On Hilbert's Nullstellensatz

Jiantong Liu

February 5, 2023

Preliminaries

This document is a general survey that introduces different concepts built up upon rings, including ideals, domains, and a little bit of algebraic geometry, so that we can make our way to (various statements of) Hilbert's Nullstellensatz. Note that most of the results' proofs are omitted, and we might add them later.

1 Rings

There has been different definitions of rings and relevant concepts, and in this document we would consider rings to be unital, and develop the relevant concepts from this standpoint.

Definition 1.1 ((Commutative) Ring)**.** A (unital) *ring* R is a set equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) such that

(a) $(R, +)$ is an (additive) Abelian group with identity element $0 \in R$,

(b) $(R, \cdot)$ is a (multiplicative) monoid with identity element $1 \in R$,

(c) and $(R, +, \cdot)$ has multiplication distributing over addition: for all $x, y, z \in R$, $x(y+z) = xy + xz$ and $(x + y)z = xz + yz$.

Moreover, a *commutative ring* R is a ring R where $(R, \cdot)$ is a commutative monoid.

Remark 1.2.

1. 0 and 1 are unique.
2. The additive identity 0 behaves in the obvious way under multiplication: $0 \cdot x = x \cdot 0 = 0$ for all $x \in R$.
3. The additive inverse behaves well under multiplication: $(-x)y = x(-y) = -xy$ for all $x, y \in R$.

4. We say an element $x \in R$ is a *unit* in R if it has a multiplicative inverse, that is, there exists $x^{-1} \in R$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1 \in R$. One should note that the multiplicative inverse, if exists, is unique (just like the additive inverse). In fact, the set of units of R forms a group under multiplication, often denoted by $(R^\times, \cdot)$, the unit group.

Example 1.3.

1. The set $\{0\}$ itself is a ring, often called the *trivial ring*. Note that $1 = 0$ in this construction. In fact, a ring R satisfies $1 = 0$ if and only if R is the trivial ring.

2. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with unit group $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \mid \gcd(a, n) = 1\}$. The unit group has order $\varphi(n)$, where φ is the Euler function.

3. Suppose R is a ring, then the *matrix ring* $M_n(R)$, the set of $n \times n$ matrices with entries belonging in R, forms a ring under matrix addition and matrix multiplication. This ring is non-commutative for $n \geq 2$. The unit group of this ring is the *general linear group* of degree n over R, i.e., $(M_n(R))^\times = \mathrm{GL}_n(R)$. For a commutative ring R, $\mathrm{GL}_n(R)$ contains exactly the $n \times n$ matrices with non-zero determinant.

4. If R is a ring, then $R[x]$, the set of polynomials of variable x and coefficients in R, forms a ring called the *polynomial ring* over R. Consequently, we can define polynomial rings with multiple variables (e.g., $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$). From a constructive standpoint, we can construct it as $R[X]$ where X is a set of variables. If R is commutative, then the polynomial ring is also commutative.

5. Note that the construction of polynomial rings above allows the variables to commute within themselves. However, if we do not allow them to commute, we also obtain non-commutative polynomial rings denoted $R\langle X \rangle$ where X is a set of variables.

Definition 1.4 (Ring Homomorphism)**.** Let R and S be rings. A map $f : R \to S$ is a ring homomorphism if

(a) $f(1) = 1$,

(b) $f(x + y) = f(x) + f(y)$ for all $x, y \in R$, and

(c) $f(xy) = f(x)f(y)$ for all $x, y \in R$.

Example 1.5. Ring homomorphisms are constructed with a stricter structure compared to those of groups. For instance, there is no ring homomorphism mapping $\mathbb{Q}$ to $\mathbb{Z}$.

In order to study the data categorically, we collect the properties above and consider the category of rings.

Definition 1.6 (Category of Rings)**.** The category of rings, denoted **Ring**, has objects to be rings and morphisms to be ring homomorphisms.

The category of commutative rings, denoted **CRing**, has objects to be commutative rings and morphisms to be ring homomorphisms between those commutative rings.

Remark 1.7.

1. **CRing** is a full subcategory of **Ring**.
2. The initial object of **Ring** is $\mathbb{Z}$, and the terminal object of **Ring** is the zero ring.
3. As we mentioned, it would be difficult to study the structure on rings. Note that the epimorphisms in **Ring**, unlike those in **Grp** and **Set**, is not the surjective ring homomorphisms. For example, the inclusion morphism $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism, but it does not have a right inverse (which is something you would expect on other structures). Similar things happen to the inclusion morphism $\mathbb{Q} \hookrightarrow \mathbb{R}$.

