of R which contains A;
2. $I = \left\{ \sum_{i=1}^{n} r_i a_i s_i : \ a_i \in A,\ r_i, s_i \in R,\ n \in \mathbb{N} \right\}$

The ideal I satisfying any of the above conditions is called the ideal generated by A. We denote it by $I = \langle A \rangle$. If A is a finite set, then we say that I is **finitely generated**; if $A = \{a\}$ is a singleton, then we say that I is a **principal ideal**, and denote it by $I = \langle a \rangle$.

Proof. Clearly if J is an ideal such that $A \subseteq J$, then J must contain all elements of the form $\sum_{i=1}^{n} r_i a_i s_i$. On the other hand, the set of elements of the form $\sum_{i=1}^{n} r_i a_i s_i$ is an ideal of R (which is true only if R has an identity!) □

Definition 1.2.5. Principal Ideal Domains, Noetherian Rings

The CRI R is called a principal ideal domain (abbreviated PID), if all ideals of R are principal. The CRI R is called a Noetherian ring, if all ideals of R are finitely generated.

Remark. In Section 6.1 we shall give some equivalent formulations of Noetherian rings.

1.2.2 Quotient Rings and Isomorphism Theorems

Definition 1.2.6. Quotient Rings: Set-Theoretic Definition

The equivalence relation defined by $r \sim r' \iff r - r' \in I$ induces the quotient set R/I. The equivalence class of $r \in R$ in R/I is denoted by $r + I$ or $\overline{r}$. We define the ring structure on R/I by

$$\forall\, r_1, r_2 \in R: \quad (r_1 + I) + (r_2 + I) := (r_1 + r_2) + I$$
$$\forall\, r_1, r_2 \in R: \quad (r_1 + I) \cdot (r_2 + I) := (r_1 r_2) + I$$

It is immediate from the discussion at the beginning of this section that these operations are well-defined.

The **canonical projection** $\pi : R \twoheadrightarrow R/I$ is the ring epimorphism such that $\pi(r) = r + I$ for all $r \in R$. We have $\ker \pi = I$. In paricular, we have the following short exact sequence:

$$0 \longrightarrow I \xhookrightarrow{\iota} R \xrightarrow{\pi} R/I \longrightarrow 0$$

Remark. A sequence

$$\cdots \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \cdots$$

is said to be exact at B, if $\operatorname{im} f = \ker g$. In particular, a short sequence

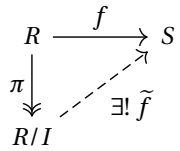
$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is said to be exact, if f is injective, g is surjective, and $\operatorname{im} f = \ker g$. We shall discuss the exact sequences of modules in Section 4.3.

Proposition 1.2.7. Quotient Rings: Universal Property

Suppose that R is a ring and I is an ideal of R. The quotient ring is the ring R/I with the canonical projection $\pi : R \twoheadrightarrow R/I$ satisfying the following universal perperty:

For any ring S and ring homomorphism $f : R \to S$ such that $I \subseteq \ker f$, there exists a unique ring homomorphism $\widetilde{f} : R/I \to S$ such that $f = \widetilde{f} \circ \pi$.



Moreover, any ring satisfying the universal property is uniquely determined up to ring isomorphism.

Remark. Given the set-theoretical definition of the quotient ring, the only choice of $\widetilde{f}$ is $\widetilde{f}(r + I) = f(r)$. Readers can check that it satisfies the universal property.

Lemma 1.2.8

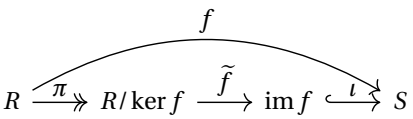
Suppose that $f : R \to S$ is a ring homomorphism. Then

1. $\ker f$ is an ideal of R;
2. $\operatorname{im} f$ is a subring of S.

Proof. Trivial. □

Theorem 1.2.9. Canonical Decomposition / First Isomorphism Theorem

Suppose that $f : R \to S$ is a ring homomorphism. Then the following diagram commutes:



In particular, $\widetilde{f}$ is an isomorphism between $R/\ker f$ and $\operatorname{im} f$.

Proof. Clearly f is a ring epimorphism from R to $\operatorname{im} f \subseteq S$. By universal property of the quotient ring, f induces $\widetilde{f} : R/\ker f \to \operatorname{im} f$. $\widetilde{f}$ is surjective because $f : R \to \operatorname{im} f$ is. $\widetilde{f}$ is injective because

$$f^{-1}(\{0\}) = \ker f \quad \Longrightarrow \quad \widetilde{f}^{-1}(\{0\}) = \{0\} + \ker f = \{\overline{0}\} \subseteq R/\ker f$$

Hence $\widetilde{f}$ is an isomorphism. $R/\ker f \cong \operatorname{im} f$. □

Theorem 1.2.10. Second Isomorphism Theorem

Suppose that I is an ideal of R and S is a subring of R. Then $I \cap S$ is an ideal of S and $I + S$ is a subring of R. In particular, we have the ring isomorphism:

$$\frac{S}{I \cap S} \cong \frac{I+S}{I}$$

Proof. Consider the composite ring homomorphism: $S \xhookrightarrow{\iota} S + I \xrightarrow{\pi} (S+I)/I$

It is not hard to see that $\pi \circ \iota$ is a ring epimorphism with kernel $\ker(\pi \circ \iota) = I \cap S$. The result follows by applying First Isomorphism Theorem 1.2.9 to $\pi \circ \iota$. □

Theorem 1.2.11. Third Isomorphism Theorem

Suppose that $I \trianglelefteq J \trianglelefteq R$. Then $J/I \trianglelefteq R/I$. In particular we have the ring isomorphism:

$$\frac{R/I}{J/I} \cong R/J$$

Proof. Consider the canonical projection $\pi_j : R \twoheadrightarrow R/J$. We have $I \subseteq J = \ker \pi_j$. By universal property 1.2.7 of quotient rings, π_j induces the ring epimorphism $\widetilde{\pi}_j : R/I \twoheadrightarrow R/J$ whose kernel is J/I. The result follows by applying First Isomorphism Theorem 1.2.9 to $\widetilde{\pi}_j$. □

1.2.3 Operations on Ideals

Definition 1.2.12. Ideal Operations

Suppose that $I, J \trianglelefteq R$. We define the sum of I and J to be:

$$I + J = \{i + j : \ i \in I, \ j \in J\}$$

We define the product of I and J to be:

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k : \ i_k \in I, \ j_k \in J, \ n \in \mathbb{N} \right\}$$

It is not hard to prove that $I + J$ and IJ are ideals of R. The union of I and J, however, is not an ideal in general.

Remark. The sum and product are associative and distributive:

$$I + (J + K) = (I + J) + K \qquad I(JK) = (IJ)K$$
$$(I + J)K = IK + JK \qquad I(J + K) = IJ + IK$$

The case involving intersection is more complicated. Readers can try to prove the following property:

$$I \cap (J + K) \supseteq I \cap J + I \cap K \qquad \text{with equality holds if } J \subseteq I \text{ or } K \subseteq I$$

Proposition 1.2.13. Ideal Contraction

Suppose that $f : R \to S$ is a ring homomorphism. For $J \trianglelefteq S$, $f^{-1}(J)$ is an ideal of R. In particular, f induces the injective map from the set of ideals of S to the set of ideals of R:

$$\{\text{ideals of } S\} \longrightarrow \{\text{ideals of } R\}$$
$$J \longmapsto f^{-1}(J)$$

Furthermore, f^{-1} preserves the inclusion relation:

$$J_1 \subseteq J_2 \implies f^{-1}(J_1) \subseteq f^{-1}(J_2)$$

Proof. Trivial. □

Corollary 1.2.14. Ideal Contraction for Quotient Rings

Suppose that I is an ideal of R. $\pi : R \twoheadrightarrow R/I$ is the canonical projection. Then π induces a bijective correspondence between the ideals of R/I and the ideals of R that contains I:

$$\{\text{ideals of } R/I\} \longleftrightarrow \{\text{ideals of } R \text{ containing } I\}$$
$$J/I \longmapsfrom J \supseteq I$$
$$K/I \longmapsto K$$

Definition 1.2.15. Ideal Extensions and Contractions

Suppose that $f : R \to S$ is a ring homomorphism. For $I \trianglelefteq R$, we define the extension of I to be the ideal in S generated by $f(I)$:

$$I^e := \langle f(I) \rangle \trianglelefteq S$$

For $J \trianglelefteq S$, we define the contraction of J to be the preimage of J under f:

$$J^c := f^{-1}(J) \trianglelefteq R$$

Notice that both extension and contraction preserve the order of ideals with repsect to inclusion.

Remark. Suppose that R is a subring of S. Then we usually talk about the ideal extension and contraction with respect to the inclusion map $\iota : R \hookrightarrow S$. In this case, we have $I^e = \langle I \rangle \trianglelefteq S$ and $J^c = R \cap J \trianglelefteq R$.

Proposition 1.2.16. Ideal Operations on Extensions and Contractions

1) $(I_1 + I_2)^e = I_1^e + I_2^e$
2) $(I_1 + I_2)^c \supseteq I_1^c + I_2^c$
3) $(I_1 I_2)^e = I_1^e I_2^e$
4) $(I_1 I_2)^c \supseteq I_1^c I_2^c$
5) $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$
6) $(I_1 \cap I_2)^c = I_1^c \cap I_2^c$

Proof. Everything follows directly from definition. □

Definition / Proposition 1.2.17. Coprime Ideals

Suppose that $I, J \trianglelefteq R$. We say that I and J are coprime, if $I + J = R$. If R is a CRI, then $I \cap J = IJ$.

Proof. It is clear that $IJ \subseteq I \cap J$. If R is a CRI and $I + J = R$, then there exists $a \in I, b \in J$ such that $a + b = 1$. For $r \in I \cap J$, $r = (a+b)r = ar + br \in IJ$. Hence we have $I \cap J \subseteq IJ$. □

Theorem 1.2.18. Chinese Remainder Theorem

Suppose that I and J are coprime ideals of R. Then we have the ring isomorphism:

$$\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}$$

Proof. Consider the ring homomorphism $f : R/(I \cap J) \to R/I \times R/J, \quad r + I \cap J \mapsto (r + I, r + J)$.
Readers can check that f is well-defined and bijective (the coprime condition is used in proving surjectivity). □

Definition 1.2.19. Ideal Quotient

Suppose that $I, J \trianglelefteq R$. We define the ideal quotient $(I : J)$ to be

$$(I : J) := \{r \in R : \ rJ \subseteq I\}$$

$(I : J)$ is an ideal of R.

1.3 Prime, Maximal and Radical Ideals

Throughout this section, we shall only consider commutative rings with identity.

1.3.1 Prime and Maximal Ideals

Definition 1.3.1. Prime Ideals, Prime Spectrum

Suppose that R is a CRI and P is a proper ideal of R. P is said to a prime ideal of R, if

$$\forall\, r, s \in R : \quad rs \in P \implies r \in P \vee s \in P$$

The set of prime ideals in R is called the prime spectrum of R and is denoted by $\operatorname{Spec} R$.

Remark. Equivalent, $P \trianglelefteq R$ is prime if for all $I_1, I_2 \trianglelefteq R$, $I_1 I_2 \subseteq P$ implies that either $I_1 \subseteq P$ or $I_2 \subseteq P$.

Definition 1.3.2. Maximal Ideals, Maximal Spectrum

Suppose that R is a CRI and M is a proper ideal of R. M is said to a maximal ideal of R, if no proper ideal of R contains M strictly.

The set of maximal ideals in R is called the maximal spectrum of R and is denoted by $\operatorname{MaxSpec} R$.

Proposition 1.3.3. Prime & Maximal Ideals v. Quotient Rings

Suppose that R is a CRI and I is a proper ideal of R.

1. I is prime if and only if R/I is an integral domain;
2. I is maximal if and only if R/I is a field.

Proof.

$$\begin{aligned} R/I \text{ is not an integral domain} &\iff \exists\, \overline{a}, \overline{b} \in (R/I) \setminus \{\overline{0}\} : \ \overline{a}\overline{b} = \overline{0} \\ &\iff \exists\, a, b \in R \setminus I : \ ab \in I \\ &\iff I \text{ is not prime.} \end{aligned}$$

$$\begin{aligned} I \text{ is maximal} &\iff \forall\, u \in R \setminus I : \ I + \langle u \rangle = R \\ &\iff \forall\, u \in R \setminus I \ \exists\, r \in R \ \exists\, a \in I : \ a + ru = 1 \\ &\iff \forall\, u \in R \setminus I \ \exists\, r \in R : \ \overline{ru} = \overline{1} \\ &\iff \forall\, u \in (R/I) \setminus \{\overline{0}\} : \ u \text{ is a unit} \\ &\iff R/I \text{ is a field.} \end{aligned}$$

□

Corollary 1.3.4. Maximal Ideal $\implies$ Prime Ideal

Every maximal ideal is prime.

Proposition 1.3.5. PID: Non-Zero Prime Ideal $\iff$ Maximal Ideal

Suppose that R is a principal ideal domain and I is a non-trivial ideal of R. Then I is prime if and only if I is maximal.

Proof. It suffices to prove that every non-trivial prime ideal is maximal. Suppose $\langle r\rangle$ is a non-trivial prime ideal and $a \notin \langle r\rangle$. Then $\langle a, r\rangle = \langle s\rangle$ for some $s \in R$. In particular, $r \in \langle s\rangle \implies r = us$ for some $u \in R$. Hence $us \in \langle r\rangle$. Since $\langle r\rangle$ is prime, either $u \in \langle r\rangle$ or $s \in \langle r\rangle$. If $s \in \langle r\rangle$, then $\langle r\rangle = \langle s\rangle = \langle a, r\rangle$, contradicting that $a \notin \langle r\rangle$. Therefore we must have $u \in \langle r\rangle$ and $u = br$ for some $b \in R$. Then $r = us = bsr \implies bs = 1 \implies s$ is a unit. Hence $\langle a, r\rangle = R \implies \langle r\rangle$ is maximal. □

Remark. As we will see in Section 6.6, Proposition 1.3.5 implies that PID have Krull dimension 1.

Theorem 1.3.6. Krull's Theorem

Every non-trivial CRI has a maximal ideal.

Proof. This is a standard application of **Zorn's Lemma**.

Let R be a CRI. Consider the set of all proper ideals $(\mathscr{S}, \subseteq)$ with a partial order given by set inclusion. $\mathscr{S}$ is non-empty as $\{0\} \in \mathscr{S}$. Suppose that $\{I_j : j \in J\} \subseteq \mathscr{S}$ is a chain of ideals. That is, for $i, j \in J$, either $I_i \subseteq I_j$ or $I_j \subseteq I_i$ (or both). Then $\bigcup\{I_j : j \in J\}$ is an ideal and is the upper bound of the chain. Since every chain of ideals has an upper bound, $\mathscr{S}$ has a maximal element, which is a maximal ideal of R by definition. □

Corollary 1.3.7

Every proper ideal of R is contained in some maximal ideal of R.

Proof. Suppose that I is a proper ideal R. In particular $R/I \neq \{0\}$. Applying Krull's Theorem 1.3.6 to R/I, we know that R/I has a maximal ideal J/I. Then J is a maximal ideal of R containing I. □

Corollary 1.3.8

Every non-unit of R is contained in some maximal ideal of R.

Proof. Suppose that $a \in R$ is not a unit. Hence $\langle a\rangle$ is a proper ideal of R. Then apply Corollary 1.3.7. □

Proposition 1.3.9. Minimal Prime Ideals

Suppose that R is a CRI. Then $\operatorname{Spec} R$ has a minimal prime ideal with respect to set inclusion.

Proof. This is again an application of Zorn's Lemma. Try to mimic the proof of Krull's Theorem 1.3.6. □

Proposition 1.3.10. Prime Avoidance

1. Suppose that $P_1, ..., P_n$ are prime ideals of R. I is an ideal of R such that $I \subseteq \bigcup_{i=1}^{n} P_i$. Then $I \subseteq P_i$ for some $i \in \{1, ..., n\}$.
2. Suppose that $I_1, ..., I_n$ are ideals of R. P is a prime ideal of R such that $P \supseteq \bigcap_{i=1}^{n} I_i$. Then $P \subseteq I_i$ for some $i \in \{1, ..., n\}$.

Proof. 1. We use induction on n to prove that if $I \not\subseteq P_i$ for all i then $I \not\subseteq \bigcup_{i=1}^{n} P_i$.

The base case $n = 1$ is trivial. Suppose that the result holds for $n-1$. Now assume that $I \not\subseteq P_i$ for $i \in \{1, ..., n\}$. For each $i \in \{1, ..., n\}$, we choose $r_i \in I$ such that $r_i \notin P_j$ for all $j \neq i$. If there is some i such that $r_i \notin P_i$, then $r_i \notin \bigcup_{k=1}^{n} P_k$ and the result is true. Otherwise we may assume that $r_i \in P_i$ for each i. Consider

$$s = \sum_{i=1}^{n} r_1 \cdots r_{i-1} r_{i+1} \cdots r_n \in I$$

We observe that the i-th term in s is not in P_i as P_i is prime, and the remaining terms are divisible by r_i, which implies that $s - r_1 \cdots r_{i-1} r_{i+1} \cdots r_n \notin P_i$. Hence $s \notin P_i$ and $s \notin \bigcup_{k=1}^{n} P_k$.

2. Suppose that $P \not\subseteq I_i$ for all i. Then for each i there exists $r_i \in I_i \setminus P$. We have $r_1 \cdots r_n \in \prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i$. But $r_1 \cdots r_n \notin P$ as P is prime. Hence $P \not\supseteq \bigcap_{i=1}^{n} I_i$. □

Proposition 1.3.11. Contraction of Prime Ideals

Suppose that $f : R \to S$ is a ring homomorphism. For a prime ideal $J \trianglelefteq S$, $f^{-1}(J)$ is an prime ideal of R. In particular, f induces the map $\operatorname{Spec}(f) : \operatorname{Spec} S \to \operatorname{Spec} R$:

$$\begin{aligned} \operatorname{Spec} S &\longrightarrow \operatorname{Spec} R \\ J &\longmapsto f^{-1}(J) \end{aligned}$$

Moreover, if f is surjective, then $\operatorname{Spec}(f)$ is injective.

Proof. Trivial. □

Remark. Prime ideals are preserved by ideal contractions. This is not true for maximal ideals in general.

Remark. In the following subsection we shall equip $\operatorname{Spec} R$ with the Zariski topology. Therefore Spec is a **contravariant functor** from Ring to Top.

1.3.2 Zariski Topology

Proposition 1.3.12

Suppose that R is a CRI and $A \subseteq R$. We define $\mathcal{V}(A)$ be the the set of all prime ideals in R that contains A. Then we have:

1. $A_1 \subseteq A_2 \implies \mathcal{V}(A_1) \supseteq \mathcal{V}(A_2)$;
2. $\mathcal{V}(A) = \mathcal{V}(\langle A \rangle)$;
3. $\mathcal{V}(\{0\}) = \varnothing, \quad \mathcal{V}(\{1\}) = \operatorname{Spec} R$;
4. $\mathcal{V}(A_1) \cup \mathcal{V}(A_2) = \mathcal{V}(\langle A_1 \rangle \langle A_2 \rangle) = \mathcal{V}(\langle A_1 \rangle \cap \langle A_2 \rangle)$;
5. $\mathcal{V}\left(\bigcup_{i \in I} A_i\right) = \bigcap_{i \in I} \mathcal{V}(A_i)$.

Proof. 1~3. Trivial.

4. We write $I_1 = \langle A_1 \rangle, I_2 = \langle A_2 \rangle$ for simplicity. By (2) we know $\mathcal{V}(A_1) = \mathcal{V}(I_1), \mathcal{V}(A_2) = \mathcal{V}(I_2)$.

   $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 I_2)$:

   By (1) we know that $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) \subseteq \mathcal{V}(I_1 I_2)$ as $I_1, I_2 \supseteq I_1 I_2$. For the other direction, suppose that $P \in \operatorname{Spec} R$ such that $P \notin \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$. That is, $I_1 \not\subseteq P$ and $I_2 \not\subseteq P$. Since P is prime, we have $I_1 I_2 \not\subseteq P \implies P \notin \mathcal{V}(I_1 I_2)$. Hence $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) \supseteq \mathcal{V}(I_1 I_2)$.

   $\mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1 I_2)$:

   By (1) we know that $\mathcal{V}(I_1 \cap I_2) \subseteq \mathcal{V}(I_1 I_2)$ since $I_1 I_2 \subseteq I_1 \cap I_2$. For the other direction, suppose that $P \subseteq \mathcal{V}(I_1 I_2)$. Then $I_1 I_2 \subseteq P$. Since P is prime we have either $I_1 \subseteq P$ or $I_2 \subseteq P$. In particular $I_1 \cap I_2 \subseteq P$. We conclude that $\mathcal{V}(I_1 \cap I_2) \supseteq \mathcal{V}(I_1 I_2)$.

5. For $P \in \operatorname{Spec} R$:

$$P \in \mathcal{V}\left(\bigcup_{i \in I} A_i\right) \iff \bigcup_{i \in I} A_i \subseteq P \iff \forall\, i \in I :\ A_i \subseteq P \iff \forall\, i \in I :\ P \in \mathcal{V}(A_i) \iff P \in \bigcap_{i \in I} \mathcal{V}(A_i)$$

□

Definition 1.3.13. Zariski Topology on the Prime Spectrum

Suppose that R is a CRI and $A \subseteq R$. From the above proposition we know that sets $\mathcal{V}(A)$ satisfies the topological axioms for closed sets. This defines a topology on the prime spectrum $\operatorname{Spec} R$, which is called the **Zariski topology**.

Remark. Unfortunately, the Zariski topology could be quite nasty: every non-trivial open set in $\operatorname{Spec} R$ is dense in $\operatorname{Spec} R$. The space is not Hausdorff. In fact it is not even T_1 since the singleton closed subsets of $\operatorname{Spec} R$ are exactly the maximal ideals.

Lemma 1.3.14. Zariski Topology: T_0-Axiom

Suppose that R is a CRI and $\operatorname{Spec} R$ is the prime spectrum with the Zariski topology. Then $\operatorname{Spec} R$ satisfies the T_0 separation axiom.[a]

[a] A topological space X is said to satisfy the T_0-axiom, if for any distinct points $x, y \in X$, there is either a neighborhood N_x of x not containing y, or a neighborhood N_y of y not containing x.

Proof. First we shall prove that the closure of a point P in $\operatorname{Spec} R$ is $\overline{\{P\}} = \mathcal{V}(P)$:

$$\overline{\{P\}} = \bigcap \{\mathcal{V}(I) : P \in \mathcal{V}(I)\} = \mathcal{V}\left(\bigcup \{I : P \in \mathcal{V}(I)\}\right) = \mathcal{V}\left(\bigcup \{I : I \subseteq P\}\right) = \mathcal{V}(P)$$

The second equality follows from Proposition 1.3.13 (5).

Second, suppose that $P_1, P_2 \in \operatorname{Spec} R$ such that every neighborhood of P_1 contains P_2 and *vise versa*. Then $P_1 \in \overline{\{P_2\}} = \mathcal{V}(P_2)$ and $P_2 \in \overline{\{P_1\}} = \mathcal{V}(P_1)$. Therefore $P_2 \subseteq P_1$ and $P_1 \subseteq P_2$. P_1 and P_2 are the same ideal. □

Proposition 1.3.15. Compactness of Zariski Topology

The prime spectrum $\operatorname{Spec} R$ with Zariski topology is compact.

