MA5202: Algebraic Geometry

Arjun Paul
Department of Mathematics and Statistics
Indian Institute of Science Education and Research Kolkata,
Mohanpur - 741 246, Nadia,
West Bengal, India.
Email: arjun.paul@iiserkol.ac.in.

Version: January 4, 2023 at 10:12pm (IST).

This note will be updated from time to time.
If there are any potential mistakes, please bring it to my notice.

Contents

List of Symbols

$\emptyset$	Empty set
$\mathbb{Z}$	The set of all integers
$\mathbb{Z}_{\geq 0}$	The set of all non-negative integers
$\mathbb{N}$	The set of all natural numbers (i.e., positive integers)
$\mathbb{Q}$	The set of all rational numbers
$\mathbb{R}$	The set of all real numbers
$\mathbb{C}$	The set of all complex numbers
$<$	Less than
$\leq$	Less than or equal to
$>$	Greater than
$\geq$	Greater than or equal to
$\subset$	Proper subset
$\subseteq$	Subset or equal to
$\subsetneq$	Subset but not equal to (c.f. proper subset)
$\exists$	There exists
$\nexists$	Does not exists
$\forall$	For all
$\in$	Belongs to
$\notin$	Does not belong to
$\sum$	Sum
$\prod$	Product
$\pm$	Plus and/or minus
∞	Infinity
$\sqrt{a}$	Square root of a
$\cup$	Union
$\bigsqcup$	Disjoint union
$\cap$	Intersection
$A \to B$	A mapping into B
$a \mapsto b$	a maps to b
$\hookrightarrow$	Inclusion map
$A \setminus B$	A setminus B
$\cong$	Isomorphic to
$A := \ldots$	A is defined to be ...
$\square$	End of a proof

Symbol	Name	Symbol	Name
α	alpha	β	beta
γ	gamma	δ	delta
π	pi	ϕ	phi
φ	var-phi	ψ	psi
ϵ	epsilon	ε	var-epsilon
ζ	zeta	η	eta
θ	theta	ι	iota
κ	kappa	λ	lambda
μ	mu	ν	nu
υ	upsilon	ρ	rho
ϱ	var-rho	ξ	xi
σ	sigma	τ	tau
χ	chi	ω	omega
Ω	Capital omega	Γ	Capital gamma
Θ	Capital theta	Δ	Capital delta
Λ	Capital lambda	Ξ	Capital xi
Σ	Capital sigma	Π	Capital pi
Φ	Capital phi	Ψ	Capital psi

Some of the useful Greek letters

Chapter 1

Basic Theory of Schemes

1.1 Classical variety

Let k be a field and let $k[x_1, \ldots, x_n]$ be the polynomial ring in n variables $x_1, \ldots, x_n$ and coefficients from the field k. Given a subset $E \subseteq k[x_1, \ldots, x_n]$, let

$$\mathcal{Z}(E) := \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0, \ \forall\, f \in E\}$$

be the subset of all common zeros of the polynomials in E. We are interested to study geometry of $\mathcal{Z}(E)$. If $f \in E$ is a linear polynomial with zero constant term, i.e., $f(0, \ldots, 0) = 0$, the map $T_f : k^n \to k$ defined by

$$T_f(a_1, \ldots, a_n) = f(a_1, \ldots, a_n), \ \ \forall\, (a_1, \ldots, a_n) \in k^n,$$

is a k-linear map, and that $\mathcal{Z}(f) = \mathrm{Ker}(T_f)$ is a k-linear subspace of k^n. Therefore, if all the polynomials in E are linear with zero constant terms, then

$$\mathcal{Z}(E) = \bigcap_{f \in E} \mathrm{Ker}(T_f)$$

is a k-linear subspace of k^n, and in this case standard linear algebra machinery could be used to study the space $\mathcal{Z}(E)$. However, when $f \in A$ is not a linear polynomial, $\mathcal{Z}(f)$ is no longer a liner space, and hence we cannot use linear algebra machinery to study geometry of $\mathcal{Z}(f)$. In this situation, the techniques from commutative algebra comes into the picture.

Proposition 1.1.1. *Let E be a non-empty subset of the polynomial ring $k[x_1, \ldots, x_n]$. Then $\mathcal{Z}(E) = \mathcal{Z}(\langle E \rangle)$, where $\langle E \rangle$ is the ideal of $k[x_1, \ldots, x_n]$ generated by E.*

Proof. Since $E \subseteq \langle E \rangle$, it follows from the definition of $\mathcal{Z}(E)$ that $\mathcal{Z}(\langle E \rangle) \subseteq \mathcal{Z}(E)$. Conversely, let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathcal{Z}(E)$. Let $f \in \langle E \rangle$ be arbitrary. Then $f = \sum\limits_{j=1}^{m} \phi_j f_j$, for some $\phi_j \in k[x_1, \ldots, x_n]$ and $f_j \in E$, for all $j \in \{1, \ldots, m\}$. Since $f_j(\mathbf{a}) = 0$, for all j, we have $f(\mathbf{a}) = \sum\limits_{j=1} \phi_j(\mathbf{a}) f_j(\mathbf{a}) = 0$. Therefore, $\mathbf{a} \in \mathcal{Z}(\langle E \rangle)$. $\square$

We now introduce a class of commutative rings with identity for which every ideals are finitely generated. Such a ring is called Noetherian. We show that polynomial ring

$k[x_1, \ldots, x_n]$ and its quotient rings are Noetherian. One of the advantage to work with such rings is that all of its ideals being finitely generated, zero locus of a given family of possibly infinitely many polynomials is determined by a finite number of polynomials among them.