Remark 1.8 (Free-Forgetful Adjunction)**.**

1. The forgetful functor **Ring** $\to$ **Set** has the (free) left adjoint to be the mapping $X \mapsto \mathbb{Z}\langle X \rangle$.
2. The forgetful functor **CRing** $\to$ **Set** has the (free) left adjoint to be the mapping $X \mapsto \mathbb{Z}[X]$.

Definition 1.9 (Subring)**.** Let R be a ring. A *subring* of R is a subset $S \subseteq R$ such that $0, 1 \in S$ and S forms a ring with the inherited operations from R.

Example 1.10.

1. Suppose R is a ring and S is a subring of R, then $i : S \hookrightarrow R$ is a (inclusion) ring homomorphism.
2. Some common structures we know are related as subrings of one another: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
3. Here is another instance where we notice that rings are hard to study. For instance, consider the matrix ring $M_2(R)$. The subset $\left\{ \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \right\}$ of $M_2(R)$ is a ring with the operations inherited from $M_2(R)$. However, it is not a subring of $M_2(R)$ because it does not contain the multiplicative identity I_2 of $M_2(R)$.

Given our knowledge of groups and their substructure (that is, subgroups), we would expect the same things happening to rings and subrings. However, this would not be the case. Fortunately, we get to study a different type of substructure with those analogous nice properties.

2 Ideals

Definition 2.1 (Ideal)**.** Let R be a ring. A subset $I \subseteq R$ is called a *left ideal* of R if

(a) $(I, +)$ is a subgroup of $(R, +)$, and

(b) if $x \in R$, then $xI \subseteq I$.

Similarly, we can define a *right ideal* of R as

(a) $(I, +)$ is a subgroup of $(R, +)$, and

(b) if $x \in R$, then $Ix \subseteq I$.

We say a subset I of R is a *two-sided ideal* if it is both a left ideal and right ideal.

In the rest of the document, if we do not specify what type of ideal it is, the statement would work for left, right, and two-sided ideals.

Example 2.2.

1. For any ring R, there is the *zero ideal* $(0) = \{0\}$ and the *unit ideal* $(1) = R$.
2. A commutative ring R is a field if and only if R only has two ideals: the zero ideal and the unit ideal.
3. If I is an ideal and $I \cap R^\times \neq \varnothing$, then I is the unit ideal.

Remark 2.3 (Operations on Ideals)**.**

1. The intersection of any family of ideals is an ideal.
2. Given two ideals $I, J \subseteq R$, the product ideal IJ is the smallest ideal containing all products ab with $a \in I$ and $b \in J$. However, this set in particular is not an ideal. To give a better description, IJ is the ideal containing all finite sums of elements of the form ab with $a \in I$ and $b \in J$.
3. The union of two ideals may not be an ideal.
4. Given a family of ideals $\{I_j\}_{j \in J}$, the sum of those ideals $\sum_{j \in J} I_j$ is an ideal, and is the smallest ideal containing I and J. Equivalently, it is the ideal generated by $\bigcup_{j \in J} I_j$.

Definition 2.4 (Generators)**.** Suppose R is a ring and X is a subset of R, then we denote $\langle X \rangle$ to be the intersection of all ideals containing X, i.e., $\langle X \rangle = \bigcap_{Y \supseteq X} Y$. Therefore, $\langle X \rangle$ is the smallest ideal containing the set X. We say that X is the generating set of $\langle X \rangle$.

We are particularly interested in the case where X is a singleton, i.e., $X = \{x\}$ for some $x \in R$.

Definition 2.5 (Principal Ideal)**.** For any $x \in R$, we say $Rx = \{ax \mid a \in R\}$ is the principal left ideal generated by x. Similarly, we define xR to be the principal right ideal generated by x. We can also define $(x) = RxR$ to be the two-sided ideal generated by x.

Remark 2.6. $u \in R$ is a unit if and only if $Ru = uR = R$.

We now explain why ideals are the desired substructures of rings.

Definition 2.7 (Quotient Ring)**.** Let R be a ring and $I \subseteq R$ be an ideal of R. The quotient ring R/I is the (additive) quotient group R/I equipped with the multiplication operation $(x + I)(y + I) = xy + I$ on the cosets.

