FINAL PROJECT - COMMUTATIVE ALGEBRA

Introduction

Commutative algebra is an important area of mathematics that studies commutative rings, ideals, and their properties. It plays a key role in fields like algebraic geometry and number theory.

This project focuses on key concepts such as Hilbert's Nullstellensatz, ideal theory, and the structure of Noetherian rings. By solving theoretical and practical problems, we aim to understand how these concepts are applied and why they are important in mathematics.

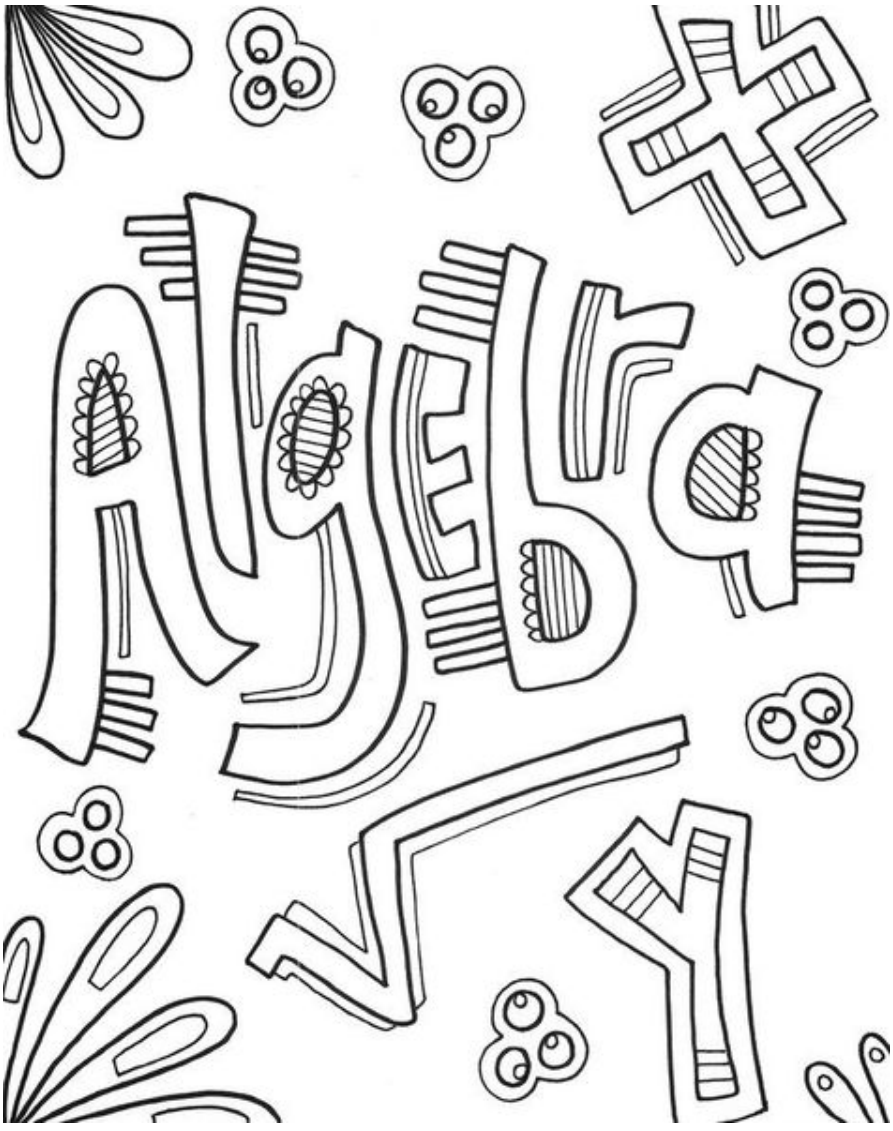
Contents

1 Hilbert's Nullstelensatz **2**

2 Theoretical Problems **3**

3 General Problems **8**

4 Individual Problems **10**



1 Hilbert's Nullstelensatz

Theorem 1. *Every maximal ideal of* $\mathbb{C}[x_1, \ldots, x_n]$ *is of the form* m_α *for some* $\alpha = (\alpha_1, \ldots, \alpha_n)$.

In the name of the theorem (in German), "null" means zero, "stellen" means place, and "satz" means theorem.
This immediately implies the following corollary (since maximal ideals in $\mathbb{C}[x_1, \ldots, x_n]/(P_1, \ldots, P_m)$ are in correspondence with maximal ideals in $\mathbb{C}[x_1, \ldots, x_n]$ containing all the P_i):

Corollary 1. *The maximal ideals in* $R = \mathbb{C}[x_1, \ldots, x_n]/(P_1, \ldots, P_m)$ *are in bijection with the common zeroes of the polynomials* P_i.

Proof of theorem. Let $m \subset \mathbb{C}[x_1, \ldots, x_n]$ be a maximal ideal; then $F = \mathbb{C}[x_1, \ldots, x_n]/m$ is a field. This gives a homomorphism from $\mathbb{C}$ to F — taking the quotient by m gives a homomorphism from $\mathbb{C}[x_1, \ldots, x_n]$ to F, and we can restrict the homomorphism to $\mathbb{C}$. It suffices to show that this map $\mathbb{C} \to F$ is an isomorphism — then the original homomorphism $\mathbb{C}[x_1, \ldots, x_n] \to F$ from taking the quotient must map $\mathbb{C}$ isomorphically to F, and we can suppose it maps $x_i \to \alpha_i$ for each i where $\alpha_i \in \mathbb{C}$ (it really maps x_i to some element of F, but F is isomorphic to $\mathbb{C}$). Then it's clear that the kernel of this homomorphism is generated by $x_1 - \alpha_1, \ldots, x_n - \alpha_n$; therefore this kernel is m_α where $\alpha = (\alpha_1, \ldots, \alpha_n)$, and we have $m = m_\alpha$. So now we want to show that the map $\mathbb{C} \to F$ is bijective.

