Commutative Algebra

Hacen ZELACI

Mathematical department, El Oued university.
Current address: University of EL-Oued
Email address: zelaci-hacen@univ-eloued.dz

Contents

Abstract

These lecture notes provide an introduction to commutative algebra for Master 1 students, focusing on commutative rings, ideals, and modules. The course explores essential topics such as prime and maximal ideals, localization, Noetherian rings, and Hilbert's Nullstellensatz. We will also discuss concepts like primary decomposition and integral closures. The goal is to equip students with a strong foundation in commutative algebra and its connections to algebraic geometry, number theory, and topology.

Keywords: Commutative algebra, commutative rings, ideals, modules, Noetherian rings, localization, Hilbert's Nullstellensatz, algebraic geometry, algebraic number theory, topology, primary decomposition, integral closures, graded rings.

1. Introduction

This course is a comprehensive lecture notes on commutative algebra for master 1 students. Commutative algebra serves as a fundamental branch of abstract algebra, focusing on the study of commutative rings and their properties. These lecture notes aim to provide a solid foundation in the key concepts, techniques, and results of commutative algebra.

In this course, we will explore the fundamental notions of commutative rings, ideals, and modules, delving into the rich interplay between algebraic structures and geometric objects. We will uncover the intrinsic connections between commutative algebra and other branches of mathematics, such as algebraic geometry, algebraic number theory, and topology.

Throughout these notes, we will cover various topics, including prime and maximal ideals, localization, integral extensions, Noetherian rings, and the celebrated Hilbert's Nullstellensatz. Additionally, we will discuss important concepts such as primary decomposition, integral closures, and the associated graded ring construction.

By studying commutative algebra, you will gain a deeper understanding of algebraic structures, develop problem-solving skills, and build a strong foundation for further exploration in advanced mathematics. Whether you are interested in algebraic geometry, algebraic number theory, or simply seeking a solid background in abstract algebra, these lecture notes will serve as a valuable resource.

I hope you find these lecture notes informative, engaging, and useful in your journey through the captivating realm of commutative algebra. Let's embark on this intellectual adventure together, exploring the intricate beauty and powerful machinery of commutative algebra.

Here is some references: [**Ati69**], [**Bou89**], [**Mat89**]

CHAPTER 1

Ring theory

This section provides an introduction to ring theory, covering essential definitions, examples, and results. It introduces the concepts of commutative rings, ideals, homomorphisms, prime and maximal ideals, Noetherian rings. Additionally, it culminates with Hilbert's Nullstellensatz, a fundamental theorem with far-reaching implications in algebraic geometry.

1. Basic Definitions and Examples

DEFINITION 1.1. A *commutative ring* is a set R equipped with two operations, addition $(+)$ and multiplication $(\cdot)$, such that $(R, +)$ is an abelian group and the multiplication is associative, commutative and distributive over addition. We denote the ring structure by $(R, +, \cdot)$.

EXAMPLE 1.2.

- The set $\mathbb{Z}$ of integers is a commutative ring.
- The set $\mathbb{R}[x]$ of polynomials in one variable x with real coefficients is a commutative ring.
- The ring $\mathbb{C}$ of complex numbers is a commutative ring.

In this notes, all rings are assumed to be unitary (i.e. the multiplication has an identity element) denoted by 1_R or just 1. Further, every ring is commutative (that is, $xy = yx$ for any $x, y \in R$).

Let R and S be two rings. A function $\phi : R \to S$ is called a ring homomorphism if it satisfies the following properties:

- **Additive Property:** For all $a, b \in R$, $\phi(a+b) = \phi(a)+\phi(b)$.
- **Multiplicative Property:** For all $a, b \in R$, $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.
- **Identity Property:** $\phi(1_R) = 1_S$, where 1_R and 1_S are the respective multiplicative identities in R and S.

EXAMPLE 1.3. The map $\mathbb{Z}[X] \to \mathbb{Z}$ that send $P(X) \mapsto P(0)$ is a ring homomorphism.

A ring homomorphism ϕ can have the following additional properties:

- If ϕ is injective (one-to-one), it is called a **monomorphism**.
- If ϕ is surjective (onto), it is called an **epimorphism**.
- If ϕ is both injective and surjective, it is called an **isomorphism**.

Let us collect some definitions

DEFINITION 1.4. Let $a, b \in R$.

- a divides b, denoted $a|b$, if there exists non-zero $c \in R$ such that $ac = b$.
- a is called invertible (or unit) if there exists $c \in R$ such that $ac = 1$.
- a is called prime if it is not unit and if for any $x, y \in R$ we have
$$a|xy \Longrightarrow a|x \text{ or } a|y.$$
- a is called irreducible if it is not unit and if for any $x, y \in R$ we have
$$a = xy \Longrightarrow \text{ either } x \text{ or } y \text{ is invertible.}$$
- a is called nilpotent if there exists $n \in \mathbb{N}^*$ such that $x^n = 0$.
- a is called zero-divisor if there exists $b \neq 0$ such that $ab = 0$.
- An element d is called *greatest commun divisor* (gcd for short) of a and b if d divides a and b and each common divisor of a and b divides d.

A *nonzero* ring R is called *integral* or *domain* if it has only one zero-divisor which is 0. In other words, whenever we have $ab = 0$, either $a = 0$ or $b = 0$.
The subset of units is denoted $R^\times$. If R is commutative, then $R^\times$ is a multiplicative group.
If $R^\times = R \setminus \{0\}$, then R is called *division ring*. A commutative division ring is called *field*.

REMARK 1.5.

- Note that a nilpotent element is zero-divisor, but not the converse. An example is given by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ in the ring $\mathcal{M}_2(k)$ of suqare 2 by 2 matrices over a field k. This element is clearly zero divisor but it is not nilpotent.
- In an integral ring, a prime element is irreducible, the converse is incorrect in genenral. However, in unique factorization domains (that's will be defined later on), primes and irreducibles are the same.

DEFINITION 1.6. A non-empty subset S of a ring R is called a *subring* of R if S is itself a ring with the same operations as those in R.

Let R be a ring. The set $Z(R)$ of all elements $z \in R$ such that $zx = xz$ for every $x \in R$ is a commutative subring of R, called the *center* of R.

More generally, let S be a subset of R, and let $C_S(R)$ be the set of all elements $z \in R$ such that $zx = xz$ for all $z \in S$. This is a subring of R, called the *centralizer* of S in R. By definition, S is contained in the center of $C_S(R)$, and $C_S(R)$ is the largest subring of R satisfying this property.

2. Ideals, and Homomorphisms

DEFINITION 2.1. An *ideal* I of a ring R is a subset of R that is closed under addition, subtraction, and multiplication by elements of R. Moreover, I must be an additive subgroup of R.

If $a \in R$, the multiples xa of a form an ideal of R denoted $\langle a \rangle$. These ideals, which are generated by one element, are called principal. Similarly, given a finite set $\{a_1, \cdots, a_n\}$, we denote by $\langle a_1, \cdots, a_n \rangle$ the ideal generated by this family whose elements are $x_1a_1 + \cdots + x_na_n$, $x_i \in R$. These ideals are called finitely generated. An ideal I different from R is said to be proper.

Let $f : R \to S$ be a ring homomorphism and $J \subset S$ be an ideal, then $f^{-1}(J)$ is and ideal of R (exercise: show it!). Particularly,

its kernel $Ker(f)$ is defined to be the ideal $f^{-1}(0)$ of R. Recall $Ker(f) = 0$ if and only if f is injective.
Note that $f(R)$ is a sub-ring of S, and that if $I \subset R$ is an ideal, $f(I)$ is an ideal of the sub-ring $f(R)$.

Let I be an ideal of R. Form the set of cosets of I:

$$R/I := \{x + I | x \in R\}$$

where $x + I = y + I \longleftrightarrow x - y \in I$.
Recall that R/I inherits a ring structure, and is called the quotient ring of R modulo I. Define the quotient map

$$\pi : R \to R/I,\ \pi(x) := x + I.$$

Note that if $I \subset Ker(f)$, then there is a ring map : $g : R/I \to R'$ with $g \circ \pi = f$; that is, the following diagram is commutative:

$$\begin{array}{ccc} R & \xrightarrow{\pi} & R/I \\ & \searrow^{f} & \downarrow g \\ & & R' \end{array}$$

Definition 2.2. A ring R is called a **principal ring** if every ideal of R is principal. When R is integral, we call it principal ideal domain (PID).

Example 2.3.

- Every field is a principal ring since the only ideals of a field are $\{0\}$ and R itself, both of which are principal.
- The ring $\mathbb{Z}$ of integers is a principal ring. Indeed, for any ideal I of $\mathbb{Z}$, there exists a unique integer $n = 0$ such that $I = \langle n \rangle$. More precisely, if $I \neq 0$, then n is the smallest strictly positive element of I. If $I = \langle 0 \rangle$, then $n = 0$ is the only integer such that $I = \langle 0 \rangle$. Assume now that $I \neq 0$. If $I = \langle n \rangle$, with $n > 0$, one observes that the strictly positive elements of I are $\{n, 2n, 3n, \cdots\}$, and n is the smallest of them. This implies the uniqueness of such an integer. So let n be the smallest strictly positive element of I. Since $n \in I$, $an \in I$ for any $a \in \mathbb{Z}$, so that $\langle n \rangle \subset I$. Conversely, let a be any element of I. Let $a = qn + r$ be the Euclidean division of a by n, with $q \in \mathbb{Z}$

and $0 \leqslant r \leqslant n-1$. Since a and $qn \in I$, $r = a - qn \in I$. Since n is the smallest strictly positive element of I and $0 \leqslant r < n$, we necessarily have $r = 0$ and $0 = qn \in \langle n \rangle$. This shows that $I = \langle n \rangle$.

- The ring of polynomials $\mathbb{Z}[X]$ is not a principal ring, indeed, the ideal generated by the set $\{2, X\}$ is not principal.

Principal rings have important applications in algebraic number theory, commutative algebra, and other areas of mathematics.

DEFINITION 2.4. A ring R is said *gcd domain* if it is a commutative integral ring such that each two elements of R have a gcd.

PROPOSITION 2.5. *If R is PID then R is a gcd domain.*

PROOF. For any $a, b \in R$, the ideal $\langle a \rangle + \langle b \rangle$ is principal, hence a generator of it is by definition a gcd of a and b. □

We say that two elements a and b are coprime if 1 is a gcd of a and b.

PROPOSITION 2.6 (Gauss's lemma). *Let a and b two elements of a gcd domain R. Then a and b are coprime if and only if for any c in R*

$$a|bc \to a|c.$$

PROOF. If a and b are coprime, then c is a gcd of ac and bc, but since $a|bc$ it divides c.
Conversely, let d be a gcd of a and b, and write $a = da'$ and $b = db'$. By taking $c = a'$, we see that $a|bc = ab'$, so $a|c = a'$, hence d is a unit, and a and b are coprime. □

PROPOSITION 2.7. *Let R be a gcd ring and $a \in R$, then a is irreducible if and only if a is prime.*

PROOF. Let a be an irreducible element of R and let $x, y \in R$ such that $a|xy$. Denote by d a gcd of a and x and $a = da'$, $x = dx'$. So a' and x' are coprime, and $a'|x'y$, so by Gauss's lemma $a'|y$. Now since a is irreducible, either d is invertible or a' is invertible, in the former case, $a|y$, and in the other one, $a|x$. Hence a is prime. □

Note that the existence of elements u, v such that $ua + vb = \gcd(a, b)$ does not hold in general. The class of rings in which this property holds are called Bézout rings.

DEFINITION 2.8. A ring is called *Bézout domain* if it is commutative integral such that the sum of any two principal ideals is again principal.