Proof. Let $\{A_i\}_{i \in I}$ be a family of ideals of R such that $\bigcap_{i \in I} \mathcal{V}(A_i) = \varnothing$. As $\bigcap_{i \in I} \mathcal{V}(A_i) = \mathcal{V}\left(\sum_{i \in I} A_i\right)$, we have $\sum_{i \in I} A_i = R$. In particular $1 \in \sum_{i \in I} A_i$. We write

$$1 = \sum_{k=1}^{n} r_{i_k} \in \sum_{k=1}^{n} A_{i_k}$$

Then $\sum_{i \in I} A_i = \sum_{k=1}^{n} A_{i_k}$ and therefore $\bigcap_{k=1}^{n} \mathcal{V}(A_{i_k}) = \varnothing$. $\operatorname{Spec} R$ is compact under the Zariski topology. □

1.3.3 Radical Ideals

Definition 1.3.16. Radicals

Suppose that R is a CRI and I is an ideal of R. Then we define the radical of I to be

$$\sqrt{I} := \{r \in R : \exists\, n \in \mathbb{Z}_+ \ (r^n \in I)\}$$

$I \trianglelefteq R$ is called a **radical ideal**, if $I = \sqrt{I}$.

Proposition 1.3.17. Radicals and Ideal Operations

1. The radical $\sqrt{I}$ of ideal I is an ideal;
2. $I_1 \subseteq I_2 \implies \sqrt{I_1} \subseteq \sqrt{I_2}$;
3. $\sqrt{\sqrt{I}} = \sqrt{I}$;
4. $\sqrt{I_1 I_2} = \sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$;
5. $\sqrt{I_1 + I_2} = \sqrt{\sqrt{I_1} + \sqrt{I_2}}$;
6. $\sqrt{P} = P$ for $P \in \operatorname{Spec} R$.

Proof. I only want to give a hint to the proof of (1): if $r,s \in \sqrt{I}$, then there are $m,n \in \mathbb{Z}_+$ such that $r^m, s^n \in I$. Then by binomial theorem

$$(r-s)^{mn} = \sum_{i=0}^{mn} (-1)^i \binom{mn}{i} s^i r^{mn-i} \in I$$

Hence $r-s \in \sqrt{I}$. □

Definition / Proposition 1.3.18. Nilpotent Elements, Nilradical

Suppose that R is CRI. $r \in R$ is said to be nilpotent, if there exists $n \in \mathbb{Z}_+$ such that $r^n = 0$.

Suppose that $I \subseteq R$. The following statements are equivalent:

1. I is the set of all nilpotent elements of R;
2. $I = \sqrt{\{0\}}$
3. $I = \bigcap \operatorname{Spec} R$.

The subset I satisfying one of the above statement is called the nilradical of R and is denoted by $N(R)$. In particular $N(R)$ is a radical ideal.

If $N(R) = \{0\}$, then R is called a **reduced ring**.

Proof. (2) is just a rephrase of (1) using the language of radical.

Suppose that $r \in R$ is nilpotent. For each $P \in \operatorname{Spec} R$, $r^n = 0 \in P \Longrightarrow r \in P$. Hence $r \in \bigcap \operatorname{Spec} R$.

Suppose that $r \in R$ is not nilpotent. Let $\mathscr{S} := \{I \trianglelefteq R : \ r \notin \sqrt{I}\}$. $\mathscr{S}$ is non-empty as $\{0\} \in \mathscr{S}$. By Zorn's Lemma, $\mathscr{S}$ has a maximal element P. For any $a, b \notin P$, we have $P \subsetneq P + \langle a \rangle$ and $P \subsetneq P + \langle b \rangle$. By maximality of P, $r \in \sqrt{P + \langle a \rangle}$ and $r \in \sqrt{P + \langle b \rangle}$. By Proposition 1.3.17 (4), $r \in \sqrt{P + \langle a \rangle} \cap \sqrt{P + \langle b \rangle} = \sqrt{(P + \langle a \rangle)(P + \langle b \rangle)} = \sqrt{P + \langle ab \rangle}$. Hence $P \subsetneq P + \langle ab \rangle$ and $ab \notin P$. Hence P is a prime ideal. Since $r \notin \sqrt{P} = P$, we have $r \notin \bigcap \operatorname{Spec} R$. □

Corollary 1.3.19. $\sqrt{I}/I = N(R/I)$

Suppose that R is a CRI and I is an ideal of R. Then $\sqrt{I}/I = N(R/I)$.

Corollary 1.3.20. $\sqrt{I} = \bigcap \{P \in \operatorname{Spec} R : \ I \subseteq P\}$

Suppose that R is a CRI and I is an ideal of R. Then $\sqrt{I} = \bigcap \{P \in \operatorname{Spec} R : \ I \subseteq P\}$.

Corollary 1.3.21. $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$

Suppose that R is a CRI and I is an ideal of R. Then $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.

Definition 1.3.22. Jacobson Radical

Suppose that R is CRI. We define the **Jacobson radical of *R*** to be the intersection of all maximal ideals of R:

$$J(R) := \bigcap \operatorname{MaxSpec} R$$

For $I \lhd R$, we define the **Jacobson radical of *I*** to be the intersection of all maximal ideals of R *that contain* I.

Remark. It is immediate from the definition that $N(R) \subseteq J(R)$. In Section 6.7.3, we shall study the **Jacobson rings**, whose nilradical $N(R)$ and Jacobson radical $J(R)$ coincide.

Proposition 1.3.23. Jacobson Radical and Units

Suppose that R is CRI and $r \in R$. Then $r \in J(R)$ if and only if $1 - rs$ is a unit of R for all $s \in R$.

Proof. "$\Longrightarrow$": Suppose that $r \in J(R)$ and $1 - rs \in R$ is not a unit. Then $1 - rs$ is contained in a maximal ideal M by Corollary 1.3.8. As $r \in J(R) \subseteq M$, we have $1 \in M$ which is a contraction.

"$\Longleftarrow$": Suppose that $r \notin J(R)$. Then there exists a maximal ideal M such that $M + \langle r \rangle = R$. Then $a + rs = 1$ for some $a \in M$ and $s \in R$. Hence $1 - rs = a \in M$ is not a unit. □

1.4 Rings of Polynomials and Formal Power Series

The polynomials have been the central objects of algebra. We shall present some equivalent definitions of the polynomial ring over a ring in this section.

Throughout this section, we shall only consider commutative rings with identity.

1.4.1 Polynomial Rings

Definition 1.4.1. Generating Subrings, Polynomials

Suppose that R is a CRI and $R \subseteq S$ is a ring extension. For $u \in S$, we consider the set

$$R[u] := \left\{a_0 + a_1 u + \cdots + a_n u^n : \ a_0, ..., a_n \in R, \ n \in \mathbb{N}\right\}$$

$R[u]$ is called the subring generated by u on R. The elements of $R[u]$ are called **polynomials** of u on R.

Remark. The polynomial $f(u) = a_0 + a_1 u + \cdots + a_n u^n \in R[u]$ such that $f(u) = 0$ is called an **algebraic relation** of u on R. We can define the ring of polynomial on R to be the extended ring $R[x]$ on an element x (called an **indeterminate**) with the trivial algebraic relation.

We shall present a set-theoretic formal definition of the ring of (single-variable) polynomials.

Definition 1.4.2. Polynomial Rings, Set-Theoretic Definition

Suppose that R is a CRI. We define the polynomial ring $R[x]$ to be the set of finite sequences of R:

$$R[x] := \{(a_0, a_1, \cdots) : \ a_0, a_1, \cdots \in R, \ \exists N \in \mathbb{N} \ \forall n > N (a_n = 0)\}$$

with addition:

$$\forall \ \{a_n\}, \{b_n\} \in R[x] : \quad \{a_n\} + \{b_n\} = \{c_n\}, \quad \text{where } c_n = a_n + b_n$$

and multiplication:

$$\forall \ \{a_n\}, \{b_n\} \in R[x] : \quad \{a_n\} \cdot \{b_n\} = \{c_n\}, \quad \text{where } c_n = \sum_{i=0}^{n} a_i b_{n-i}$$

Remark. From the definition of $R[x]$ we immediately obtain an embedding $r \mapsto (r, 0, 0, \cdots)$ from R to $R[x]$. Hence we can identify R as a subring of $R[x]$ and denote $(1, 0, 0, \cdots)$ by 1. It is common to denote $(0, 1, 0, \cdots)$ by x. It follows from induction that $x^n = (0, \cdots, 0, 1, 0, \cdots)$, where 1 is in the $(n+1)$-st coordinates. Therefore we have:

$$(a_0, a_1, \cdots, a_n, 0, 0 \cdots) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$$

which is the usual way of writing a polynomial.

If we relax the condition of finite sequences, we will obtain the ring of formal power series:

Definition 1.4.3. Rings of Formal Power Series

Suppose that R is a CRI. We define the ring of formal power series $R[[x]]$ to be the set of finite sequences of R:

$$R[[x]] := \{(a_0, a_1, \cdots) : \ a_0, a_1, \cdots \in R\}$$

with addition:

$$\forall \ \{a_n\}, \{b_n\} \in R[[x]] : \quad \{a_n\} + \{b_n\} = \{c_n\}, \quad \text{where } c_n = a_n + b_n$$

and multiplication:

$$\forall \ \{a_n\}, \{b_n\} \in R[[x]] : \quad \{a_n\} \cdot \{b_n\} = \{c_n\}, \quad \text{where } c_n = \sum_{i=0}^{n} a_i b_{n-i}$$

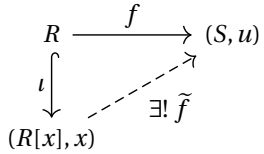
Remark. There is a natural embedding $R[x] \hookrightarrow R[[x]]$. As a subring of $R[[x]]$, $R[x]$ is generated by R and x.

From the discussion at the beginning of this section, we can formulate the universal property of polynomial rings as follows:

Proposition 1.4.4. Polynomial Rings, Universal Property

Suppose that R is a CRI. The polynomial ring is the ring $R[x]$ with the embedding $\iota : R \hookrightarrow R[x]$ satisfying the following universal property:

For any CRI S, $u \in S$, and unital ring homomorphism $f : R \to S$, there exists a unique ring homomorphism $\widetilde{f} : R[x] \to S$ such that $\widetilde{f} \circ \iota = f$ and $\widetilde{f}(x) = u$.



Moreover, any ring satisfying the universal property is uniquely determined up to ring isomorphism.

The homomorphism $\widetilde{f}$ is called the **evalution homomorphism** and is sometimes denoted by ev_u.

Remark. In proving that the set-theoretic definition implies the universal property the only interesting part is the uniqueness. We consider a category C[1] whose objects are 3-tuples (f, S, u) where f, S and u are defined as above. A morphism in C

$$(f, S, u) \xrightarrow{\varphi} (g, T, w)$$

is a unital ring homomorphism $\varphi : S \to T$ such that $\varphi \circ f = g$ and $\varphi(u) = w$. It is not hard to show that φ is an isomorphism between objects (f, S, u) and (g, T, w) if and only if $\varphi : S \to T$ is a ring isomorphism. Finally, one shall prove that $(\iota, R[x], x)$ is an initial object of C so that $R[x]$ is unique up to ring isomorphism.

Proposition 1.4.5

Suppose that R and S are CRI and $R \subseteq S$. For $u \in S$, there exists an ideal $I \trianglelefteq R[x]$ such that $R[u] \cong R[x]/I$ and that $I \cap R = \{0\}$.

Proof. Apply First Isomorphism Theorem 1.2.9 to the evalution homomorphism. We have $\ker \mathrm{ev}_u = I$ and $\mathrm{im}\, \mathrm{ev}_u = R[u]$. $I \cap R = \{0\}$ because it is the kernel of the embedding ι. □

Proposition 1.4.6

Suppose that R is a CRI and I is an ideal of R. Then $I[x] := I + \langle x \rangle$ is an ideal of $R[x]$. We have $R[x]/I[x] \cong (R/I)[x]$. In particular, if $I \trianglelefteq R$ is prime, then $I[x] \trianglelefteq R[x]$ is also prime.

Proof. Consider the composite ring homomorphism: $R \xrightarrow{\pi} R/I \xhookrightarrow{\iota} (R/I)[x]$

By universal property of $R[x]$, $\iota \circ \pi$ induces a ring homomorphism $\varphi : R[x] \to (R/I)[x]$ such that $\varphi(r) = \overline{r} = r + I$ and $\varphi(x) = x$. It is not hard to verify that φ is surjective and $\ker \varphi = I[x]$. By First Isomorphism Theorem 1.2.9, $R[x]/I[x] \cong (R/I)[x]$.

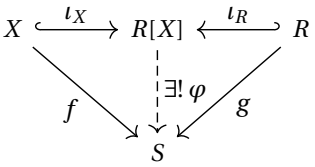
If $I \trianglelefteq R$ is prime, then by Proposition 1.3.3 R/I is an integral domain. By Proposition 1.4.9, $(R/I)[x] \cong R[x]/I[x]$ is also an integral domain. By Proposition 1.3.3, $I[x] \trianglelefteq R[x]$ is prime. □

Remark. The universal property of single-variable polynomial rings can be easily generalised to polynomial rings with arbitrarily many indeterminates.

Definition 1.4.7. Polynomial Rings with arbitrarily many Indeterminates

Suppose that R is a CRI and X is a set. The polynomial ring of X on R is the ring $R[X]$ with the ring monomorphism $\iota_R : R \hookrightarrow R[X]$ and injective map $\iota_X : X \hookrightarrow R[X]$ satisfying the following universal property:

For any CRI S, map $f : X \to S$, and unital ring homomorphism $g : R \to S$, there exists a unique ring homomorphism $\varphi : R[X] \to S$ such that $\varphi \circ \iota_X = f$ and $\varphi \circ \iota_R = g$.



[1] This is an example of what is called **comma category**.

Remark. Notice that ι_X and f are maps between sets, whereas ι_R and g are ring homomorphisms.

Remark. If X is a finite set (e.g. $|X| = n$), it is common to denote $R[X]$ by $R[x_1, ..., x_n]$. The traditional way to define $R[x_1, .., x_n]$ is as follows. First we define $R[x_1]$. Next, $R[x_1, x_2]$ is defined by $R[x_1][x_2]$, the (single-variable) polynomial ring on $R[x_1]$. Inductively we can define $R[x_1, .., x_n]$. The polynomial ring on countably many indeterminates

$$R[x_1, x_2, ...] = \bigcup_{n\in\mathbb{N}} R[x_1, ..., x_n]$$

If we wish to define the polynomial ring with uncountably many indeterminates, however, using universal property might be the best way.

Remark. The results in Proposition 1.4.5 and 1.4.6 can be easily generalised to polynomial rings of several indeterminates by induction.

1.4.2 Zero-Divisors and Units in Polynomial Rings

Lemma 1.4.8. Zero-Divisors in $R[x]$

$f \in R[x]$ is a zero-divisor if and only if there exists $a \in R \setminus \{0\}$ such that $af = 0$.

Proof. "$\Longleftarrow$": Trivial.

"$\Longrightarrow$": Suppose that $g \in R[x] \setminus \{0\}$ is the polynomial of minimal degree such that $fg = 0$. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$.

Assume that there is a smallest integer k such that $a_k g \neq 0$. Then $f(x)g(x) = \left(\sum_{i=0}^{k} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = 0$. In particular $a_k b_m = 0$.

We have $\deg(a_k g) < \deg g$ and $f \cdot a_k g = 0$, contradicting the minimality of the degree of g. Hence $a_0 g = \cdots = a_n g = 0 \Longrightarrow a_0 b_m = \cdots = a_n b_m = 0 \Longrightarrow b_m f = 0$. By minimality of $\deg g$, we must have $\deg g = 0$ and the result follows. □

Proposition 1.4.9. R Integral Domain $\Longleftrightarrow$ $R[x]$ Integral Domain

R is an integral domain if and only if $R[x]$ is an integral domain.

Proof. "$\Longleftarrow$": It follows from that R is a subring of $R[x]$.

"$\Longrightarrow$": Suppose that R is an integral domain and $f \in R[x]$ is a zero-divisor. By Lemma 1.4.8 there exists $a \in R \setminus \{0\}$ such that $af = 0$. If b is the leading coefficient of f, then $ab = 0$ and hence $b = 0$. It follows that $f = 0$, which is a contradiction. Hence $R[x]$ has no zero-divisors. □

Lemma 1.4.10. Nilpotents and Units

Suppose that R is a CRI. If $r \in R$ is nilpotent, then $1 + r$ is a unit.

Proof. If r is nilpotent, then so is $s = -r$. Suppose that $n \in \mathbb{N}$ is the least integer such that $s^n = 0$. Then

$$1 = 1 - s^n = (1 - s)(1 + s + \cdots + s^{n-1})$$

Hence $1 + r = 1 - s$ is a unit. □

Proposition 1.4.11. Units in $R[x]$

For $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$, $f \in R[x]$ is a unit if and only if $a_0 \in R$ is a unit and $a_1, ..., a_n \in R$ are nilpotent.

Proof. "$\Longleftarrow$" Suppose a_0 is a unit and $a_1, ..., a_n$ are nilpotent. Then $a_1 x, ..., a_n x^n$ are all nilpotent elements in $R[x]$. Then f is the sum of a unit a_0 and a nilpotent polynomial. By Lemma 1.4.10 f is a unit in $R[x]$.

"$\Longrightarrow$" Suppose $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ is the inverse of f. For simplicity, we put $a_i = b_j = 0$ for $i \notin \{0, .., n\}$ and $j \notin \{0, ..., m\}$. We have:

$$1 = (a_0 + \cdots + a_n x^n)(b_0 + \cdots + b_m x^m) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + \sum_{i=0}^{n+m} a_i b_{n+m-i} x^{n+m}$$

Comparing the coefficients we obtain:

$$a_0 b_0 = 1;\ \ a_0 b_1 + a_1 b_0 = 0;\ \ \cdots \sum_{i=0}^{n+m} a_i b_{n+m-i} = 0$$

The first equality implies that a_0 is a unit.

We shall prove by induction on r that $a_n^{r+1} b_{m-r} = 0$. For $r = 0$, $a_n b_m$ is the coefficient of x^{n+m} and is equal to 0. Suppose the relation holds for all $r < r_0$. Then for $r = r_0$, the coefficient of x^{n+m-r} is given by $a_n b_{m-r} + a_{n-1} b_{m-r+1} + \cdots + a_{n-r} b_m$. We have:

$$a_n^{r+1} b_{m-r} = -a_n^r (a_{n-1} b_{m-r+1} + \cdots + a_{n-r} b_m) = -(a_{n-1} \cdot a_n^r b_{m-r+1} + \cdots + a_{n-r} a_n^{r-1} \cdot a_n b_m) = 0$$

If a_n is not nilpotent, then $a_n^{r+1} \neq 0$ for all $r \in \mathbb{N}$. Then $b_0 = \cdots = b_m = 0$ and $g = 0$, contradicting that g is the inverse of a unit in $R[x]$. Hence a_n is nilpotent. In particular $a_n^{m+1} = 0$. Hence $-a_n x^n \in R[x]$ is also nilpotent. By Lemma 1.4.10,

$$f(x) - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

is a unit. Following the same argument we can deduce that a_{n-1} is nilpotent. Recursively, $a_1, ..., a_n$ are all nilpotent elements. □

Proposition 1.4.12. Units in $R[[x]]$

For $f(x) \in \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$, $f \in R[[x]]$ is a unit if and only if $a_0 \in R$ is a unit.

Proof. "$\Longrightarrow$" Take $g = \sum_{n=0}^{\infty} b_n x^n$ such that $fg = 1$. Then we have $a_0 b_0 = 1$. Hence a_0 is a unit.

"$\Longleftarrow$" We wish to construct $g = \sum_{n=0}^{\infty} b_n x^n$ such that $fg = 1$. By comparing the coefficients, we must have:

$$a_0 b_0 = 1; \;\; a_0 b_1 + a_1 b_0 = 0; \;\; \cdots \;\; \sum_{i=0}^{n} a_i b_{n-i} = 0 \;\; (\forall n \in \mathbb{Z}_+)$$

The first equality suggests that $b_0 = a_0^{-1} \neq 0$ because a_0 is a unit. Therefore we can solve each b_n successively by multiplying b_0 in every equations. Explicitly, suppose that we have solved $b_0, ..., b_n$. Then b_{n+1} is given by:

$$b_{n+1} = -b_0 \left(\sum_{i=0}^{n} a_{i+1} b_{n-i} \right)$$

Hence there exists $g \in R[[x]]$ such that $fg = 1$. f is a unit in $R[[x]]$. □

Corollary 1.4.13. Jacobson Radical of $R[[x]]$

For $f(x) \in \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$, $f \in J(R[[x]])$ if and only if $a_0 \in J(R)$.

Proof. It follows immediately from Proposition 1.4.12 and 1.3.23:

$$\begin{aligned} a_0 \in J(R) &\Longleftrightarrow \forall\, b_0 \in R: \quad 1 - a_0 b_0 \text{ is a unit} \\ &\Longleftrightarrow \forall\, g = \sum_{n=0}^{\infty} b_n x^n \in R[[x]]: \quad 1 - fg \text{ is a unit} \\ &\Longleftrightarrow f \in J(R[[x]]) \end{aligned}$$

□

Corollary 1.4.14. $F[[x]]$ as a Local Ring

Suppose that F is a field. Then $F[[x]]$ has the unique maximal ideal $\langle x \rangle$.

Proof. Suppose that I is a proper ideal of $F[[x]]$. For $f \in I$, f is not a unit. Since F is field, the constant coefficient a_0 of f is zero by Proposition 1.4.12. Hence $f \in \langle x \rangle$ and $I \subseteq \langle x \rangle$. Therefore $\langle x \rangle$ is the unique maximal ideal. □

Remark. If a ring R has a unique maximal ideal M, then the Jacobson radical $J(R) = M$. We say that R is a **local ring**. The field R/M is called the **residue field** of R.

1.5 Rings and Fields of Fractions

Throughout this section, we shall only consider commutative rings with identity.

1.5.1 Field of Fractions

Definition 1.5.1. Fields of Fractions, Set-Theoretic Definition

Suppose that R is an integral domain. We define an equivalence relation on $R \times R^\times$ by

$$(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1$$

The equivalence class of (r, s) in $(R \times R^\times)/\sim$ is denoted by r/s. We define a ring structure on $F(R) := (R \times R^\times)/\sim$ by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

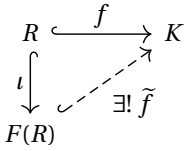
It is not hard to verify (though requires many details) that:

1. The operations are well-defined;
2. $F(R)$ forms a field with $0_{F(R)} = 0_R/1_R$ and $1_{F(R)} = 1_R/1_R$;
3. $r \mapsto r/1_R$ is an embedding of R into $F(R)$.

Proposition 1.5.2. Fields of Fractions, Universal Property

Suppose that R is an integral domain. The field of fractions of R is the field $F(R)$ with the ring monomorphism $\iota : R \hookrightarrow F(R)$ satisfying the following universal property:

For any field K and ring monomorphism $f : R \hookrightarrow K$, there exists a unique field monomorphism $\widetilde{f} : F(R) \hookrightarrow K$ such that $f = \widetilde{f} \circ \iota$.



F is unique up to field isomorphism.

In other words, $F(R)$ is **the smallest field that contains R.**

Remark. Consider the category C_R whose objects are pairs (f, K) where f and K are defined as above. A morphism in C_R

$$(f, K) \xrightarrow{\varphi} (g, L)$$

is a field homomorphism $\varphi : K \to L$ such that $g = \varphi \circ f$. Then $(\iota, F(R))$ is an initial object in C_R.