But any homomorphism between fields is injective — the kernel of the homomorphism must be an ideal, but the only ideals of a field are $\{0\}$ and the entire field. Since the homomorphism cannot map 1 to 0, the kernel cannot be the entire field, so must be $\{0\}$.

Therefore it suffices to show that the homomorphism is surjective. Assume not. Then F strictly contains $\mathbb{C}$ (since we have an injective map $\mathbb{C} \to F$, so $\mathbb{C}$ is isomorphic to its image), so we can pick $z \in F$ with $z \notin \mathbb{C}$. Then consider the elements

$$\frac{1}{z - \lambda} \quad \text{for} \quad \lambda \in \mathbb{C}.$$

Now we'll use a bit of set theory — $\mathbb{C}[x_1, \ldots, x_n]$ is a countable union of finite-dimensional vector spaces $U_1 \subset U_2 \subset \ldots$ over $\mathbb{C}$, where U_i is the vector space of polynomials with degree at most i. Then since F is a quotient of $\mathbb{C}[x_1, \ldots, x_n]$, it must also be a countable union of finite-dimensional vector spaces $V_1 \subset V_2 \subset \ldots$, where V_i is simply the image of U_i in this quotient.

On the other hand, $\mathbb{C}$ is not countable, so there are uncountably many terms $\frac{1}{z-\lambda}$. Since all such terms are elements of F, one of the finite-dimensional vector spaces that F consists of must contain infinitely many of them.

But then since these terms all belong to the same finite-dimensional vector space, and there are infinitely many of them, we can find a finite set which is linearly dependent — so then we have an identity

$$\sum a_i \frac{1}{z - \lambda_i} = 0,$$

where $a_i \in \mathbb{C}$ for all i and there are finitely many terms. But by clearing denominators, we can translate this into a polynomial relation in z — we then have $P(z) = 0$ for some $P \in \mathbb{C}[x]$. Then since all polynomials over $\mathbb{C}$ factor, we can write

$$P(x) = c \prod (x - r_i),$$

for some $r_i \in \mathbb{C}$. But $z \notin \mathbb{C}$, so z cannot equal any of the r_i, contradiction (as F is a field, so the product of nonzero terms cannot be zero).

Hence the map $\mathbb{C} \to F$ must be an isomorphism, as desired. □

2 Theoretical Problems

Problem 1. Describe how to construct the quotient ring R/I and provide an example illustrating the quotient ring R/I.

Solution
Let R be a ring and I be an ideal of R. Consider the equivalence relation on R

$$a \sim b \iff a - b \in I.$$

Take $a, b, c \in R$. Then:

- $a - a = 0 \in I \iff a \sim a$, which implies that $\sim$ is reflexive.
- $a \sim b \iff a - b \in I \iff b - a = -(a - b) \in I \iff b \sim a$. This implies that $\sim$ is symmetric.
- Assume $a \sim b$ and $b \sim c$, meaning $a - b \in I$ and $b - c \in I$. Then $a - c = (a - b) + (b - c) \in I$. Thus, $a \sim c$, so $\sim$ is transitive.

Therefore, $\sim$ is an equivalence relation on R. This relation partitions R into equivalence classes of the form

$$[a] = \{r \in R \mid r - a \in I\}.$$

The equivalence class $[a]$ is also denoted as $a + I$ or $\bar{a}$.
On the set of equivalence classes R/I, we define addition and multiplication as follows:

- Addition: $(a + I) + (b + I) = (a + b) + I$.
- Multiplication: $(a + I)(b + I) = ab + I$.
- Identity element: $1 + I$.
- Zero element: $0 + I = I$.

The set R/I with these two operations forms a ring, called the quotient ring of R by I.

Example. Consider a specific case of *Example 2.10* [Sha00], where $n = 3$. Let $R = \mathbb{Z}$ be the ring of integers, and $I = 3\mathbb{Z}$ be the ideal of multiples of 3. The equivalence classes in $\mathbb{Z}/3\mathbb{Z}$ are

- $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.
- $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$.
- $[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Consider the operations

- Addition: $[1] + [2] = [3] = [0]$.
- Multiplication: $[2] \cdot [2] = [4] = [1]$.

Thus, $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$ is a quotient ring of $\mathbb{Z}$ by $3\mathbb{Z}$. This is the ring of equivalence classes modulo 3 in $\mathbb{Z}$.

Problem 2. Provide the definition and properties of a type of ideal that you know (e.g., finitely generated ideal, principal ideal, prime ideal, maximal ideal, primary ideal, etc.). What is the meaning of this type of ideal?

Solution. In this problem, we will state the definition, some properties, and the meaning of a **primary ideal**. However, We only present several properties of **primary ideal** in the form of propositions, lemmas, and theorems. Among these, we provide proofs for a few representative properties, while others are stated without proof.

Definition 1. *A primary ideal of ring R is a proper ideal of R such that if $ab \in I$ then $x \in I$ or $y \in \sqrt{I}$.*

From this definition, we easily to show that *A prime ideal is primary*.