Note that any PID is by definition a Bézout ring.

PROPOSITION 2.9. *A Bézout domain is a gcd domain.*

PROOF. If a and b are two elements of R. Then $\langle a\rangle + \langle b\rangle = \langle c\rangle$, hence c is a gcd of a and b. □

In particular, this gives another proof of the fact that PIDs are gcd domains.

PROPOSITION 2.10. *Let R be a Bézout ring, a and b two elements. Then a and b are coprime if and only if there exists u and v such that*

$$au + bv = 1.$$

PROOF. If a and b are coprime, then 1 is the greatest common divisor (gcd) of a and b. Moreover, $\langle a\rangle + \langle b\rangle = \langle d\rangle$, where d divides both a and b, implying that d divides 1. Thus, d is invertible, meaning $\langle a\rangle + \langle b\rangle = R$. Therefore, the required identity holds.
The converse is straightforward. □

PROPOSITION 2.11. *Let k be a field. Then the ring $k[X]$ is a principal ideal domain. More precisely, if $I \subset k[X]$ is a non-zero ideal and P is a non-zero element of I with minimal degree, say $\deg(P) = n$, then we have $I = \langle P\rangle$. Furthermore, the images of $1, X, X^2, \ldots, X^{n-1}$ form a basis of $k[X]/I$ as a vector space over k.*

PROOF. The key idea is to apply polynomial division with remainder. To verify that P generates the ideal I, take any $Q \in I$. By the division algorithm, we can express Q as

$$Q = P \cdot S + R,$$

where S and R are in $k[X]$, and $\deg(R) < \deg(P)$. Since $R \in I$, if $R \neq 0$, this would contradict the choice of P as the element of minimal degree in I. Therefore, $R = 0$, implying that P divides Q. Hence, P generates I.

Now, consider the quotient $k[X]/\langle P\rangle$, and denote the images of the polynomials $1, X, \ldots, X^{n-1}$ in the quotient ring by $1, \bar{X}, \ldots, \bar{X}^{n-1}$. These images must be linearly independent. Indeed, for any polynomials $P, Q \in k[X]$, the degree of the product satisfies $\deg(P \cdot Q) = \deg(P) + \deg(Q)$ (since k is a field and thus has no nonzero zero divisors). This means that no polynomial of degree less than n can be divisible by P.

If the set $\{1, \bar{X}, \ldots, \bar{X}^{n-1}\}$ were not linearly dependent, then there would exist coefficients $a_0, \ldots, a_{n-1} \in k$ such that

$$a_0 \cdot 1 + a_1 \cdot \bar{X} + \cdots + a_{n-1} \cdot \bar{X}^{n-1} = 0.$$

This would imply that the polynomial $a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$ is divisible by P, contradicting the fact that its degree is less than $\deg(P)$.

Conversely, these images span the quotient. Using polynomial division again, for any $Q \in k[X]$, we can write

$$Q = P \cdot S + R,$$

with $\deg(R) < n$. Thus, $Q \equiv R \pmod{\langle P\rangle}$, where R is a linear combination of $1, X, \ldots, X^{n-1}$. This shows that $\{1, \bar{X}, \ldots, \bar{X}^{n-1}\}$ spans $k[X]/(P)$ as a vector space over k.

□

The converse of the last proposition is also true.

PROPOSITION 2.12. *Let A be an integral ring. If $A[X]$ is PID, the A is a field.*

PROOF. Let a be any non-zero element of A. Then the ideal $\langle a, X\rangle$ of $A[X]$ is a principal ideal $\langle f(X)\rangle$ with $f(X)$ a non-zero polynomial. Therefore,

$$a = f(X)g(X), \quad X = f(X)h(X),$$

with $g(X)$ and $h(X)$ certain polynomials in $A[X]$. From these equations, one infers that $f(X)$ is a polynomial c and $h(X)$ is a first-degree polynomial $b_0 + b_1X$ (where $b_1 \neq 0$).

Thus, we obtain the equation

$$cb_0 + cb_1X = X,$$

which shows that cb_1 is the unity 1 of A. Thus, $c = f(X)$ is a unit of A, whence

$$\langle a, X\rangle = \langle f(X)\rangle = \langle 1\rangle = A[X].$$

So, we can write

$$1 = a \cdot u(X) + X \cdot v(X),$$

where $u(X), v(X) \in A[X]$. This equation cannot hold unless the constant term of $u(X)$ times a is the unity. Accordingly, a must have a multiplicative inverse in A. Since a was an arbitrary non-zero element of the integral domain A, it follows that A is a field.

□

Given two ideals I, and J, we define their sum by

$$I + J = \{x + y | x \in I, y \in J\},$$

and their product to be the ideal generated by $\{xy | x \in I, y \in J\}$. Precisely

$$IJ = \{\sum_{\text{finite}} x_i y_j | x_i \in I, y_j \in J\}.$$

REMARK 2.13. We have $IJ \subset I \cap J$ and $I + J = \langle I \cup J\rangle$.

DEFINITION 2.14. Two ideals I and $J \subset R$ are called comaximals if $I + J = R$.

The concept of comaximal ideals extends the idea of relatively prime integers.

PROPOSITION 2.15.

(*i*) *If I and J are comaximal, then $IJ = I \cap J$.*

(*ii*) *If R is principal and I and J nonzero ideals such that $IJ = I \cap J$, then I and J are comaximal.*

PROOF. (*i*) The inclusion $IJ \subset I \cap J$ is always true. Let $x \in I \cap J$. Since I and J are comaximal, there exists $u \in I$ and $v \in J$ such that $u+v=1$, so $x = xu+xv$, but since both xu xv are in IJ, we deduce that $x \in IJ$.

(*ii*) Let $I = \langle a \rangle$, $J = \langle b \rangle$. Then $IJ = \langle ab \rangle = I \cap J$. Let $c \in R$ such that $I + J = \langle c \rangle$. We have $c = xa + yb$, and since a and b are in $I + J$, we also have $a = \alpha c$, $b = \beta c$. So we get $c = x\alpha c + y\beta c$, hence $c(1 - x\alpha - y\beta) = 0$, since $c \neq 0$, it follows that $1 = x\alpha + y\beta$, which gives $1 \in I + J$. So $I + J = R$. □

We generalize the above proposition to a finite number of ideals. We have the following lemma:

LEMMA 2.16. *Let I and $I_1, \cdots, I_n$ be ideals of a commutative ring R such that I is comaximal with each one of I_n. Then I is commaximal with their product $I_1 \cdots I_n$.*

PROOF. Let $\mathfrak{p} = I_1 \cdots I_n$. Since for any i we have I is comaximal with I_i, then for any i there exists $x_i \in I_i$ and $a_i \in I$ such that

$$a_i + x_i = 1,$$

taking their product we get

$$\Pi_i(a_i + x_i) = 1,$$

developing this product we get

$$b + \Pi_i x_i = 1,$$

where b is a sum of terms with at least one a_i, hence it belongs to I. But $\Pi_i x_i \in \mathfrak{p}$, we deduce that I and $\mathfrak{p}$ are comaximal. □

PROPOSITION 2.17. *Let $I_1, I_2, \ldots, I_n$ be pairwise comaximal ideals. Denote by $\mathfrak{p} = I_1 I_2 \cdots I_n$ their product. Then we have $\mathfrak{p} = I_1 \cap I_2 \cap \cdots \cap I_n$*

PROOF. We proceed by induction on n. If $n = 2$, it is the Proposition 2.15. Assume the result is true for $n-1$. Let $I = I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_n$, we have by the last lemma that I and I_n are comaximal, hence $I \cdot I_n = I \cap I_n$ as wished. □

One of the renowned results utilizing the notion of comaximal ideals is the following theorem known as the Chinese Remainder Theorem.

THEOREM 2.18. *Let $I_1, I_2, \ldots, I_n$ be pairwise comaximal ideals. Denote by $\mathfrak{p} = I_1 I_2 \cdots I_n$ their product. Then the canonical map*

$$\varphi : R/\mathfrak{p} \longrightarrow R/I_1 \times R/I_2 \times \cdots R/I_n$$
$$x + \mathfrak{p} \mapsto (x + I_1, x + I_2, \cdots, x + I_n)$$

is an isomorphism.

PROOF. **Injectivity:** Let $x, y \in R$, such that $\varphi(x+\mathfrak{p}) = \varphi(y+\mathfrak{p})$, so for any $1 \leqslant i \leqslant n$, $x - y \in I_i$, hence $x - y \in I_1 \cap I_2 \cap \cdots \cap I_n$, but this last ideal equals $I_1 \cdots I_n = \mathfrak{p}$. Hence $x + \mathfrak{p} = y + \mathfrak{p}$.
Surjectivity: Let $x_1, \cdots, x_n \in R$, it enough to show that there exists $x \in R$ such that $x - x_i \in I_i$. Let $r \in \{1, \cdots, n\}$ and consider

$$J_r = \bigcup_{i=1\ ,i\neq r}^{n} I_i,$$

note that I_r and J_r are comaximal by Lemma 2. In particular, there exist $a_r \in I_r$ and $b_r \in J_r$ such that $a_r + b_r = 1$. Note that $b_r \in I_i$ for all $i \neq 1$. Define $x = \Sigma_{r=1}^{n} b_r x_r$. We have

$$x - x_i = \Sigma_{r=1\ ,r\neq i}^{n} b_r x_r + (b_i - 1)x_i.$$

Since $b_r \in I_i$ for $r \neq i$ and because of $b_i - 1 = a_i \in I_i$ we deduce that $x - x_i \in I_i$. This ends the proof. □

3. Prime and Maximal Ideals

Prime and maximal ideals are fundamental concepts in ring theory. They provide crucial insights into the structure and properties of rings. Understanding prime and maximal ideals is essential for various areas of mathematics, including commutative algebra, algebraic geometry, and number theory.

DEFINITION 3.1. An ideal $\mathfrak{p}$ of a commutative ring R is called a *prime ideal* it is a proper ideal (i.e., $\mathfrak{p} \neq R$) and if for any $a, b \in R$, their product ab belongs to $\mathfrak{p}$ implies that at least one of a or b is in $\mathfrak{p}$.

In other words, a prime ideal is an ideal that "behaves" like a prime number in the sense that it generates a proper subset of R, and whenever the product of two elements is in the ideal, at least one of the elements must be in the ideal.

EXAMPLE 3.2. Examples of prime ideals include:

- In the ring of integers $\mathbb{Z}$, the prime ideals are precisely the ideals generated by prime numbers.
- In the ring of polynomials $k[X]$ over a field k, the ideal generated by an irreducible polynomial is a prime ideal.

PROPOSITION 3.3. *Let $f : R \to R'$ be a ring homomorphism, and $\mathfrak{q} \subset R'$ an ideal. If $\mathfrak{q}$ is prime, then $f^{-1}(\mathfrak{q})$ is prime; the converse holds if f is surjective.*

PROOF. Exercise. □

PROPOSITION 3.4 (Prime Avoidance lemma). *Let R be a ring. Let $I_i \subset R$, for $i = 1, \ldots, r$, and let $J \subset R$ be ideals. Assume that*

- *$J \not\subseteq I_i$ for $i = 1, \ldots, r$, and*
- *all but two of the I_i are prime ideals.*

Then there exists an $x \in J$ such that $x \notin I_i$ for all i.

PROOF. The result is true for $r = 1$. If $r = 2$, then let $x, y \in J$ with $x \notin I_1$ and $y \notin I_2$. We are done unless $x \in I_2$ and $y \in I_1$. In this case, the element $x + y$ cannot be in I_1 (since that would mean $x + y - y \in I_1$) and it also cannot be in I_2.