Example 1.5.3. Examples of Fields of Fractions

1. The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$;
2. If F is a field, then the field of fractions of $F[x]$ is $F(x)$, which is the set of all rational functions on F.
3. The field of fractions of $\mathbb{Z}[x]$ is $\mathbb{Q}(x)$.

1.5.2 Rings of Fractions

Next we shall generalise the construction above to a broader class of objects, rings of fractions.

Definition 1.5.4. Multiplicative Subsets

Suppose that R is a CRI and $S \subseteq R$. S is called a multiplicative subset of R, if $1 \in S$ and $a, b \in S \implies ab \in S$.

Proposition 1.5.5. Multiplicative Subsets and Prime Ideals

Suppose that I is a proper ideal of R. I is a prime ideal if and only if $R \setminus I$ is a multiplicative subset.

Proof. Trivial by definition. □

Definition 1.5.6. Rings of Fractions, Set-Theoretic Definition

Suppose that R is a CRI and $S \subseteq R$ is a multiplicative subset. We define an equivalence relation on $R \times S$ by

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists s \in S : \ s(r_1 s_2 - r_2 s_1) = 0$$

The equivalence class of (r, s) in $(R \times S)/\sim$ is denoted by r/s. We define a ring structure on $S^{-1}R := (R \times S)/\sim$ by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

By essentially the same argument we can verify that:

1. The operations are well-defined;
2. $S^{-1}R$ forms a CRI with $0_{S^{-1}R} = 0_R/1_R$ and $1_{S^{-1}R} = 1_R/1_R$;
3. $\varphi_S : R \to S^{-1}R$ given by $\varphi_S(r) = r/1_R$ is a ring homomorphism but is *not injective in general.*

Remark. Notice that if $0 \in S$, then $S^{-1}R$ is the trivial ring because $R \times S$ has only one equivalence class.

Remark. If R is an integral domain and $0 \notin S$, then $S^{-1}R$ is also an integral domain, and $\varphi_S : r \mapsto r/1_R$ is injective. In particular, if $S = R^\times$, then the ring of fractions $S^{-1}R$ coincides with the field of fractions $F(R)$.

Proposition 1.5.7. Properties of φ_S

Suppose that R is a CRI and $S^{-1}R$ is a ring of fractions of R. $\varphi_S : R \to S^{-1}R$ is given by $\varphi_S(r) = r/1_R$. Then:

1. $\varphi_S(s)$ is a unit in $S^{-1}R$ for $s \in S$;
2. $\ker \varphi_S = \{r \in R : \ \exists s \in S \ (rs = 0)\}$;
3. Every element of $S^{-1}R$ is of the form $\varphi_S(r)\varphi_S(s)^{-1}$ for some $r \in R$ and $s \in S$.

Proof.

1. $\varphi_S(s) = s/1_R$ has an inverse $1_R/s$ in $S^{-1}R$;
2. Trivial by definition;
3. $r/s = r/1_R \cdot (s/1_R)^{-1} = \varphi_S(r)\varphi_S(s)^{-1}$.

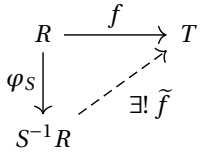
□

Remark. These properties of $\varphi_S : R \to S^{-1}R$ motivates us to consider the universal property of rings of fractions.

Proposition 1.5.8. Rings of Fractions, Universal Property

Suppose that R is a CRI and $S \subseteq R$ is a multiplicative subset. The ring of fractions of R with respect to S is the ring $S^{-1}R$ with a ring homomorphism $\varphi_S : R \to S^{-1}R$ satisfying the following universal property:

For any CRI T and ring homomorphism $f : R \to T$ such that $f(s)$ is a unit in T for all $s \in S$, there exists a unique ring homomorphism $\widetilde{f} : S^{-1}R \to T$ such that $f = \widetilde{f} \circ \varphi_S$.



$S^{-1}R$ is unique up to ring isomorphism.

Remark. Suppose that $S^{-1}R$ is given by the set-theoretic definition. The only choice of $\widetilde{f}$ is given by $\widetilde{f}(r/s) = f(r)f(s)^{-1}$. The details are left to readers. We should be already familiar in the techinques of proving the uniqueness. Consider a category $\mathsf{C}_{R,S}$, whose objects are (f, T), where f and T are defined as above. A morphism in $\mathsf{C}_{R,S}$

$$(f,T) \xrightarrow{\psi} (g,U)$$

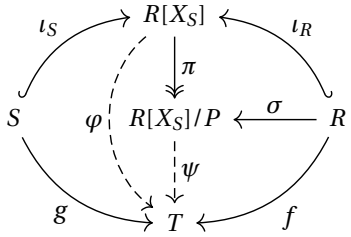
is a ring homomorphism $\psi : T \to U$ such that $g = \psi \circ f$. Then $(\varphi_S, S^{-1}R)$ is an initial object in $\mathsf{C}_{R,S}$.

Proposition 1.5.9. Ring of Fractions as a Quotient of Polynomial Ring

Suppose that R is a CRI and $S \subseteq R$ is a multiplicative subset. We consider a copy of S as indeterminates: $X_S := \{x_s : s \in S\}$. Then we have a ring isomorphism:

$$S^{-1}R \cong \frac{R[X_S]}{\langle \{sx_s - 1_R : s \in S\} \rangle}$$

Proof. Let $P = \langle \{sx_s - 1_R : s \in S\} \rangle$. It suffices to check that $R[X_S]/P$ satisfies the universal property of $S^{-1}R$. For a CRI T and a ring homomorphism $f : R \to T$ such that $f(s)$ is a unit in T for any $s \in S$. We consider the following diagram, which is a combination of the diagrams in 1.2.7, 1.4.7, and 1.5.8:



In the diagram, ι_R is the embedding of R into $R[X_S]$; $\iota_S : S \hookrightarrow R[X_S]$ is given by $\iota_S(s) = x_s$; $\pi : R[X_S] \twoheadrightarrow R[X_S]/P$ is the canonical projection; $\sigma := \pi \circ \iota_R$.

Since $f(s)$ is a unit in T for each $s \in S$, there exists $a_s \in S$ such that $a_s f(s) = 1$. $g : S \to T$ is given by $g(s) = a_s$.

By universal property of $R[X_S]$, there exists a unique ring homomorphism $\varphi : R[X_S] \to T$ such that the diagram commutes. In particular, $\varphi(x_s) = \varphi \circ \iota_S(s) = g(s) = a_s$ and $\varphi(s) = f(s)$. We have $\varphi(sx_s - 1) = a_s f(s) - 1 = 0$ for any $s \in S$. Hence $sx_s - 1 \in \ker\varphi$ for any $s \in S$. Then $P \subseteq \ker\varphi$. By universal property of $R[X_S]/P$, there exists a unique ring homomorphism $\psi : R[X_S]/P \to T$ such that the diagram commutes. As $f = \psi \circ \sigma$, we have shown that $R[X_S]/P$ satisfies the universal property of $S^{-1}R$. □

1.5.3 Ideal Extensions and Localisations

Definition / Proposition 1.5.10. Ideal Extension of φ_S

Suppose that R is a CRI and $S^{-1}R$ is a ring of fractions of R. $\varphi_S : R \to S^{-1}R$ is given by $\varphi_S(r) = r/1_R$. $S^{-1}I = \{a/s \in S^{-1}R : a \in I, s \in S\}$ is an ideal in $S^{-1}R$. It is the extension of I under the homomorphism φ_S.

Remark. It is not true general that $r/s \in S^{-1}I$ implies that $r \in I$. It could be the case that $r/s = r'/s'$, where $r' \in I$ and $r \notin I$.

Proposition 1.5.11. Properties of Ideal Extension of φ_S

1. Every ideal in $S^{-1}R$ is an extended ideal;
2. $S^{-1}I_1 + S^{-1}I_2 = S^{-1}(I_1 + I_2)$;
3. $(S^{-1}I_1)(S^{-1}I_2) = S^{-1}I_1 I_2$;
4. $S^{-1}I_1 \cap S^{-1}I_2 = S^{-1}(I_1 \cap I_2)$;
5. $\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$.

Proof.

1. Suppose that $J \trianglelefteq S^{-1}R$. For $r/s \in J$, $r/1 = r/s \cdot s/1 \in J$. Hence $r = \varphi_S^{-1}(r/1) \in J^c$ and $r/s = 1/s \cdot \varphi_S(r) \in J^{ce}$. Therefore $J^{ce} = J$ and J is an extended ideal.

2&3. These are general properties of any ideal extensions (see Proposition 1.2.16).

4. It suffices to prove that $S^{-1}I_1 \cap S^{-1}I_2 \subseteq S^{-1}(I_1 \cap I_2)$. Suppose that $r_1 \in I_1$, $r_2 \in I_2$, and $s_1, s_2 \in S$ such that $r_1/s_1 = r_2/s_2$. Then there exists $s \in S$ such that $s(r_1 s_2 - r_2 s_1) = 0$. Then $sr_1 s_2 = sr_2 s_1 \in I_1 \cap I_2$. We have $r_1/s_1 = sr_1 s_2/ss_1 s_2 \in S^{-1}(I_1 \cap I_2)$.

5. It suffices to prove that $\sqrt{S^{-1}I} \subseteq S^{-1}\sqrt{I}$. For $r/s \in \sqrt{S^{-1}I}$, there exists $n \in \mathbb{N}$, $r_1 \in I$ and $s_1 \in S$ such that $r^n/s^n = r_1/s_1$. Then $s_0(r^n s_1 - s^n r_1) = 0$ for some $s_0 \in S$. Then $r^n s_0 s_1 = r_1 s_0 s^n \in I$. Hence $r s_0 s_1 \in \sqrt{I}$ and $r/s = r s_0 s_1/ss_0 s_1 \in S^{-1}\sqrt{I}$. □

Lemma 1.5.12

Suppose that $S \subseteq R$ is a multiplicative subset and $I \trianglelefteq R$. Then $S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \varnothing$.

Proof. $\exists s \in S \cap I \iff 1_{S^{-1}R} = s/s \in S^{-1}I \iff S^{-1}R = S^{-1}I$ □

Proposition 1.5.13. Prime Ideals of $S^{-1}R$

Suppose that P is a prime ideal of R such that $P \cap S = \varnothing$. Then $S^{-1}P$ is a prime ideal of $S^{-1}R$. In particular, the operation S^{-1} induces a bijection from $\{P \in \operatorname{Spec} R : P \cap S = \varnothing\}$ to $\operatorname{Spec} S^{-1}R$.

Proof. Suppose that $P \in \operatorname{Spec} R$ such that $P \cap S = \varnothing$. Then by Lemma 1.5.12 $S^{-1}P$ is a proper ideal of $S^{-1}R$. Suppose that $r_1/s_1 \cdot r_2/s_2 \in S^{-1}P$. Then $r_1r_2/s_1s_2 = a/s$ for some $a \in P$ and $s \in S$. There exists $s_0 \in S$ such that $ss_0r_1r_2 = s_0s_1s_2a \in P$. Since $ss_0 \in S$ and $S \cap P = \varnothing$, we have $r_1r_2 \in P$. Since P is prime, either $r_1 \in P$ or $r_2 \in P$. Hence either $r_1/s_1 \in S^{-1}P$ or $r_2/s_2 \in S^{-1}P$. Hence $S^{-1}P$ is a prime ideal.

On the other hand, suppose that $S^{-1}P \in \operatorname{Spec}(S^{-1}R)$. By Proposition 1.5.11, it is an extension of some ideal. As the operation S^{-1} is injective, there is a unique prime ideal $P \trianglelefteq R$ such that P extends to $S^{-1}P$. □

Remark. Recall that $R \setminus P$ is a multiplicative subset for $P \in \operatorname{Spec} R$. This motivates us to define a ring of fractions that has a unique maximal ideal.

Definition 1.5.14. Localisation on a Prime Ideal

Suppose that R is a CRI and $P \trianglelefteq R$ is a prime ideal. As $R \setminus P$ is a muliplcative subset, the ring of fraction $(R \setminus P)^{-1}R$ is called the localisation of R on P and is denoted by R_P.

Remark. By Proposition 1.5.13, we observe that P extends to the unique maximal ideal in R_P. That is, R_P is a local ring (see the remark after Corollary 1.4.14). We have a bijective correspondence between $\{Q \in \operatorname{Spec} R : Q \subseteq P\}$ and $\operatorname{Spec} R_P$.

Example 1.5.15. Localisation of $\mathbb{Z}$

Suppose that $p \in \mathbb{Z}$ is a prime integer. Then the localisation of $\mathbb{Z}$ on $\langle p \rangle$, $\mathbb{Z}_{\langle p \rangle}$, is the set of rational numbers m/n such that $\gcd(n, p) = 1$. The Jacobson radical $J(\mathbb{Z}_{\langle p \rangle}) = p\mathbb{Z}_{\langle p \rangle}$.

Definition 1.5.16. Localisation on an Element

Suppose that R is a CRI. For $f \in R \setminus \{0\}$, consider the multiplicatively closed set $S := \{f^n : n \in \mathbb{N}\}$. the ring of fraction $(S)^{-1}R$ is called the localisation of R at f and is denoted by R_f.

Remark. We shall see that the construction of rings of fractions extend naturally to modules. We will discuss the localisation of modules and local properties in Section 6.2.

Chapter 2

Factorisation in Integral Domains

The inclusion relation of the classes of rings can be summarized as below:

$$\text{Fields} \Longrightarrow \text{ED} \Longrightarrow \text{PID} \Longrightarrow \text{UFD} \Longrightarrow \text{Factorisation Domains} \Longrightarrow \text{Integral Domains} \Longrightarrow \text{CRI}$$

2.1 Unique Factorisation Domains

2.1.1 Divisibility and Factorisation

Definition 2.1.1. Divisibility

Suppose that R is a CRI and $a, b \in R \setminus \{0\}$.

We say that a divides b, or $a \mid b$, if there exists $x \in R$ such that $ax = b$, or equivalently, $\langle b \rangle \subseteq \langle a \rangle$.

We say that a and b are associates, or $a \sim b$, if $a \mid b$ and $b \mid a$, or equivalently, $\langle a \rangle = \langle b \rangle$.

Lemma 2.1.2

Suppose that R is an integral domain and $a, b \in R \setminus \{0\}$, then $a \sim b$ if and only if there exists a unit $u \in R$ such that $au = b$.

Proof. The backward direction is trivial. The forward direction follows from the cancellation law of integral domains. □

Definition 2.1.3. Prime Elements, Irreducible Elements

Suppose that R is a CRI and $a \in R \setminus \{0\}$ is a non-unit.

a is called a prime element, if $\forall\, x, y \in R:\ a \mid xy \implies a \mid x \ \vee\ a \mid y$;

a is called an irreducible element, if $\forall\, x, y \in R:\ a = xy \implies x \in R^\times \ \vee\ y \in R^\times$.

Remark. As the name suggests, $a \in R$ is a prime element if and only if $\langle a \rangle$ is a non-zero prime ideal of R.

Remark. For the irreducible elements, we have the following observation:

$$\begin{aligned} a \in R \text{ is irreducible} &\iff a = xy \Longrightarrow a \sim x \ \vee\ a \sim y \\ &\iff \langle a \rangle \subseteq \langle b \rangle \Longrightarrow \langle a \rangle = \langle b \rangle \ \vee\ \langle b \rangle = R \\ &\iff \langle a \rangle \text{ is maximal among proper principal ideals} \end{aligned}$$

Remark. In $\mathbb{Z}$ prime elements and irreducible elements coincide. This is not true for general integral domains. Being a prime element turns out to be a stronger condition.

Proposition 2.1.4. Integral Domain: Prime $\Longrightarrow$ Irreducible

Suppose that R is an integral domain. If $a \in R$ is a prime element, then it is irreducible.

Proof. For $x, y \in R$ such that $a = xy$, since a is prime, we have $a = xy \Longrightarrow a \mid xy \Longrightarrow a \mid x \vee a \mid y$. But also $a = xy \Longrightarrow x \mid a \wedge y \mid a$. Hence we have $a \sim x$ or $a \sim y$. Since R is an integral domain, by Lemma 2.1.2 $x \in R^\times$ or $y \in R^\times$. Hence a is irreducible. □

2.1.2 Factorisation in UFD and PID

Definition 2.1.5. Factorisation Domains, Unique Factorisation Domains

Suppose that R is an integral domain. R is called a factorisation domain, if for any non-zero non-unit $a \in R$, there exists irreducibles $q_1, ..., q_n \in R$ such that $a = q_1 \cdots q_n$.

We say that the factorisation of $a \in R$ is unique, if for any two factorisations of a:

$$a = q_1 \cdots q_n = p_1 \cdots p_m$$

we must have $n = m$ and $q_i \sim p_i$ after some permutation of the irreducibles.

A factorisation domain R is called a unique factorisation domain (abbreviated UFD), if every non-zero non-unit of R has a unique factorisation into irreducibles.

Remark. Suppose that R is a UFD and $a, b \in R$ are non-zero non-unit. Then $a \sim b$ if and only if a and b have the same factorisation (up to permutation of irreducibles).

The set of irreducible factors (counting multiplicities) of ab is the union of the set of the irreducible factors (counting multiplicities) of a and b.

Working in UFD has the advantage of reducing ring-theoretic statements to set-theoretic statements about the irreducible factors.

Proposition 2.1.6. Ascending Chain Condition for Principal Ideals (ACCP) $\implies$ Factorisation Domain

Suppose that R is an integral domain. R is a factorisation domain if and only if it satisfies the ascending chain condition for principal ideals, that is, for any ascending chain of principal ideals in R:

$$\langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \langle r_3 \rangle \subseteq \cdots$$

there exists $n \in \mathbb{N}$ such that $\langle r_n \rangle = \langle r_{n+1} \rangle = \cdots$ (the chain "stablises").

Proof. Suppose that R is not a factorisation domain. There exists $r \in R$ which cannot be factorized into finitely many irreducibles. In particular, r is not irreducible. Then there exists $r_1, s_1 \in R$ such that $r = r_1 s_1$ and $\langle r \rangle \subsetneq \langle r_1 \rangle$, $\langle r \rangle \subsetneq \langle s_1 \rangle$. Without loss of generality we may assume that r_1 cannot be factorized into irreducibles. Inductively we can construct an strictly ascending chain of principal ideals:

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_2 \rangle \subsetneq \cdots$$

Hence R does not satisfy ACCP. □

Remark. We shall see that the ascending chain condition (on all ideals) is equivalent to the condition that all ideals are finitely generated, which is the definition of a Noetherian ring. The ACC and DCC will be further discussed in Section 6.1.

Lemma 2.1.7. UFD: Prime $\iff$ Irreducible

Suppose that R is a unique factorisation domain. $a \in R$ is a prime element if and only if it is irreducible.

Proof. The forward direction is proven in Proposition 2.1.4. For the backward direction, suppose that a is an irreducible and $a \mid bc$. Since R is a UFD, the irreducible factor of a, which is a itself, is the subset of the union of the irreducible factors of b and c (counting multiplicities). Then we must have $a \mid b$ or $a \mid c$. Hence a is a prime element. □

Theorem 2.1.8. UFD $\iff$ ACCP + (Prime = Irreducible)

Suppose that R is an integral domain. Then R is a unique factorisation domain if and only if it satisfies the following conditions:

1. R satisfies the ascending chain condition for principal ideals;
2. every irreducible element in R is prime.

Proof. "$\implies$": Suppose that R is a unique factorisation domain. The second statement is proven in Lemma 2.1.7. For an ascending chain of principal ideals:

$$\langle r \rangle \subseteq \langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \cdots$$

Suppose that r has the unique factorisation $r = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$. Then $\langle r \rangle \subseteq \langle r_1 \rangle \implies r_1 \mid r$, which implies that $r_1 \sim q_1^{\beta_1} \cdots q_n^{\beta_n}$ where $0 \leqslant \beta_i \leqslant \alpha_i$ for $i \in \{1, ..., n\}$. As all α_i are finite, the chain will eventually stablise.

"$\Longleftarrow$": If R has ACCP, then by Proposition 2.1.6 R is a factorisation domain. So it suffices to prove the uniqueness of factorisation. For $r \in R$, suppose that it has two factorisations into irreducibles:

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

We have $p_1 \cdots p_m \in \langle q_1 \rangle$. By hypothesis $\langle q_1 \rangle$ is prime. Then we must have $p_i \in \langle q_1 \rangle$ for some $i \in I$. After possible permutations we may assume that $p_1 \in \langle q_1 \rangle$. Since p_1 is irreducible, we must have $\langle p_1 \rangle = \langle q_1 \rangle$ or $p_1 \sim q_1$. Then $q_2 \cdots q_n \sim p_2 \cdots p_m$. We can repeat this process. If $n \neq m$ then after some steps we will have $1 \sim a$ where a is a product of irreducibles, which is impossible. Hence $n = m$ and $q_i \sim p_i$ for all $i \in \{1, ..., n\}$ after possible permutations. We conclude that R is a UFD. □

Definition 2.1.9. Greatest Common Divisors, Least Common Multiples

Suppose that R is an integral domain and $a, b \in R$.

$l \in R$ is called a least common multiple (abbreviated lcm) of a and b, if $\langle l \rangle = \langle x \rangle \cap \langle y \rangle$. Equivalently, $l \in R$ is a lcm of a and b, if $a \mid l$, $b \mid l$, and any $m \in R$ with $a \mid m$ and $b \mid m$ has $l \mid m$.

$g \in R$ is called a greatest common divisor (abbreviated gcd) of a and b, if $\langle g \rangle = \bigcap \{\langle d \rangle : \langle a, b \rangle \subseteq \langle d \rangle\}$. Equivalently, $g \in R$ is a gcd of a and b, if $g \mid a$, $g \mid b$, and any $d \in R$ with $d \mid a$ and $d \mid b$ has $d \mid g$.

Remark. In general, neither exixtence nor uniqueness of the gcd and lcm is assured. We may write $g \in \gcd(a, b)$ when g is a gcd of a and b. This notation is not standard.

Proposition 2.1.10. UFD $\Longrightarrow$ Existence & Uniqueness of GCD

Suppose that R is a unique factorisation domain. For any $a, b \in R \setminus \{0\}$, $\gcd(a, b)$ is unique (up to associates).

Proof. Suppose that $q_1, ..., q_n \in R$ are irreducibles such that $a \sim q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ and $b \sim q_1^{\beta_1} \cdots q_n^{\beta_n}$ where $q_i \not\sim q_j$ for $i \neq j$ and $\alpha_i, \beta_i \geqslant 0$. One may verify that $g = q_1^{\min(\alpha_1, \beta_1)} \cdots q_n^{\min(\alpha_n, \beta_n)}$ is the unique gcd of a and b. □

Theorem 2.1.11. PID $\Longrightarrow$ UFD

Suppose that R is a principal ideal domain. Then R is a unique factorisation domain.

Proof. We shall make use of Theorem 2.1.8. To prove that R satisfies ACCP, consider an ascending chain of principl ideals:

$$\langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \langle r_3 \rangle \subseteq \cdots$$

Then $\bigcup_{n=1}^{\infty} \langle r_n \rangle$ is an ideal and an upper bound of this chain. Since R is a PID, $\langle r_0 \rangle = \bigcup_{n=1}^{\infty} \langle r_n \rangle$ for some $r_0 \in R$. Then there exists $N \in \mathbb{N}$ such that $r_0 \in \langle r_N \rangle$. But also $r_N \in \langle r_0 \rangle$. As a result we have $\langle r_0 \rangle = \langle r_N \rangle = \langle r_{N+1} \rangle = \cdots$. The chain stablises.