Proposition 1. *The power of a maximal ideal J is a J-primary ideal.*

Proof. Since J is a maximal ideal then it is a prime ideal, we have $\sqrt{J^n} = J$. As J is a maximal ideal, it follows that J^n is a J-primary ideal. □

Proposition 2. *If I is a primary ideal of the ring R, then $\sqrt{I}$ is the smallest prime ideal containing I.*

Proof. We prove that $\sqrt{I}$ is a prime ideal. Let $xy \in \sqrt{I}$. Then there exists some m such that $(xy)^m \in I$. Thus, either $x^m \in I$ or $y^{mn} = (y^m)^n \in I$ (for some $n \in \mathbb{N}^*$), which implies that either $x \in \sqrt{I}$ or $y \in \sqrt{I}$. Therefore, $\sqrt{I}$ is a prime ideal. Furthermore, since $\sqrt{I}$ is the intersection of all the prime ideals containing I, we conclude the proof. □

Proposition 3. *The intersection of a finite collection of primary ideals is a primary ideal.*

Proof. Let P be a prime ideal of R. Let $Q_1, \ldots, Q_n$ be P-primary ideals of R. In *2.30*, we have:

$$\sqrt{(Q_1 \cap \ldots \cap Q_n)} = \sqrt{Q_1} \cap \ldots \cap \sqrt{Q_n} = P \subset R$$

It is clear that $\bigcap_{i=1}^n Q_i$ is a proper ideal of R. Suppose $a, b \in R$ such that $ab \in \bigcap_{i=1}^n Q_i$ but $b \notin \bigcap_{i=1}^n Q_i$. Then, there exists an index j with $1 \leq j \leq n$ such that $b \notin Q_j$. Since $ab \in Q_j$ and Q_j is P-primary, we conclude that $a \in P = \sqrt{(Q_1 \cap \ldots \cap Q_n)}$. Therefore, $\bigcap_{i=1}^n Q_i$ is P-primary. □

Lemma 1. *Let R be a commutative ring and I be an ideal of R. Then, I is a primary ideal if and only if R/I is not trivial and every non-zero divisor of R/I is nilpotent.*

Proof. ($\Rightarrow$) Suppose I is a primary ideal. Then, since I is a proper ideal of R, it follows that R/I is not trivial. Let $b \in R$ such that $b + I$ is a non-zero divisor of R/I. Then, there exists $a \in R$ such that $a + I \neq I$ and $(a + I)(b + I) = I$, implying $ab + I = I$, or $ab \in I$. Since $a \notin I$ and I is a primary ideal, there exists $n \in \mathbb{N}$ such that $b^n \in I$, implying that $(b + I)^n = b^n + I = I$, so $b + I$ is nilpotent.
($\Leftarrow$) Conversely, assume that R/I is not trivial and every non-zero divisor of R/I is nilpotent. Since $R/I \neq 0$, I is a proper ideal of R. Let $a, b \in R$ such that $ab \in I$ and $a \notin I$. Then, $(a + I)(b + I) = I$ with $(a + I) \neq I$. Therefore, $b + I$ is a non-zero divisor of R/I, so there exists $n \in \mathbb{N}$ such that $(b + I)^n = I$, implying $b^n \in I$. Thus, I is a primary ideal. □

Theorem 2. *Let Q be a P-primary ideal of the commutative ring R, and let $a \in R$.*
(i) If $a \in Q$, then $(Q : a) = R$.
(ii) If $a \notin Q$, then $(Q : a)$ is P-primary, so that, in particular, $\sqrt{(Q : a)} = P$.
(iii) If $a \notin P$, then $(Q : a) = Q$.

The special property of primary ideal is that every proper ideal can be decomposed into an intersection of primary ideals. We consider some definitions and theorems.

Definition 2. *Let I be a proper ideal of the commutative ring R. A primary decomposition of I is an expression for I as an intersection of finitely many primary ideals of R. Such a primary decomposition*

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

with $Q_i = P_i$ for $i = 1, \ldots, n$ of I is said to be a minimal primary decomposition of I precisely when:

1. *$P_1, \ldots, P_n$ are n different prime ideals of R;*
2. *For all $j = 1, \ldots, n$, we have:*

$$Q_j \not\supseteq \bigcup_{j \neq i} Q_i.$$

We say that I is a decomposable ideal of R precisely when it has a primary decomposition.

Theorem 3. *Let I be a decomposable ideal of the commutative ring R, and let*

$$I = Q_1 \cap \cdots \cap Q_n \quad \text{with} \quad Q_i = P_i \text{ for } i = 1, \ldots, n$$

be a minimal primary decomposition of I. Let $P \in Spec(R)$. Then the following statements are equivalent:

1. *$P = P_i$ for some i with $1 \leq i \leq n$;*
2. *There exists $a \in R$ such that $(I : a)$ is P-primary;*
3. *There exists $a \in R$ such that $\sqrt{(I : a)} = P$.*

Corollary 2. *Let I be a decomposable ideal of the commutative ring R, and let*

$$I = Q_1 \cap \cdots \cap Q_n \quad \text{with} \quad \sqrt{Q_i} = P_i \text{ for } i = 1, \ldots, n,$$

and

$$I = Q'_1 \cap \cdots \cap Q'_{n'} \quad \text{with} \quad \sqrt{Q'_i} = P'_i \text{ for } i = 1, \ldots, n'$$

be two minimal primary decompositions of I. Then $n = n'$, and

$$\{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_n\}.$$

Theorem 4. *Let I be a decomposable ideal of the commutative ring R. Suppose*

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

where $Q_i = P_i$, for all $i = 1, \ldots, n$, and

$$I = Q'_1 \cap \cdots \cap Q'_{n'},$$

where $Q'_i = P'_i$, for all $i = 1, \ldots, n'$, are two minimal primary decompositions of I. Then $n = n'$ and

$$\{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_{n'}\}.$$

Proposition 4. *Let R be a commutative Noetherian ring and let I be an irreducible of R. Then I is a primary.*

Corollary 3. *Let I be a proper ideal in the commutative Noetherian ring R. Then I has a primary decomposition, and it also has a minimal primary decomposition.*

The meaning of a primary ideal: Primary ideals allow any ideal in a commutative ring to be expressed as the intersection of primary ideals, generalizing the concept of unique factorization from Euclidean domains and principal ideal domains to Noetherian rings. They are closely connected to maximal ideals through the radical of the ideal and have important applications in algebraic geometry, helping to decompose algebraic sets into fundamental components.

Problem 3. Introduce the basic properties of a Noetherian ring.

Note: We present several properties of **Noetherian ring** in the form of propositions, lemmas, and theorems. Among these, we provide proofs for a few representative properties, while others are stated without proof.