Remark 2.8. Suppose $f : R \to S$ is a ring homomorphism, then $\ker(f)$ is an ideal of R, and $\mathrm{im}(f)$ is a subring of S.

Therefore, the ideals act in rings just like how (normal) subgroups act in groups. Therefore, many results in groups still work in rings.

Theorem 2.9 (First Isomorphism Theorem)**.** Let $f : R \to S$ be a ring homomorphism, then $R/\ker(f) \cong \mathrm{im}(f)$.

We now look into some interesting type of ideals that play a big role in the rest of the document.

Definition 2.10 (Prime Ideal)**.** An ideal $\mathfrak{p}$ in a commutative ring R is *prime* if $\mathfrak{p} \neq R$ and whenever $xy \in \mathfrak{p}$, either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Definition 2.11 (Maximal Ideal)**.** An ideal $\mathfrak{m}$ in a commutative ring R is *maximal* if $\mathfrak{m} \neq R$ and whenever there exists an ideal $I \supseteq \mathfrak{m}$, either $I = \mathfrak{m}$ or $I = R$.

Definition 2.12 (Radical Ideal)**.** The radical of an ideal I in a commutative ring R is $\mathrm{rad}(I)$ (often denoted $\sqrt{I}$), defined by

$$\mathrm{rad}(I) = \{x \in R \mid x^n \in I \text{ for some } n \geq 1\}.$$

Alternatively, the radical of I is the intersection of all prime ideals in R containing I.

An ideal I in a commutative ring R is *radical* if $\mathrm{rad}(I) = I$. That is, I is its own radical in R.

Note that these structures correspond to nice quotient structures over the ring R.

Proposition 2.13. 1. An ideal $\mathfrak{p} \subseteq R$ is prime if and only if $R/\mathfrak{p}$ is a domain.

2. An ideal $\mathfrak{m} \subseteq R$ is maximal if and only if $R/\mathfrak{p}$ is a field.

3. An ideal $I \subseteq R$ is radical if and only if $R/\mathfrak{p}$ is a reduced ring.

Example 2.14. 1. $\mathbb{Z}/n\mathbb{Z}$ is a quotient ring, i.e., the quotient of $\mathbb{Z}$ by the ideal $n\mathbb{Z}$. In fact, it is a domain if and only if n is prime, in which case $\mathbb{Z}/n\mathbb{Z}$ is a field. By the correspondence, we know $n\mathbb{Z}$ is prime if and only if $n = 0$ or n is prime.

2. The surjective ring homomorphism $R[x] \twoheadrightarrow \mathbb{C}$ defined by $f(z) = z(i)$, i.e., evaluating the polynomial z at i, has kernel $(x^2 + 1)$. Therefore, $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.

3. There is a canonical surjective ring homomorphism $\pi : R \to R/I$ defined by $x \mapsto x + I$.

In particular, notice that the maximal ideal is a type of natural structure, but it seems to be rare. However, it is guaranteed that they always exists.

Theorem 2.15. Every non-zero commutative ring has a maximal ideal.

Proof. This is an application of Zorn's Lemma. □

Corollary 2.16. Every non-zero commutative ring has a prime ideal.

Proposition 2.17. Every non-zero commutative ring has a minimal prime ideal.

General correspondence theorem also exists.

Theorem 2.18 (Correspondence Theorem)**.** 1. Let $f : R \twoheadrightarrow S$ be a surjective ring homomorphism and I be an ideal of R, then $f(I)$ is an ideal in S.

2. Let $f : R \twoheadrightarrow S$ be a surjective ring homomorphism and I be an ideal in S. The preimage $f^{-1}(I)$ is an ideal in R containing $\ker(f)$. In fact, there is a correspondence between the set of all ideals in S and the set of all ideals in R that contain $\ker(f)$.

3. Let R be a ring and I be an ideal of R. There is a bijective correspondence between ideals of R/I and ideals of R containing I.

Remark 2.19. Note that a ring homomorphism usually do not send ideals to ideals.

3 Domains

To continue our studies of rings even further, we want to look into rings with special properties. We would think of commutative rings as a bit weak, but the fields as a bit strong. To find a middle ground between them, we study the (integral) domains instead.

Definition 3.1 ((Integral) Domain)**.** Let R be a ring and $0 \neq x \in R$. We say x is a left zero divisor if there exists $0 \neq y \in R$ such that $xy = 0$. Similarly we can define right zero divisors or zero divisors in general.