Suppose that $r \in R$ is irreducible. Then $\langle r \rangle$ is maximal among proper principal ideals in R. But R is a PID, so $\langle r \rangle$ is a maximal ideal. In particular, $\langle r \rangle$ is a non-zero prime ideal and hence r is a prime element. □

Corollary 2.1.12. Irreducibles in PID

Suppose that R is a PID. For $r \in R$, the following statements are equivalent:

1. r is a prime element;
2. r is an irreducible element;
3. $\langle r \rangle$ is a non-zero prime ideal;
4. $\langle r \rangle$ is a non-zero maximal ideal.

Example 2.1.13. $\mathbb{Z}$ is a UFD

$\mathbb{Z}$ is a UFD. This is known as the **fundamental theorem of arithmetics**.

Example 2.1.14. A UFD that is not a PID

$\mathbb{Z}[x]$ is not a principal ideal domain, because the ideal $\langle 2, x\rangle \trianglelefteq \mathbb{Z}[x]$ is not principal. But $\mathbb{Z}[x]$ is a unique factorisation domain. We shall prove this fact in Theorem 2.3.19.

Example 2.1.15. An integral domain that is not a UFD

$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : \ a, b \in \mathbb{Z}\}$ is an integral domain as a subring of $\mathbb{C}$. It is not a UFD because

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}],$$

where 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducibles but no two of them are associates.

2.2 Euclidean Domains

We know from elementary algebra that we can perform Euclidean algorithm in $\mathbb{Z}$ and $\mathbb{R}[x]$. We shall generalise this to a broader class of rings, namely the Euclidean domains.

Definition 2.2.1. Euclidean Valuation, Euclidean Domains

Suppose that R is an integral domain. A Euclidean valuation is a map $v : R \setminus \{0\} \to \mathbb{N}$ satisfying that, for all $a \in R, b \in R \setminus \{0\}$ there exists $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $v(r) < v(b)$.

An integral domain is called a Euclidean Domain (abbreviated ED) if it admits a Euclidean valuation.

Example 2.2.2. Euclidean Domains

1. $\mathbb{Z}$ is a Euclidean domain with valuation $v(n) = |n|$.
2. $\mathbb{R}[x]$ is a Euclidean domain with valuation $v(f) = \deg f$.
3. The **Gaussian integers** $\mathbb{Z}[\mathrm{i}] := \{a + b\mathrm{i} : \ a, b \in \mathbb{Z}\}$ is a Euclidean domain with valuation $v(a, b) = a^2 + b^2$.

Theorem 2.2.3. ED $\Longrightarrow$ PID

Suppose that R is a Euclidean domain. Then R is a principal ideal domain.

Proof. Let I be a non-zero ideal of R. We choose $a \in I$ such that $v(a) = \min\{v(x) : x \in I \setminus \{0\}\}$. For $b \in I$, there exists $q, r \in I$ such that $b = qa + r$ with either $r = 0$ or $v(r) < v(a)$. As $a, b \in I$, $r = b - qa \in I$. We must have $r = 0$ by minimality of $v(a)$. Hence $b = qa \in \langle a\rangle$. We have $I = \langle a\rangle$. R is a principal ideal domain. □

Theorem 2.2.4. Euclidean Algorithm

Suppose that R is a Euclidean domain. Let $a_1, a_2 \in R \setminus \{0\}$ such that $v(a_1) \geqslant v(a_2)$. The Euclidean algorithm uniquely determines the sequences q_i and a_i of integers:

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 && v(a_3) < v(a_2) \\ a_2 &= q_1 a_3 + a_4 && v(a_4) < v(a_3) \\ a_3 &= q_1 a_4 + a_5 && v(a_5) < v(a_4) \\ &\cdots \end{aligned}$$

The algorithm terminates at $a_k = 0$ for some k. Then $a_{k-1} = \gcd(a_1, a_2)$.

Proof. The termination of the algorithm is clear as $\{v(a_i)\}$ is a strictly decreasing sequence which is bounded below. Tp prove that $a_{k-1} = \gcd(a_1, a_2)$, first we can use reverse induction to prove that a_{k-1} divides a_i for all i. Second, suppose that $m \in R$ such that $m \mid a_1$ and $m \mid a_2$. Then clearly $m \mid a_3 = a_1 - q_1 a_2$. Inductively $m \mid a_i$ for all i and $m \mid a_{k-1}$. □

Corollary 2.2.5. Bézout's Lemma

Suppose that R is a Euclidean domain. For $a, b \in R \setminus \{0\}$ with a greatest common divisor g, there exists $u, v \in R$ such that $au + bv = g$.

Proof. We use reverse induction. Without loss of generality we assume that $v(a) \geqslant v(b)$. We set $a_1 = a$ and $a_2 = b$. By Euclidean algorithm we can obtain a sequence $a_1, a_2, ..., a_k$ where $a_k = 0$ and $a_{k-1} = g$ and the corresponding sequence $q_1, ..., q_{k-1}$. We shall prove that for $i \in \{1, .., k\}$ there exists $u_i, v_i \in R$ such that $a_i u_i + a_{i+1} v_i = g$.

Base case: We set $u_{k-2} = 0$ and $v_{k-2} = 1$ so that $a_{k-2}u_{k-2} + a_{k-1}v_{k-2} = a_{k-1} - g$.

Induction case: Suppose the result holds for all $i > n$. Then for $i = n$:

$$g = a_{n+1}u_{n+1} + a_{n+2}v_{n+1} = a_{n+1}u_{n+1} + (a_n - q_{n+1}a_{n+1})v_{n+1} = a_n v_{n+1} + a_{n+1}(u_{n+1} - q_{n+1}v_{n+1})$$

We complete the induction by setting $u_n = v_{n+1}$ and $v_n = u_{n+1} - q_{n+1}v_{n+1}$. □

Remark. Although we prove Bézout's Lemma in Euclidean domains, it holds in any PID (unsurprisingly the proof is even simplier).

Definition 2.2.6. Dedekind-Hasse Valuation

Suppose that R is an integral domain. A Dedekind-Hasse valuation is a map $v : R \setminus \{0\} \to \mathbb{N}$ satisfying that, for all $a, b \in R$, either $b \mid a$ or there exists $r \in \langle a, b\rangle$ such that $v(r) < v(b)$.

Remark. The latter condition of Dedekind-Hasse valuation requires that $\exists\, q, s \in R :\ as = bq + r,\ v(r) < v(b)$. Therefore we see that a Dedekind-Hasse valuation is a generalisation of a Euclidean valuation.

Theorem 2.2.7. PID $\Longleftrightarrow$ Dedekind-Hasse Domain

Suppose that R is an integral domain. R is a principal ideal domain if and only if it admits a Dedekind-Hasse valuation.

Proof. "$\Longrightarrow$": For a non-zero non-unit $r \in R$, let $v(r)$ be the number of irreducible factors (counting multiplicities). For a unit $r \in R$, we define $v(r) = 0$. $v : R \setminus \{0\} \to \mathbb{N}$ is well-defined as R is a UFD. We shall verify that v is a Dedeking-Hasse valuation. For $a, b \in R \setminus \{0\}$, if $b \nmid a$, then $\langle b\rangle \subsetneq \langle a, b\rangle$. Since R is a PID, there exists $r \in R$ such that $\langle r\rangle = \langle a, b\rangle$. Then $r \mid b$ and $r \not\sim b$. We have $v(r) < v(b)$.

"$\Longleftarrow$": Just repeat the proof of Theorem 2.2.3 verbatim. □

Example 2.2.8. PID that are not ED

1. The most classical example is the ring of algebraic integers $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$. It is a principal ideal domain but not a Euclidean domain.
2. Another example given in **[Sanders]** is the ring $\dfrac{R[x, y]}{\langle x^2 + y^2 + 1\rangle}$. Interested readers may find the detailed proof in the referred notes.

2.3 Factorisation of Polynomials

2.3.1 Divison and Roots of Polynomials

Proposition 2.3.1. Divison Algorithm

Suppose that R is a CRI. $f, g \in R[x]$ are non-zero polynomials and the leading coefficient of g is a unit in R. Then there exists unique $q, r \in R[x]$ such that $f = qg + r$ and $\deg r < \deg g$.

Proof. Existence: If $\deg g > \deg f$, then we can set $q = 0$ and $r = f$. Now we assume that $\deg g \leqslant \deg f$. We use induction on $\deg f$. Suppose that $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$. Base case: If $\deg f = \deg g = 0$, then $f = a_0$, $g = b_0$. We can set $q = a_0 b_0^{-1}$ and $r = 0$.

Induction case: Suppose that the result holds for $\deg f < n$. Suppose that $\deg f = n$. Notice that $h(x) := a_n b_m^{-1} x^{n-m} g(x)$ is a polynomial of degree n and leading coefficient a_n. Then $f - h$ is a polynomial of degree less than n. By induction hypothesis,

there exists $q', r \in R[x]$ such that $f - h = q'g + r$ and $\deg r < \deg g$. Hence

$$f(x) = h(x) + q'(x)g(x) + r(x) = \left(a_n b_m^{-1} x^{n-m} + q'(x)\right) g(x) + r(x) = q(x)g(x) + r(x)$$

where $q(x) = q'(x) + a_n b_m^{-1} x^{n-m}$.

Uniqueness: Suppose that $f = q_1 g + r_1 = q_2 g + r_2$ and $\deg r_1 < \deg g$, $\deg r_2 < \deg g$. Then

$$(q_1 - q_2)g = r_1 - r_2$$

Suppose that $r_1 \neq r_2$. As the leading coefficient of g is a unit, we have:

$$\begin{aligned} \max\{\deg r_1, \deg r_2\} &\geqslant \deg(r_1 - r_2) = \deg(q_1 - q_2)g = \deg(q_1 - q_2) + \deg g \\ &\geqslant \deg g > \max\{\deg r_1, \deg r_2\} \end{aligned}$$

which is a contraction. Hence $r_1 = r_2$ and $q_1 = q_2$. □

Corollary 2.3.2. F **Field** $\Longrightarrow$ $F[x]$ **ED**

If F is a field, then $F[x]$ is a Euclidean domain.

Proof. If F is a field, then the leading coefficient of every non-zero polynomial must be a unit. It follows from Proposition 2.3.1 that $F[x]$ is a ED with Euclidean valuation $v(f) = \deg f$. □

Proposition 2.3.3. F **Field** $\Longleftrightarrow$ $F[x]$ **PID**

F is a field if and only if $F[x]$ is a principal ideal domain.

Proof. "$\Longrightarrow$": It follows from Corollary 2.3.2 and Theorem 2.2.3.

"$\Longleftarrow$": Suppose that $u \in F \setminus \{0\}$. Consider the ideal $\langle u, x\rangle \subseteq F[x]$. As $F[x]$ is a PID, there exists $f \in F[x]$ such that $\langle u, x\rangle = \langle f \rangle$. Since F is an integral domain, $u \in \langle f \rangle \Longrightarrow 0 = \deg u \geqslant \deg f \Longrightarrow f(x) = v \in F$. $x \in \langle v\rangle$ implies that v is a unit in F. Hence $\langle u, x\rangle = \langle 1\rangle = F$. Therefore u is unit of F and F is a field. □

Proposition 2.3.4. Remainder Theorem

Suppose that R is a CRI and $f \in R[x]$. For any $c \in R$, there exists a unique $q \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$.

Proof. If $f = 0$ then set $q = 0$. Suppose that $f \neq 0$. As $x - c \in R[x]$ is monic, by Proposition 2.3.1 there exists $q, r \in R[x]$ such that $f(x) = q(x)(x - c) + r(x)$ and $\deg r(x) < \deg(x - c) = 1$. Hence $\deg r = 0$ and $r \in R$. Evaluate f at c: $f(c) = q(c)(c - c) + r = r$. Hence we have $f(x) = q(x)(x - c) + f(c)$ as required. □

Remark. Writing $f(c)$ for $\mathrm{ev}_c(f)$ might be an abuse of notation, as we are considering f as a polynomial function $f : R \to R$. We shall prove in Corollary 2.3.8 that polynomials and the functions they represent are not different for infinite integral domains.

Definition 2.3.5. Roots of Polynomials

Suppose that R, S are CRI and $R \subseteq S$. For $f \in R[x]$ and $c \in S$, u is called a root or zero of f on S, if $f(c) = 0$.

Corollary 2.3.6

Suppose that R is a CRI. For $f \in R[x]$, $c \in R$ is a root of f if and only if $x - c$ divides $f(x)$.

Proof. Trivial by Remainder Theorem. □

Proposition 2.3.7. Maximum Number of Distinct Roots

Suppose that R is an integral domain. Let $f \in R[x]$ with $\deg f = n$. Then f has at most n distinct roots in R.

Proof. Suppose that f has roots $c_1, ..., c_m \in R$. Then by Corollary 2.3.6, we have $g(x) = (x - c_1) \cdots (x - c_m) \mid f(x)$. As $\deg g = m$, we must have $m \leqslant n = \deg f$. □

Corollary 2.3.8. Polynomials as Functions

Suppose that R is an *infinite* integral domain. For $f, g \in R[x]$, $f = g$ if and only if the evalutions $\mathrm{ev}_r(f) = \mathrm{ev}_r(g)$ (or $f(r) = g(r)$) for all $r \in R$.

Proof. The forward direction is trivial. For the backward direction, $f(r) = g(r)$ for all $r \in R$ implies that $f - g$ has infinitely many roots in R. Hence $f - g = 0$ by Proposition 2.3.7. □

Definition 2.3.9. Multiplicity of Roots

Suppose that R is an integral domain. From Corollary 2.3.6 and Proposition 2.3.7 we can infer that, if $c \in R$ is a root of $f \in R[x]$, then there exists a unique integer $1 \leqslant m \leqslant \deg f$ such that $f(x) = (x - c)^m g(x)$ and $g(c) \neq 0$. m is called the multiplicity of the root c of f. If $m = 1$, we say that c is a **simple root** of f. Otherwise we say that c is a **multiple root** of f.

Definition 2.3.10. Formal Derivatives of Polynomials

Suppose that R is an integral domain and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. The formal derivative of f is defined to be

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1} \in R[x]$$

Remark. It is not hard to verify that the formal derivatives satisfy the ordinary properties of derivatives (although we do not really have a differential structure on R). That is, for $c \in R$ and $f, g \in R[x]$:

1. $(cf)' = cf'$;
2. $(f + g)' = f' + g'$;
3. $(fg)' = f'g + fg'$;
4. $(f^n)' = nf^{n-1}f'$.

Proposition 2.3.11. Formal Derivatives and Roots

Suppose that R is an integral domain and $f \in R[x]$. Then $c \in R$ is a multiple root of f if and only if $f(c) = 0$ and $f'(c) = 0$.

Proof. Suppose that the c is a root of f on R of multiplicity m. Then $f(x) = (x - c)^m g(x)$ and $g(c) \neq 0$. The formal derivative $f'(x) = m(x - c)^{m-1} g(x) + (x - c)^m g'(x)$. $f'(c) = 0$ if and only if $m > 1$. □

Corollary 2.3.12

Suppose that R is an integral domain and $f \in R[x]$. f has no multiple roots in R if and only if f and f' are coprime.

2.3.2 Factorisation of Polynomials in UFD

Now we begin to discuss the factorisation of polynomials in a UFD. Our ultmate goal is to prove that $R[x]$ is a UFD if R is a UFD.

Definition 2.3.13. Contents, Primitive Polynomials

Suppose that R is a unique factorisation domain. For $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$, we define the content of f to be $\mathrm{c}(f) := \gcd(a_0, ..., a_n)$. If $\mathrm{c}(f)$ is a unit in R, we say that f is a primitive polynomial.

Remark. The definition of contents is inherently ambiguous as it involves gcd. Hence all equality should be interpreted as "associates". In fact it is the ideal generated by the content that truly matters. From definition we know that $\mathrm{c}(af) = a\,\mathrm{c}(f)$ for $a \in R$. In particular, for any non-zero $f \in R[x]$, $f = \mathrm{c}(f) f_0$ where f_0 is primitive.

Lemma 2.3.14

Suppose that R is a unique factorisation domain and $f \in R[x]$. f is not primitive if and only if there exists a prime and pricipal ideal $P \trianglelefteq R$ such that $f \in P[x]$.

Proof. For $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$:

$$\begin{aligned} f \text{ is not primitive} &\iff \mathrm{c}(f) = \gcd(a_0, ..., a_n) \nsim 1 \\ &\iff \exists \text{ irreducible } q \in R : \langle a_0, ..., a_n \rangle \subseteq \langle q \rangle \\ &\iff f \in \langle q \rangle R[x] \end{aligned}$$

Since R is a UFD, q is prime and $\langle q \rangle$ is a prime ideal. □

Theorem 2.3.15. Gauss' Lemma

Suppose that R is a unique factorisation domain and $f, g \in R[x]$. Then $\mathrm{c}(fg) = \mathrm{c}(f)\,\mathrm{c}(g)$. In paricular, the product of primitive polynomials is primitive.

Proof. Write $f = \mathrm{c}(f) f_0$ and $g = \mathrm{c}(g) g_0$. We have $\mathrm{c}(fg) = \mathrm{c}\big(\mathrm{c}(f) f_0\, \mathrm{c}(g) g_0\big) = \mathrm{c}(f)\,\mathrm{c}(g)\,\mathrm{c}(f_0 g_0)$. It suffices to prove that $f_0 g_0$ is primitive. Suppose that it is not. Then by Lemma 2.3.14 there exists a prime and principal ideal $P \trianglelefteq R$ such that $f_0 g_0 \in P[x]$. We know from Proposition 1.4.6 that $P[x]$ is a prime ideal of $R[x]$. Hence either $f_0 \in P[x]$ or $g_0 \in P[x]$, which implies that either f_0 or g_0 is not primitive. Contradiction. □

Corollary 2.3.16

Suppose that R is a unique factorisation domain and $f, g \in R[x]$. Then $\langle f \rangle \subseteq \langle g \rangle \implies \langle \mathrm{c}(f) \rangle \subseteq \langle \mathrm{c}(g) \rangle$.

Lemma 2.3.17

Suppose that R is a unique factorisation domain and F is the field of fractions of R. Let $f, g \in R[x]$. If $fF[x] \subseteq gF[x]$ and $\langle \mathrm{c}(f) \rangle \subseteq \langle \mathrm{c}(g) \rangle$, then $fR[x] \subseteq gR[x]$.[a]

[a] To clarify, $fR[x]$ is the ideal generated by f in $R[x]$ and $fF[x]$ is the ideal generated by f in $F[x]$.

Proof. Since $fF[x] \subseteq gF[x]$, there exists $h \in F[x]$ such that $f = gh$. By collecting the common denominators of coefficients of h, we can write $h = \frac{a}{b} h_0$ where $h_0 \in R[x]$ is a primitive polynomial. Then we have $bf = agh_0$. By Gauss' Lemma the contents are multiplicative, We have $b\,\mathrm{c}(f) = a\,\mathrm{c}(g)\,\mathrm{c}(h_0) = a\,\mathrm{c}(g)$. As R is an integral domain and $\langle \mathrm{c}(f) \rangle \subseteq \langle \mathrm{c}(g) \rangle$, $\langle a \rangle \subseteq \langle b \rangle$. That is, $a = bc$ for some $c \in R$. Hence $h = \frac{a}{b} h_0 = ch_0 \in R[x]$ and $fR[x] \subseteq gR[x]$ as required. □

Proposition 2.3.18. Irreducibility of Polynomials in Field of Fractions

Suppose that R is a unique factorisation domain and F is the field of fractions of R. Let $f \in R[x]$ be a non-constant polynomial. Then f is irreducible in $R[x]$ if and only if f is irreducible in $F[x]$ and is primitive in $R[x]$.

Proof. "$\Longleftarrow$": Trivial.

"$\Longrightarrow$": Suppose that $f \in R[x]$ is irreducible. Then f must be primitive, otherwise $f = c(f) f_0$ where $c(f) \nsim 1$, which is a contradiction. Assume that $f = gh$ for some $g, h \in F[x]$. Let $a, b \in F$ such that $g = ag_0$, $h = bh_0$, where $g_0, h_0 \in R[x]$ are primitive. By Gauss' Lemma $g_0 h_0$ is primitive.

Hence $f = abg_0 h_0$ implies that $\mathrm{c}(f) = \mathrm{c}(g_0 h_0) = 1$ and $fF[x] = g_0 h_0 F[x]$. By Lemma 2.3.17 we have $fR[x] = g_0 h_0 R[x]$. Hence $f \sim g_0 h_0$ in $R[x]$. Since f is irreducible in $R[x]$, either g_0 or h_0 is a unit in $R[x]$. It follows that either g or h is a unit in $F[x]$. Hence f is irreducible in $F[x]$. □

Theorem 2.3.19. R **UFD** $\Longrightarrow$ $R[x]$ **UFD**

Suppose that R is a unique factorisation domain. Then $R[x]$ is a unique factorisation domain.

Proof. We shall make use of Theorem 2.1.8. First we verify that $R[x]$ satisfies ACCP. Suppose that

$$\langle f_1\rangle \subseteq \langle f_2\rangle \subseteq \langle f_3\rangle \subseteq \cdots$$

is an ascending chain of principal ideals in $R[x]$. By Corollary 2.3.16 it induces an ascending chain of ideals in R:

$$\langle \mathrm{c}(f_1)\rangle \subseteq \langle \mathrm{c}(f_2)\rangle \subseteq \langle \mathrm{c}(f_3)\rangle \subseteq \cdots$$

Suppose that F is the field of fractions of R. Then the chain also induces an ascending chain of ideals in $F[x]$:

$$f_1F[x] \subseteq f_2F[x] \subseteq f_3F[x] \subseteq \cdots$$

By hypothesis R is a UFD. Since F is a field, $F[x]$ is a UFD. Then the chains in R and $F[x]$ stablise. By Lemma 2.3.17 the chain in $R[x]$ also stablises.

Next suppose that $f \in R[x]$ is an irreducible, If $\deg f = 0$, then $f \in R$ and f is a prime element as R is UFD. So we assume that f is non-constant. By Proposition 2.3.18, f is irreducible in $F[x]$. Since $F[x]$ is a UFD, $fF[x] \trianglelefteq F[x]$ is a prime ideal. Consider the composite homomorphism: $R[x] \xhookrightarrow{\iota} F[x] \xrightarrow{\pi} F[x]/fF[x]$

We shall prove that $\ker \pi\circ\iota = \langle f\rangle$. Clearly $f \in \ker\pi\circ\iota$. For $g \in \ker\pi\circ\iota$, we have $g \mid f$ in $F[x]$ or $gF[x] \subseteq fF[x]$. In addition we notice that $\langle \mathrm{c}(g)\rangle \subseteq \langle \mathrm{c}(f)\rangle = \langle 1\rangle$. Hence by Lemma 2.3.17 we have $\langle g\rangle \subseteq \langle f\rangle$ and $\ker\pi\circ\iota = \langle f\rangle$.

Finally, by First Isomorphism Theorem, $\pi\circ\iota$ induces a monomorphism $\varphi : R[x]/\langle f\rangle \to F[x]/fF[x]$. $F[x]/fF[x]$ is an integral domain because $fF[x]$ is prime. Hence $R[x]/\langle f\rangle$ is also an integral domain and $\langle f\rangle \trianglelefteq R[x]$ is prime. It follows that every irreducible in $R[x]$ is a prime element. □

Corollary 2.3.20. R **UFD** $\Longrightarrow$ $R[x_1,\ldots,x_n]$ **UFD**

Suppose that R is a unique factorisation domain. Then $R[x_1,\ldots,x_n]$ is a unique factorisation domain.