Theorem 5. *Let R be a commutative ring with identity element. The following are equivalent:*

i) R is a Noetherian ring.
ii) Every non-empty collection of ideals of R has a maximal element.
iii) Every ideal of R is finitely generated.

Proof
$(i \Rightarrow ii)$ Suppose $\Delta = \{I_\alpha\}_{\alpha\in\Gamma}$ is a non-empty collection of ideals of R, and Δ has no maximal element. Take $I_1 \in R$. Since Δ has no maximal element, there exists $I_2 \in \Delta$ such that $I_1 \subset I_2$. Similarly, there exists I_3 such that $I_1 \subset I_2 \subset I_3$. Continuing in this way, we obtain an infinite chain of ideals $I_1 \subset I_2 \subset I_3 \subset \ldots$, which contradicts the assumption that R is Noetherian.
$(ii \Rightarrow iii)$ Let I be any ideal of R, and let Δ be the set of all finitely generated ideals of R contained in I. By (ii), there exists a maximal element $J \in \Delta$. Take $a \in I$, we have $J \subseteq J + \langle a\rangle \in \Delta$. Since J is maximal in Δ, either $J + \langle a\rangle = J$ or $J + \langle a\rangle = I$. If $J + \langle a\rangle = I$, then since J is finitely generated, I is finitely generated. If $J + \langle a\rangle = J$, then $a \in J$, so $I = J$, implying that I is finitely generated. In both cases, I is finitely generated.
$(iii \Rightarrow i)$ Suppose every ideal of R is finitely generated. Consider an increasing chain of ideals of R, $I_1 \subseteq I_2 \subseteq \ldots$. Let $I = \bigcup_{n=1}^{\infty} I_n$. By assumption, I is finitely generated, so $I = \langle a_1, a_2, \ldots, a_m\rangle$. Since $a_i \in I$, there exists n_i such that $a_i \in I_{n_i}$. Let $n = \max\{n_1, \ldots, n_m\}$. Then $a_i \in I_n$ for all i, so $I \subseteq I_n$. Therefore, $I = I_n$, and the chain stops at I_n. □

Theorem 6. *Let R and R' be commutative rings, and let $f : R \to R'$ be a ring homomorphism. If R is Noetherian, then R' is also Noetherian. In particular, if I is an ideal of R and R is Noetherian, then R/I is also a Noetherian commutative ring.*

Proof. By the Isomorphism Theorem for commutative rings (*Proposition 2.13* [Sha00]), we have

$$R/\operatorname{Ker} f \cong R'.$$

By *Proposition 2.46* [Sha00], if two commutative rings are isomorphic, then one ring is Noetherian if and only if the other is Noetherian. Therefore, to prove the second statement, it suffices to show that R/I is Noetherian for every ideal I of R, when R is Noetherian.
Suppose R is Noetherian. We will prove that R/I is Noetherian.

By *Propositions 2.37* and *2.39* [Sha00], an increasing sequence of ideals in R/I has the form

$$\overline{I_1} \subseteq \overline{I_2} \subseteq \cdots \subseteq \overline{I_n} \subseteq \cdots,$$

where $\overline{I_k} = I_k/I$, and $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is an increasing sequence of ideals of R, all containing I. Since R is Noetherian, there exists $k \in \mathbb{N}$ such that $I_k = I_{k+1}$ for all $k \geq K$. Therefore,

$$I_k/I = I_{k+1}/I \quad \forall k \geq K.$$

Hence, the increasing chain of ideals in R/I stops. Thus, R/I is Noetherian. □

Theorem 7. *Let R be a Noetherian commutative ring and S a multiplicatively closed subset of R. Then the localization of R at S, denoted $S^{-1}R$, is also Noetherian.*

Proof. Suppose there is an increasing chain of ideals in $S^{-1}R$:

$$J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n \subseteq \cdots$$

Using the expansion and contraction notation from *Propositions 2.41* and *Proposition 2.45* [Sha00] with the natural ring homomorphism $\varphi : R \to S^{-1}R$, we have:

$$J_1^c \subseteq J_2^c \subseteq \cdots \subseteq J_n^c \subseteq \cdots$$

which is an increasing chain of ideals in R.
Since R is Noetherian, there exists $k \in \mathbb{N}$ such that $J_k^c = J_{k+1}^c$ for all $k \geq K$. Therefore,

$$J_k = J_{k+1} \quad \forall k \geq K.$$

Furthermore, by *Proposition 5.24* [Sha00], we have $J_k^e = J_k$ for all k. Thus, the increasing chain of ideals in $S^{-1}R$ also stops. Therefore, $S^{-1}R$ is Noetherian. □

Theorem 8. *Let R and R' be commutative rings, and $f : R \to R'$ a ring homomorphism. Suppose that R is Noetherian and that R', viewed as an R-module via f, is finitely generated. Then R' is a Noetherian ring.*

Proof. By *Proposition 7.22* [Sha00], R' is a Noetherian R-module. Moreover, each ideal of R' is automatically a submodule of R' over R. Therefore, since R' satisfies the ascending chain condition for submodules, it also satisfies the ascending chain condition for ideals. Thus, R' is a Noetherian ring. □

Theorem 9. *(I. S. Cohen) Let R be a commutative ring such that every prime ideal of R is finitely generated. Then R is a Noetherian ring.*

Proof. Suppose for contradiction that R is not Noetherian. We define

$$\mathcal{Q} := \{I \mid I \text{ is an ideal of } R \text{ and } I \text{ is not finitely generated}\}.$$

By assumption, for every prime ideal P of R, the ideal P is finitely generated. Since R is not Noetherian, it has an ideal which is not finitely generated, so the collection $\mathcal{Q}$ is non-empty. Using Zorn's Lemma, there exists a maximal element $I \in \mathcal{Q}$. Then I is a proper ideal of R, which is not finitely generated. Since every prime ideal of R is finitely generated, it follows that I is contained in a prime ideal P. However, this contradicts the assumption that I is maximal in $\mathcal{Q}$. Therefore, R must be Noetherian. □

Theorem 10. *(Hilbert's Basis Theorem) If R is a commutative Noetherian ring, then the polynomial ring $R[x]$ is also a commutative Noetherian ring.*

Proof. Let A be an ideal of $R[x]$. If $A = 0$, then it is trivially finitely generated. If $A \neq 0$, define $I_n = \{a \in R \mid f(x) \in A, \deg f = n, \mathrm{lc}(f) = a\} \cup \{0\}$, where $\mathrm{lc}(f)$ denotes the leading coefficient of $f(x)$. It follows that I_n is an ideal of R.