A commutative ring R is a (integral) domain if $R \neq 0$ and R has no zero divisors.

Example 3.2. 1. A field is a (integral) domain.

2. $\mathbb{Z}$ is a (integral) domain.

In some sense, $\mathbb{Z}$ is the prototypical object in our study of (integral) domains (for reasons we would see later).

Remark 3.3. A (integral) domain is just a ring that satisfies cancellation laws: $a \cdot b = a \cdot c$ should imply $b = c$. This is often used as an alternative definition.

Throughout this section, R is assumed to be a domain unless specified otherwise.

Definition 3.4 (Divisibility)**.** Let $a, b \in R$ with $b \neq 0$. We say that b divides a (equivalently, a is divisible by b), denoted $b \mid a$, if there exists $c \in R$ such that $= bc$.

Remark 3.5. 1. $b \mid a$ if and only if $(b) \supseteq (a)$.

2. If $a \mid b$, then $a \mid bc$ for all $c \in R$.

3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

4. $(a) = (b)$ if and only if there exists some $u \in R^\times$ such that $b = au$. In this case, we say $a, b \in R$ are *associates*, often denoted by $a \sim b$.

Note that $\mathbb{Z}$ is a domain, and many well-known properties on $\mathbb{Z}$ collected by Euclid appears in arbitrary domains. However, these properties usually are not enough to support the validity of Euclidean algorithm (also known as the division algorithm) on arbitrary domains.

Definition 3.6 (Euclidean Domain)**.** A Euclidean domain is a domain R for which there is a function $\varphi : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $a \in R$ and $0 \neq b \in R$, there exists $q, r \in R$ with $a = bq + r$, where either $r = 0$ or $\varphi(r) < \varphi(b)$. φ is usually called a Euclidean function for R. Note that Euclidean function for an Euclidean domain may not be unique.

In many occasions, norm functions happen to be Euclidean functions.

Remark 3.7. 1. $\mathbb{Z}$ is a Euclidean domain equipped with $\varphi(x) = |x|$.

2. For $R = F[x]$ where F is a field, R is a Euclidean domain with $\varphi(f) = \deg(f)$.

3. The ring of Gaussian integers $\mathbb{Z}[i]$ is a domain with $\varphi(a + bi) = a^2 + b^2 = |a + bi|^2$.

4. $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with $\varphi(a + b\sqrt{2}) = |a^2 - 2b^2|$.

We have seen principal ideals when introducing ideals. There is a type of domains with related properties.

Definition 3.8 (Principal Ideal Domain)**.** A domain R is a principal ideal domain (often abbreviated as PID) if every ideal of R is principal.

Essentially, this is saying every ideal of a PID R can be generated by a single element, which is sometimes not so easy to prove.

To see how this related to Euclidean domains, consider the following theorem.

Theorem 3.9. Every Euclidean domain is a PID.

Example 3.10. 1. One can show that $\mathbb{Z}[\sqrt{-5}]$ is not a PID by identifying $(2, 1 + \sqrt{-5})$ as a non-principal ideal of R.

2. $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but not is not Euclidean.

3. $\mathbb{Z}$ is a PID.

Now we have seen that certain domains would satisfy useful properties, with $\mathbb{Z}$ as a prototype. However, the properties we examined are usually pretty fancy and do not discuss the crucial property of $\mathbb{Z}$: what makes the integers such a good structure for us to work on? A strong candidate would be the unique factorization of integers. That is, given any integer, it is either 1 or a product of primes, with a possible sign change. We will see that certain domains also have this property.

Definition 3.11 (Irreducible Element)**.** Consider a non-zero non-unit element $c \in R$. We say c is irreducible if whenever $c = xy$ for $x, y \in R$, either $x \in R^\times$ or $y \in R^\times$.

Note that irreducible elements have a certain kind of "primeness", especially if you think of them in $\mathbb{Z}$. However, the prime elements are usually different from irreducible elements.

Definition 3.12 (Prime Element)**.** Consider a non-zero non-unit element $p \in R$. We say p is prime if whenever $p \mid xy$, either $p \mid x$ or $p \mid y$.

We actually have a correspondence between these elements and the principal ideals generated by those elements.

Proposition 3.13. 1. An element $c \in R$ is irreducible if and only if $c \neq 0$, $c \notin R^\times$, and (c) is maximal in the set of principal ideals different from R.