Proof. Notice that $R[x_1,\ldots,x_n] = R[x_1,\ldots,x_{n-1}][x_n]$. We can do induction on n. □

2.3.3 Irreducibility of Polynomials

Next we shall present some practical propositions about the irreducibility of polynomials. The propositions are commonly stated in the rings of $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, but can be generalised to arbitrary UFD without any difficulty.

Proposition 2.3.21. Irreducibility of Polynomials with $\deg \leqslant 3$

Suppose that F is a field and $f \in F[x]$ with $\deg f = 2$ or 3. Then f is irreducible if and only if f has no roots on F.

Proof. Trivial. □

Proposition 2.3.22. Rational Root Test

Suppose that R is a unique factorisation domain and F is the field of fractions of R. For $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$, let $p/q \in F$ be a root of f, where $p, q \in R$ and $\gcd(p,q) = 1$. Then $p \mid a_0$ and $q \mid a_n$ in R.

Proof. Since $f(p/q) = 0$, we have $a_0q^n + a_1pq^{n-1} + \cdots + a_np^n = 0$. Move a_0q^n to one side and factor out p:

$$a_0q^n = -p(a_1q^{n-1} + \cdots + a_np^{n-1})$$

Hence $p \mid a_0q^n$. As $\gcd(p,q) = 1$, we have $p \mid a_0$ as required.

The other part follows from a similar argument. □

Proposition 2.3.23. Reduction Test

Suppose that $f \in \mathbb{Z}[x]$ is a monic polynomial. For a prime integer $p > 0$, let $\pi : \mathbb{Z}[x] \twoheadrightarrow \mathbb{F}_p[x]$ be the homomorphism induced by the canonical projection. If $\pi(f)$ is irreducible in $\mathbb{F}_p[x]$, then f is irreducible in $\mathbb{Z}[x]$.

Proof. Suppose that $f = gh$. Then $\pi(f) = \pi(g)\pi(h) \in \mathbb{F}_p[x]$. As $\pi(f)$ is irreducible, either $\pi(g)$ or $\pi(h)$ is a unit in $\mathbb{F}_p[x]$. Without loss of generality we assume that $\pi(g)$ is a unit. Then $\deg \pi(g) = 0$. Since f is monic,

$$\deg g + \deg h = \deg f = \deg \pi(f) = \deg \pi(g) + \deg \pi(h) = \deg \pi(h)$$

As $\deg \pi(h) \leqslant \deg h$, we must have $\deg \pi(h) = \deg h$ and hence $\deg g = 0$. Therefore g divides the leading coefficient of f and is a unit. It follows that f is irreducible. □

Theorem 2.3.24. Eisenstein's Criterion

Suppose that R is a unique factorisation domain. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ be a non-constant primitive polynomial. If there exists a prime $p \in R$ such that:

1. $p \nmid a_n$;
2. $p \mid a_0, a_1, \ldots, a_{n-1}$;
3. $p^2 \nmid a_0$.

Then f is irreducible in $R[x]$.

Proof. Suppose that f is not irreducible. $f = gh$ for some non-units $g, h \in R[x]$. Let $\pi : R[x] \to (R/\langle p \rangle)[x]$ be the homomorphism induced by the canonical projection $R \twoheadrightarrow R/\langle p \rangle$ and $\overline{f}, \overline{g}, \overline{h}$ be the images of f, g, h under π.

Write $g(x) = \sum_{i=0}^{r} b_i x^i$ and $h(x) = \sum_{i=0}^{s} c_i x^i$. By hypothesis, $\overline{f}(x) = \overline{a_n} x^n$ where $\overline{a_n} \neq 0$ in $R/\langle p \rangle$. Since $\langle p \rangle$ is prime in R, $R/\langle p \rangle$ is an integral domain. Since $\overline{f} = \overline{g}\,\overline{h}$, $\overline{g}(x) = \overline{b_r} x^r$ and $\overline{h}(x) = \overline{c_s} x^s$. Since $r, s > 0$, we have $b_0, c_0 \in \langle p \rangle$ or $p \mid b_0, c_0$. But then $a_0 = b_0 c_0$ can be divided by p^2. Contradiction. □

Example 2.3.25. Irreducibility of Cyclotomic Polynomials

Let $p > 0$ be a prime integer. Let $f(x) = 1 + x + \cdots + x^{p-1} \in \mathbb{Z}[x]$. These polynomials are called **cyclotomic polynomials**. They are irreducible in $\mathbb{Z}[x]$.

Proof. This is a non-standard application of Eisenstein's criterion.

It is obvious that $f(x)$ is irreducible if and only if $f(x+1)$ is. As

$$f(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}$$

we have

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \binom{p}{1} + \binom{p}{2} x + \cdots + \binom{p}{p-1} x^{p-2} + x^{p-1}$$

Notice that $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ is divisible by p for $k < p$ and $a_0 = p$ is not divisible by p^2. By Eisenstein's criterion f is irreducible in $\mathbb{Z}[x]$. □

Chapter 3

Field Extensions

In this chapter, we will briefly introduce some concepts of field extensions without going too far into field and Galois theory. The target is to provide some powerful tools for the study of commutative rings.

3.1 Algebraic Extensions

Definition 3.1.1. Field Extensions

Suppose that F and K are fields and $F \subseteq K$. We say that K is an extension field of F. The field extension is sometimes denoted by $F \subseteq K$, K/F, or $K \mid F$.

If $F \subseteq K$ is a field extension, then K is a vector space over F. The dimension of K over F is called the degree of field extension and is denoted by $[K : F] = \dim_F K$. If $[K : F] < \infty$, then $F \subseteq K$ is called a **finite extension**. Otherwise it is called an **infinite extension**.

Theorem 3.1.2. Tower Law

Suppose that $F \subseteq K \subseteq L$ are field extensions. The degree of field extension is multiplicative:

$$[L : F] = [L : K][K : F]$$

Proof. Suppose that $\{x_i\}_{i\in I}$ is a basis of K over F and $\{y_j\}_{j\in J}$ is a basis of L over K. It is not hard to verify that $\{x_i y_j\}_{i\in I, j\in J}$ is a basis of L over F. □

Definition 3.1.3. Algebraic and Transcendental Extensions

Suppose that $F \subseteq K$ is a field extension. If for any $u \in K$ there exists $f \in R[u] \setminus \{0\}$ such that $f(u) = 0$, then u is said to be **algebraic** over F. Otherwise u is said to be **transcendental** over F.

If every element of K is algebraic over F, then $F \subseteq K$ is called an algebraic extension. Otherwise it is called a transcendental extension.

Proposition 3.1.4. Finite Extension $\Longrightarrow$ Algebraic Extension

If $F \subseteq K$ is a finite extension, then it is an algebraic extension.

Proof. Suppose that $[K : F] = n$. For $u \in K$, $1, u, ..., u^n$ are linearly dependent over F. Hence there exists $a_0, ..., a_n \in F$ such that $f(u) = a_0 + a_1 u + \cdots = a_n u^n = 0$. u is algebraic over F. □

Definition 3.1.5. Simple Extensions

Suppose that $F \subseteq K$ is a field extension. For $u \in K$, the subfield of K generated by u on F is denoted by $F(u)$. $F(u)$ is the field of fraction of $F[u]$.

If there exists $u \in K$ such that $K = F(u)$, then $F \subseteq K$ is called a simple extension.

Similarly, if there exists $u_1, ..., u_n \in K$ such that $K = F(_1, ..., u_n)$, then $F \subseteq K$ is called a finitely generated extension.

Proposition 3.1.6. Simple Extension of a Transcendental Element

Suppose that $F \subseteq K$ is a field extension and $u \in K$ is transcendental over F. Then there is a field isomorphism $\sigma : F(x) \to F(u)$ such that $\sigma|_F = \mathrm{id}_F$, where $F(x)$ is the field of fraction of the polynomial ring $F[x]$.

Proof. $\sigma : f/g \mapsto f(u)/g(u)$ is induced by the evalution homomorphism.. It is obvious that σ is a field isomorphism as there is only trivial algebraic relation on $F(u)$. □

Definition 3.1.7. Minimal Polynomials

Suppose that $F \subseteq K$ is a field extension and $u \in K$ is algebraic over F. Then there is a unique monic polynomial $m \in F[x]$ such that $m(u) = 0$ and $f(u) = 0$ if and only if m divides f. m is called the minimal polynomial of u over F.

Proposition 3.1.8. Simple Extension of an Algebraic Element

Suppose that $F \subseteq K$ is a field extension and $u \in K$ is algebraic over F. Suppose that $m \in F[x]$ is the minimal polynomial of u and $\deg m = n$.

1. $F[u] = F(u)$;
2. $F[u] \cong F[x]/\langle m(x)\rangle$;
3. $[F[u] : F] = \deg m = n$;
4. $\{1, u, ..., u^{n-1}\}$ is a basis of $F[u]$ over F.

Proof.

2. Apply First Isomorphism Theorem 1.2.9 to the evalution homomorphism: $R[u] = \mathrm{im}\,\mathrm{ev}_u \cong R[x]/\ker \mathrm{ev}_u$. Since F is a field, by Proposition 2.3.3, $F[x]$ is a PID. As m is the polynomial of least degree in $\ker \mathrm{ev}_u$, we have $\ker \mathrm{ev}_u = \langle m(x)\rangle$ and the result follows.

1. Since m is the minimal polynomial of u, m is irreducible. Since $R[x]$ is a PID, by Corollary 2.1.12, $\langle m(x)\rangle$ is maximal. In particular, $R[u] \cong R[x]/\langle m(x)\rangle$ is a field. We know that the field of fraction of a field is exactly itself.

4. For $f \in F[x]$, by division algorithm, there exists $q, r \in F[x]$ such that $f = qm + r$ and $\deg r < \deg m = n$. Then $f(u) = r(u) = a_0 + a_1 u + \cdots a_{n-1}u^{n-1} \in \mathrm{span}\{1, u, ..., u^{n-1}\}$. That is, $\{1, u, ..., u^{n-1}\}$ spans $F[u]$. On the other hand, suppose that $a_0, ..., a_{n-1} \in F$ such that $a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} = 0$. Then $a_0 = \cdots = a_{n-1} = 0$ by minimality of of degree of m. Hence $\{1, u, ..., u^{n-1}\}$ is linearly independent.

3. Follows immediately from (4). □

Corollary 3.1.9. Algebraic Extensions are Transitive

Suppose that $F \subseteq K \subseteq L$ are fields. If $F \subseteq K$ and $K \subseteq L$ are both algebraic extensions, then $F \subseteq L$ is also an algebraic extension.

Proof. For $u \in L$, since u is algebraic over K, there exist $a_0, ..., a_n \in K$ such that $f(u) = a_0 + a_1 u + \cdots + a_n u^n = 0$. Hence u is algebraic over the subfield $F(a_0, ..., a_n)$. By Tower Law,

$$[F(a_0, ..., a_n, u) : F] = [F(a_0, ..., a_n, u) : F(a_0, ..., a_n)][F(a_0, ..., a_n) : (a_0, ..., a_{n-1})] \cdots [F(a_0) : F] < \infty$$

By Proposition 3.1.4, u is algebraic over F. Hence $F \subseteq L$ is an algebraic extension. □

Corollary 3.1.10. Algebraic Elements form a Field

Suppose that $F \subseteq K$ is a field extension. Let E be the set of elements of K that are algebraic over F. Then E is a field.

Proof. For $u, v \in E$, since they are algebraic over F, $F \subseteq F(u, v)$ is a finite extension and hence is algebraic. We have $u \pm v, uv, uv^{-1} \in F(u, v) \subseteq E$. Hence E is a field. □

Proposition 3.1.11. Simple Extensions lift Field Isomorphisms

Suppose that $\sigma : F_1 \to F_2$ is a field isomorphism which extends to a ring isomorphism $\widetilde{\sigma} : F_1[x] \to F_2[x]$. Suppose that u_1 is a root of an irreducible polynomial $p_1 \in F_1[x]$ and u_2 is a root of $p_2 := \widetilde{\sigma}(p_1) \in F_2[x]$. Then $F_1[u_1] \cong F_2[u_2]$.

$$\begin{array}{ccc} F_1[u_1] & \longrightarrow & F_2[u_2] \\ \uparrow & & \uparrow \\ F_1 & \xrightarrow{\sigma} & F_2 \end{array}$$

Proof. Since p_1, p_2 are irreducible polynomials, they are the minimal polynomials of u_1 and u_2, repsectively. The field isomorphism is given by the following composition:

$$F_1[u_1] \xrightarrow{\sim} F_1[x]/\langle p_1(x)\rangle \xrightarrow{\sim} F_2[x]/\langle p_2(x)\rangle \xrightarrow{\sim} F_2[u_2] \qquad \square$$

Remark. In particular, we are interested in the field isomorphisms onto the field itself, which are called **field automorphisms**. It motivates us to introduce the following concept:

Definition 3.1.12. Automorphisms, Galois Group

Suppose that $F \subseteq K$ is a field extension. $\sigma : K \to K$ is called a F-automorphism, if σ is both a field isomorphism and a linear isomorphism of vector space K over F. The set of F-automorphisms of K is called the Galois group of K over F and is denoted by $\mathrm{Aut}_F K$ or $\mathrm{Gal}(K \mid F)$.

3.2 Splitting Fields and Algebraic Closure

Definition 3.2.1. Splitting Fields

Suppose that F is a field and $f \in F[x]$ has positive degree. We say that f splits over F, if f can be factorized into linear factors on F.

Suppose that $S \subseteq F[x]$ is a set of polynomials of positive degrees. K is called the splitting field of S over F, if K is the smallest extension of F such that every $f \in S$ splits over K.

When $S = \{f\}$, K is called the splitting field of f over F, if K is the smallest extension of F such that f splits over K. In particular, if $f(x) = c(x-u_1)\cdots(x-u_n) \in K[x]$, then $K = F(u_1, ..., u_n)$.

Remark. The extension of a F to a splitting field K of $S \subseteq F[x]$ is equivalent to adjoining all roots of the polynomials in S to F. It is immediate from definition that $F \subseteq K$ is an algebraic extension.

Lemma 3.2.2. Splitting Field of a Finite Set of Polynomials

Suppose that F is a field and $S = \{f_1, ..., f_n\} \subseteq F[x]$ are polynomials of positive degrees. K is the splitting field of S over F if and only if K is the splitting field of $f_1 \cdots f_n$ over F.

Proof. Suppose that $F \subseteq K$ is an algebraic extension. The result follows from a simple observation that $f_1, ..., f_n$ split over K if and only if $f_1 \cdots f_n$ splits over K. $\square$

Remark. The proposition suggests that the only cases we concern are that S is a singleton and that S is infinite.

Theorem 3.2.3. Existence of Splitting Field: Single Polynomial

Suppose that F is a field and $f \in F[x]$ has positive degree. Then there exists a splitting field K of f over F. Moreover, $[K : F] \leqslant (\deg f)!$.

Proof. Existence: We use induction on $\deg f$. Base case: If $\deg f = 1$, $f(x) = ax + b$ splits over F. Then $K = F$ and $[K : F] = 1$.

Induction case: Suppose that the result holds for $\deg f < n$. Suppose that $f \in F[x]$ has degree n and does not split over F. Let g be an irreducible factor of f ($\deg g > 1$). There exists a simple extension $F \subseteq F(u)$ such that g is the minimal polynomial of u on F. Then $[F(u) : F] = \deg g$. $f(x) = (x-u)h(x)$ for some $h \in F[x]$. As $\deg h < n$, by induction hypothesis, there exists a

splitting field K of h over $F(u)$. Hence K is a splitting field of f over F. By Tower Law:

$$[K:F] = [K:F(u)][F(u):F] \leqslant (n-1)! \cdot \deg g \leqslant n!$$

which completes the induction.

Uniqueness: Again we use induction on $\deg f$. □

The following proposition is a generalisation of Proposition 3.1.11.

Proposition 3.2.4. Splitting Fields lift Field Isomorphisms

Suppose that $\sigma : F_1 \to F_2$ is a field isomorphism which extends to a ring isomorphism $\widetilde{\sigma} : F_1[x] \to F_2[x]$. Suppose that K_1 is a splitting field of $f_1 \in F_1[x]$ over F_1 and K_2 is a splitting of $f_2 := \widetilde{\sigma}(f_1) \in F_2[x]$ over F_2. Then $K_1 \cong K_2$.

Proof. We use induction on $\deg f_1$. The base case is trivial. Suppose that $K_1 \cong K_2$ for $\deg f_1 < n$. For $\deg f_1 = n$, let g_1 be an irreducible factor of f_1 with $\deg g_1 > 1$ and $g_2 := \widetilde{\sigma}(g_1)$. Let u be a root of g_1 on K_1 and v a root of g_2 on K_2. By Proposition 3.1.11, we have a field isomorphism $F_1(u) \cong F_2(v)$. As $[K_1 : F_1(u)] < n$ and $[K_2 : F_2(v)] < n$, by induction hypothesis $F(u) \cong F(v)$ extends to a field isomorphism $K_1 \cong K_2$. □

Corollary 3.2.5. Uniqueness of Splitting Field: Single Polynomial

Suppose that F is a field and $f \in F[x]$ has positive degree. Any splitting fields of f over F are F-isomorphic.

Definition / Proposition 3.2.6. Algebraically Closed Fields

The following statements of a field F are equivalent:

1. Every non-constant polynomial $f \in F[x]$ has a root in F;
2. Every non-constant polynomial $f \in F[x]$ splits over F;
3. If $f \in F[x]$ is irreducible then $\deg f = 1$;
4. Every algebraic extension of F is F itself;
5. There exists a subfield $E \subseteq F$ such that F is algebraic over E and all irreducible polynomials in $E[x]$ split over F.

A field satisfying any of the above conditions is called an algebraically closed field.

Proof. Trivial. □

Proposition 3.2.7. Algebraically Closed Fields are Infinite

If F is an algebraically closed field, then F is infinite.

Proof. We can adapt Euclid's proof on the infinitude of prime integers.

Suppose that $F = \{a_1, ..., a_n\}$ is a finite field. Then

$$f(x) = \prod_{i=1}^{n} (x - a_i) + 1 \in F[x]$$

is a non-constant polynomial with no roots in F. Contradiction. □

Definition / Proposition 3.2.8. Algebraic Closure

Suppose that $F \subseteq K$ is a field extension. The following statements are equivalent:

1. $F \subseteq K$ is an algebraic extension and K is algebraically closed;
2. K is the splitting field over F of all non-constant polynomials in $F[x]$.

K is called the algebraic closure of F.

Proof. Trivial. □

Example 3.2.9. $\mathbb{C}$ is Algebraically Closed

$\mathbb{C} := \mathbb{R}[\mathrm{i}] = \mathbb{R}[x]/\langle x^2+1\rangle$ is the algebraic closure of $\mathbb{R}$. This is known as the **fundamental theorem of algebra**. The proof of this theorem, however, uses mainly the tools from analysis. (There is no "pure" algebraic definition of $\mathbb{R}$.)

Next we turn to the problem of existence and uniqueness of algebraic closure. Suppose that $\overline{F}$ is the algebraic closure of F. For $S \subseteq F[x]$, the splitting field of S over F is a subfield of $\overline{F}$. Therefore the existence of arbitrary splitting fields is equivalent to the existence of algebraic closure. Unsurprisingly, the main difficulty in the proof is set-theoretic instead of ring-theoretic.

Theorem 3.2.10. Existence of Algebraic Closure

Every field F has an algebraic closure $\overline{F}$.

Proof. The construction is due to *Emil Artin*.

Step 1: *There exists a field extension $F \subseteq K_1$ such that every non-constant polynomial $f \in F[x]$ has at least one root in K_1.*

Let $S \subseteq F[x]$ be the set of polynomials which are non-constant and monic. Consider a copy of S as indeterminates $X_F := \{x_f : f \in S\}$. We consider the polynomial ring $F[X_F]$ (see Definition 1.4.7) and the ideal $I := \langle \{f(x_f) : f \in S\}\rangle \trianglelefteq F[X_F]$. We claim that I is proper in $F[X_F]$.

Suppose that it is not. Then there exists $g_1, ..., g_n \in F[X_F]$ and $f_1, ..., f_n \in S$ such that $1 = \sum_{i=1}^{n} g_i f_i(x_{f_i})$. By applying Proposition 3.1.8 repeatly, we can construct a field extension E of F on which $f_1, ..., f_n \in F[x]$ have roots $\alpha_1, ..., \alpha_n$ respectively. The map of sets $\varphi : X_F \to E$ defined by $\varphi(x_{f_i}) = \alpha_i$ induces the evalution homomorphism $\widetilde{\varphi} : F[X_F] \to E$. We have:

$$1 = \widetilde{\varphi}\left(\sum_{i=1}^{n} g_i f_i(x_{f_i})\right) = \sum_{i=1}^{n} \widetilde{\varphi}(g_i) f_i(\alpha_i) = 0$$

which is a contradiction.

Since I is proper, by Corollary 1.3.7 there exists a maximal ideal $M \trianglelefteq F[X_F]$ such that $I \subseteq M$. Let $K_1 := F[X_F]/M$. Clearly K_1 is a field and $\theta : F \to K_1$ defined by $\theta(a) = a + M$ is a field monomorphism. We can embed F into K_1. Every non-constant monic polynomial f has a root $t_f + M$ in K_1.

Step 2: *For K_1, we can similarly construct K_2 in which every non-constant polynomial $f \in K_1[x]$ has a root. By repeating this process we obtain a chain of field extensions:*

$$F \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$$

Let $L := \bigcup_{i=1}^{\infty} K_i$. We claim that L is an algebraically closed field.

It is obvious that L is a field, as for any $a, b \in L$ there exists $i \in \mathbb{N}$ such that $a, b \in K_i$. For a non-constant $f \in L[x]$, $f \in K_i[x]$ for some $i \in \mathbb{N}$. Then f has a root on $K_{i+1} \subseteq L$. By Proposition 3.2.6 L is algebraically closed.

Step 3: *Let $\overline{F}$ be the set of algebraic elements of L over F. We claim that $\overline{F}$ is an algebraic closure of F.*

By Corollary 3.1.10 $\overline{F}$ is a field. It is clear from the above discussions that $\overline{F}$ is algebraically closed as L is algebraically closed. Moreover $F \subseteq \overline{F}$ is an algebraic extension. Hence by Proposition 3.2.8 $\overline{F}$ is an algebraic closure of F. □

Remark. We have indirectly used Zorn's Lemma (existence of maximal ideals) in the proof. As **[Aluffi]** states in his remark, however, the existence of algebraic closure is a consequence of the **compactness theorem for first-order logic**, which is known to be weaker than the axiom of choice (equivalent to Zorn's Lemma). An online discussion of this problem may be found on `https://mathoverflow.net/questions/46566/`.

Remark. It may be tempting to try to formulate some universal properties for algebraic closure. However this is impossible and the morphisms are by no means unique. As suggested in Proposition 3.1.11 for the case of single polynomial, the $F-$isomorphisms depend on the choice of roots of the polynomial.

The tool of proving uniqueness is again Zorn's Lemma.

Lemma 3.2.11

Suppose that $F \subseteq L$ is a field extension and L is algebraically closed. Then for any algebraic extension $F \subseteq K$, there exists a field monomorphism $\iota : K \hookrightarrow L$ with $\iota|_F = \mathrm{id}_F$.