Since $\mathrm{lc}(f) = \mathrm{lc}(xf)$, we have $I_n \subseteq I_{n+1}$. Define $J = \bigcup_{n=0}^{\infty} I_n$. Then J is an ideal of R, and since R is Noetherian, J is finitely generated. Assume $J = \langle a_1, \ldots, a_k \rangle$. By construction of J, there exists $n \in \mathbb{N}$ such that $a_1, \ldots, a_k \in I_n$. Therefore, $J \subseteq I_n$. Since $I_n \subseteq J$, we conclude that $J = I_n$.

For each m, suppose $I_m = \langle a_{m1}, \ldots, a_{mk_m} \rangle$, and for each j, choose $f_{mj}(x) \in A$ such that $\mathrm{lc}(f_{mj}) = a_{mj}$. Let $\bar{A} = \langle f_{mj}(x) \mid 0 \leq m \leq n, 1 \leq j \leq k_m \rangle$. We claim that $A = \bar{A}$.

Let $f(x) \in A$ and set $r = \deg f$. We prove $f(x) \in \bar{A}$ by induction on r:

- If $r = 0$ or $r = -\infty$, then clearly $f(x) \in \bar{A}$.
- If $0 < r < n$, then $\mathrm{lc}(f) \in I_r$, so we can write $\mathrm{lc}(f) = c_1 a_{r1} + \ldots + c_{k_r} a_{rk_r}$. Hence, $\mathrm{lc}(f) = \mathrm{lc}\left(\sum c_i f_{ri}\right)$, and $\deg\left(f - \sum c_i f_{ri}\right) < r$. By induction, $f(x) - \sum c_i f_{ri}(x) \in \bar{A}$, so $f(x) \in \bar{A}$.
- If $r \geq n$, then $\mathrm{lc}(f) \in I_r = I_n$, so $\mathrm{lc}(f) = c_1 a_{n1} + \ldots + c_{k_n} a_{nk_n}$. Similarly, $\deg\left(f - \sum c_i x^{r-n} f_{ni}\right) < r$, which implies $f(x) \in \bar{A}$ by induction.

Therefore, $A \subseteq \bar{A}$. Clearly, $\bar{A} \subseteq A$, so $A = \bar{A}$, meaning A is finitely generated. Apply *Theorem 5 - (iii)*, $R[x]$ is a Noetherian ring. □

Corollary 4. *If R is a commutative Noetherian ring, then the polynomial ring $R[x_1, \ldots, x_n]$ is also a commutative Noetherian ring.*

Proof. Write $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. By induction on n, the result follows immediately. □

Similarly, we have this theorem.

Theorem 11. *Let R be a commutative Noetherian ring. Then the ring $R[[X]]$ of formal power series in the indetermitate X with coefficients in R is again Noetherian.*

Corollary 5. *Let R be a commutative Noetherian ring. Then the ring $R[[X_1, \ldots, X_n]]$ of formal power series in n indeterminaties $X_1, \ldots, X_n$ with coefficients in R is again Noetherian.*

Theorem 12. *Let I be and ideal of the commutative Noetherian ring R, and let $J = \bigcap_{n=1}^{\infty} I^n$. Then $J = IJ$.*

Theorem 13. *(Nakayama's Lemma) Let M be a finitely generated module over the commutative ring R, and let I be an ideal of R such that $I \subseteq Jac(R)$, the Jacobson radical of R. Assume that $M = IM$. Then $M = 0$.*

Corollary 6. *(Krull's Intersection Theorem) Let I be an ideal of the commutative Noetherian ring R such that $J \subseteq Jac(R)$. Then $\bigcap_{i=1}^{\infty} I^n = 0$.*

3 General Problems

Problem 1. Let R be a commutative ring with identity element. Prove that:
(a) If P is a prime ideal of R, then $\sqrt{P} = P$.
(b) For ideals I and J of R, we have $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Lemma 2. *If P is a prime ideal of the ring R, then $\sqrt{P^n} = P$ for all $n > 0$.*

Proof. Let $x \in \sqrt{P^n}$. Then, there exists $k > 0$ such that $x^k \in P^n$. Thus, $x \in P$ or $x^k \in P$. Repeating this process at most k times, we conclude that $x \in P$. Therefore, $\sqrt{P^n} \subseteq P$. Conversely, any power of an element in P that lies in P^n implies $P \subseteq \sqrt{P^n}$. Hence, $\sqrt{P^n} = P$. □

Proof of Problem 1.