2. An element $p \in R$ is prime if and only if (p) is a non-zero prime ideal.

We now look into the similarities between these elements.

Proposition 3.14. Every prime element is irreducible.

One would ask: when are irreducible elements prime? That is, when are irreducible elements and prime elements equivalent, just like what we would see in $\mathbb{Z}$? A preliminary result shows that it already works in PID:

Proposition 3.15. In a PID, irreducible elements and prime elements are equivalent.

Definition 3.16 (Factorization)**.** We say that R admits a factorization if for any non-zero non-unit $a \in R$, there exists irreducible elements $a_1, \ldots, a_n$ such that $a = a_1 \cdots a_n$. Equivalently, R admits factorization when we can write $(a) = (a_1) \cdots (a_n)$ as ideals with a_i's irreducible.

Definition 3.17 (Unique Factorization)**.** We say that R has unique factorization if whenever $b_1 \cdots b_m = c_1 \cdots c_n$ where b_i's and c_j's are irreducible elements, then $n = m$ and after certain rearrangement of labeling, $b_i \sim c_i$ as associates for all i. Therefore, in terms of ideals, we say R has unique factorization if $(b_1) \cdots (b_n) = (c_1) \cdots (c_n)$ for irreducible elements b_i's and c_j's, then $n = m$ and after certain rearrangement of labeling, $(b_i) = (c_i)$ for all i.

It is usual for a domain to acquire a factorization. The question is, when is the factorization unique? This relates back to the elements we just studied.

Proposition 3.18. 1. Suppose R admits factorization. If the factorization of R is unique, then every irreducible element of R is prime, i.e., prime elements and irreducible elements are equivalent.

2. If every irreducible element in R is prime, then the factorization in R is unique.

Therefore, there is a strong relation between the uniqueness of factorization in a domain R and the equivalence between irreducible elements and prime elements.

Definition 3.19 (Unique Factorization Domain)**.** A domain R is a unique factorization domain (often abbreviated as UFD) if R admits a unique factorization.

Corollary 3.20. A domain R is a UFD if and only if R admits factorization and every irreducible element if prime.

Corollary 3.21. In a UFD, prime elements and irreducible elements are the same.

Before we look into the relation between these domains, we introduce one last type of important domain.

Definition 3.22 (Noetherian Ring)**.** Let R be a commutative ring. We say R is a Noetherian ring if any of the following properties hold:

(a) Every ideal in R is finitely-generated, that is, every ideal has a generating set of finite size.

(b) Every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ eventually stabilizes, i.e., there exists some $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \cdots$, so $I_n = I_m$ for all $n, m \geq N$. This is usually called the ascending chain condition (often abbreviated as ACC).

(c) Every non-empty set of ideals in R has a maximal element.

A Noetherian domain is a Noetherian ring that happens to be a domain.

Theorem 3.23. The three properties stated above are equivalent.

Remark 3.24. There is an analogous type of rings called the Artinian rings, which satisfies the descending chain condition (often abbreviated as DCC).

Theorem 3.25. A commutative Artinian ring is Noetherian.

Remark 3.26. Many structures we have discussed so far actually also works on groups and rings.

Proposition 3.27. Every PID is Noetherian.

Proposition 3.28. Noetherian rings admit factorization. Therefore, if R is a Noetherian domain, then R is a UFD if and only if every irreducible element is prime.

Corollary 3.29. Every PID is a UFD.

Therefore, we can look into a classification of domains.

Remark 3.30. The Euclidean domains are a subset of the PIDs, which is a subset of the UFDs, which is a class of domains. Moreover, the PIDs are a subset of the Notherian domains.

An interesting question one would ask is how these different types of domains play a role in the structure of polynomial rings.

Theorem 3.31. If R is a UFD, then $R[x]$ is a UFD.

Corollary 3.32. If R is a UFD and X is an arbitrary set of variables (possibly infinite), then $R[X]$ is a UFD.

Proposition 3.33. If $R[x]$ is a UFD, then R (as an integral domain) is a UFD.

Remark 3.34. A subring of a UFD maynot be a UFD.

Theorem 3.35. Let F be a commutative ring, then F is a field if and only if $F[x]$ is a PID.

Proposition 3.36. A finite integral domain is a field.

Theorem 3.37 (Hilbert's Basis Theorem)**.** If R is a Noetherian ring, then so is $R[x]$.

We now show how to deduce if an element in the polynomial ring is irreducible.