Proof. Consider the set

$$\mathscr{S} := \{(E, \iota_E) : F \subseteq E \subseteq K,\ \iota_E : E \hookrightarrow L \text{ is a field monomorphism such that } \iota_E|_F = \mathrm{id}_F\}$$

with a partial order

$$(E, \iota_E) \preceq (E', \iota_{E'}) \iff E \subseteq E' \wedge \iota_{E'}|_E = \iota_E.$$

$\mathscr{S}$ is non-empty, as $(F, \iota_F) \in \mathscr{S}$. Suppose that $\mathscr{C} \subseteq \mathscr{S}$ is a chain. Let $E_C := \bigcup_{E \in \mathscr{C}} E$. For $\alpha \in E_C$, there exists $E \in \mathscr{C}$ such that $\alpha \in E$. We can define $\iota_{E_C}(\alpha) := \iota_E(\alpha)$. It is clear that it is independent of the choice of E. Then (E_C, ι_{E_C}) is an upper bound of $\mathscr{C}$. By Zorn's Lemma, $\mathscr{S}$ has a maximal element. We denote it by (G, ι_G). We claim that $G = K$.

Let $H := \iota_G(G) \subseteq L$. Suppose that $G \subsetneq K$. There exists $\alpha \in K \setminus G$. Consider the simple extension $G \subseteq G(\alpha)$. Since $F \subseteq K$ is algebraic extension, α is algebraic over G. Let $m \in G[x]$ be the minimal polynomial of α. ι_G induces the ring isomorphism $\widetilde{\iota_G} : G[x] \to H[x]$. Since L is algebraically closed, $\widetilde{\iota_G}(m)$ has a root β in L. By Proposition 3.1.11, the field isomorphism $G \cong H$ lifts to $G[\alpha] \cong H[\beta]$. We have $(G[\alpha], \iota_{G[\alpha]})$ strictly larger than (G, ι_G) in $\mathscr{S}$, contradicting the maximality of (G, ι_G). □

Corollary 3.2.12. Uniqueness of Algebraic Closure

Suppose that K_1 and K_2 are algebraic closures of the field F. Then there exists an $F-$isomorphism $K_1 \cong K_2$.

Proof. Since K_1 is algebraic over F and K_2 is algebraically closed, by Lemma 3.2.11, there exists a field monomorphism $\sigma : K_1 \hookrightarrow K_2$ with $\sigma|_F = \mathrm{id}_F$. If σ is not surjective, then $K_1 \subseteq K_2$ is a non-trivial algebraic extension, contradicting that K_1 is algebraically closed. Hence σ is an $F-$isomorphism. □

Corollary 3.2.13. Existence and Uniqueness of Splitting Field: General Case

Suppose that F is a field and $S \subseteq F[x]$ is a set of polynomials. Then there exists a splitting field K of S over F, which is unique up to $F-$isomorphism.

Proof. The existence of splitting fields follows from the existence of algebraic closure. The proof of uniqueness is a simple adaptation of Lemma 3.2.11. □

3.3 Separable, Normal and Galois Extensions

Definition 3.3.1. Normal Extensions

The field extension $F \subseteq K$ is called a normal extension, if the minimal polynomial over F of every element in K splits over K.

Proposition 3.3.2. Normal Extension $\iff$ Splitting Extension

A finite field extension $F \subseteq K$ is normal if and only if K is the splitting field of some $f \in F[x]$.

Definition 3.3.3. Separable Extensions

Let F be a field, and $f \in F[x] \setminus \{0\}$. We say that p is separable, if all the irreducible factors of f have no multiple roots in the splitting field of f.

Suppose that $F \subseteq K$ is an algebraic field extension. We say that it is a separable extension, if the minimal polynomial over F of every element in K is separable.

Remark. By Corollary 2.3.12, we see that $f \in F[x]$ is separable if and only if f and f' are coprime. Moreover, if f is inseparable and irreducible, then $f' = 0$.

Proposition 3.3.4. Separability and Characteristic

Suppose that F is a field with $\mathrm{char}\, F = 0$. Then any finite extension of F is a separable extension.

Proof. Suppose that $F \subseteq K$ is an inseparable extension. Let $f \in F[x]$ be a monic irreducible polynomial. Then $f' = 0$. If $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$, then $f'(x) = nx^{n-1} \sum_{k=1}^{n-1} k a_k x^{k-1} \neq 0$, since $n \neq 0$ in F. This is a contradiction. □

Proposition 3.3.5. Separability of Tower of Extensions

Suppose that $F \subseteq K \subseteq L$ are field extensions. If $F \subseteq L$ is separable, then both $F \subseteq K$ and $K \subseteq L$ are separable.

Definition / Proposition 3.3.6. Fixed Fields, Galois Extension

Suppose that $F \subseteq K$ is a finite extension. The Galois group $\mathrm{Gal}(K \mid F)$ has a natural group action on F. The elements fixed by $\mathrm{Gal}(K \mid F)$ form a subfield of K:

$$K^{\mathrm{Gal}(K|F)} := \{u \in K : \ \forall \sigma \in \mathrm{Gal}(K \mid F)\ \sigma(u) = u\}$$

which is called the fixed field of $\mathrm{Gal}(K \mid F)$. The following statements are equivalent:

1. $F = K^{\mathrm{Gal}(K|F)}$;
2. $F \subseteq K$ is a separable and normal extension;
3. K is the splitting field of some separable polynomial $f \in F[x]$.

If $F \subseteq K$ satisfies any of the conditions, then it is called a Galois extension.

3.4 Galois Correspondence

In this section, we fix a finite field extension $F \subseteq K$ and its Galois group $\mathrm{Gal}(K \mid F)$. We introduce the *prime notation* temporarily:

- For a subgroup H of the Galois group $\mathrm{Gal}(K \mid F)$, we denote the subfield of K fixed by H by K^H or simply H';
- For an intermediate field M of $F \subseteq K$, we denote the Galois group of $M \subseteq K$ by $\mathrm{Gal}(K \mid M)$ or simply M'.

Lemma 3.4.1. Artin's Lemma

Suppose that K is field and $G \leqslant \mathrm{Aut}(K)$ is a finite subgroup of the group of all field automorphisms of K. Then $K^G \subseteq K$ is a finite Galois extension, and the inclusion $G \hookrightarrow \mathrm{Gal}\left(K \mid K^G\right)$ is an isomorphism of groups.

Theorem 3.4.2. Galois Correspondence, Part 1

Suppose that $F \subseteq K$ is a finite Galois extension. There is a bijective correspondence between the intermediate fields of $F \subseteq K$ and the subgroups of $\mathrm{Gal}(K \mid F)$, given by

$$\{\text{intermediate fields of } K \mid F\} \longleftrightarrow \{\text{subgroups of } \mathrm{Gal}(K \mid F)\}$$

$$M \longmapsto \mathrm{Gal}(K \mid M)$$

$$K^H \longmapsfrom H$$

where $[K : M] = |\mathrm{Gal}(K \mid M)|$. Moreover, the correspondence reverses inclusion relations:

$$\{\text{intermediate fields of } K \mid F\} \longleftrightarrow \{\text{subgroups of } \mathrm{Gal}(K \mid F)\}$$

$$L \subseteq M \longmapsto \mathrm{Gal}(K \mid L) \geqslant \mathrm{Gal}(K \mid M)$$

$$K^H \subseteq K^J \longmapsfrom H \geqslant J$$

Remark. In our prime notation, we can write things in a more elegant way. If L, M are intermediate fields with $L \subseteq M$, then $[M : L] = [M' : L']$. If H, J are subgroups of $\mathrm{Gal}(K \mid F)$ with $J \leqslant H$, then $[H : J] = [H' : J']$.

Corollary 3.4.3

Suppose that $F \subseteq K$ is a finite Galois extension. Then it has finitely many intermediate fields.

Theorem 3.4.4. Galois Correspondence, Part 2

Suppose that $F \subseteq K$ is a finite Galois extension. Let M be an intermediate field. Then $F \subseteq M$ is an Galois extension if and only if $\mathrm{Gal}(K \mid M)$ is a normal subgroup of $\mathrm{Gal}(K \mid F)$. In such case, there is a group isomorphism:

$$\frac{\mathrm{Gal}(K \mid M)}{\mathrm{Gal}(K \mid F)} \cong \mathrm{Gal}(M \mid F)$$

3.5 Finite and Perfect Fields

In this section we consider fields with non-zero characteristic p.

Definition 3.5.1. Frobenius Automorphisms, Perfect Fields

Suppose that F is a field with $\mathrm{char}\, F = p$. Then the map $x \mapsto x^p$ is a ring homomorphism on F, and is called the Frobenius homomorphism.

F is called a perfect field, if all the finite extensions of K are separable.

Proposition 3.5.2. Perfect Fields

Suppose that F is a field.

1. If $\mathrm{char}\, F = 0$, then F is perfect;
2. If $\mathrm{char}\, F = p$, then F is perfect if and only if the Frobenius homomorphism is surjective.
3. Finite fields are perfect.

Proposition 3.5.3. Extensions of Perfect Fields

Suppose that $F \subseteq K$ is a separable extension. Then F is perfect if and only if K is perfect.

Proposition 3.5.4. Finite Fields

Let p be a prime number, and $m, n \in \mathbb{Z}_+$.

1. For each p^m, there exists a unique finite field $\mathbb{F}_{p^m}$ up to isomorphism, which is the splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$.
2. $\mathrm{Gal}\left(\mathbb{F}_{p^m} \mid \mathbb{F}_p\right) \cong \mathbb{Z}/m\mathbb{Z}$, whose generator is given by the Frobenius automorphism.
3. For each divisor d of m, there is a unique subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_{p^m}$.

Corollary 3.5.5. Primitive Element Theorem for Finite Fields

Suppose that F and K are finite fields and $F \subseteq K$. Then there exists $\alpha \in K$ such that $K = F(\alpha)$.

Theorem 3.5.6. Primitive Element Theorem

Suppose that $F \subseteq K$ is a finite separable extension. Then it is a simple extension.

3.6 Cyclotomic and Cyclic Extensions

Definition 3.6.1. Roots of Unity

Suppose that F is a field. The n-th roots of unity of F forms a group:

$$\mu_n(F) := \{\rho \in F : \ \rho^n = 1\}$$

which is a subgroup of $F^\times$. $\mu_n(F)$ is a **finite cyclic group**.

Suppose that $|\mu_n(F)| = n$. Then $\omega \in \mu_n(F)$ is called a primitive n-th root of unity, if ω generates $\mu_n(F)$.

Definition 3.6.2. Cyclotomic Extensions, Cyclotomic Polynomials

Suppose that F is a field with $\operatorname{char} F \nmid n$. Then the splitting field of $x^n - 1$ over F is denoted by $F(\omega_n)$, where ω_n is a primitive n-th root of unity of $F(\omega_n)$. The extension $F \subseteq F(\omega_n)$ is called a cyclotomic extension.

The n-th cyclotomic polynomial of F is defined by

$$\Phi_n(x) := \prod_{\substack{\omega \in \mu_n(F(\omega_n)) \\ \omega \text{ primitive}}} (x - \omega)$$

Proposition 3.6.3

$$x^n - 1 = \prod_{d|n} \Phi_n(x)$$

Proposition 3.6.4. Galois Group of Cyclotomic Extension

Suppose that $F \subseteq F(\omega_n)$ is a cyclotomic extension. Then it is a Galois extension with Galois group

$$\operatorname{Gal}(F(\omega_n) \mid F) \cong \operatorname{Aut}(\mu_n(F(\omega_n))) \cong (\mathbb{Z}/k\mathbb{Z})^\times$$

where $k := |\mu_n(F(\omega_n))|$.

Proposition 3.6.5. Cyclotomic Polynomials of $\mathbb{Q}$

Suppose that Φ_n is the n-th cyclotomic polynomial of $\mathbb{Q}$.

1. $\Phi_n \in \mathbb{Z}[x]$;
2. Φ_n is irreducible;
3. If $m, n \in \mathbb{Z}_+$ are coprime, then $\deg(\Phi_n \Phi_m) = \deg \Phi_n \deg \Phi_m$.

Definition 3.6.6. Kummer Extensions

Suppose that F is field with $\operatorname{char} F \nmid n$ in which $x^n - 1$ splits. Let K be the splitting field of $x^n - a$ over F for some $a \in F$. Then $F \subseteq K$ is called a Kummer extension.

Proposition 3.6.7. Galois Group of Kummer Extension

Suppose that $F \subseteq K$ is a Kummer extension defined as above. Then it is a Galois extension. Let α be a root of $x^n - a$ in K. Then there exists a group monomorphism $\varphi : \operatorname{Gal}(K \mid F) \to \mu_n(F)$ given by $\varphi(\sigma) = \sigma(\alpha)/\alpha$. The map is independent of the choice of α.

3.7 Radical Extensions

Definition 3.7.1. Radical Extension, Solution by Radicals

Suppose that $F \subseteq F(\alpha_1, ..., \alpha_k)$ is a finite extension. It is called a radical extension, if there exists $n_1, ..., n_k \in \mathbb{N}$ such that $\alpha_i^{n_i} \in F(\alpha_1, ..., \alpha_{i-1})$ for each i.

Let $f \in F[x]$. We say that f is solvable by radicals, if the splitting field of f is a radical extension of F.

Theorem 3.7.2. Solvability by Radicals

The finite extension $F \subseteq K$ is a radical extension if $\mathrm{Gal}(K \mid F)$ is a solvable group.

3.8 Transcendental Extensions

Definition 3.8.1. Algebraic Independence

Suppose that $F \subseteq K$ is a field extension. $S \subseteq K$ is said to algebraically independent over F, if for any $\alpha_1, ..., \alpha_n \in S$, there is no $f(x_1, ..., x_n) \in F[x_1, ..., x_n]$ such that $f(\alpha_1, ..., \alpha_n) = 0$.

Definition 3.8.2. Transcendence Bases

Suppose that $F \subseteq K$ is a field extension. A subset $S \subseteq K$ is called a transcendence basis of K over F, if S is algebraically independent over F and K is an algebraic extension of $F(S)$.

Proposition 3.8.3. Cardinality of Transcendence Bases

Suppose that $F \subseteq K$ is a field extension. If S and T are transcendence bases of K over F, then $\mathrm{card}\, S = \mathrm{card}\, T$.

Definition 3.8.4. Transcendence Degree

Suppose that $F \subseteq K$ is a field extension. We define the transcendence degree $\mathrm{tr.deg}(K \mid F)$ of $F \subseteq K$ to be the cardinality of any transcendence basis of K over F

Proposition 3.8.5. Tower Law of Transcendence Degree

Suppose that $F \subseteq K \subseteq L$ are field extensions. The transcendence degree of field extensions is additive:

$$\mathrm{tr.deg}(L \mid F) = \mathrm{tr.deg}(L \mid K) + \mathrm{tr.deg}(K \mid F)$$

Chapter 4

Modules

4.1 Modules and Algebras

4.1.1 Definitions and Examples

For a category C (in particular for $\mathsf{C} = \mathsf{Set}$) and a object S in C, the set of automorphisms $\mathrm{Aut}_{\mathsf{C}}(S)$ is a group. Hence we can define a group (left-)action of a group G on S via a group homomorphism $\sigma : G \to \mathrm{Aut}_{\mathsf{C}}(S)$. Similarly, if M is an Abelian group, then the set of automorphisms $\mathrm{Aut}_{\mathsf{Ab}}(M)$ naturally forms a unital ring. We can define a ring (left-)action of a ring R on M via a unital ring homomorphism $\sigma : R \to \mathrm{Aut}(M)$. In this way we identify M as a **left R-module**.

For $r \in R$, $m \in M$, we often consider $\sigma(r)(m)$ as the multiplication rm. In this way we obtain our familiar definition of left R-modules:

Definition 4.1.1. Left R-Modules

A left R-module M is an Abelian group $(M, +)$ with a map (namely **scalar multiplication**) $R \times M \to M$, $(r, m) \mapsto rm$, satisfying the following axioms:

1. Associativity: $\forall\, r, s \in R \;\; \forall\, m \in M : \quad r(sm) = (rs)m$
2. Distributivity: $\forall\, r, s \in R \;\; \forall\, m, n \in M : \quad (r+s)m = rm + sm, \quad r(m+n) = rm + rn$
3. Identity: $\forall\, m \in M : \quad 1_R m = m$

Remark. Analogusly we can define a right R-module M to be an Abelian group M with a map $M \times R \to M$, $(m, r) \mapsto mr$ satisfying similar axioms.

For a ring $(R, +, \cdot)$, we can define the **opposite ring** $R^{\mathrm{op}} = (R, +, \star)$, where $r \star s := s \cdot r$ for all $r, s \in R$. If R is commutative, we in fact have $R \cong R^{\mathrm{op}}$.

Now we immediately observe that a right R-module is simply a left R^{op}-module. If R is commutative, then there is essentially no need to distinguish between the left and right modules[1]. We shall say ***R*-modules** instead of left R-modules.

Definition 4.1.2. R-Module Homomorphisms

Suppose that M and N are left R-modules. A group homomorphism $f : M \to N$ is said to be an R-module homomorphism, if

$$\forall\, r \in R \;\; \forall\, m \in M : \quad f(rm) = r f(m)$$

In other words, R-module homomorphism = group homomorphism + compactible module structure.

Definition 4.1.3. Submodules

Suppose that M is an R-module. $N \subseteq M$ is said to be a submodule of M, if the inclusion map $\iota : N \hookrightarrow M$ is a R-module homomorphism.

Definition 4.1.4. The Category R-Mod

It is clear that left R-modules together with their homomorphisms form a catgory, which is denoted by R-Mod.

Correspondingly, the category of right R-modules is denoted by Mod-R.

[1] Even if R is commutative, M can have compatible left and right R-module structures which are not identical, in which case M is said to be a **bimodule**.

Example 4.1.5. Examples of Modules

1. Every Abelian group G has a unique $\mathbb{Z}$-module structure:
$$\forall\, n \in \mathbb{Z}\ \ \forall\, g \in G\colon \quad ng := \underbrace{g + \cdots + g}_{n \text{ times}}$$
This is because $\mathbb{Z}$ is initial in Ring, so there is a unique ring homomorphism $\sigma : \mathbb{Z} \to \mathrm{Aut}(G)$.
In fact, the category $\mathbb{Z}$-Mod is just Ab.
2. If F is a field, then a F-module V is called a **vector space** over F. The F-module homomorphisms between vector spaces are called **linear maps**. The category of all vector spaces over F is denoted by $\boldsymbol{F}$**-Vect**.
3. Suppose that R and S are unital rings. Then a unital ring homomorphism $\alpha : R \to S$ defines an R-module structure on S by $(r, s) \mapsto \alpha(r)s$ for $r \in R$ and $s \in S$.
4. Take $S = R$ and $\alpha = \mathrm{id}_R$ in the previous example. Then R itself is an R-module. In particular, the (left-)submodules of R is exactly the (left-)ideals of R.
5. Suppose that R is a CRI and M, N are R-modules. Then the set of R-module homomorphisms from M to N, $\mathrm{Hom}_R(M, N)$, also has an R-module structure. For $r \in R$ and $\varphi \in \mathrm{Hom}_R(M, N)$, the prescription:
$$\forall\, m \in M\colon \quad (r\varphi)(m) := r\varphi(m)$$
defines a map $r\varphi : M \to N$. It is a group homomorphism because M and N are Abelian groups. It is an R-module homomorphism because R is commutative:
$$\forall\, a \in R\ \ \forall\, m \in M\colon \quad (r\varphi)(am) = r\varphi(am) = ra\varphi(m) = ar\varphi(m) = a(r\varphi)(m)$$
Therefore $(r, \varphi) \mapsto r\varphi$ endows $\mathrm{Hom}_R(M, N)$ with an R-module structure.
If R is non-commutative, then $\mathrm{Hom}_R(M, N)$ may be just an Abelian group.
6. Suppose that R is a CRI, M is a R-module, and $\varphi : M \to M$ is a R-module homomorphism. Then φ defines a $R[x]$-module structure on M by $(f, m) \mapsto f(\varphi)(m)$ for $f \in R[x]$ and $m \in M$. [1]

4.1.2 Submodules and Quotient Modules

Proposition 4.1.6. Kernels and Images are Submodules

Suppose that $f : M \to N$ is an R-module homomorphism. Then $\ker f$ is a submodule of M, and $\mathrm{im}\, f$ is a submodule of N.

Proposition 4.1.7

Suppose that M is an R-module.

For $r \in R$, $rM := \{rm \in M\colon\ m \in M\}$ is a submodule of M.

For $I \lhd R$, $IM := \{rm \in M\colon\ r \in I,\ m \in M\}$ is a submodule of M.

Just as groups and rings, we can define the quotient modules, which satisfy the three isomorphism theorems:

Definition 4.1.8. Quotient Modules

Suppose that M is an R-module and $N \leqslant M$ is a submodule. Then it is easy to check that $m \sim m' \iff m - m' \in M$ defines an equivalence relation on M. In particular M/N is a quotient group. We define scalar multiplication on M/N by:
$$\forall\, r \in R\ \ \forall\, m + N \in M/N\colon \quad r(m + N) := rm + N$$
Then M/N is an R-module. We call it a quotient module.

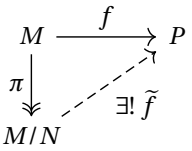
As usual, we can formulate the universal property as follows:

[1] This follows from the fact that the set of endomorphisms of M, $\mathrm{End}_R(M)$, is not only an R-module, but also an R-algebra.

Proposition 4.1.9. Quotient Modules: Universal Property

Suppose that M is an R-module and N is a submodule of M. The quotient module is the module M/N with the canonical projection $\pi : M \twoheadrightarrow M/N$ satisfying the following universal perperty:

For any R-module P and R-module homomorphism $f : M \to P$ such that $N \subseteq \ker f$, there exists a unique R-module homomorphism $\widetilde{f} : M/N \to P$ such that $f = \widetilde{f} \circ \pi$.



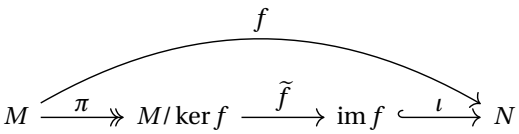
Moreover, any R-module satisfying the universal property is uniquely determined up to R-module isomorphism.

Remark. From the universal property, we note that every submodule N is the kernel of the canonical projection $\pi : M \twoheadrightarrow M/N$. Unlike in Grp or Ring, being a kernel poses no restriction on the sub-structures in R-Mod. We shall see that R-Mod is a very "nice" category in some sense (see Section 4.2).

Next we shall present the three isomorphisms for modules. The proofs are identical to those for the rings.

Theorem 4.1.10. Canonical Decomposition / First Isomorphism Theorem

Suppose that $f : M \to N$ is an R-module homomorphism. Then the following diagram commutes:



In particular, $\widetilde{f}$ is an isomorphism between $M/\ker f$ and $\operatorname{im} f$.

Theorem 4.1.11. Second Isomorphism Theorem

Suppose that N and P are submodules of an R-module M. Then $N \cap P$ is a submodule of N and $N + P$ is a submodule of M. In particular, we have the R-module isomorphism:

$$\frac{N}{N \cap P} \cong \frac{N+P}{P}$$

Theorem 4.1.12. Third Isomorphism Theorem

Suppose that M is an R-module and $N \leqslant P \leqslant M$. Then $P/N \leqslant M/N$. In particular we have the R-module isomorphism:

$$\frac{M/N}{P/N} \cong M/P$$

Definition 4.1.13. Submodules generated by a subset

Suppose that M is an R-module and $A \subseteq M$ is a subset. The submodule of M generated by A is the intersection of all submodules of M that contain A. It is denoted by $\langle A \rangle$. Explicitly,

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i m_i : \ r_1, ..., r_n \in R, \ m_1, ..., m_n \in A, \ n \in \mathbb{N} \right\}$$

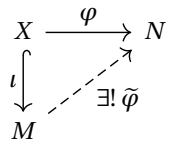
A module is said to be **finitely generated**, if it is generated by a finite set; a module is said to be **cyclic**, if it is generated by a single element.