For $r \geq 3$, assume the result holds for $r - 1$. After renumbering, we may assume that I_r is a prime ideal. We may also assume there are no inclusions among the I_i. Pick $x \in J$ such that $x \notin I_i$ for all $i = 1, \ldots, r - 1$. If $x \notin I_r$, we are done. So assume $x \in I_r$. If $JI_1 \cdots I_{r-1} \subset I_r$, then $J \subset I_r$, a contradiction. Pick $y \in JI_1 \cdots I_{r-1}$ such that $y \notin I_r$. Then $x + y$ works. □

DEFINITION 3.5. An ideal $\mathfrak{m}$ of a commutative ring R is called a *maximal ideal* if it is a proper ideal (i.e., $\mathfrak{m} \neq R$) and there are no other proper ideals properly containing $\mathfrak{m}$ within R.

In other words, a maximal ideal is an ideal that cannot be properly contained within any other nontrivial ideal of R.

Example 3.6.

- In $\mathbb{Z}$, the maximal ideals are precisely the ideals generated by prime numbers.
- In the ring of polynomials $k[x]$ over a field k, the ideal generated by an irreducible polynomial is a maximal ideal. If k is algebraicly closed, the maximal ideals are exactly $\langle X - a \rangle$ for $a \in k$.
- In a field F, the only ideals are $\{0\}$ and F itself, hence $\{0\}$ is the only maximal ideal.

Proposition 3.7. *Let $I \subset R$ be an ideal, then*

(*i*) *I is prime if and only if R/I is a integral. In particular, R is integral if and only if $\{0\}$ is prime.*

(*ii*) *I is maximal if and only if R/I is a field. In particular, R is a field if and only if $\{0\}$ is maximal.*

Proof.

(*i*) Let I be a prime ideal, and let $\bar{a}, \bar{b} \in R/I$ s.t. $\bar{a}\bar{b} = 0$, this means $ab \in I$, hence $a \in I$ or $b \in I$, which means $\bar{a} = 0$ or $\bar{b} = 0$.

(*ii*) Let I is maximal, and $\bar{a} \in R/I$ nonzero. This means $a \notin I$, hence the ideal $\langle a, I \rangle$ generated by a and I equals R. So there exists $b \in R$ and $c \in I$ such that $ab + c = 1$, hence $\bar{a}\bar{b} = \bar{1}$.

□

Corollary 3.8. *Every maximal ideal is a prime ideal. If R is PID, a prime ideal is maximal.*

Proof. Let M be a maximal ideal, then R/M is a field, so it is integral, hence M is prime. If R is PID, and $I = \langle a \rangle$ is prime. Then a is prime, so it is irreducible. Assume that $I \subset J = \langle b \rangle \subsetneq R$. Since $a \in \langle b \rangle$, we have $a = bc$ for some $c \in R$. Since b is not unit, c is a unit. So $I = J$ is maximal. □

THEOREM 3.9. *Any proper ideal I is contained in some maximal ideal.*

This is a consequence of the following lemma, known as *Zorn's lemma.*

LEMMA 3.10 (Zorn's lemma). *Suppose a partially ordered set P has the property that every chain in P has an upper bound in P. Then the set P contains at least one maximal element.*

Note that this lemma is a consequence of the axiom of choice.

COROLLARY 3.11. *Let R be a ring, $x \in R$. Then x is a unit if and only if x does not belong to any maximal ideal of R.*

PROOF. if x is unit, then $\langle x \rangle = R$, hence x belongs to no maximal ideal. Conversily, assume that x is not a unit. Then the ideal generated by x, denoted $\langle x \rangle$, is a proper ideal of R. By Zorn's Lemma, every proper ideal is contained in a maximal ideal. Thus, x belongs to some maximal ideal $\mathfrak{m}$. □

In a Principal Ideal Domain, every ideal is principal by definition. Interestingly, we can characterize PIDs by requiring that only the prime ideals are principal.

THEOREM 3.12. *Let R be an integral domain. Then R is a PID if and only if each prime ideal of R is principal.*

PROOF. The direct implication is trivial. For the other implication, suppose that all prime ideal in R are principal and that R is not a PID.

Let S denote the set of all non-principal ideals of R. Since S is nonempty, it forms a partially ordered set. Consider a chain $\{I_\gamma : \gamma \in \Gamma\}$ in S. The ideal

$$I = \bigcup_{\gamma \in \Gamma} I_\gamma$$

is also a non-principal ideal of R and it is a upper bound for this chain. By Zorn's lemma, S contains a maximal element denoted M.

Since M is not principal, it cannot be a prime ideal. Therefore, there exist elements $x, x' \in R \setminus M$ such that $xx' \in M$. The ideals $I = M + (x)$ and $I' = M + (x')$ properly contain M, so by the maximality of M, they are not in S, this induces that there exists an element $\alpha \in R$ such that $I = (\alpha)$.

Define

$$K = (M : I) = \{r \in R : rI \subseteq M\}.$$

It is straightforward to show that $I' \subseteq K$, implying $M \subsetneq K$. Therefore, K must also be principal, and we can select $\beta \in R$ such that $K = (\beta)$.

By the definition of K, we have $KI \subseteq M$. We claim that the reverse inclusion holds as well. Take any $a \in M$; since $M \subseteq I$, we can express $a = r\alpha$ for some $r \in R$. Note that $r \in K$, which implies $a = r\alpha \in KI$. Thus, $M \subseteq KI$.

Finally, we conclude that $M = KI = (\alpha\beta)$, which contradicts the fact that M is an element of S.

□

4. Radicals

In Commutative Algebra, two essential radicals of a ring find common application: the Jacobson radical, defined as the intersection of all maximal ideals, and the nilradical, constituted by all nilpotent elements. Additionally, we establish two pivotal general theorems: Prime Avoidance, asserting that if an ideal belongs to a finite union of prime ideals, then it must belong to one of them, and the Scheinnullstellensatz, which affirms that the nilradical of an ideal equals the intersection of all prime ideals containing it.

Definition 4.1. Let R be a ring. Its (Jacobson) radical $\mathrm{J}(R)$ is defined to be the intersection of all its maximal ideals.

A ring is called *local* if it has only one maximal ideal which coincides with its Jacobson radical.

Proposition 4.2. *Let R be a ring, $x \in R$, and $u \in R^\times$. Then $x \in \mathrm{J}(R)$ if and only if $u - xy \in \mathrm{J}(R)$ is a unit for all $y \in R$. In particular, the sum of an element of $\mathrm{J}(R)$ and a unit is a unit.*

PROOF. Assume $x \in \mathrm{J}(R)$. Let $\mathfrak{m}$ be a maximal ideal. Suppose $u - xy \in \mathfrak{m}$. Since $x \in \mathfrak{m}$ too, also $u \in \mathfrak{m}$, a contradiction. Thus $u - xy$ is a unit. In particular, taking $y := -1$ yields $u + x \in R$. Conversely, assume $x \notin \mathrm{J}(R)$. Then there is a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$. So $\langle x \rangle + \mathfrak{m} = R$. Hence there exist $y \in R$ and $m \in \mathfrak{m}$ such that $xy + m = u$. Then $u - xy = m \in \mathfrak{m}$. So $u - xy$ is not a unit. □

PROPOSITION 4.3. *A ring R is local if and only if the set of non-units $\mathfrak{n}$ is an ideal; if so, then $\mathfrak{n}$ is the maximal ideal.*

PROOF. Every proper ideal I is included in $\mathfrak{n}$ as it contains no unit. So, if $\mathfrak{n}$ is an ideal, then it is a maximal ideal, and the only one. Thus R is local. Conversely, assume R is local with maximal ideal $\mathfrak{m}$. Then $R - \mathfrak{n} = R - \mathfrak{m}$, hence $\mathfrak{n} = \mathfrak{m}$. □

DEFINITION 4.4. Let S be a subset of R. The radical of S, denoted $\sqrt{S}$, is defined by

$$\sqrt{S} = \{x \in R | x^n \in S \text{ for some } n \in \mathbb{N}^*\}.$$

An ideal I is called *radical* if $I = \sqrt{I}$.

Note that if I is an ideal, then so is $\sqrt{I}$. We have also $\sqrt{\sqrt{I}} = \sqrt{I}$. It is clear that $\sqrt{\langle 0 \rangle}$ is the set of nilpotent elements of R. Is called the *nilradical* of R and denoted $\mathrm{nil}(R)$.

PROPOSITION 4.5. *Let R be a commutative ring, and let $I, I_1, \ldots, I_n$ be ideals of R. Then*

$$\sqrt{I_1 \cdots I_n} = \sqrt{\bigcap_{j=1}^{n} I_j} = \bigcap_{j=1}^{n} \sqrt{I_j},$$

and consequently,

$$\sqrt{I^n} = \sqrt{I}.$$

PROOF. Since $I_1 \cdots I_n \subseteq \bigcap_{j=1}^{n} I_j$, we have

$$\sqrt{I_1 \cdots I_n} \subseteq \sqrt{\bigcap_{j=1}^{n} I_j}.$$

Additionally, since $\bigcap_{j=1}^{n} I_j \subseteq I_i$ for every $i \in \mathbb{N}$, it follows that

$$\sqrt{\bigcap_{j=1}^{n} I_j} \subseteq \bigcap_{j=1}^{n} \sqrt{I_j}.$$

Finally, if $r \in \bigcap_{j=1}^{n} \sqrt{I_j}$, then part (1) guarantees the existence of $m_1, \ldots, m_n \in \mathbb{N}$ such that $r^{m_j} \in I_j$ for every $j \in \{1, \ldots, n\}$. Thus,

$$r^{m_1+\cdots+m_n} \in I_1 \cdots I_n,$$

which implies that $r \in \sqrt{I_1 \cdots I_n}$. Hence,

$$\bigcap_{j=1}^{n} \sqrt{I_j} \subseteq \sqrt{I_1 \cdots I_n}.$$

The second statement is a special case of the first one. □

THEOREM 4.6. *Let R be a ring, I an ideal. Then*

$$\sqrt{I} = \bigcap_{I \subset \mathfrak{p}} \mathfrak{p},$$

where the intersection is over all the prime ideals containing I. In particular, taking $I = \langle 0 \rangle$, we deduce

$$\operatorname{nil}(R) = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p},$$

PROOF. Let $x \in \sqrt{I}$ and $\mathfrak{p}$ a prime ideals containing I. Then $x^n \in I \subset \mathfrak{p}$, hence either x or x^{n-1} is in $\mathfrak{p}$, after a finite number of steps, we deduce that $x \in \mathfrak{p}$. So $\sqrt{I} \subset \bigcap_{I \subset \mathfrak{p}} \mathfrak{p}$.
Conversely, let $x \notin \operatorname{nil}(R)$, Let S be the set of ideals I of R with the property that for any $n > 0$, $x^n \notin I$. When ordered by inclusion, note that every chain in S, denoted as $I_1 \subseteq I_2 \subseteq \cdots$, is bounded above: if $I = \bigcup I_i$, then I is an upper bound and clearly belongs to S. By Zorn's lemma, S has a maximal element, denoted as $\mathfrak{p}$, which we claim is prime.

Suppose $uv \in \mathfrak{p}$ but $u \notin \mathfrak{p}$ and $v \notin \mathfrak{p}$. Then the ideals $\mathfrak{p} + (u)$ and $\mathfrak{p} + (v)$ strictly contain $\mathfrak{p}$, so they do not belong to S by the

maximality of $\mathfrak{p}$. Consequently, there exist m and n such that $x^n \in \mathfrak{p} + (u)$ and $x^m \in \mathfrak{p} + (v)$. This implies that $x^{m+n} \in \mathfrak{p} + (uv) = \mathfrak{p}$, thus contradicting the assumption that $\mathfrak{p}$ is in S. Hence, either u or v lies in $\mathfrak{p}$, making $\mathfrak{p}$ prime.