(a) The inclusion $\supseteq$ is obvious. We now prove the reverse inclusion. Let $x \in \sqrt{P}$. Then there exists an $n \in \mathbb{N}$ such that $x^n \in P$. Sine P is a prime ideal, we have $x \in P$ or $x^n \in P$. Repeating this process $n-1$ times, we conclude that $x \in P$. Hence, $\sqrt{P} \subseteq P$. Combining both inclusions, we obtain the desired result. Moreover, by applying *Lemma 2*, we can directly conclude this result. □

(b) Let $x \in \sqrt{IJ}$. Then there exists an $n \in \mathbb{N}$ such that $x^n \in IJ$. Since $x^n \in IJ$, we have $x^n \in I \cap J$. Therefore, $x \in \sqrt{I \cap J}$. Hence, $\sqrt{IJ} \subseteq \sqrt{I \cap J}$.
Let $x \in \sqrt{I \cap J}$. Then there exist $n \in \mathbb{N}$ such that $x^n \in I \cap J$, meaning that $x^n \in I$ and $x^n \in J$. Thus, $x \in \sqrt{I}$ and $x \in \sqrt{J}$. Therefore, $x \in \sqrt{I} \cap \sqrt{J}$. Hence, $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$.
Let $x \in \sqrt{I} \cap \sqrt{J}$. Then there exist $m, n \in \mathbb{N}$ such that $x^m \in I$ and $x^n \in J$. Therefore, $x^{mn} \in IJ$. We deduce that $x \in \sqrt{IJ}$. Hence, $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$.
From $\sqrt{IJ} \subseteq \sqrt{I \cap J}$, $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$, and $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$, we obtain the desired result. □

Problem 2. Let $M_1, \ldots, M_n$ be distinct maximal ideals of a commutative ring R with identity element. Define

$$S = R \setminus (M_1 \cup \cdots \cup M_n).$$

Prove that:
(a) S is a multiplicative subset of R.
(b) The ring of fractions $S^{-1}R$ has exactly n maximal ideals, namely $S^{-1}M_1, \ldots, S^{-1}M_n$.

Proof.

(a) For $i = \overline{1,n}$, M_i is a maximal ideal of R, so M_i is also a prime ideal of R and $M_i \subsetneq R$. Notice that if $1 \in M_i$, then $M_i = R$ because for all $r \in R$, we have $r = 1 \cdot r \in M_i$, which is a contradiction. Therefore, $1 \notin M_i$ for all $i = \overline{1,n}$, or equivalently $1 \notin M_1 \cup \cdots \cup M_n$, which implies that $1 \in S$. Let $x, y \in S$, i.e., $x, y \notin M_1 \cup \cdots \cup M_n$, or $x, y \notin M_i$ for all $i = \overline{1,n}$. Since M_i are prime ideals, we have $xy \notin M_i$ for all $i = \overline{1,n}$, meaning $xy \notin M_1 \cup \cdots \cup M_n$. Thus, $xy \in S$. Therefore, S is a multiplicative subset of R. □

(b) It is easy to check that for all $i = \overline{1,n}$, $S^{-1}M_i$ is an ideal of $S^{-1}R$. Moreover, $S^{-1}M_i$ is a maximal ideal of $S^{-1}R$. Indeed, since M_i is maximal in R, R/M_i is a field. Consider the natural homomorphism

$$\varphi : R \to S^{-1}R, \quad r \mapsto \frac{r}{1}.$$

Then for every $i = \overline{1,n}$, $\varphi(M_i) = S^{-1}M_i$, and $(S^{-1}R)/(S^{-1}M_i) \cong R/M_i$. Since R/M_i is a field, $(S^{-1}R)/(S^{-1}M_i)$ is also a field, implying that $S^{-1}M_i$ is a maximal ideal of $S^{-1}R$. We note that the

map from R to $S^{-1}R$ preserves maximality. Next, assume there are more than n maximal ideals in $S^{-1}R$. Let J be a maximal ideal of $S^{-1}R$ such that $J \notin \{S^{-1}M_1, \ldots, S^{-1}M_n\}$. Then there exists a maximal ideal I of R such that $J = S^{-1}I$. Suppose $I \in \{M_1, \ldots, M_n\}$, then $I = S^{-1}M_i$ for some i, which contradicts our assumption. Therefore, $I \notin \{M_1, \ldots, M_n\}$, meaning $I \cap S \neq \emptyset$. Applying *Theorem 5.32 - (i)* [Sha00], we deduce that $J = S^{-1}R$. This leads to a contradiction. Hence, $S^{-1}R$ has exactly n maximal ideals: $S^{-1}M_1, \ldots, S^{-1}M_n$. □

Problem 3. Consider the integer ring $\mathbb{Z}$. Find all the primary ideals of $\mathbb{Z}$. From that, indicate a minimal primary factorization of the ideal $n\mathbb{Z}$, with $n > 1$.

Proof. Notice that $\mathbb{Z}$ is a PID, so according to *Example 4.10* [Sha00], we immediately conclude that all primary ideals of $\mathbb{Z}$ are $0 \cup \{p^n\mathbb{Z} \mid n \in \mathbb{N}, p \text{ is a prime number}\}$. Indeed, let's check this result. Clearly, 0 is a primary ideal of $\mathbb{Z}$. Naturally, for a prime p and $n \in \mathbb{N}$, we also easily see that $\sqrt{p^n\mathbb{Z}} = p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$, and by *Proposition 4.9* [Sha00], $p^n\mathbb{Z}$ is a primary ideal of $\mathbb{Z}$. Now consider P to be a proper ideal of $\mathbb{Z}$. Then, $P = m\mathbb{Z}$ for some $m \in \mathbb{Z}^+$ and $m \neq 1$, since $P \neq \mathbb{Z}$. Thus, there exists a prime number p, an integer q, and an index $i \geq 1$ such that $p \nmid q$. However, $p + m\mathbb{Z}$ is not a divisor of $\mathbb{Z}/m\mathbb{Z}$, and $p + m\mathbb{Z}$ is not primary. By *Lemma 1*, P is not a primary ideal. Therefore, the primary ideals of $\mathbb{Z}$ are only 0 and $p^n\mathbb{Z}$.