Remark. We give the definition of free modules using universal property. The case is analogous to the free groups in Grp. The detailed discussion of free and finitely gerenated modules will be delayed to Section 5.1.

Definition 4.1.14. Free Modules, Universal Property

Suppose that M is a R-module and $X \subseteq M$. We say that M is a free module on X, if:

For any R-module N and map $\varphi : X \to N$, there exists a unique R-module homomorphism $\widetilde{\varphi} : M \to N$ such that $\varphi = \widetilde{\varphi} \circ \iota$.



where $\iota : X \hookrightarrow M$ is the inclusion map. X is called a **basis** of M.

Moreover, any free module on X is unique up to R-module isomorphism.

Remark. After defining direct products of modules in Section 4.2, we shall see that the set-theoretic constuction of a free R-module on X is $R^{\oplus X}$.

Proposition 4.1.15. Finitely Generated R-Modules

Suppose that M is a finitely generated R-module. Then M is isomorphic to a quotient of R^n for some $n \in \mathbb{N}$.

Proof. Let I be a generating set of M. We choose $X = \{1, ..., n\}$ where $n = \operatorname{card} I$. Then $R^{\oplus X} = R^n$ and $\widetilde{\varphi} : R^n \to M$ is surjective. By first isomorphism theorem the result follows. □

4.1.3 Algebra

Next we briefly introduce the concept of algebra. Roughly speaking, an R-algebra is a ring with a compatible R-module structure defined in the way of Example 4.1.5.3.

Definition 4.1.16. R-Algebras

Suppose that $\alpha : R \to S$ is a unital ring homomorphism such that $\alpha(R)$ commutes with S. Then we say that (S, α) is an R-algebra, or that α defines an R-algebra structure on S.

Remark. To see why this definition makes sense, we consider the compatibility of ring multiplication and scalar multiplcation. For $r_1, r_2 \in R$ and $s_1, s_2 \in S$:

$$r_1 r_2 \cdot s_1 s_2 = \alpha(r_1)\alpha(r_2)s_1 s_2 = \alpha(r_1)s_1\alpha(r_2)s_2 = (r_1 \cdot s_1)(r_2 \cdot s_2)$$

where $\cdot$ denotes scalar multiplcation and juxitaposition denotes ring multiplication. In order to let the second equality to hold, we must have that $\alpha(R)$ commutes with S.

Definition 4.1.17. R-Algebra Homomorphisms

Suppose that S and T are R-algebras. A map $f : S \to T$ is said to be an R-algebra homomorphism, if it is both a ring homomorphism and an R-module homomorphism.

Definition 4.1.18. The Category R-Alg

R-algebras with their homomorphisms form a catgory, which is denoted by R-Alg.

Example 4.1.19. Ring $\cong \mathbb{Z}$-Alg

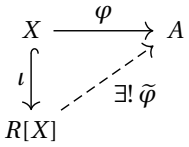
Every unital ring R is has a unique $\mathbb{Z}$-algebra structure:

$$\forall\, n \in \mathbb{Z}\ \ \forall\, r \in R : \quad nr := \underbrace{r + \cdots + r}_{n \text{ times}}$$

Example 4.1.20. Free Commutative R-Algebras

Suppose that R is a CRI. The polynomial ring $R[X]$ on R is a free commutative R-algebra. It is "free" in the sense that it satisfies the universal property of a free object on the set X in the category of commutative R-algebras:

For any commutative R-algebra A and map $\varphi : X \to A$, there exists a unique R-algebra homomorphism $\widetilde{\varphi} : F[X] \to A$ such that $\varphi = \widetilde{\varphi} \circ \iota$.



Proposition 4.1.21. Finitely Generated Commutative R-Algebras

Suppose that R is a CRI and A is a finitely generated commutative R-algebra. Then A is isomorphic to a quotient of the polynomial ring $R[x_1, ..., x_n]$ for some $n \in \mathbb{N}$.

Proof. Let I be a generating set of A. We choose $X = \{x_1, ..., x_n\}$ where $n = \operatorname{card} I$. Then $\widetilde{\varphi} : R[x_1, ..., x_n] \to A$ is surjective. By first isomorphism theorem the result follows. □

Definition 4.1.22. Finite v.s. Finite-Type

Suppose that S is an R-algebra. Then the ring homomorphism $\alpha : R \to S$ is said to be *finite*, if S is a *finitely generated R-module*; it is said to be *of finite-type*, if S is a *finitely generated R-algebra*.

Remark. It is obvious that being finite is a stronger condition than being of finite type. A special case of the converse, where a finite-type field extension is finite, is known as **Hilbert's Weak Nullstellensatz ??**.

4.2 The Category R-Mod

We shall introduce some categorical construction that makes R-Mod an Abelian category.

This section can be skipped in the first reading.

4.2.1 Products and Coproducts

The construction of products and coproducts of R-modules by universal properties is idential to those of rings.

Definition 4.2.1. Products and Coproducts in R-Mod

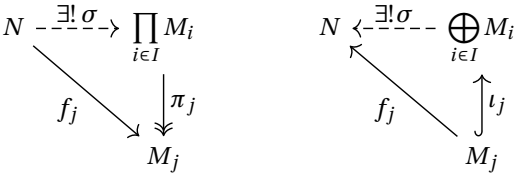
Suppose the $\{M_i\}_{i \in I}$ is a family of R-modules.

The **product** is the R-module $\prod_{i \in I} M_i$ with the canonical projections $\pi_j : \prod_{i \in I} M_i \twoheadrightarrow M_j$ satisfying the following universal property:

For any R-module N and R-module homomorphisms $f_j : N \to M_j$, there exists a unique R-module homomorphism $\sigma : N \to \prod_{i \in I} M_i$ such that $f_j = \pi_j \circ \sigma$.

The **coproduct** or the **direct sum** is the R-module $\bigoplus_{i \in I} M_i$ with the canonical inclusions $\iota_j : M_j \hookrightarrow \bigoplus_{i \in I} M_i$ satisfying the following universal property:

For any R-module N and R-module homomorphisms $f_j : M_j \to N$, there exists a unique R-module homomorphism $\sigma : \bigoplus_{i \in I} M_i \to N$ such that $f_j = \sigma \circ \iota_j$.



Lemma 4.2.2. Existence of Products and Coproducts

Let $\{M_i\}_{i\in I}$ be a the family of R-modules. Then the product $\prod_{i\in I} M_i$ and the coproduct $\bigoplus_{i\in I} M_i$ exists in R-Mod.

Remark. Products are special cases of limits, and coproducts are speccial cases of colimits. In general, the small limits and small colimits exist in R-Mod. Therefore the category R-Mod is **complete** and **cocomplete**.

Proposition 4.2.3. Finite Product and Coproduct Coincide

Let $\{M_i\}_{i\in I}$ be a the family of R-modules, where I is a finite index set. Then the product $\prod_{i\in I} M_i$ and the coproduct $\bigoplus_{i\in I} M_i$ coincide.

Remark. Let M and N be R-modules. The product ans coproduct of M and N concide. It is called a **biproduct** or a **direct sum** of M and N, and is denoted by $M \oplus N$.

4.2.2 Kernels and Cokernels

In set-theoretic language, the cokernel of a morphism $f : A \to B$ is the quotient object $\operatorname{coker} f := B/\operatorname{im} f$. $\operatorname{coker} f$ may not exist. For example, if f is a ring homomorphism, then $\operatorname{im} f$ is generally not an ideal of B. However, the cokernels always exist in R-Mod. Below we shall give a categorical description of kernels and cokernels.

Definition 4.2.4. (Categorical) Kernels and Cokernels

Let $\varphi : M \to N$ be an R-module homomorphism.

The kernel of φ is the R-module homomorphism $\ker\varphi : K \to M$ satisfying the following universal property:

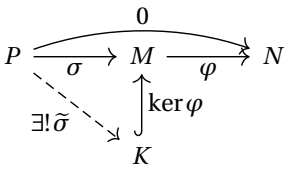
For any R-module P and R-module homomorphism $\sigma : P \to M$ such that $\varphi\circ\sigma = 0$, there exists a unique R-module homomorphism $\widetilde{\sigma} : P \to K$ such that $\sigma = \ker\varphi\circ\widetilde{\sigma}$.

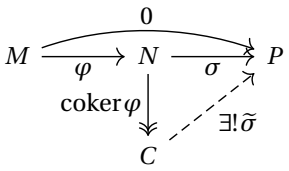
We say that $\ker\varphi$ **exhibits** K **as the kernel of** φ. The universal property essentially says that $\varphi\circ\sigma = 0$ implies that σ factors through the kernel of φ.

The cokernel of φ is the R-module homomorphism $\operatorname{coker}\varphi : N \to C$ satisfying the following universal property:

For any R-module P and R-module homomorphism $\sigma : N \to P$ such that $\sigma\circ\varphi = 0$, there exists a unique R-module homomorphism $\widetilde{\sigma} : C \to P$ such that $\sigma = \widetilde{\sigma}\circ\operatorname{coker}\varphi$.

We say that $\operatorname{coker}\varphi$ **exhibits** C **as the cokernel of** φ. The universal property essentially says that $\sigma\circ\varphi = 0$ implies that σ factors through the cokernel of φ.





Remark. In the categorical language, the **image** of φ is defined by $\operatorname{im}\varphi := \ker(\operatorname{coker}\varphi)$. The **coimage** of φ is defined by $\operatorname{coim}\varphi := \operatorname{coker}(\ker\varphi)$.

The following lemma is straightforward.

Lemma 4.2.5. Existence of Kernels and Cokernels

Let $\varphi : M \to N$ be an R-module homomorphism. Then the kernel $\ker\varphi : K \to M$ and the cokernel $\operatorname{coker}\varphi : N \to C$ exist in R-Mod.

Lemma 4.2.6

Let $\varphi : M \to N$ be an R-module homomorphism.

1. φ is a monomorphism if and only if it is the kernel of some R-module homomorphism;
2. φ is an epimorphism if and only if it is the cokernel of some R-module homomorphism.

Corollary 4.2.7

1. Every kernel in R-Mod is the kernel of its cokernel;
2. Every cokernel in R-Mod is the cokernel of its kernel.

4.2.3 Abelian Categories

Definition 4.2.8. Ab-Enriched Categories, Additive Categories, Pre-Abelian Categories, Abelian Categories

Let C be a locally small[a] category. Consider the following properties:

(1) Every Hom set in C is equipped with the structure of an Abelian group, such that the composition

$$\mathrm{Hom}(X,Y)\times\mathrm{Hom}(Y,Z)\to\mathrm{Hom}(X,Z)$$

is $\mathbb{Z}$-bilinear.

(2) The zero object 0 exists in C.

(3) Finite products and coproducts exist in C.

(4) Kernels and cokernels exist in C.

(5) Every monomorphism is a kernel, and every epimorphism is a cokernel.

We say that C is

- Ab-enriched, if it satisfies (1);
- additive, if it satisfies (1)-(3);
- pre-Abelian, if it satisfies (1)-(4);
- Abelian, if it satisfies (1)-(5).

[a] Informally, every $\mathrm{Hom}(X,Y)$ is a set.

Remark. Abelian categories can be viewed as a vast generalisation of the category of Abelian groups Ab.

Corollary 4.2.9. R-Mod is Abelian

R-Mod is an Abelian Category.

Remark. The following powerful theorem states that, in most cases working in Abelian categories are the same as working in R-Mod. A sketch of proof can be found in Charles Weibel's *An Introduction to Homological Algebra*, §1.6.

Theorem 4.2.10. Freyd-Mitchell Embedding Theorem

If A is a small[a] Abelian category, then there is a (not necessarily commutative) ring R and an exact[b], fully faithful functor from A into R-Mod, which embeds A as a full subcategory in the sense that $\mathrm{Hom}_{\mathsf{A}}(M,N)\cong\mathrm{Hom}_R(M,N)$.

[a] Informally, the class of morphisms $\mathrm{Mor}(\mathsf{A})$ is a set.
[b] See Definition **??**.

4.3 Exact Sequences

4.3.1 Chain Complexes and Exact Sequences

Definition 4.3.1. Chain Complexes, Exactness

A chain complex $(M_\bullet, d_\bullet)$ of R-modules is a sequence

$$\cdots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots$$

such that $d_i \circ d_{i+1} = 0$. $d_\bullet$ are called the **differential maps**.

Note that $d_i \circ d_{i+1} = 0$ is equivalent to $\operatorname{im} d_{i+1} \subseteq \ker d_i$. We say that the sequence is exact at M_i if $\operatorname{im} d_{i+1} = \ker d_i$.[a]

[a] In a more "categorical" description, the exactness means that $d_{i+1} = \ker d_i$ and $d_i = \operatorname{coker} d_{i+1}$.

It is immediate from the definition that:

- The chain $0 \longrightarrow A \xrightarrow{f} B \longrightarrow \cdots$ is exact at A if and only if f is a monomorphism;
- The chain $\cdots \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ is exact at B if and only if f is an epimorphism;
- The chain $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ is exact at A and B if and only if f is an isomorphism.

Definition 4.3.2. Short Exact Sequence

The following sequence is called a short exact sequence if it is exact at A, B and C.

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Equivalently, f is a monomorphism, g is an epimorphism, and $\ker g = \operatorname{im} f$.

Short exact sequences are ample in R-Mod.

Example 4.3.3. Examples of short exact sequences

1. Let $\varphi\colon M \to N$ be a R-module homomorphism. Then we have the short exact sequence:
$$0 \longrightarrow \ker\varphi \longrightarrow M \longrightarrow \operatorname{im}\varphi \longrightarrow 0$$
2. Let M be an R-module and N be a submodule of M. Then we have the short exact sequence:
$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$
where $\iota : N \to M$ is the inclusion and $\pi : M \to M/N$ is the quotient map.
3. Let M_1 and M_2 be R-modules. We have the short exact sequence:
$$0 \longrightarrow M_1 \xrightarrow{\iota_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$$
where $\iota_1 : M_1 \to M_1 \oplus M_2$ is the inclusion and $\pi_2 : M_1 \oplus M_2 \to M_2$ is the projection.

Remark. Let $\varphi\colon M \to N$ be a R-module homomorphism. In fact we can construct a slightly longer exact sequence:

$$0 \longrightarrow \ker\varphi \longrightarrow M \xrightarrow{\varphi} N \longrightarrow \operatorname{coker}\varphi \longrightarrow 0$$

Definition 4.3.4. Splitting Short Exact Sequences

We say that the short exact sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

splits, if there is an isomorphism of short exact sequences given by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} & & \\ 0 & \longrightarrow & M & \xrightarrow{\iota} & M \oplus N & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array}$$

In particular, $B \cong A \oplus C$ as R-modules.

Example 4.3.5. Non-Example of Splitting Short Exact Sequence

The following sequence is exact but does not split:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Theorem 4.3.6. Splitting Lemma

Consider the short exact sequence of R-modules:

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

The following are equivalent:

1. There exists a retraction $r : B \to A$ such that $r \circ f = \mathrm{id}_A$;
2. There exists a section $s : C \to B$ such that $g \circ s = \mathrm{id}_C$;
3. The short exact sequence splits.

4.3.2 Diagram Chase

We present two crucial lemmata. Their proofs illustrate the principle of diagram chase.

Theorem 4.3.7. Snake Lemma

Suppose that we have the following commutative diagram:

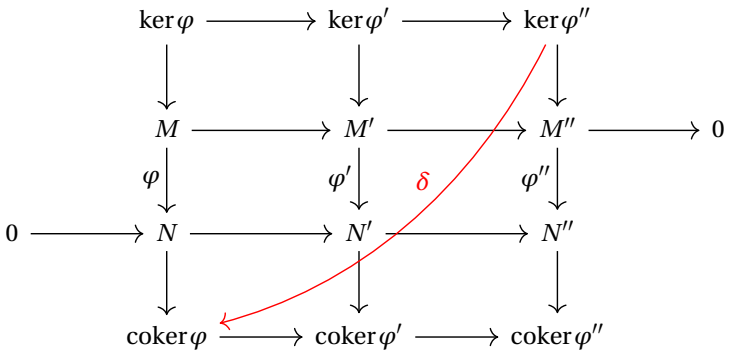
$$\begin{array}{ccccccccc} & & M & \longrightarrow & M' & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi''} & & \\ 0 & \longrightarrow & N & \longrightarrow & N' & \longrightarrow & N'' & & \end{array}$$

where the rows are exact sequences. Then there is a long exact sequence

$$\ker\varphi \longrightarrow \ker\varphi' \longrightarrow \ker\varphi'' \xrightarrow{\delta} \operatorname{coker}\varphi \longrightarrow \operatorname{coker}\varphi' \longrightarrow \operatorname{coker}\varphi''$$

Remark. $\delta : \ker\varphi'' \to \operatorname{coker}\varphi$ is called the **connecting map**.

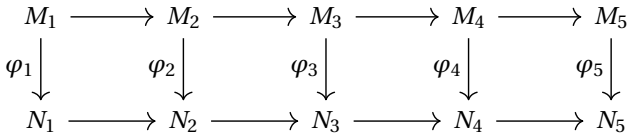
Proof.



□

Theorem 4.3.8. Five Lemma

Suppose that we have the following commutative diagram:



where the rows are exact sequences.

1. If φ_1 is an epimorphism, and φ_2, φ_4 are monomorphisms, then φ_3 is a monomorphism;
2. If φ_5 is a monomorphism, and φ_2, φ_4 are epimorphisms, then φ_3 is an epimorphism;
3. In particular, if φ_1 is an epimorphism, φ_5 is a monomorphism, and φ_2, φ_4 are isomorphisms, then φ_2 is an isomorphism.

4.3.3 Exact Functors

Definition 4.3.9. Additive Functors

Let $F\colon R\text{-Mod} \to S\text{-Mod}$ be a functor. We say that F is additive, if for all R-modules M and N,

$$F\colon \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_S(F(M),F(N))$$

is a homomorphism of Abelian groups.

Definition 4.3.10. Exact Functors

Let $F\colon R\text{-Mod} \to S\text{-Mod}$ be an additive functor. F is said to be

1. left exact, if for any exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C$, the sequence $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C)$ is exact;
2. right exact, if for any exact sequence $A \longrightarrow B \longrightarrow C \longrightarrow 0$, the sequence $F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$ is exact;
3. exact, if it is both left and right exact.

Proposition 4.3.11. Characterisations of Exact Functors

Let $F\colon R\text{-Mod} \to S\text{-Mod}$ be an additive functor. The following are equivalent:

1. F is exact;
2. F preserves any short exact sequence;
3. F preserves any exact sequence.

4.3.4 Homology

Homology is a central tool in algebraic topology and algebraic geometry.

Definition 4.3.12. Homology

Let $(M_\bullet, d_\bullet)$ be a chain complex of R-modules. We define the n-th homology to be the R-module:

$$H_n(M_\bullet) := \frac{\ker d_n}{\operatorname{im} d_{n+1}}$$

Remark. We note that the chain is exact at M_n if and only if $H_n(M_\bullet) = 0$. We can view the homology as a meaure of failure of the chain from being exact.

Remark. Homology can be considered as a vast generalisation of the notion of kernels and cokernels. Take the chain complex

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M_0 \longrightarrow 0$$

Then $H_1(M_\bullet) = \ker\varphi$ and $H_0(M_\bullet) = \operatorname{coker}\varphi$.

Lemma 4.3.13

Let $(M_\bullet, d_\bullet)$ be a chain complex of R-modules. Then $d_n : M_n \to M_{n-1}$ induces $\widetilde{d}_n : \operatorname{coker} d_{n+1} \to \ker d_{n-1}$ such that $H_n(M_\bullet) = \ker \widetilde{d}_n$ and $H_{n-1}(M_\bullet) = \operatorname{coker} \widetilde{d}_n$.

Definition 4.3.14. Chain maps

Let $(M_\bullet, d_\bullet)$ and $(N_\bullet, d'_\bullet)$ be two chain complexes. A morphism or chain map of chain complexes $f_\bullet : (M_\bullet, d_\bullet) \to (N_\bullet, d'_\bullet)$ is a family of R-module homomorphisms $f_i : M_i \to N_i$ such that the following diagram commutes:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & M_{i+1} & \xrightarrow{d_{i+1}} & M_i & \xrightarrow{d_i} & M_{i-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{i+1}} & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_{i-1}} & & \\
\cdots & \longrightarrow & N_{i+1} & \xrightarrow{d'_{i+1}} & N_i & \xrightarrow{d'_i} & N_{i-1} & \longrightarrow & \cdots
\end{array}$$

Remark. The chain complexes of R-modules form a category $\mathsf{Ch}(R\text{-}\mathsf{Mod})$, whose morphisms are chain maps.

Lemma 4.3.15. Ch(R-Mod) is Abelian

The category $\mathsf{Ch}(R\text{-}\mathsf{Mod})$ of chain complexes of R-modules is an Abelian category.

Lemma 4.3.16

Let $f_\bullet : (M_\bullet, d_\bullet) \to (N_\bullet, d'_\bullet)$ be a chain map between chain complexes of R-modules. Then $f_\bullet$ induces the R-module homomorphism $H_n(f) \colon H_n(M_\bullet) \to H_n(N_\bullet)$.

In particular, the n-th homology H_n is a covariant functor from $\mathsf{Ch}(R\text{-}\mathsf{Mod})$ to R-Mod.

Theorem 4.3.17. Long Exact Sequence of Homology

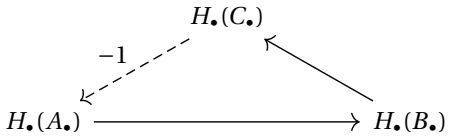
A short exact sequence of chain complexes of R-modules

$$0 \longrightarrow A_\bullet \xrightarrow{f_\bullet} B_\bullet \xrightarrow{g_\bullet} C_\bullet \longrightarrow 0$$

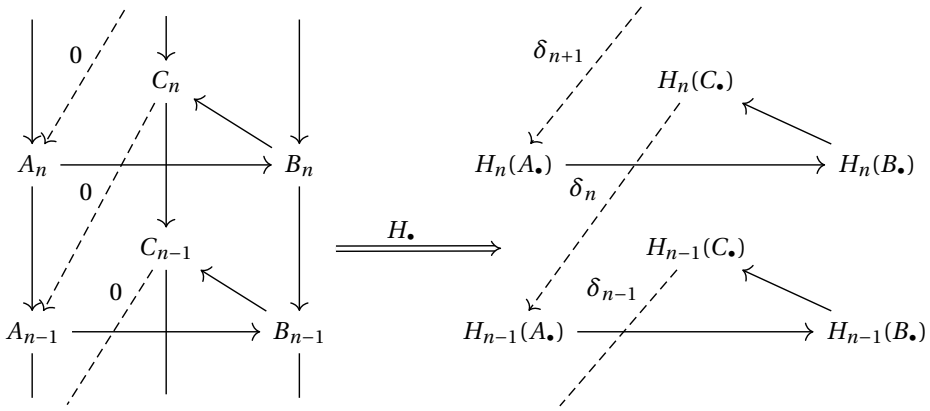
induces a long exact sequence of homology

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & H_n(A_\bullet) & \longrightarrow & H_n(B_\bullet) & \longrightarrow & H_n(C_\bullet) & & \\
 & & & & & \overset{\delta_n}{\swarrow} & & & \\
 & & H_{n-1}(A_\bullet) & \longrightarrow & H_{n-1}(B_\bullet) & \longrightarrow & H_{n-1}(C_\bullet) & \longrightarrow & \cdots
\end{array}$$

Remark. The long exact sequence can be represented by the **exact triangle**:



The theorem can also be drawn as three-dimensional commutative diagrams:



Chapter 5

Linear Algebra

Chapter 6

Commutative Algebra

6.1 Chain Conditions and Noetherian Rings

6.1.1 Chain Conditions

Definition 6.1.1. Ascending and Descending Chain Conditions

Suppose that R is a ring. We say that (the ideals of) R satisfy the ascending (*resp.* descending) chain condition, if any ascending (*resp.* descending) chain of ideals $\{I_n\}_{n\in\mathbb{N}}$ eventually stablises.