From this, it follows that x is not contained in the prime ideal $\mathfrak{p}$, and therefore x is not contained in the intersection $\bigcap_{I \subset \mathfrak{p}} \mathfrak{p}$, of all prime ideals containing I. □

5. Unique factorisation domain

Definition 5.1. An integral ring R is called Unique Factorization Domain (UFD) if every nonzero element of R which is not invertible is a product of irreducible elements in a unique way up to order and units.

Example 5.2.

(1) The ring of integers $\mathbb{Z}$ is a classic example of a UFD. Here, irreducible elements are prime numbers, and every non-zero integer can be uniquely factored into a product of primes, known as the Fundamental Theorem of Arithmetic.
(2) The ring $k[X]$ is UFD for any field k.

Theorem 5.3. *Let R be an integral ring. R is a unique factorization domain iff it satisfies the following two conditions:*

(*i*) *Every increasing sequence of principal ideals of A is stationary;*
(*ii*) *Every irreducible element is prime.*

Proof. See [**?**, Théorème 9.115]. □

Theorem 5.4. *Let R be UFD, then $R[X]$ is also UFD.*

For the proof we refer to [**?**].

Proposition 5.5. *A principal ideal domain is unique factorisation domain.*

This can be see as a consequence of Theorem 5.3. In fact, we have already seen in a PID, that an irreducible element is prime.

THEOREM 5.6. *Let R be an integral domain. Then R is a UFD if and only if any nonzero prime ideal of R contains a prime element.*

PROOF. For the direct implication, assume that R is a Unique Factorization Domain (UFD), and let P be a nonzero prime ideal of R. Consider a nonzero element $r \in P$, and since R is a UFD, we can express r as

$$r = p_1 \cdot p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are prime elements in R. Because P is prime, it follows that $p_j \in P$ for some $j \in \{1, 2, \ldots, k\}$.
Conversely, assume that every nonzero prime ideal of R contains a prime element. Let S denote the set of elements in R that can be expressed as a product of prime elements. We know that S is a saturated multiplicative subset[1], and thus, $R \setminus S$ is the union of prime ideals[2]. Now, let $x \in R \setminus S$. Since S is saturated, the ideal Rx is disjoint from S. Therefore, there exists a prime ideal P that is disjoint from S and contains Rx. Given that every nonzero prime ideal contains a prime element and $P \cap S = \emptyset$, it follows that P must be the zero ideal, leading to the conclusion that $x = 0$. Therefore, every nonzero element of R can be expressed as a product of prime elements, which confirms that R is a UFD.

□

6. Noetherian and Artinian Rings

Noetherian and Artinian rings are fundamental concepts in algebra, particularly in ring theory. Named after Emmy Noether and Emil Artin respectively, these rings capture essential properties related to the finiteness and well-behavedness of ideals. Noetherian rings satisfy the ascending chain condition on ideals, while Artinian rings satisfy the descending chain condition.

[1] A saturated subset of $R \setminus \{0\}$ is a multiplicative submonoid S of $R \setminus \{0\}$ such that for all $x \in S$ if $y|x$ in R, then $y \in S$.

[2] This is a non trivial fact, see [**?**, Proposition 6].

DEFINITION 6.1. A commutative ring R is said to be *Noetherian* if every ascending chain of ideals

$$I_1 \subset I_2 \subset \cdots$$

is stationary.

EXAMPLE 6.2.

(1) $\mathbb{Z}$ and $K[X]$ are Noetherian.
(2) Let K be a field and consider the ring $K[X_1, X_2, \dots]$ of polynomials with infinite indeterminates. This ring is a typical example of a non-Noetherian because one can take the ascending chain

$$\langle X_1 \rangle \subset \langle X_1, X_2 \rangle \subset \cdots .$$

PROPOSITION 6.3. *A ring R is Noetherian if and only if every ideal of R can be generated by a finite set of elements.*

PROOF. Assume that R is a Noetherian, let $I \subset R$. Take $S = \{x_1, x_2, \cdots\}$ be a generating set of I and define $I_i := \langle x_1, x_2, \cdots, x_n \rangle$. Then we have an ascending chain

$$I_1 \subset I_2 \subset \cdots .$$

Since this is a stationary and $I = \bigcup I_i$, we deduce that I is finitely generated.
Conversely, assume that any ideal is finitely generated and let

$$I_1 \subset I_2 \subset \cdots$$

be an ascending chain. Let $I = \bigcup_i I_i$, then I is finitly generated, and clearly this implies that this ascending chain is stationary. □

THEOREM 6.4. *If R is a Noetherian ring, then $R[X]$ is a Noetherian.*

For the proof, see [**Eis95**].

DEFINITION 6.5. An *Artinian ring* is a ring that satisfies the descending chain condition on ideals. Specifically, this means that for any descending sequence of ideals

$$I_1 \supset I_2 \supset I_3 \supset \cdots ,$$

there exists some integer n such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

In other words, every decreasing sequence of ideals stabilizes after a finite number of steps. This condition imposes significant structural constraints on the ring and is a fundamental notion in ring theory.

Note that in a Noetherian ring, every element has only a finite number of divisors, whereas in an Artinian ring, each element has only a finite number of multiples. This is one of the key differences between the two concepts. It is worth noting that, as we have seen, there are many Noetherian rings, while Artinian rings are much less common.

Example 6.6.

(1) A ring with finitely many ideals is Artinian. In particular, a finite ring (e.g., $\mathbb{Z}/n\mathbb{Z}$) is Artinian.
(2) Let k be a field. Then $k[\epsilon]/(\epsilon^n)$ is Artinian for every positive integer n.

Proposition 6.7. *An integral domain is Artinian if and only if it is a field.*

Proof. Let $a \in R$ be nonzero, and consider the sequence $I_i = \langle a^i \rangle$. There exists a positive integer n such that $I_n = I_{n+1}$; in other words, $a^{n+1} \mid a^n$, which means there exists $b \in R$ such that $a^n = ba^{n+1}$. Since R is integral, we deduce that $ba = 1$, as desired. The converse is trivial. □

7. Hilbert's Nullstellensatz

Hilbert's Nullstellensatz is a fundamental result in algebraic geometry that connects algebraic sets and ideals in polynomial rings. It establishes a deep relationship between geometric objects defined as the zero sets of polynomials and the algebraic structure of the corresponding polynomial ideals. In particular, for an algebraically closed field k, the theorem provides key insights into the nature of maximal ideals in the ring of polynomials $k[X_1, \ldots, X_n]$.

In this section, we focus on the characterization of maximal ideals in the polynomial ring over an algebraically closed field, which is

a direct consequence of Hilbert's Nullstellensatz. We show that these maximal ideals correspond to points in affine space, leading to a bridge between algebraic structures and their geometric counterparts.

THEOREM 7.1 (Weak Nullstellensatz). *Let k be an algebraically closed field and let n be a positive integer. The maximal ideals of $k[X_1, \ldots, X_n]$ are the ideals of the form*

$$\langle X_1 - a_1, \ldots, X_n - a_n \rangle,$$

where $(a_1, \ldots, a_n) \in k^n$.

PROOF. Let $I = (x_1 - c_1, \ldots, x_n - c_n)$. Since $x_i \equiv c_i \mod I$, it follows that

$$f(x_1, \ldots, x_n) \equiv f(c_1, \ldots, c_n) \mod I$$

for all $f \in K[x_1, \ldots, x_n]$. Therefore, $f(c_1, \ldots, c_n) = 0$ if and only if $f(x_1, \ldots, x_n) \in I$. Consequently, the evaluation homomorphism

$$K[x_1, \ldots, x_n] \to K, \quad f(x_1, \ldots, x_n) \mapsto f(c_1, \ldots, c_n)$$

has kernel I. This homomorphism is surjective, as elements of K map to themselves, which implies that

$$K[x_1, \ldots, x_n]/I \cong K.$$

Since the right-hand side, K, is a field, it follows that I is a maximal ideal in $K[x_1, \ldots, x_n]$.

Conversely, let m be a maximal ideal of $K[x_1, \ldots, x_n]$ when K is algebraically closed. The quotient $K[x_1, \ldots, x_n]/m$ is a finite extension of K. Given that K is algebraically closed, its only finite extension is itself. Therefore, $K[x_1, \ldots, x_n]/m$ has degree 1 over K, meaning each coset modulo m can be represented by an element of K. Thus, there exist $c_i \in K$ such that $x_i \equiv c_i \mod m$. This implies that $x_i - c_i \in m$, leading to the containment $(x_1 - c_1, \ldots, x_n - c_n) \subset m$. The containment must be an equality, as the ideal $(x_1 - c_1, \ldots, x_n - c_n)$ is maximal.

If the ideals $(x_1 - c_1, \ldots, x_n - c_n)$ and $(x_1 - c_1', \ldots, x_n - c_n')$ in $K[x_1, \ldots, x_n]$ are equal, then $c_i - c_i'$ is contained in the ideal, as it can be expressed as $(c_i - x_i) - (c_i' - x_i)$. A proper ideal in $K[x_1, \ldots, x_n]$

cannot contain an element of $K^\times$, so it follows that $c_i - c_i' = 0$ for all i. Thus, $c_i = c_i'$.

□

THEOREM 7.2 (Hilbert's Nullstellensatz). *Let k be an algebraically closed field and let I be an ideal of the polynomial ring $k[x_1, x_2, \ldots, x_n]$. Then the radical $\sqrt{I}$ of I is equal to the set of all polynomials $f \in k[x_1, x_2, \ldots, x_n]$ such that $f(a_1, a_2, \ldots, a_n) = 0$ for all $(a_1, a_2, \ldots, a_n)$ in the common zeros of all polynomials in I.*

PROOF. Note by $\mathcal{V}(I)$ the set of commun solutions of polynomials in I and $\mathcal{I}(\mathcal{V}(I))$ the set of polynomials that are zero on $\mathcal{V}(I)$. The assertion that $\sqrt{I} \subset I(\mathcal{V}(I))$ is clear. Suppose that G belongs to the ideal $\mathcal{I}(\mathcal{V}(F_1, \ldots, F_r))$, where $F_i \in k[X_1, \ldots, X_n]$. We define the ideal

$$J = (F_1, \ldots, F_r, X_{n+1}G^{-1}) \subseteq k[X_1, \ldots, X_n, X_{n+1}].$$

Since G vanishes wherever all the F_i's are zero, the set $\mathcal{V}(J) \cap k^{n+1}$ is empty. By applying the Weak Nullstellensatz to the ideal J, we can conclude that $1 \in J$. Therefore, there exists a polynomial equation of the form:

$$1 = P(X_1, \ldots, X_{n+1}) + B(X_1, \ldots, X_{n+1})(X_{n+1}G^{-1}),$$

for some polynomials P and B in $k[X_1, \ldots, X_{n+1}]$.

Next, let $Y = \frac{1}{X_{n+1}}$, and multiply the equation by a sufficiently high power of Y to obtain an equation of the form:

$$Y^N = \sum_i C_i(X_1, \ldots, X_n, Y)F_i - D(X_1, \ldots, X_n, Y)(G - Y),$$

where C_i and D are polynomials in $k[X_1, \ldots, X_n, Y]$. Substituting G for Y yields the desired polynomial equation.

□

8. Exercises

EXERCISE 1. *Let X be a nonempty set. Consider the set $R = \mathcal{P}(X)$ of subsets of X, together with the set operations of symmetric difference*

$$A + B := A\Delta B = (A \cap \overline{B}) \cup (B \cap \overline{A})$$

and intersection

$$A \cdot B = A \cap B.$$

(1) Show that R is a ring.
(2) Is R commutative? Does it have a unity?