Definition 3.38 (Greatest Common Divisor)**.** Let $\{a_i\}_{i\in I}$ be non-zero elements in R. A greatest common divisor (gcd) for $\{a_i\}_{i\in I}$ is a principal ideal $(d) \subseteq R$ such that $(d) \mid (a_i)$ for all $i \in I$ and, if $(c) \mid (a_i)$ for all $i \in I$, then $(c) \mid (d)$.

Proposition 3.39. The gcd is unique, if exists.

Because UFDs allow unique factorization, the existence of a greatest common divisor is ensured. For now, let R be a UFD unlesss stated otherwise.

Proposition 3.40. In a UFD, the GCD of a finite set of elements exists.

Definition 3.41 (Content)**.** Let $f = a_n x^n + \cdots + a_0 \in R[x]$ be a non-zero polynomial. The *content* of f, denoted $C(f)$, is the gcd of all non-zero coefficients $a_n, \ldots, a_0$.

Definition 3.42 (Primitive)**.** A polynomial $f \in R[x]$ is *primitive* if $C(f) = R = (1)$.

For instance, monic polynomials are primitive.

Proposition 3.43. If $a \in R$ and $f \in R[x]$, then $C(af) = aC(f)$.

Lemma 3.44 (Gauss)**.** Let $f, g \in R[x]$ be primitive, then fg is primitive.

Corollary 3.45. If $f, g \in R[x]$, then $C(fg) = C(f)C(g)$.

Lemma 3.46. Let R be a UFD and F be the quotient field of R, and $f, g \in R[x]$. If f is primitive and f divides g in $F[x]$, then f divides g in $R[x]$.

Lemma 3.47. Let R be a UFD and F be the quotient field of R. Then a non-constant polynomial $f \in R[x]$ is irreducible if and only if f is primitive and f is irreducible in $F[x]$.

Theorem 3.48 (Eisenstein Criterion)**.** Let R be a UFD and F be the quotient field of R. Let $f = a_n x^n + \cdots + a_0 \in R[x]$. Let $p \in R$ be a prime element such that

- $p \nmid a_n$,
- $p \mid a_i$ for all $0 \leq i \leq n-1$,
- $p^2 \nmid a_0$,

then f is irreducible in $F[x]$.

Finally, we take a glimpse at two other types of domain.

Definition 3.49 (Integrally Closed Domain)**.** Suppose R is an integral domain and F is the quotient field of R. We say $x \in F$ is *integral* if it is a root of a monic polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_i \; in R$ for all i.

The *integral closure* of R in F is the set of integral elements of R in F, which happens to be a domain. In particular, we say an integral domain R is *integrally closed* if it is its own integral closure.

Theorem 3.50. A UFD is integrally closed.

Remark 3.51. A Notherian domain may not be integrally closed: see $\mathbb{Z}[\sqrt{5}]$.

Definition 3.52 (Algebraically Closed Field)**.** A field F is to be *algebraically closed* if every non-constant polynomial $f \in F[x]$ has a root $a \in F$.

4 Basic Algebraic Geometry

Let R be a commutative ring throughout this section.

Definition 4.1 (Spectrum)**.** The *spectrum* of R, denoted $\mathrm{Spec}(R)$, is the set of prime ideals of R.

Definition 4.2 (Vanishing Set)**.** For any subset $S \subseteq R$, let $V(S) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid S \subseteq \mathfrak{p}\}$ be the vanishing set of S.

The notion of the vanishing set defines a topology on the spectrum of R, making it a topological space.

Lemma 4.3. 1. If I is the ideal generated by S, then $V(S) = V(I) = V(\sqrt{I})$.

2. $V(\{0\}) = \mathrm{Spec}(R)$ and $V(\{1\}) = V(R) = \varnothing$.

3. If $\{I_j\}_{j\in J}$ is a family of ideals in R, then $\bigcap\limits_j V(I_j) = V(\sum\limits_j I_j)$.

4. $V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$.

Definition 4.4 (Zariski Topology)**.** The *Zariski topology* is the topology on $\mathrm{Spec}(R)$ defined by taking the closed sets to be the sets $V(I)$ for ideals $I \subseteq R$.

Example 4.5. 1. If F is a field, then $\mathrm{Spec}(F) = \{0\}$.

2. $\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \in \mathbb{Z} \text{ is prime or } 0\}$.