Suppose that M is a R-module. Similarly we can define the ascending (*resp.* descending) chain condition for the submodules of M.

Proposition 6.1.2. Chain Conditions and Exact Sequences

Let R be a CRI. Suppose that we have a short exact sequence of R-modules:

$$0 \longrightarrow M' \hookrightarrow M \twoheadrightarrow M'' \longrightarrow 0$$

Then M satisfies the ascending (*resp.* descending) chain condition if and only if both M' and M'' satisfy the ascending (*resp.* descending) chain condition.

Definition / Proposition 6.1.3. Noetherian Rings

Suppose that R is a CRI. The following are equivalent:

1. every ideal of R is finitely generated;
2. the ideals of R satisfy the ascending chain condition;
3. every non-empty set of ideals of R has a maximal element.

If R satisfies any of the above conditions, then we say that R is a Noetherian ring.

Definition / Proposition 6.1.4. Noetherian Modules

Suppose that R is a CRI and M is a R-module. The following are equivalent:

1. every submodule of M is finitely generated;
2. the submodules of M satisfy the ascending chain condition;
3. every non-empty set of submodules of M has a maximal element.

If M satisfies any of the above conditions, then we say that M is a Noetherian module.

Proposition 6.1.5. Quotient and Fraction Ring of Noetherian Rings

Suppose that R is a Noetherian ring,

1. For $I \lhd R$, the quotient ring R/I is also Noetherian.
2. For a multiplicatively closed subset $S \subseteq R$, the ring of fractions $S^{-1}R$ is also Noetherian.

Proposition 6.1.6. Modules over Noetherian Rings

Suppose that M is a finitely generated module over a Noetherian ring R, then M is a Noetherian module.

6.1.2 Properties of Noetherian Rings

Theorem 6.1.7. Hilbert's Basis Theorem

Suppose that R is a Noetherian ring. Then the polynomial ring $R[x]$ is also Noetherian.

Corollary 6.1.8. Polynomial Ring $R[x_1,...,x_n]$

If R is a Noetherian ring, then $R[x_1,...,x_n]$ is also Noetherian.

Lemma 6.1.9. Artin-Tate Lemma

Suppose that $R \subseteq S \subseteq T$ are ring extensions, where R is Noetherian. If T is finitely generated as a R-algebra and is finitely generated as a S-module, then S is finitely generated as a R-algebra.

Theorem 6.1.10. Hilbert's Weak Nullstellensatz

Suppose that $F \subseteq K$ is a field extension. If K is a finitely generated F-algebra, then $F \subseteq K$ is a finite extension.

6.2 Localisation of Rings and Modules

We have introduced the concept of localisation of rings in Section 1.5.3. We shall further develop this idea and extend it to modules in this section.

Definition / Proposition 6.2.1. Modules over Ring of Fractions

Suppose that R is a CRI, and $S \subseteq R$ is multiplicatively closed. Let M be a R-module such that, for each $s \in S$, the scalar multiplication $m \mapsto sm$ is an isomorphism of M. Then there exists a unique $S^{-1}R$ structure on M such that $(r/1_R)m = rm$ for all $m \in M$. The resulting $S^{-1}R$-module is denoted by $S^{-1}M$.

Proposition 6.2.2. Localisations Preserve Exactness

Suppose that R is a CRI, and $S \subseteq R$ is multiplicatively closed. Consider the complex of R-modules:

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \longrightarrow \cdots$$

The sequence is exact at M_i if and only if the following complex of $S^{-1}R$-modules is exact at $S^{-1}M_i$:

$$\cdots \longrightarrow S^{-1}M_{i-1} \xrightarrow{(\varphi_{i-1})_S} S^{-1}M_i \xrightarrow{(\varphi_i)_S} S^{-1}M_{i+1} \longrightarrow \cdots$$

Proposition 6.2.3

Suppose that R is a CRI, and $S \subseteq R$ is multiplicatively closed. Let M be an R-module. There exists an isomorphism of $S^{-1}R$-modules $f : S^{-1}R \otimes_R M \to S^{-1}M$ given by $f(r/s \otimes_R m) = rm/s$.

Corollary 6.2.4. Flatness of Localisations

Suppose that R is a CRI, and $S \subseteq R$ is multiplicatively closed. Let M be an R-module. The $S^{-1}R$-module $S^{-1}M$ is flat.

A property ψ of a CRI R (or a R-module M) is said to be a local proerty, if R (or M) has ψ if and only if R_P (or M_P) has ψ for all prime ideals $P \in \operatorname{Spec} R$.

Proposition 6.2.5

Suppose that R is a CRI. Let I, J be ideals of R. The following are equivalent:

1. $I = J$;
2. $IR_P = JR_P$ for all $P \in \operatorname{Spec} R$;
3. $IR_M = JR_M$ for all $M \in \operatorname{MaxSpec} R$.

6.3 Primary Decomposition

Definition 6.3.1. Primary Ideals

[] Suppose that R is a CRI. A non-trivial ideal I is said to be primary, if all zero-divisors of R/I are nilpotent.

Proposition 6.3.2. Radical of Primary Ideals

Suppose that R is a CRI. If I is a primary ideal of R, then $\sqrt{I}$ is the smallest prime ideal containing I.

Remark. If I is a primary ideal and $\sqrt{I} = P$ is a prime ideal, we also say that I is P-primary.

Proposition 6.3.3

Suppose that R is a CRI and $I \lhd R$. If $\sqrt{I}$ is a maximal ideal of R, then I is a primary ideal.

Lemma 6.3.4

Suppose that R is a CRI and I is a P-primary ideal.

1. For $r \in I$, $(I : r) = R$;
2. For $r \notin I$, $\sqrt{(I : r)} = P$;
3. For $r \notin P$, $(I : r) = I$.

Lemma 6.3.5

Suppose that R is a CRI and $P \in \operatorname{Spec} R$. If $Q_1, ..., Q_n$ are P-primary ideals, then the intersection $\bigcap_{k=1}^{n} Q_k$ is also P-primary.

Definition 6.3.6. Primary Decomposition

Suppose that R is a CRI and $I \lhd R$. We say that I is **decomposable**, if there is a set of primary ideals $Q_1, ..., Q_n$ of R such that $I = \bigcap_{k=1}^{n} Q_k$. The set is called a primary decomposition of I. The decomposition is said to be minimal, if

1. All radicals $\sqrt{Q_k}$ are distinct;
2. For each $k \in \{1, ..., n\}$, $\bigcap_{j \neq k} Q_j \not\subseteq Q_k$.

Remark. Every decomposable ideal has a minimal primary decomposition.

Theorem 6.3.7. First Uniqueness Theorem of Primary Decomposition

Suppose that R is a CRI, and $I \lhd R$ is decomposable. Let $I = \bigcap_{k=1}^{n} Q_k$ be a minimal primary decomposition of I. Let $P_i := \sqrt{Q_i}$. Then the set $\{P_1, ..., P_n\}$ of prime ideals coincides with the set $\{\sqrt{(I : r)} : \ r \in R\}$ and hence is independent of the choice of $\{Q_1, ..., Q_n\}$.

Corollary 6.3.8. Primary Decomposition of Radical Ideals

Suppose that R is a CRI, and I is a decomposable radical ideal of R. If $I = \bigcap_{k=1}^{n} Q_k$ is a primary decomposition of I, then $Q_1, ..., Q_n$ are prime ideals.

Theorem 6.3.9. Lasker-Noether Theorem

Suppose that R is a Noetherian ring. Then every ideal of R is decomposable.

Corollary 6.3.10. Minimal Prime Ideals in Noetherian Ring

Suppose that R is a Noetherian ring. Then R has finitely many minimal prime ideals

6.4 Integral Extension

6.4.1 Integral Dependence

In this section we focus on a special type of ring extensions $R \subseteq S$, integral extensions, which is the generalisation to algebraic field extensions.

Definition 6.4.1. Integral Elements, Integral Extensions

Suppose that $R \subseteq S$ is a ring extension. $\alpha \in S$ is said to be integral over R, if there exists a **monic** polynomial $f \in R[x]$ such that $f(\alpha) = 0$.

S is said to integral over R if every $\alpha \in S$ is integral over R.

Proposition 6.4.2. Characterisations of Integral Elements

Suppose that $R \subseteq S$ is a ring extension. The following are equivalent:

1. $\alpha \in S$ is integral over R;
2. $R[\alpha]$ is a finitely generated R-module;
3. There exists a faithful $R[\alpha]$-module M which is finitely generated as an R-module.

Proposition 6.4.3. Integral Closure forms a Subring

Suppose that $R \subseteq S$ is a ring extension. The set of integral elements of S over R is a subring of S, and is called the **integral closure** of R in S.

Definition 6.4.4. Integrally Closed Domains

Suppose that $R \subseteq S$ is a ring extension. We say that R is integrally closed in S, if the integral closure of R in S is R itself.

If R is an integral domain, we say that R is integrally closed (without qualifications), if R is integrally closed in its field of fractions.

Corollary 6.4.5. Transitivity of Integral Dependence

Suppose that $R \subseteq S \subseteq T$ are ring extensions. If T is integral over S, and S is integral over R, then T is integral over R.

Corollary 6.4.6. Finite Type + Integral $\iff$ Finite

Suppose that $f : R \to S$ is a ring homomorphism, so that S is an R-algebra. If S is a finite-generated as an R-algebra and S is integral over $f(A)$, then S is a finitely generated as an R-module.

Proposition 6.4.7. Quotient and Fraction Ring of Integral Extensions

Suppose that $R \subseteq S$ is an integral ring extension.

1. For $J \lhd S$, let $I := J \cap R \lhd R$. Then S/J is integral over R/I.
2. For a muliplcatively closed subset $T \subseteq R$, $T^{-1}S$ is integral over $T^{-1}R$.

Proposition 6.4.8. Integral Closure is a Local Property

Suppose that R is an integral domain. The following are equivalent:

1. R is integrally closed;
2. R_P is integrally closed for all $P \in \operatorname{Spec} R$;
3. R_M is integrally closed for al $M \in \operatorname{MaxSpec} R$.

6.4.2 Prime Ideals in Integral Extensions

Suppose that $R \subseteq S$ is an integral ring extension. The inclusion map $\iota : R \hookrightarrow S$ induces the pull-back of prime spectrum $\operatorname{Spec}(\iota) : \operatorname{Spec} S \to \operatorname{Spec} R$. We aim to study the relation between $\operatorname{Spec} R$ and $\operatorname{Spec} S$.

Lemma 6.4.9

Suppose that $R \subseteq S$ is an integral extension and R is an integral domain. Then R is a field if and only if S is a field.

Corollary 6.4.10

Suppose that $R \subseteq S$ is an integral extension. Let $Q \in \operatorname{Spec} S$. Then $Q \in \operatorname{MaxSpec} S$ if and only if $P := Q \cap R \in \operatorname{MaxSpec} R$.

Theorem 6.4.11. Lying-Over Theorem

Suppose that $R \subseteq S$ is an integral ring extension. Then $\operatorname{Spec}(\iota) : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective and closed (map closed sets to closed sets) under Zariski topology.

Corollary 6.4.12. Going-Up Theorem

Suppose that $R \subseteq S$ is an integral extension. Suppose that $P_1 \subseteq P_2$ are two prime ideals of R. Let $Q_1 \in \operatorname{Spec} S$ such that $P_1 = Q_1 \cap R$. Then there exists $Q_2 \in \operatorname{Spec} S$ such that $P_2 = Q_2 \cap R$ and $Q_1 \subseteq Q_2$.

Proposition 6.4.13. $\operatorname{Spec}(\iota)$ **has finite fibre**

Suppose that $R \subseteq S$ is an integral ring extension. For any $P \in \operatorname{Spec} R$, $\operatorname{Spec}(\iota)^{-1}(P)$ is finite.

6.5 Dimension Theory

6.5.1 Krull's Dimension

Definition 6.5.1. Height, Krull's Dimension

Suppose that R is a CRI. For $P \in \operatorname{Spec} R$, we define the height $\operatorname{ht}(P)$ of P in R to be the largest integer n such that there exists a chain of prime ideals:

$$\{0\} = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$$

The Krull's dimension of R is defined by

$$\dim R := \sup\left\{\operatorname{ht}(P) : \ P \in \operatorname{Spec} R\right\}$$

We collect some elementary facts about the dimension:

Proposition 6.5.2. Properties of Height and Dimension

Suppose that R is a CRI, and $N := N(R)$ is its nilradical. Then

1. $\dim R = \dim R/N$;
2. For $P \in \operatorname{Spec} R$, $\operatorname{ht}(P) = \operatorname{ht}(P/N)$;
3. $\dim R = \sup\{\operatorname{ht}(P) : P \in \operatorname{MaxSpec} R\}$.

Proposition 6.5.3. Dimension of Integral Extensions

Suppose that $R \subseteq S$ is an integral extension. Then $\dim R = \dim S$.

6.5.2 Graded Rings and Modules

Definition 6.5.4. Graded Rings and Modules

Suppose that R is a CRI. A grading of R is a sequence $(R_n)_{n\in\mathbb{N}}$ of additive subgroups of R such that $R = \bigoplus_{n=0}^{\infty} R_n$ and $R_i \cdot R_j \subseteq R_{i+j}$. In such case R_0 is a subring of R and R has a natural R_0-module structure.

Suppose that M is a module over the graded ring R. A grading of M (with respect to the grading $(R_n)_{n\in\mathbb{N}}$) is a sequence $(M_n)_{n\in\mathbb{N}}$ of additive subgroups of M such that $M = \bigoplus_{n=0}^{\infty} M_n$ and $R_i \cdot M_j \subseteq M_{i+j}$.

Proposition 6.5.5. Noetherian Graded Rings

Suppose that R is a graded ring with grading (R_n). Then R is Noetherian if and only if R_0 is Noetherian and R is finitely generated as an R_0-algebra.

Definition 6.5.6. I-Filtration of Modules, Rees Algebra

Suppose that R is a CRI and $I \lhd R$. The descending chain of M-modules

$$M = M_0 \supseteq M_1 \supseteq \cdots$$

is said to be an I-filtration, if $IM_i \subseteq M_{i+1}$ for all $i \in \mathbb{N}$.

Consider the direct sum of R-modules: $R^\sharp := \bigoplus_{n=0}^{\infty} I^n$. It has a natural structure of a graded ring and an R-module, and is called the Rees algebra associated to R and I. The direct sum $M^\sharp := \bigoplus_{n=0}^{\infty} M^n$ is naturally an $R^\sharp$-module.

Theorem 6.5.7. Artin-Rees Lemma

Suppose that R is a Noetherian ring and $I \lhd R$. Let M be a finitely generated R-module and (M_n) be a stable I-filtration on M. For a submodule $N \leqslant M$, the filtration $(N \cap M_n)$ is a stable I-filtration on N.

Theorem 6.5.8. Krull's Intersection Theorem

Suppose that R is a Noetherian ring and $I \lhd R$. Let M be a finitely generated R-module. Then

$$\bigcap_{n=0}^{\infty} I^n M = \bigcup_{r\in 1+I} \ker r_M$$

where r_M is the map $m \mapsto rm$.

Corollary 6.5.9

Suppose that R is a Noetherian ring and $I \lhd R$. Then $\bigcap_{n=0}^{\infty} I^n = \{0\}$.

Corollary 6.5.10

Suppose that R is a Noetherian ring and $I \lhd R$. Let M be a finitely generated R-module. If $I \subseteq J(R)$, then $\bigcap_{n=0}^{\infty} I^n M = \{0\}$.

6.5.3 Artinian Rings

Definition 6.5.11. Artinian Rings

A ring R is said to be an Artinian ring, if the ideals of R satisfy the descending chain condition.

Proposition 6.5.12. Artinian Local Rings

Suppose that R is a Noetherian local ring with the unique maximal ideal M. The following are equivalent:

1. $\dim R = 0$;
2. M is the nilradical of R;
3. $M^n = 0$ for some $n \geqslant 1$;
4. R is Artinian.

Corollary 6.5.13. Artinian = Noetherian + Dimension 0

R is an Artinian ring if and only if R is a Noetherian ring of dimension 0.

Theorem 6.5.14. Sturcture Theorem of Artinian Rings

Suppose that R is an Artinian ring. Then R is uniquely (up to isomorphism) a finite product of Artinian local rings.

6.5.4 Dimension of Noetherian Rings

Theorem 6.5.15. Krull's Principal Ideal Theorem

uppose that R is a Noetherian ring. Let $f \in R$ be a non-unit and let P be a minimal prime ideal among those containing f. Then $\mathrm{ht}(P) \leqslant 1$.

Corollary 6.5.16

Suppose that R is a Noetherian ring. Let $f_1, ..., f_k \in R$ be non-units and let P be a minimal prime ideal among those containing $\langle f_1, ..., f_k \rangle$. Then $\mathrm{ht}(P) \leqslant k$.

Remark. The corollary shows that every prime ideal in a Noetherian ring has finite height. Moreover, if R is a local ring, then $\dim R < \infty$.

Theorem 6.5.17. Dimension of Noetherian Polynomial Rings

Suppose that R is a Noetherian ring. Then $\dim R[x] = \dim R + 1$.

Corollary 6.5.18

Suppose that R is a Noetherian ring. Then $\dim R[x_1, ..., x_n] = \dim R + n$.

Theorem 6.5.19. Dimension and Transcendence Degree

Suppose that F is a field and R is a finitely generated F-algebra. Suppose that F is an integral domain with field of fractions K. Then we have

$$\dim R = \text{tr.deg}(K \mid F) < \infty$$

6.6 Dedekind Domains

Definition 6.6.1. Dedekind Domains

A ring R is called a Dedekind domain, if it is an integrally closed Noetherian integral domain of dimension 1.

Proposition 6.6.2

Suppose that R is a Dedekind domain.

1. All non-zero prime ideals of R are maximal;
2. If Q_1, Q_2 are primary ideals of R such that $\sqrt{Q_1} \neq \sqrt{Q_2}$, then Q_1 and Q_2 are coprime.

Corollary 6.6.3

Suppose that R is a Dedekind domain. If $I \lhd R$ has the minimal primary decomposition $I = \bigcap_{k=1}^{n} Q_k$, then $\bigcap_{k=1}^{n} Q_k = \prod_{k=1}^{n} Q_k$.

Proposition 6.6.4

Suppose that R is a Noetherian local domain of dimension 1, with the unique maximal ideal M. The following are equivalent:

1. R is integrally closed;
2. M is a principal ideal;
3. For every non-zero $I \lhd R$, $I = M^n$ for a unique $n \in \mathbb{N}$.

Corollary 6.6.5

Suppose that R is a Dedekind domain.

1. For non-zero $P \in \operatorname{Spec} R$, R_P is a principal ideal domain.
2. If Q is a P-primary ideal of R, then $Q = P^n$ for some n.

Theorem 6.6.6. Prime Decomposition in Dedekind Domain

In a Dedekind domain, every ideal has a unique decomposition into products of distinct prime ideals, which is unique up to reindexing.

Proposition 6.6.7. Ideal Generators in Dedekind Domain

Every ideal in a Dedekind domain is generated by at most two elements.

6.7 Hilbert's Nullstellensatz

6.7.1 Noether's Normalisation Lemma

We have already presented a proof of Weak Nullstellensatz using Artin-Tate Lemma in Theorem 6.1.10. In this section we present another proof using the following Noether's Normalisation Lemma:

Theorem 6.7.1. Noether's Normalisation Lemma

Suppose that F is a field and R is a finitely generated F-algebra. Then there exists an injective homomorphism of F-algebras:

$$F[x_1,...,x_n] \hookrightarrow R$$

such that R is finitely generated as an $F[x_1,...,x_n]$-module.

Proof of Weak Nullstellensatz 6.1.10 from Noether's Normalisation Lemma. □

6.7.2 Nullstellensatz in Algebraic Geometry

Fix F to be an algebraically closed field. We study the affine space F^n and the action of the polynomial ring $R := F[x_1,...,x_n]$ acting on it.

Definition 6.7.2. Algebraic Sets, Vanishing Ideals

For $S \subseteq F[x_1,...,x_n]$, we define the algebraic set of S to be

$$\mathcal{V}(S) := \{(a_1,...,a_n) \in F^n : \forall f \in S\ f(a_1,...,a_n) = 0\}$$

For $X \subseteq F^n$, we define the vanishing ideal of X to be

$$\mathcal{I}(X) := \{f \in F[x_1,...,x_n] : \forall (a_1,...,a_n) \in Y\ f(a_1,...,a_n) = 0\}$$

It is easy to verify that $\mathcal{I}(X)$ is an ideal in $F[x_1,...,x_n]$.

Similar to Galois correspondence in Section 3.4, we have the following correspondence between $\mathcal{V}$ and $\mathcal{I}$:

Proposition 6.7.3

Let $S \subseteq F[x_1,...,x_n]$ and $X \subseteq F^n$.

1. $\mathcal{V}(F[x_1,...,x_n]) = F^n$ and $\mathcal{I}(F^n) = F[x_1,...,x_n]$;
2. $\mathcal{V}(S) = \mathcal{V}(\langle S\rangle)$ and $\mathcal{I}(X) = \langle \mathcal{I}(X)\rangle$;
3. For $S \subseteq T \subseteq F[x_1,...,x_n]$, we have $\mathcal{V}(S) \supseteq \mathcal{V}(T)$;
4. For $X \subseteq Y \subseteq F^n$, we have $\mathcal{I}(X) \supseteq \mathcal{I}(Y)$;
5. $S \subseteq \mathcal{I}\mathcal{V}(S)$ and $X \subseteq \mathcal{V}\mathcal{I}(X)$;
6. $S = \mathcal{V}\mathcal{I}\mathcal{V}(S)$ and $X = \mathcal{I}\mathcal{V}\mathcal{I}(X)$.

Proposition 6.7.4. Maximal Ideals of $F[x_1,...,x_n]$

Let F be an algebraically closed field. I is a maximal ideal of $F[x_1,...,x_n]$, if and only if there exists $(a_1,...,a_n) \in F^n$ such that

$$I = \langle x_1 - a_1,...,x_n - a_n\rangle$$

Moreover, $f \in \langle x_1 - a_1,...,x_n - a_n\rangle$ if and only if $f(a_1,...,a_n) = 0$.

Theorem 6.7.5. Hilbert's Strong Nullstellensatz

Let F be an algebraically closed field. Let $I \lhd F[x_1,...,x_n]$. Then $\sqrt{I} = \mathcal{I}\mathcal{V}(I)$ in F^n.

Remark. The Strong Nullstellensatz tell us that the algebraic sets in F^n are in bijective correspondence with the radical ideals in $F[x_1,...,x_n]$.

6.7.3 Jacobson Rings