EXERCISE 2.

(1) Find all ring homomorphisms of the ring $\mathbb{Z}$ to $\mathbb{Z}$.
(2) Find all ring homomorphisms of $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

EXERCISE 3. *Let R be a ring without nonzero nilpotents. Then, for every idempotent $e \in R$ and every $x \in R$, show that $xe = ex$.* Hint: compute $(ex - exe)^2$ and $(xe - exe)^2$).

EXERCISE 4. *Show that $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ has a zero-divisor which is not zero if and only if n is not a prime.*

EXERCISE 5. *Prove that the center of a ring R is a subring.*

EXERCISE 6. *Let $f : R \to S$ be a non-zero ring homomorphism such that S is integral, show that $Ker(f)$ is prime ideal.*

EXERCISE 7. *Prove Proposition 3.3*

EXERCISE 8. *Show that the ring R does not contain a nonzero nilpotent if and only if 0 is the only solution of the equation $x^2 = 0$ in R.*

EXERCISE 9. *Let $f : R \to K$ be a ring homomorphism. Show that* $\ker(f)$ *is a prime ideal.*

EXERCISE 10.

(i) Prove that $\langle a \rangle$ is prime iff a is prime.
(ii) If R is integral, then a prime element is irreducible.
(iii) If R is integral, if $\langle a \rangle$ is maximal, then a is irreducible.
(iii) If R is PID, then $\langle a \rangle$ is maximal iff a is irreducible.

EXERCISE 11. *Let n be an integer such that $n \geqslant 1$.*

(1) What are the invertible elements of $\mathbb{Z}/n\mathbb{Z}$? For which integers n is that ring a domain? a field?

(2) *Let m be an integer such that $m \geqslant 1$. Show that the canonical map from $\mathbb{Z}/nm\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ is a ring morphism. Show that it induces a surjection from $(\mathbb{Z}/nm\mathbb{Z})^\times$ to $(\mathbb{Z}/n\mathbb{Z})^\times$ (Hint: Use Chinese reminder theorem to reduce to the case $nm = p^k$ and $n = p^l$).*

(3) *Determine the nilpotent elements of the ring $\mathbb{Z}/n\mathbb{Z}$.*

EXERCISE 12. *If R is an integral finite ring with unity $1 \neq 0$, then R is a division ring (i.e. every nonzero element is invertible).*

EXERCISE 13. *Let R be a ring such that for any element $x \in R$, we have $x^2 = x$. Show that R is commutative.*

EXERCISE 14. *Let R be a ring and $x \in R$. Suppose there exists a positive integer n such that $x^n = 0$. Show that $1 + x$ and $1 - x$ are units.*

EXERCISE 15. *Let R be a commutative ring. Define*

$$\mathrm{nil}(R) = \{r \in R \mid \exists n \geq 1, r^n = 0\}.$$

(1) *Prove that $\mathrm{nil}(R)$ is an ideal of R.*

(2) *Show that $\mathrm{nil}(R)$ is contained in any prime ideal.*

(3) *Show that if $r \in \mathrm{nil}(R)$, then $1 - r$ is invertible in R.*

(4) *Show, with a counter-example, that $\mathrm{nil}(R)$ is not necessarily an ideal if R is not commutative (Hint: look at the ring of matrices).*

EXERCISE 16. *Let I be an ideal, and $\mathfrak{p}$ and $\mathfrak{q}$ two prime ideals such that $I \subset \mathfrak{p} \cup \mathfrak{q}$. Show that $I \subset \mathfrak{p}$ or $I \subset \mathfrak{q}$.*

EXERCISE 17. *Let I and J be ideals, and $\mathfrak{p}$ a prime ideal of a ring R. Prove that the following are equivalent:*

(*i*) $I \subset \mathfrak{p}$ *or* $J \subset \mathfrak{p}$.

(*ii*) $I \cap J \subset \mathfrak{p}$

(*iii*) $IJ \subset \mathfrak{p}$

EXERCISE 18. *Let R be a principal ideal domain. Show that for a non-zero ideal of R to be prime, it is necessary and sufficient that it be generated by an irreducible element; it is then a maximal ideal. In particular, an irreducible element is prime.*

EXERCISE 19. *Let R be a ring, $J(R)$ its Jacobson radical. Let I be an ideal of R such that $I \subset \mathrm{J}(R)$. For $x \in R$ we denote $\bar{x} \in R/I$ its residue modulo I.*

(1) Prove that x is invertible if and only if $\bar{x} \in (R/I)$ is invertible.
(2) What if $I \not\subset J(R)$?

EXERCISE 20. *Let R and R' be commutative rings and let $f : R \to R'$ be a ring homomorphism. Let $I \subseteq R$ and $I' \subseteq R'$ be ideals of R and R', respectively.*

(a) Prove that $f(\sqrt{I}) \subseteq \sqrt{f(I)}$.
(b) Prove that $\sqrt{f^{-1}(I')} = f^{-1}(\sqrt{I'})$.
(c) Suppose that f is surjective and $\ker(f) \subseteq I$. Then prove that $f(\sqrt{I}) = \sqrt{f(I)}$.

EXERCISE 21. *Let R be a commutative ring with $1 \neq 0$, and let $\phi : R \to R$ be a ring homomorphism. Assume that R is Noetherian and ϕ is surjective.*

(a) *Show that ϕ must be injective, and thus an isomorphism.* Hint*: Consider the iterates of ϕ and their kernels.*
(b) *Can you provide a counterexample where ϕ is not injective if R is not Noetherian?*

EXERCISE 22. *Suppose that $f : R \to R'$ is a surjective ring homomorphism. If R is a Noetherian ring, show that R' is also Noetherian.*

EXERCISE 23. *Let R be a commutative ring with unity $1 \neq 0$. Suppose that for each element $a \in R$, there exists a positive integer $n > 1$ such that $a^n = a$. Prove that every prime ideal in R is maximal.*

CHAPTER 2

Modules over Commutative Rings

1. Definitions and examples of modules

In this section, we will delve into the definitions and examples of modules over commutative rings. Modules are a generalization of vector spaces, where the scalars come from a commutative ring instead of a field. Understanding the key definitions and exploring examples will provide us with a solid foundation in module theory.

To begin, let's define what a module is.

DEFINITION 1.1. A module over a commutative ring R is a set M equipped with two operations: addition, denoted by $+$, and scalar multiplication, denoted by $\cdot$, satisfying the following properties:

(1) $(M, +)$ is an abelian group, meaning it satisfies the properties of associativity, commutativity, existence of identity element, and existence of inverses.
(2) For any $r, s \in R$ and $x, y \in M$, the scalar multiplication $r \cdot x$ is defined and satisfies the properties:
   (i) Distributivity over addition: $(r + s) \cdot x = r \cdot x + s \cdot x$.
   (ii) Compatibility with ring multiplication: $(rs) \cdot x = r \cdot (s \cdot x)$.
   (iii) Compatibility with scalar addition: $r \cdot (x + y) = r \cdot x + r \cdot y$.
   (iv) Identity element of the ring: $1 \cdot x = x$, where 1 is the multiplicative identity of R.

These properties ensure that a module is a structure where we can add elements and multiply elements by scalars from the commutative ring R in a consistent manner. Let's explore some examples:

EXAMPLE 1.2.

- If R is a commutative ring, then R itself is a module over itself.

- If R is a commutative ring and $I \subset R$ an ideal, then I is an R-module.
- Let V be a vector space over a field $\mathbb{F}$. Then V can be naturally viewed as a module over the ring $\mathbb{F}$ by defining scalar multiplication in the usual way.
- Consider the ring $R = \mathbb{Z}$ of integers. A module over $\mathbb{Z}$ is simply an abelian group, as scalar multiplication by an integer is equivalent to repeated addition.
- The ring of polynomials $R[X]$ is an R-module.
- Let $I \subset R$ be an ideal. Then the quotient R/I is an R-module with an exterior product $a \cdot (x + I) = ax + I$.

DEFINITION 1.3. Let R be a ring. A ring $(A, +, \times)$ is called an R-algebra if it is an $R-$module such that the multiplication $\times$ and the exterior product $\cdot$ satisfy for any $a \in R$ and $x, y \in A$:

$$a \cdot (x \times y) = (a \cdot x) \times y = x \times (a \cdot y).$$

EXAMPLE 1.4.

(1) As an example, for any ring extension $R \subseteq S$, an S-module is just an R-algebra structure on S.
(2) The rings $R[X]$ and $\mathcal{M}_n(R)$ are examples of R-algebras.
(3) The ring R is not always an R-algebra unless it is commutative.

Let M and N be two submodules, The Cartesian product of M and N, denoted $M \times N$ equipped with the operations

- $(x, y) + (x', y') = (x + x', y + y')$;
- $a \cdot (x, y) = (x \cdot x, a \cdot y)$

is an R-module. We can repeat this operation to generate the Cartesian product of a finite number of R-modules.

DEFINITION 1.5. Let R be a ring and let M and N be R-modules. A function

$$f : M \to N$$

is called a *morphism of R-modules* (or an R-module homomorphism) if it satisfies the following properties for all $x, y \in M$ and $a \in R$:

(1) $f(x+y) = f(x) + f(y)$ (additivity),
(2) $f(a \cdot x) = a \cdot f(a)$ (R-linearity).

A morphism $f : M \to N$ is an *isomorphism* if it is bijective. If f is an isomorphism, M and N are said to be *isomorphic*, denoted $M \cong N$. We also have the definitions:

(*i*) $f : M \to N$ is a *monomorphism* if $\ker(f) = \{0\}$, i.e. f is injective.
(*ii*) $f : M \to N$ is an *epimorphism* if $\mathrm{im}(f) = N$, i.e. f is surjective.

If $f : M \to N$ and $g : N \to P$ are R-module homomorphisms, then the composition $g \circ f : M \to P$ is also an R-module homomorphism.

Example 1.6.

(1) If N is a submodule of M, then the natural injection of N into M defines a morphism of A-modules. The canonical surjection of M onto M/N defines a morphism of A-modules.
(2) For any set I, the groups A^I (the set of families of elements of A indexed by I) and $A(I)$ (the subset of A^I consisting of families with finite support, i.e., the families $(a_i)_{i\in I} \in A^I$ such that almost all a_i are zero) are A-modules with the obvious definition of the external operation:
$$a \cdot (a_i)_{i\in I} := (aa_i)_{i\in I}.$$
(3) More generally, if we have a family of A-modules M_i, the product group $\prod M_i$ is an A-module with the obvious definition of the external operation:
$$a \cdot (x_i)_{i\in I} := (ax_i)_{i\in I}.$$
The same holds for the direct sum subgroup $\bigoplus M_i$ of $\prod M_i$ (consisting of $(x_i)_{i\in I} \in \prod M_i$ such that almost all x_i are zero).
(4) Let M be an A-module, and let $f : A' \to A$ be a ring homomorphism. Defining $a' \cdot x := f(a')x$, we make M into a A'-module. In particular, if A' is a subring of A, the restriction of the external operation $A \times M \to M$ to $A' \times M$ turns M into an A'-module (this is the restriction of scalars).

PROPOSITION 1.7. *The set of all R-module homomorphisms from M to N is denoted* $\mathrm{Hom}_R(M,N)$. *This set is itself an R-module when R is commutative, with operations defined point-wise.*

A submodule of a module M over a commutative ring R is a subset $N \subseteq M$ that is itself a module over R with respect to the operations of addition and scalar multiplication inherited from M. In other words, N is closed under addition and scalar multiplication, and it satisfies the module axioms. Submodules can be viewed as "substructures" within a larger module, and they allow us to analyze specific components or subspaces of the module.
As and example, the $R-$submodules of R are precisely the ideals of R. Moreover, let M be an R-module and $I \subset R$ be an ideal, and define

$$IM = \{\sum_{i=1}^{n} a_i x_i \,|\, n \in \mathbb{N}^*, a_i \in I, x_i \in M\},$$

then IM is an R-submodule of M (exercice).