Write n as the product of prime powers, i.e., $n = p_1^{k_1}p_2^{k_2}\ldots p_n^{k_n}$, with $k_i \in \mathbb{N}^*$, for all $i = \overline{1,n}$. As mentioned above, $p^{k_i}\mathbb{Z}$ is a primary ideal of $\mathbb{Z}$, and for $i \neq j$, we have

$$p_i\mathbb{Z} = \sqrt{p_i^{k_i}}\mathbb{Z} \neq \sqrt{p_j^{k_j}}\mathbb{Z} = p_j\mathbb{Z}.$$

On the other hand, we have $\prod_{i\neq j} p_i^{k_i} \in \bigcap_{i\neq j} p_i^{k_i}\mathbb{Z}$, but $\prod_{i\neq j} p_i^{k_i} \notin p_j^{k_j}\mathbb{Z}$, so $\bigcap_{i\neq j}(p_i^{k_i}\mathbb{Z}) \not\subseteq p_j^{k_j}\mathbb{Z}$. By the definition of the minimal primary factorization in *Definition 2*, we find that $n\mathbb{Z} = p_1^{k_1}\mathbb{Z} \cap p_2^{k_2}\mathbb{Z} \cap \ldots \cap p_n^{k_n}\mathbb{Z}$. □

4 Individual Problems

Note: In this section, we will always consider the **commutative ring** with an **identity element**.

Problem 1. Let $R = \mathbb{C}[x, y]/\langle x^2 + y^2 - 1\rangle$. Determine all the maximal ideals of R.

Solution. We apply the property that $M \subseteq R$ is a maximal ideal of R if and only if $M = \mathfrak{M}/\langle x^2 + y^2 - 1\rangle$, where $\mathfrak{M}$ is a maximal ideal of $\mathbb{C}[x, y]$ containing $\langle x^2 + y^2 - 1\rangle$. Therefore, we need to find the maximal ideals of $\mathbb{C}[x, y]$ that contain $\langle x^2 + y^2 - 1\rangle$.
By *Hilbert's Nullstellensatz Theorem* (*Theorem 1*), the maximal ideals $\mathfrak{M}$ of $\mathbb{C}[x, y]$ are of the form

$$\mathfrak{M} = \langle x - a, y - b\rangle,$$

where $a, b \in \mathbb{C}$. Thus, $\langle x^2 + y^2 - 1\rangle \subseteq \mathfrak{M} = \langle x - a, y - b\rangle$ if and only if $x^2 + y^2 - 1 \in \langle x - a, y - b\rangle$. This means that $x^2 + y^2 - 1$ vanishes at (a, b), i.e.,

$$a^2 + b^2 - 1 = 0.$$

Therefore, $a^2 + b^2 = 1$, which means that (a, b) lies on the unit circle in the complex plane.
From this reasoning, we conclude that the maximal ideals of R are of the form

$$M = \langle x - a, y - b\rangle/\langle x^2 + y^2 - 1\rangle, \text{ where } a^2 + b^2 = 1.$$

□

Problem 2. Let $R = \mathbb{Z}[x]/\langle x^3 - 2x + 1\rangle$. Determine the structure of the ring R and its ideals.

Solution. We start by factoring the polynomial $x^3 - 2x + 1 = (x - 1)(x^2 + x - 1)$. The factor $x - 1$ is a linear polynomial and is irreducible in $\mathbb{Z}[x]$. To check the irreducibility of $x^2 + x - 1$, we assume it factors as $(x - \alpha)(x - \beta)$, where $\alpha, \beta \in \mathbb{Z}$. The roots of $x^2 + x - 1 = 0$ are $\alpha = \frac{-1\pm\sqrt{5}}{2}$, which are not integers. Therefore, $x^2 + x - 1$ is irreducible in $\mathbb{Z}[x]$.

Next, we divide $x^2 + x - 1$ by $x - 1$, yielding $x^2 + x - 1 = (x - 1)(x + 2) + 1$. This shows that $1 \in I_1 + I_2$, where $I_1 = \langle x - 1\rangle$ and $I_2 = \langle x^2 + x - 1\rangle$ are ideals of $\mathbb{Z}[x]$. Hence, $I_1 + I_2 = \mathbb{Z}[x]$.

Now, we consider the ideal $I = \langle x^3 - 2x + 1\rangle$. To prove that $I = I_1 \cap I_2$, let $f(x) \in I_1$. We can write $f(x) = (x - 1)(x^2 + x - 1)k(x)$, where $k(x) \in \mathbb{Z}[x]$. Since $f(x) \in I_2$, it follows that $f(x) \in I_1 \cap I_2$. Conversely, if $f(x) \in I_1 \cap I_2$, then $f(x)$ is divisible by both $x - 1$ and $x^2 + x - 1$. Since these two factors are coprime (as they are irreducible and distinct), $f(x)$ must be divisible by their product, $(x - 1)(x^2 + x - 1) = x^3 - 2x + 1$, implying $f(x) \in I$. Therefore $I = I_1 \cap I_2$.

Thus, we have $I = I_1 \cap I_2$ and $I_1 + I_2 = \mathbb{Z}[x]$. Using the *Chinese Remainder Theorem*, we have $\mathbb{Z}[x]/I \cong \mathbb{Z}[x]/I_1 \times \mathbb{Z}[x]/I_2$, through the isomorphism $\varphi : \mathbb{Z}[x]/I \to \mathbb{Z}[x]/I_1 \times \mathbb{Z}[x]/I_2$, defined by $\varphi(f + I) = (f + I_1, f + I_2)$.

Next, define $\phi : \mathbb{Z}[x]/I_1 \to \mathbb{Z}$ by $\phi(f + I_1) = f(1)$. This is a well-defined homomorphism because $f(1)$ is constant modulo $I_1 = \langle x - 1\rangle$. The kernel of ϕ is I_1, so $\mathbb{Z}[x]/I_1 \cong \mathbb{Z}$. The ideals of $\mathbb{Z}$ are of the form $\langle n\rangle$ with $n \in \mathbb{N}$, so the ideals of $\mathbb{Z}[x]/I_1$ are of the form $\langle n + I_1\rangle$ for $n \in \mathbb{N}$. For $\mathbb{Z}[x]/I_2$, the quotient ring is isomorphic to $\mathbb{Z}[\alpha]$, where α is a root of $x^2 + x - 1 = 0$. This is because $x^2 + x - 1$ is irreducible in $\mathbb{Z}[x]$, and $\mathbb{Z}[x]/I_2$ is a ring extension of $\mathbb{Z}$ by α.