3. If R is a commutative ring and $I \subseteq R$ is an ideal, then there is a bijection $V(I) \to \mathrm{Spec}(R/I)$ by sending $\mathfrak{p} \mapsto \mathfrak{p}/I$.

Proposition 4.6. $\mathrm{Spec}(R)$ is compact.

Definition 4.7 (Irreducible)**.** A topological space X is *irreducible* if for every two open subsets $A_1, A_2 \neq \varnothing$, we have $A_1 \cap A_2 \neq \varnothing$. Equivalently, every non-empty open subset is dense.

Definition 4.8 (Nilradical)**.** The nilradical of a commutative ring R, denoted $\mathrm{Nil}(R)$, is the intersection of all prime ideals.

Proposition 4.9. $\mathrm{Spec}(R)$ is irreducible if and only if $\mathrm{Nil}(R) \in \mathrm{Spec}(R)$.

Corollary 4.10. The spectrum $\mathrm{Spec}(R)$ of a domain R is irreducible.

Definition 4.11 (Affine Space)**.** Let k be an algebraically closed field. The *affine n-space over k* is

$$\mathbb{A}_k^n = k^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\}.$$

Definition 4.12 (Vanishing Set)**.** Let $R = k[x_1, \ldots, x_n]$. An element $f \in R$ determines a function $\mathbb{A}_k^n \to k$. For an element $f \in R$, its vanishing set (often called the zero set in this case) is $\{f = 0\} \subseteq \mathbb{A}_k^n$, often defined by

$$Z(f) = \{f = 0\} := \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n : f(a_1, \ldots, a_n) = 0\}.$$

Similarly, for a set T, its zero set is

$$Z(T) = \{a \in \mathbb{A}_k^n : f(a) = 0 \ \forall f \in T\}.$$

Note that the properties discussed above still works on the affine space.

5 Hilbert's Nullstellensatz

Lemma 5.1 (Zariski's Lemma)**.** Let L/K be a field extension. If L is of finite type over K, then L is finite over K.

Proof. The proof makes use of Noether Normalization Lemma. □

Theorem 5.2 (Hilbert's Weak Nullstellensatz, Version 1)**.** Let k be a field and $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ be a maximal ideal, then $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field extension of k. In particular, if k is algebraically closed, then $k[x_1, \ldots, x_n]/\mathfrak{m} \cong k$.

Theorem 5.3 (Hilbert's Weak Nullstellensatz, Version 2)**.** Let k be an algebraically closed field, then the maximal ideals of $k[x_1, \ldots, x_n]$ are of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for $a_i \in k$.

Theorem 5.4 (Hilbert's Weak Nullstellensatz, Version 3)**.** Let k be an algebraically closed field and suppose $I = (f_1, \ldots, f_r)$ is an ideal in $k[x_1, \ldots, x_n]$. Then $Z(I)$ is the empty set if and only if I is the unit ideal. Moreover, if $I \subsetneq R$, then there exists some $a \in k^n$ such that $f_i(a) = 0$ for all $1 \leq i \leq r$.

Remark 5.5. Note that a maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$ now consists of all polynomials which vanish at the point $(a_1, \ldots, a_n) \in k^n$, so there is a correspondence between points in k^n and maximal ideals in $k[x_1, \ldots, x_n]$.

Theorem 5.6 (Hilbert's Strong Nullstellensatz, Version 1)**.** Let k be an algebraically closed field and I be an ideal of $k[x_1, \ldots, x_n]$. Suppose $f \in k[x_1, \ldots, x_n]$ vanishes on $Z(I)$, then $f \in \sqrt{I}$.

Proof. The proof makes use of Rabinowitsch trick. □

Corollary 5.7. Let $I(S)$ be the ideal of $k[x_1, \ldots, x_n]$ generated by polynomials vanishing on $S \subseteq k^n$, then $I(Z(J)) = \sqrt{J}$ for ideal J in $k[x_1, \ldots, x_n]$. In particular, if J is radical, then $I(Z(J)) = J$.

Theorem 5.8 (Hilbert's Strong Nullstellensatz, Version 2)**.** Let k be an algebraically closed field and suppose $I = (f_1, \ldots, f_r)$ is an ideal in $k[x_1, \ldots, x_n]$. Consider $f \in k[x_1, \ldots, x_n]$ such that $f(a) = 0$ for all $a \in Z(I)$, then $f \in \sqrt{I}$. In particular, if I is prime, then $f \in I$.