The *kernel* of a morphism $f : M \to N$ is defined as

$$\ker(f) = \{m \in M \mid f(m) = 0\}.$$

It is a submodule of M.

The *image* of f is defined as

$$\mathrm{im}(f) = \{f(m) \mid m \in M\}.$$

It is a submodule of N.

Let M ba an $R-$module, $P \subset M$ an R-submodule. The quotient group M/P is naturally equipped with the structure of an $R-$module as follows : for $x \in M, a \in R$

$$a \cdot (x + P) = ax + P.$$

Quotient modules provide a way to "collapse" a submodule to a single element, allowing us to study the relationship between the original module and its submodules.

PROPOSITION 1.8. *Let M be an $R-$module and $P \subset N$ two submodules, then we have a canonical isomorphism*

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

PROOF. Define the map

$$\varphi : M \to (M/P)/(N/P)$$

by $\varphi(m) = m + N/P$, where $m \in M$. This map is well defined since the elements of N are mapped to N/P in M/P, ensuring that φ respects the structure of the quotient.

The map φ induces a homomorphism

$$\psi : M/N \to (M/P)/(N/P)$$

given by

$$\psi(m + N) = (m + P) + (N/P),$$

where $m + N \in M/N$ and $(m + P) + (N/P) \in (M/P)/(N/P)$. The map ψ is well-defined because $P \subseteq N$, so if $m' \equiv m \pmod{N}$, then $m' + P \equiv m + P \pmod{N/P}$.

Injectivity of ψ: Suppose $\psi(m + N) = 0$. This means that $(m + P) + (N/P) = 0$ in $(M/P)/(N/P)$, or equivalently, $m + P \in N/P$. Thus, there exists some $n \in N$ such that $m + P = n + P$, which implies $m - n \in P$. Since $n \in N$, we have $m \in N$, and hence $m + N = 0$ in M/N. Therefore, ψ is injective.

The surjectivity of ψ is clear. Since ψ is both injective and surjective, it is an isomorphism. □

EXAMPLE 1.9. Let E be a vector space over a field K and u an endomorphism of E. Then, we can equip E with a structure of a $K[X]$-module by defining

$$P \cdot x = P(u)(x), \quad P \in K[X], x \in E.$$

DEFINITION 1.10. Let $x \in M$; we define its annihilator as

$$\mathrm{Ann}(x) = \mathrm{Ann}_R(x) = \{a \in R \mid ax = 0\}.$$

Note that $\mathrm{Ann}(x)$ is an ideal of R, and we have:

$$x = 0 \iff \mathrm{Ann}(x) = (1).$$

We also define the annihilator of M as:

$$\mathrm{Ann}(M) = \bigcap_{x \in M} \mathrm{Ann}(x) = \{a \in R \mid aM = (0)\}.$$

PROPOSITION 1.11. *Let $x \in M$ and $I = Ann_R(x)$. The map $a + I \mapsto ax$ is an isomorphism of A-modules:*

$$R/I \xrightarrow{\sim} Rx \subseteq M.$$

PROOF. Left to the reader □

COROLLARY 1.12. *Let M be a simple R-module. Then $M \cong R/I$, where I is a maximal ideal.*

PROOF. Let $x \in M$ be nonzero. Then $M = Rx$. Setting $I = \mathrm{Ann}(x)$, we obtain, from Proposition 1.11 □

$$R/I \cong Rx = M.$$

Since M is simple, this implies that I is maximal.

1.1. Linear algebra. Let A be a $n \times n$ matrix with entries in a ring R. We can compute its determinant in the usual way and get

$$A \times \tilde{A} = \det(A) I_n.$$

THEOREM 1.13. *Let A be a nonzero $m \times n$ matrix over a principal ideal domain R. There exist invertible $m \times m$ and $n \times n$ matrices S and T (with entries in R) such that the product SAT is*

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & \ddots & & \vdots & & \vdots \\ \vdots & & & \alpha_r & & & \\ 0 & & \cdots & & 0 & \cdots & 0 \\ \vdots & & & & \vdots & & \vdots \\ 0 & & \cdots & & 0 & \cdots & 0 \end{pmatrix}.$$

The diagonal elements α_i satisfy $\alpha_i \mid \alpha_{i+1}$ for all $1 \leq i < r$.

This is the Smith normal form of the matrix A. The elements α_i are unique up to multiplication by a unit and are called elementary divisors, invariants, or invariant factors. They can be computed (up to multiplication by a unit) as

$$\alpha_i = \frac{d_i(A)}{d_{i-1}(A)},$$

where $d_i(A)$ (called the i-th determinant divisor) equals the greatest common divisor of the determinants of all $i \times i$ minors of the matrix A, and $d_0(A) := 1$.

2. Finitely Generated Modules

In this section, we discuss the concept of finitely generated modules and generators. Finitely generated modules play a crucial role in module theory, as they allow us to understand and analyze modules in terms of a finite set of generators. The concept of finitely generated modules has applications in various areas of mathematics, including algebraic geometry, representation theory.

Definition 2.1. A module M over a commutative ring R is said to be *finitely generated* (or *of finite type*) if there exist elements $m_1, m_2, \ldots, m_n \in M$ such that every element $m \in M$ can be expressed as a linear combination of these generators. In other words, M is of finite type if there exist $m_1, m_2, \ldots, m_n \in M$ such that for every $m \in M$, we can write $m = r_1m_1 + r_2m_2 + \ldots + r_nm_n$, for some $r_i \in R$.

The set $\{m_1, \cdots, m_n\}$ is called a generating set.
A set of generators $m_1, m_2, \ldots, m_n$ for a finitely generated module M is said to be *minimal* if no proper subset of the generators can generate M. Minimal generators provide a concise representation of the module structure and are often useful in computations and proofs.

Module homomorphisms between finitely generated modules can be understood in terms of generators. If M and N are finitely generated modules with generators $m_1, m_2, \ldots, m_k$ and $n_1, n_2, \ldots, n_l$, respectively, then a module homomorphism $\varphi : M \to N$ is completely determined by its action on the generators. This property allows us to study module homomorphisms by considering their matrices.

PROPOSITION 2.2. *If M is a module of finite type and N is a submodule of M, then M/N is also a module of finite type.*

PROOF. Easy. □

Note that every module of finite type over a commutative ring is Noetherian. This means that the ascending chain condition holds for submodules, i.e., there are no infinite strictly ascending chains of submodules.

2.1. Finitely generated modules over a PID. The structure theorem for finitely generated modules over a principal ideal domain (PID) is a generalization of the fundamental theorem of finitely generated abelian groups. It asserts that such modules can be uniquely decomposed in a manner analogous to the prime factorization of integers.

THEOREM 2.3. *For every finitely generated module M over a principal ideal domain R, there exists a unique decreasing sequence of proper ideals*

$$(a_1) \supseteq (a_2) \supseteq \cdots \supseteq (a_n)$$

such that M is isomorphic to the direct sum of cyclic modules:

$$M \cong \bigoplus_i R/(a_i) = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n).$$

PROOF. □

REMARK 2.4.
- **Classification of Modules:** The structure theorem provides a classification of finitely generated modules over principal ideal domains, allowing us to understand and analyze their structure in a systematic way. It breaks down

a complicated module into simpler cyclic modules, which are isomorphic to ideals of the underlying principal ideal domain.
- **Solving Systems of Linear Equations:** The structure theorem has applications in solving systems of linear equations over principal ideal domains. By expressing the coefficient matrix as a module, the structure theorem helps in understanding the possible solutions and the relationship between the solutions.

3. Free Modules

Let M be an R-module and let $M := (m_i)_{i\in I}$ be a family of elements of M. We say that the family M is:

- A **free family** if the equality
$$0 = \sum_{i\in I} a_i m_i$$
for a collection of elements $(a_i)_{i\in I} \in R^{(I)}$ implies that all a_i are zero.
- A **basis** if the family is both free and generating.

Remark 3.1. Every module has a generating set: one can take all its elements.

Definition 3.2. A module is called **free** if it has a basis.

The notion of a basis is crucial in the case of vector spaces, as it provides a minimal and complete set of elements that determine the space. This allows us to:

- Develop a dimension theory,
- Define morphisms easily by sending basis elements to linear combinations of basis elements in the target,
- Develop the concept of matrices and related notions (determinants, invertibility, similarity of matrices, etc.).

However, in the general context of R-modules, certain problems arise even in basic examples:

- If R is not an integral domain, it has zero divisors. If we take an ideal generated by a zero divisor $a \in R$, it cannot have a

basis. Indeed, there exists $b \in R$ such that $ab = 0$, and for every x in the ideal, we have $bx = 0$ without b being zero. For example, in the ring $\mathbb{Z}/4\mathbb{Z}$, the set $\{\bar{2}, \bar{0}\}$ is an ideal and satisfies $(\bar{2}) \cdot (\bar{2}) = \bar{0}$. This ideal is not a free $\mathbb{Z}/4\mathbb{Z}$-module.

- Even in an integral domain, consider $R = \mathbb{Z}$ and $M = \mathbb{Z}/4\mathbb{Z}$. Since $4x = 0$ for all $x \in M$, no family in M can be free!

REMARK 3.3. A subfamily of a free family is necessarily free, and a superfamily of a generating family is generating.

For any integer $n \geq 1$, we denote by R^n the Cartesian product of n copies of R, i.e., the set of n-tuples $(a_1, \ldots, a_n)$ with $a_i \in R$. This is an R-module with the usual multiplication:

$$a \cdot (a_1, \ldots, a_n) = (aa_1, \ldots, aa_n).$$

DEFINITION 3.4. A free R-module M is said to have **rank** n if it is isomorphic to R^n. Or equivalently, it has a basis with n elements.

LEMMA 3.5. *An R-module V is free of rank n if and only if it has a basis consisting of n elements.*

EXAMPLE 3.6.

The module R^n has a standard basis given by the elements $e_j = (0, \ldots, 1, \ldots, 0)$, where 1 is in the j-th position. If $f : R^n \to R^m$ is an R-module morphism, it is completely determined by the images $f(e_j)$. These images can be expressed in the standard basis of R^m, allowing us to store the information in an $m \times n$ matrix. The matrix of a composition of morphisms is given by the product of their matrices, just as in linear algebra.

PROPOSITION 3.7. *Every module M is isomorphic to a quotient of a free module.*

PROOF. Take a generating set $(m_i)_{i \in I}$ of M and define the R-module morphism:

$$\Psi : R^{(I)} \to M, \quad (a_i)_{i \in I} \mapsto \sum_{i \in I} a_i m_i.$$

By definition, this map is surjective. Taking the quotient by its kernel, we obtain:

$$M \cong R^{(I)}/\ker(\Psi),$$

which proves the proposition. □

EXAMPLE 3.8. The direct sum of two free modules M and N is also a free module. If M has basis $\{m_1, m_2, \ldots, m_n\}$ and N has basis $\{n_1, n_2, \ldots, n_m\}$, then the direct sum $M \oplus N$ has basis $\{m_1, m_2, \ldots, m_n, n_1, n_2, \ldots, n_m\}$.

REMARK 3.9. A submodule of a free module is not necessarily free. Take for example $R = [X_1, \cdots, X_n, \cdots]$ and $I = \langle X_1, \cdots \rangle$. Then R is a free module over itself but I is not free as $R-$module.