From this, we determine the ideals of the ring $\mathbb{Z}[x]/I_1 \times \mathbb{Z}[x]/I_2$ as being of the form $\mathcal{I}_1 \times \mathcal{I}_2$, where $\mathcal{I}_1$ is an ideal of $\mathbb{Z}[x]/I_1$ and $\mathcal{I}_2$ is an ideal of $\mathbb{Z}[x]/I_2$. When viewed as ideals of $\mathbb{Z}[x]/I$, they have the form $\varphi^{-1}(\mathcal{I}_1 \times \mathcal{I}_2)$. □

Problem 3. Assume that every proper ideal of R is a primary ideal. Prove that:
(a) For any ideal I of R and a prime ideal P, we have $I \subseteq P$ or $IP = P$.
(b) A proper ideal I of R is prime if and only if for every $r \in R$, $r^2 \in I$ implies $r \in I$.

Proof.

(a) Suppose $I \not\subseteq P$ and $IP \neq P$. Since $IP \subseteq I \cap P \subseteq P$, there exists $x \in I \setminus P$ and $y \in P \setminus IP$. Then $xy \in IP$. Because IP is a proper ideal of R, it is primary by assumption. Since $y \notin IP$, there exists some $n \in \mathbb{N}$ such that $x^n \in IP$. From $IP \subseteq P$, we deduce $x^n \in P$. Since P is prime, $x \in P$ (see in *Problem 1 - (a), Section 3*). This contradicts $x \in I \setminus P$. Therefore, $I \subseteq P$ or $IP = P$. □

(b) ($\Rightarrow$) Suppose I is a prime ideal. If $r^2 \in I$, then since I is prime, $r \in I$.
($\Leftarrow$) Assume for contradiction that I is not a prime ideal. Then there exist $a, b \in R$ such that $a \notin I$, $b \notin I$, and $ab \in I$. Since I is a proper ideal of R, I is primary by assumption. Because, $a \notin I$, there exists $n \in \mathbb{N}$ such that $b^n \in I$. Choose $k \in \mathbb{N}$ such that $2^k > n$. Then $b^{2^k} \in I$. By the given condition, since $b^{2^k} = (b^{2^{k-1}})^2 \in I$, we have $b^{2^{k-1}} \in I$. Repeating this process $k - 1$ times, we eventually obtain $b \in I$, which is a contradiction. Therefore, I must be a prime ideal. □

Problem 4. Prove that:
(a) If P_1 and P_2 are two prime ideals of R such that $P_1 \cap P_2$ is primary, then $P_1 \subseteq P_2$ or $P_2 \subseteq P_1$.
(b) Assume that every proper ideal of R is primary. Prove that R has at most one non-zero primary ideal.

Proof.

(a) Suppose $P_2 \nsubseteq P_1$, meaning there exists $y \in P_2 \setminus P_1$. We will prove that $P_1 \subseteq P_2$. Indeed, let $x \in P_1$. Then $xy \in P_1P_2 \subseteq P_1 \cap P_2$. Since $P_1 \cap P_2$ is a primary ideal, we have $x \in P_1 \cap P_2 \subseteq P_2$ or $y \in \sqrt{P_1 \cap P_2} \subseteq \sqrt{P_1} = P_1$. As $y \notin P_1$, it follows that $x \in P_2$. Thus, $P_1 \subseteq P_2$. □

Lemma 3. *Let J be the Jacobson radical of R and $a \in R \setminus \{0\}$. Prove that if the ideal aJ is primary, then $J \subseteq \sqrt{aJ}$.*

Proof of Lemma Let $x \in J$. We will prove that $x \in \sqrt{aJ}$. Indeed, $ax \in aJ$. It follows that $a \in aJ$ or $x \in \sqrt{aJ}$. If $a \in aJ$, then there exists $y \in J$ such that $a = ay$. Thus, $a(1-y) = 0$. Since $y \in J$, $1-y$ is invertible. Therefore, $a = 0$, which is a contradiction. Hence, $x \in \sqrt{aJ}$. Thus, $J \subseteq \sqrt{aJ}$.

(b) Let M be a maximal ideal of R. Suppose $x \in R \setminus M$. We will prove $x \in R^*$ by contradiction. Indeed, assume $x \notin R^*$. Then $Rx \neq R$. By hypothesis, Rx is primary. It follows that $\sqrt{Rx}$ is prime. Since $M \cap \sqrt{Rx}$ is a proper ideal of R, it is also a primary ideal. Thus, $\sqrt{Rx} \subseteq M$ or $M \subseteq \sqrt{Rx}$ (by (a)). Since $x \in \sqrt{Rx}$ and $x \notin M$, we have $\sqrt{Rx} \nsubseteq M$. Therefore, $M \subseteq \sqrt{Rx}$. As M is maximal, we conclude $M = \sqrt{Rx} \ni x$, contradicting $x \notin M$. Thus, $x \in R^*$. This shows that R is a local ring with maximal ideal M (by [AM69] 1.6.1). Hence, $J = M$.
Now suppose P is a nonzero prime ideal of R. We will prove $P = M$. Indeed, let $0 \neq x \in P$. By *Lemma 3*, we have $M \subseteq \sqrt{xM} \subseteq \sqrt{P} = P$, so $P = M$. Thus, R has at most one nonzero prime ideal.
□

References

[1] R. Y. Sharp, *Steps in Commutative Algebra*, 2nd ed., Cambridge University Press, 2000.

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] Trinh Thanh Deo, *Modern Algebra Textbook*, University of Science, Vietnam National University Ho Chi Minh City, 2010.