Let's consider some examples of free modules:

EXAMPLE 3.10.

(1) **Free Abelian Groups:** The concept of a free module generalizes the notion of a free abelian group. Every abelian group can be viewed as a $\mathbb{Z}$-module, and a free abelian group is a free module over $\mathbb{Z}$.
(2) **Polynomial Rings:** Consider the polynomial ring $R[x]$ over a commutative ring R. The module $R[x]$ is a free module with basis $\{1, x, x^2, \ldots\}$. Any polynomial in $R[x]$ can be uniquely expressed as a linear combination of the powers of x with coefficients from R.
(3) **Free Vector Spaces:** Finite-dimensional vector spaces over a field are free modules. The concept of a basis for a vector space aligns with the notion of a basis for a free module.

3.1. Exact sequences. In this subsection, we will delve into the concepts of exact sequences and homological algebra. Exact sequences play a fundamental role in module theory, allowing us to study the interplay between modules and the maps between them. Homological algebra provides a powerful framework for analyzing the structure and properties of modules through the study of exact sequences.

An *exact sequence* is a sequence of module homomorphisms that captures the notion of "exactness" or "preservation of structure" between modules. Let M_i be modules over a commutative ring R. A sequence of modules

$$\cdots \to M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \to 0$$

is exact if for all i, we have $\mathrm{Im}(\varphi_i) = \mathrm{Ker}(\varphi_{i+1})$. A short sequence is a sequence of the form:

$$0 \to M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \to 0.$$

A short sequence is exact if and only if ϕ_1 is injective, ϕ_2 is surjective and $\mathrm{Im}(\varphi_1) = \mathrm{Ker}(\varphi_2)$,

where φ_1 and φ_2 are module homomorphisms. The exactness of the sequence is captured by the properties:

Exact sequences allow us to study the relationship between modules and understand how information is transferred between them through module homomorphisms.

4. Localization of Rings and Modules

In this section, we will explore the concept of localization of rings and modules. Localization allows us to extend the ring or module structure by introducing denominators and creating a localized version of the original structure. We will discuss the construction of localized rings and modules, properties of localization, and applications in various contexts.

Definition 4.1. A multiplicative subset of R is a subset S containing 1, stable under multiplication, and not containing 0.

Example 4.2.

(*i*) For any non-nilpotent $f \in R$, the set $\{f^n \mid n \in \mathbb{N}\}$ (with the convention $f^0 = 1$) is a multiplicative subset.

(*i*) If R is an integral domain, then $R \setminus \{0\}$ is a multiplicative subset. More generally, if P is a prime ideal, its complement $S = R \setminus P$ is a multiplicative subset.

Let M be an R-module. We want to construct an R-module $S^{-1}M$, consisting of "fractions" $\frac{m}{s}$ with $m \in M$, $s \in S$, such that the action of any $s \in S$ is invertible. Moreover, we require the usual rules of addition and multiplication of fractions to hold. In particular, for all $x, y \in M$ and $s, t, u \in S$, we must have:

$$(*) \quad u(tx - sy) = 0 \Rightarrow \frac{x}{s} - \frac{y}{t} = \frac{u(tx - sy)}{ust} = 0.$$

This leads to defining $S^{-1}M$ as follows. On the set $M \times S$, we consider the following relation:

$$(m, s) \sim (m', t) \iff \exists u \in S \text{ such that } u(tm - sm') = 0.$$

This relation is clearly reflexive and symmetric. It is also transitive. Indeed, if

$$(x, s) \sim (y, t) \sim (z, u),$$

then there exist $v, v' \in S$ such that $v(tx - sy) = 0 = v'(uy - tz)$. Then,

$$vv'utx = svv'uy = svv'tz,$$

which implies $vv't(ux - sz) = 0$, and since $tvv' \in S$ (as S is closed under multiplication), we conclude that $(x, s) \sim (z, u)$, proving that $\sim$ is an equivalence relation.

We denote by $S^{-1}M$ the set of equivalence classes and, for each $(m, s) \in M \times S$, we write $\frac{m}{s}$ for its image in $S^{-1}M$. We define addition in $S^{-1}M$ by:

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}.$$

To verify that this formula is well-defined, suppose that $\frac{x'}{s'}$ represents the same class as $\frac{x}{s}$ and show that:

$$(*) \quad \frac{tx'}{s't} + \frac{s'y}{s't} = \frac{tx + sy}{st}.$$

By hypothesis, there exists $u \in S$ such that $us'x = usx'$, hence:

$$u(st(tx' + s'y) - s't(tx + sy)) = t^2u(sx' - s'x) = 0.$$

Thus, equality $(*)$ holds. This shows that the right-hand side of (1) depends only on the class of $\frac{x}{s}$ and similarly only on the class of $\frac{y}{t}$. Therefore, addition is well-defined.

One can verify that this addition is associative and commutative, that $\frac{0}{1}$ is a zero element, and that $-\frac{m}{1}$ is the additive inverse of $\frac{m}{1}$. Thus, $S^{-1}M$ is an abelian group, and the map

$$\tau_M : M \to S^{-1}M, \quad m \mapsto \frac{m}{1}$$

is a group homomorphism.

Furthermore, when $M = R$, we define a multiplication on $S^{-1}R$ by:

$$\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st}.$$

Again, we need to verify that this formula makes sense, i.e., that if $\frac{x'}{s'}$ represents the same class as $\frac{x}{s}$, we have:

$$(**) \quad \frac{x'y}{s't} = \frac{xy}{st}.$$

By hypothesis, there exists $u \in S$ such that $us'x = usx'$, then

$$u(s'txy - stx'y) = tyu(s'x - sx') = 0,$$

which establishes $(**)$, proving that multiplication is well-defined. One can easily verify that this multiplication is associative, distributive over addition, and that $\frac{1}{1}$ is a multiplicative identity. Thus, $S^{-1}R$ is a ring, and the map

$$\tau_R : R \to S^{-1}R, \quad a \mapsto \frac{a}{1}$$

is a ring homomorphism.

Finally, for arbitrary M, we define a scalar multiplication of $S^{-1}R$ on $S^{-1}M$ by:

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}.$$

Following the same verifications as above, this defines an $S^{-1}R$-module structure on $S^{-1}M$. In particular, $S^{-1}M$ is an R-module via restriction of scalars through $\tau_R : R \to S^{-1}R$, meaning that for $a \in R$ and $m \in M$:

$$a \cdot \frac{m}{1} = \frac{am}{1}.$$

This shows that $\tau_M : M \to S^{-1}M$, $m \mapsto \frac{m}{1}$, is an R-module homomorphism. However, this homomorphism is not necessarily injective.

More precisely, from the construction, we have:

$$\ker \tau_M = \{m \in M \mid \exists s \in S \text{ such that } sm = 0\}.$$

THEOREM 4.3. *(1) $S^{-1}R$ is a ring, and $\tau_R : R \to S^{-1}R$, $a \mapsto \frac{a}{1}$, is a ring homomorphism with kernel:*

$$\ker \tau_R = \{a \in R \mid \exists s \in S \text{ such that } sa = 0\}.$$

(2) $S^{-1}M$ is an $S^{-1}R$-module, and $\tau_M : M \to S^{-1}M$, $m \mapsto \frac{m}{1}$, is an R-module homomorphism with kernel:

$$\ker \tau_M = \{m \in M \mid \exists s \in S \text{ such that } sm = 0\}.$$

The Integral Case. In the case where R is an integral domain, the construction of $S^{-1}R$ simplifies for two reasons.

First, the equivalence relation on $R \times S$ is defined more simply as:

$$(*) \quad (a, s) \sim (b, t) \iff at = bs.$$

Denoting $\frac{a}{s}$ as the image of (a, s) in the quotient set $S^{-1}R$, the ring structure is defined as before by:

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}, \quad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}.$$

(The fact that these formulas make sense follows from the general case, or can be verified directly by a similar, slightly simpler calculation.)

Second, the ring homomorphism $R \to S^{-1}R$, given by $a \mapsto \frac{a}{1}$, is injective. Indeed, if $\frac{a}{1} = 0 = \frac{0}{1}$, then by $(*)$ and the fact that R is an integral domain, we conclude that $a = 0$. Thus, in this case, we can consider R as a subring of $S^{-1}R$.

Moreover, since R is an integral domain, we can take as the multiplicative subset $S = R \setminus \{0\}$. In this case, the resulting ring $S^{-1}R$, which we denote by K, is a field. Indeed, every nonzero element of K is of the form as^{-1} with $a \neq 0$, so it has an inverse sa^{-1}. We call K the field of fractions of R.

Examples 4.7.

(1) $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

(2) Let k be a field and let $R = k[X]$ be the polynomial ring with coefficients in k. This is an integral domain because if P, Q are nonzero, then:

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Its field of fractions is the field of rational functions:

$$k(X) = \left\{ \frac{P(X)}{Q(X)} \mid P, Q \in k[X], Q \neq 0 \right\}.$$

The localization of a ring or module satisfies a universal property, which ensures the existence of unique homomorphisms that make computations with localized objects consistent and well-defined.

Let R be a ring, $S \subset R$ a multiplicative subset, and $S^{-1}R$ the localization of R at S. The ring $S^{-1}R$ satisfies the following universal property:

Given any ring R' and a ring homomorphism $\varphi : R \to R'$ such that $\varphi(s)$ is invertible in R' for all $s \in S$, there exists a unique ring homomorphism $\tilde{\varphi} : S^{-1}R \to R'$ such that the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ {\scriptstyle \tau_R}\downarrow & \nearrow_{\tilde{\varphi}} & \\ S^{-1}R & & \end{array}$$

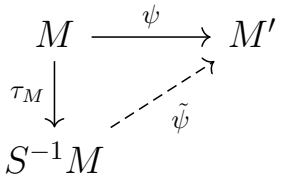
where $\tau_R : R \to S^{-1}R$ is the natural localization map given by $\tau_R(a) = \frac{a}{1}$. The homomorphism $\tilde{\varphi}$ is uniquely determined by the condition:

$$\tilde{\varphi}\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1}, \quad \forall a \in R, s \in S.$$

Similarly, for an R-module M, the localization $S^{-1}M$ satisfies the following universal property:

Given an $S^{-1}R$-module M' and an R-module homomorphism $\psi : M \to M'$ such that $\psi(s \cdot m)$ is invertible for all $s \in S$, there exists a unique $S^{-1}R$-module homomorphism $\tilde{\psi} : S^{-1}M \to M'$ making the

diagram commute:



where $\tau_M : M \to S^{-1}M$ is the canonical map given by $\tau_M(m) = \frac{m}{1}$. The homomorphism $\tilde{\psi}$ is uniquely determined by the condition:

$$\tilde{\psi}\left(\frac{m}{s}\right) = \psi(m)\psi(s)^{-1}, \quad \forall m \in M, s \in S.$$

These universal properties ensure that localization is a functorial construction and allow us to work with localized rings and modules in a well-defined and systematic way.

5. Primary Decomposition of Ideals

In this section, we will explore the concept of primary decomposition of ideals. Primary decomposition provides a way to break down an ideal into a finite intersection of primary ideals, revealing information about the structure of the original ideal. We will discuss the definition of primary ideals, the primary decomposition theorem, and related concepts.

Definition 5.1 (Primary Ideal). An ideal $Q \subseteq R$ in a ring R is called a **primary ideal** if whenever $ab \in Q$ for $a, b \in R$, then either $a \in Q$ or $b^n \in Q$ for some $n \in \mathbb{N}$.

Definition 5.2 (Associated Prime). Let Q be a primary ideal. The radical $\sqrt{Q}$ is a prime ideal, called the **associated prime** of Q.

Theorem 5.3. *Let R be a Noetherian ring and $I \subseteq R$ an ideal. Then I can be written as a finite intersection of primary ideals:*

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

where each Q_i is a primary ideal. Furthermore, the set of associated primes $\{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\}$ is uniquely determined (up to ordering) by the ideal I.

5.1. Remarks.

- The decomposition may not be unique, but the set of associated primes is unique.
- The decomposition is called **irredundant** if no Q_i can be omitted.
- If each Q_i corresponds to a distinct minimal prime over I, the decomposition is said to be **minimal**.

5.2. Example. Let $R = \mathbb{Z}$ and consider the ideal $I = (12)$. Then we can write:

$$(12) = (4) \cap (3)$$

where (4) is 2-primary and (3) is 3-primary. Note that $\sqrt{(4)} = (2)$ and $\sqrt{(3)} = (3)$ are prime ideals in $\mathbb{Z}$.

6. Noether Normalization Lemma

The Noether Normalization Lemma is a cornerstone result in commutative algebra and algebraic geometry. It states that every finitely generated algebra over a field can be made to look like a finite module over a polynomial ring. This is crucial for understanding the dimension theory of algebras and algebraic varieties.

6.1. Setup and Definitions.

Definition 6.1 (Finitely Generated k-Algebra). Let k be a field. A ring A is called a **finitely generated k-algebra** if there exist elements $a_1, \ldots, a_n \in A$ such that

$$A = k[a_1, \ldots, a_n],$$

i.e., A is generated as a k-algebra by finitely many elements.

Definition 6.2 (Integral Element). Let $A \subseteq B$ be rings. An element $b \in B$ is said to be **integral** over A if it satisfies a monic polynomial with coefficients in A, i.e., there exists a relation:

$$b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0 \quad \text{with } a_i \in A.$$

6.2. Statement of the Lemma.

THEOREM 6.3 (Noether Normalization Lemma). *Let k be a field and let $A = k[x_1, \ldots, x_n]/I$ be a finitely generated k-algebra. Then there exist algebraically independent elements $y_1, \ldots, y_d \in A$ such that:*

$$A \text{ is integral over } k[y_1, \ldots, y_d].$$

In other words, A is a finite module over the subring $k[y_1, \ldots, y_d]$, where $d = \dim A$.

This means that any affine k-algebra looks like a finite extension of a polynomial ring in d variables, where d is the Krull dimension of the algebra.

Let $A = k[x_1, \ldots, x_n]/I$. The main idea is:

(1) Choose a generic linear change of variables so that some subset of the variables become algebraically independent modulo I.
(2) Show that the other variables satisfy monic polynomial equations over the subring generated by the independent ones.

This uses the fact that polynomial rings over fields are Noetherian and techniques from elimination theory.

6.3. Example. Let $A = k[x, y]/(y^2 - x^3)$. This is the coordinate ring of the affine curve defined by $y^2 = x^3$.

- We can take $y_1 = x$. Then y satisfies the equation $y^2 = x^3$, so y is integral over $k[x]$.
- Hence, A is integral over $k[x]$, and $k[x] \subseteq A$ is a Noether normalization.
- The dimension of A is 1, as expected for a curve.

6.4. Geometric Interpretation. Geometrically, the Noether Normalization Lemma says that any affine variety of dimension d over a field k can be mapped dominantly and finitely onto affine d-space $\mathbb{A}^d_k$.

$$X = \mathrm{Spec}(A) \xrightarrow{\text{finite}} \mathbb{A}^d_k = \mathrm{Spec}(k[y_1, \ldots, y_d])$$
$$\searrow$$
$$\dim = d$$

This is an essential tool for reducing geometric and algebraic problems to those in affine space.

7. Structure Theorem for Finitely Generated Modules over PID

Let R be a principal ideal domain (PID) and M be a finitely generated R-module. The Structure Theorem for finitely generated modules over a PID gives a canonical form for such modules.

THEOREM 7.1. *Let A be a principal ideal domain.*

(1) Let $n \geq 1$ and N be a non-zero submodule of the free A-module A^n. Then, there exists a basis $(e_1, \ldots, e_n)$ of A^n, an integer $r \in \{1, \ldots, n\}$, and non-zero elements $a_1, \ldots, a_r \in A$ such that $a_i \mid a_{i+1}$ for $i = 1, \ldots, r-1$, and:

$$(a_1 e_1, \ldots, a_r e_r)$$

is a basis of N. In particular, r is the rank of N. Furthermore, the ideals $(a_r) \subseteq \cdots \subseteq (a_1)$ are uniquely determined by the submodule N. Finally, the submodule of A^n generated by $e_1, \ldots, e_r$ depends only on N and is equal to:

$$N' = \{x \in A^n \mid \exists a \in A \setminus \{0\} \text{ such that } ax \in N\}.$$

(2) Let M be a finitely generated A-module. Then, there exists an integer $s \geq 0$ and non-zero elements $a_1, \ldots, a_r \in A$ such that $a_i \mid a_{i+1}$ for $i = 1, \ldots, r-1$, such that:

$$M_{tors} = A/(a_1) \oplus A/(a_2) \oplus \cdots \oplus A/(a_r),$$
$$Ann(M_{tors}) = (a_r),$$
$$M \cong A^s \oplus M_{tors}, \quad \text{and} \quad A^s \cong M/M_{tors}.$$

*In particular, M is free if and only if M is torsion-free. Moreover, the ideals $(a_r) \subseteq \cdots \subseteq (a_1)$ are uniquely determined. These are called the *invariant ideals (or factors)* of M.*

(3) For a finitely generated torsion A-module M, the decomposition (1) above refines as follows. Let $Ann(M) = (p_1)^{m_1} \cdots (p_n)^{m_n}$ be the decomposition of $Ann(M)$ into a product of maximal ideals. Then, we have the primary decomposition:

$$M = \bigoplus_{i=1}^{n} M(p_i),$$

and, by point (2), each $M(p_i)$ decomposes as a direct sum:

$$M(p_i) = \bigoplus_{s=1}^{t_i} A/(p_i)^{n_s(p_i)},$$

where the sequence $1 \leq n_1(p_i) \leq \cdots \leq n_{t_i}(p_i)$ is uniquely determined. In particular, $n_{t_i}(p_i) = m_i$ and $Ann(M(p_i)) = (p_i^{m_i})$.

As a direct consequence of the Structure Theorem, we can deduce the following important corollary:

COROLLARY 7.2. *Any finitely generated torsion module over a PID is isomorphic to a direct sum of cyclic modules of the form $R/(d_i)$, where $d_i \in R$ and d_i divides d_{i+1} for each i.*

8. Exercises

EXERCISE 24. *Show that IM is an R-submodule of M.*

EXERCISE 25. *Let R be a non-zero commutative ring which is not a field. Give examples of the following:*

- *A free family of n elements in R^n that is not a basis.*
- *A minimal generating set that is not a basis.*
- *Submodules that do not have a complement.*
- *A free module with a submodule that is not free.*

EXERCISE 26. *Let R be a non-zero commutative ring. Provide examples for an R-modules that are not free, and show that if every R-module is free, then R is a field.*

EXERCISE 27. *Let R be a non-zero commutative ring.*

(1) *Let $f : R^r \to R^r$ be a linear map with matrix P in the canonical basis. Show that f is surjective if and only if $\det(P)$ is invertible in R, and that this is equivalent to f being bijective.*
(2) *Show that f is injective if and only if $\det(P)$ is non-zero and not a zero divisor in R.*

   ***Hint**: If $\det(P) = a$ is a zero divisor, fix a non-zero $b \in R$ such that $ab = 0$. Consider a maximal minor m of size s in P such that $mb \neq 0$. Then construct a non-zero column vector annihilated by P using minors of size s of P.*
(3) *Deduce that if $s > r$, a linear map $R^s \to R^r$ is not injective.*

Exercise 28. *Let R be a non-zero commutative ring.*

(1) *Show that if an R-module M is generated by a set of r elements, then any set containing more than r elements in M is linearly dependent.*
(2) *Let I be a non-principal ideal of R. Show that I is not a free R-module. More generally, prove that an ideal I of R is a free submodule of R if and only if I is principal and generated by a non-zero divisor of R.*

Exercise 29. *Let R be a ring, M an R-module of finite type, and $\varphi : M \to R^n$ a surjective morphism of R-modules.*

(1) *Show that φ admits a right inverse (i.e., there exists $\psi : R^n \to M$ such that $\varphi \circ \psi = \mathrm{id}_{R^n}$).*
(2) *Show that $M \cong \ker(\varphi) \oplus \mathrm{Im}(\psi)$.*
(3) *Show that $\ker(\varphi)$ is of finite type.*

Exercise 30. *Let k be a field, $P \in k[X]$, and $R = k[X]/(P)$.*

(1) *What is the dimension of R as a k-vector space? Provide a basis.*
(2) *Define $M = \mathrm{Hom}_k(R, k)$; provide a basis for M.*
(3) *For $f \in R$ and $u \in M$, define $f \cdot u \in M$ by*

$$(f \cdot u)(g) = u(f \cdot g)$$

   for all $g \in R$. Show that this operation equips M with the structure of a free R-module of rank 1. Provide a basis.

EXERCISE 31. ***Nakayama's Lemma.*** *This exercise is related to Exercises 11 and 12 from the tutorial sheet III on rings.*

(1) *Let M be an R-module of finite type, and I an ideal of R. Suppose $M = IM$. Show that there exists $a \in I$ such that $(1-a)M = 0$.* ***Hint****: Choose a as the determinant of a matrix.*
(2) *Deduce that if R is local, $I = M$, its maximal ideal, and $M = IM$, then $M = 0$.*
(3) *Let $J(R)$ denote the Jacobson radical of R (i.e., the intersection of all its maximal ideals). Show that if $J(R)M = M$, then $M = 0$.*
(4) *Let R be a ring and I a finitely generated ideal of R such that $I^2 = I$. Show that there exists $e \in R$ such that $e^2 = e$ and $I = (e)$. Such an element e is called an idempotent of R.*

CHAPTER 3

Solution

Let I be a prime ideal of A, and assume that $I \neq 0$. Since A is a principal ideal domain, there exists an element $a \in A$ such that $I = \langle a \rangle$. Since $I \neq 0$, we have $a \neq 0$. We will now show that a is irreducible. Since I is a prime ideal, a cannot be a unit. Let b and c be elements of A such that $a = bc$. Because I is prime, either $b \in I$ or $c \in I$. Suppose $b \in I$; then, there exists some element $d \in A$ such that $b = ad$, which implies $a = adc$. Simplifying by a, we get $dc = 1$, showing that c is a unit. Similarly, if $c \in I$, then b is a unit. Therefore, a is irreducible, as claimed.

Conversely, let a be an irreducible element of A, and let us show that the ideal $I = \langle a \rangle$ is a maximal ideal in A. Let $g \in A$ be an element that is not a multiple of a, and let $J = I + \langle g \rangle$. Let $b \in A$ be such that $J = \langle b \rangle$. Since $a \in J$, there exists some element $c \in A$ such that $a = bc$. If c were a unit, then $\langle a \rangle = \langle b \rangle = I + \langle g \rangle$, implying $g \in \langle a \rangle$, which contradicts the assumption. Since a is irreducible, it follows that b is a unit, and thus $J = A$. This shows that I is a maximal ideal in A.

Bibliography

[Ati69] Ian G. Atiyah, Michael; Macdonald. *Introduction to Commutative Algebra*. CRC Press, 1969.

[Bou89] Nicolas Bourbaki. *Commutative algebra*. Elements of Mathematics. Springer, 1989.

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, 1995.

[Mat89] Hideyuki Matsumura. *Commutative algebra*. Mathematics Lecture Note Series, 1989.