Let A be a commutative ring with identity.

Definition 1.1.2. An A-module M is said to be *finitely generated* if there exists finitely many elements $x_1, \ldots, x_n \in M$ such that given any $x \in M$ there exists $a_1, \ldots, a_n \in A$ such that $x = a_1x_1 + \cdots + a_nx_n$.

Example 1.1.3. For each $n \in \mathbb{N}$, the A-module $A^{\oplus n}$ is finitely generated. Indeed, it is generated by $\{e_1, \ldots, e_n\}$, where $e_j \in A^{\oplus n}$ is the ordered n-tuple of elements of A whose j-th coordinate is $1 \in A$, and all other coordinates are $0 \in A$.

Example 1.1.4. Let $f : M \to N$ be a surjective A-module homomorphism. If M is a finitely generated A-module, so is N. Indeed, if M is generated by $\{x_1, \ldots, x_n\}$ as an A-module, then N is generated by $\{f(x_1), \ldots, f(x_n)\}$ as an A-module.

Corollary 1.1.5. *An A-module M is finitely generated if and only if there exists a surjective A-module homomorphism $f : A^{\oplus n} \to M$, for some $n \in \mathbb{N}$.*

Note that, an A-submodule of a finitely generated A-module need not be finitely generated. For example, take $A = k[X_1, X_2, \ldots]$ be the polynomial ring over a field k with countably infinitely many variables $\{X_n : n \in \mathbb{N}\}$. Clearly, A is a commutative ring with identity. Let $\mathfrak{a}$ be the ideal of A generated by its variables $(X_n : n \in \mathbb{N})$. Clearly $\mathfrak{a}$ is a non-zero proper ideal of A (and hence an A-module), which is clearly not finitely generated.

Definition 1.1.6. An A-module M is said to be *noetherian* if every A-submodule of M is finitely generated. We say that A is *noetherian* if it is noetherian as a module over itself.

In particular, a noetherian A-module is a finitely generated A-module. However, the converse may not be true (see above Example).

Proposition 1.1.7. *A is noetherian if and only if every ideal of A is finitely generated.*

Proof. Since any A-submodule of A is an ideal of A, the result follows. □

Lemma 1.1.8. *Let*

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of A-modules. Then M is noetherian if and only if both M' and M'' are noetherian.

Proof. Suppose that M is noetherian. Let N' be an A-submodule of M'. Then N is isomorphic to the A-submodule $\phi(N')$ of M, and hence is finitely generated. Therefore, M' is noetherian. Let N'' be an A-submodule of M''. Then $N := \psi^{-1}(N'')$ is an A-submodule of M, and so is finitely generated. Since the A-module homomorphism $\psi|_N : N \to N''$ is surjective and N is finitely generated, N'' is finitely generated. Therefore, M'' is noetherian.

Conversely, suppose that both M' and M'' are noetherian A-modules. Let N be an A-submodule of M. Since $N' := \phi^{-1}(N)$ and $N'' := \psi(N)$ are A-submodule of noetherian A-modules, they are finitely generated. Then we have an exact sequence of A-modules

$$0 \to N' \xrightarrow{\phi} N \xrightarrow{\psi} N'' \to 0.$$

Suppose that $\phi^{-1}(N)$ and $\psi(N)$ are generated as A-modules by $x_1, \ldots, x_m \in \phi^{-1}(N)$ and $y_1, \ldots, y_n \in \psi(N)$, respectively. Fix an element $z_j \in \psi^{-1}(y_j) \subseteq N$, for each $j \in \{1, \ldots, n\}$. Let $x \in N$ be given. Then $\psi(x) = b_1y_1 + \cdots + b_ny_n$, for some $b_1, \ldots, b_n \in A$. Consider the element $w = x - (b_1z_1 + \cdots + b_nz_n) \in N$. Since $\phi(w) = 0$, there exists $a_1, \ldots, a_m \in A$ such that $w = a_1x_1 + \cdots + a_mx_m$. Then we have $x = a_1x_1 + \cdots + a_mx_m + b_1z_1 + \cdots + b_nz_n$. Therefore, N is generated as an A-module by $\{x_1, \ldots, x_m\} \cup \{z_1, \ldots, z_n\}$. Therefore, M is noetherian. □

Corollary 1.1.9. *If M and N are noetherian A-modules, so is $M \oplus N$.*

Proof. Follows from Lemma 1.1.8. □

Corollary 1.1.10. *Any finitely generated module over a noetherian ring is noetherian.*

Proof. Let A be a noetherian ring and let M be a finitely generated A-module. Then there exists a surjective A-module homomorphism

$$\varphi : A^{\oplus n} \to M,$$

for some $n \in \mathbb{N}$. Since $A^{\oplus n}$ is noetherian by Corollary 1.1.9, that M is noetherian by Lemma 1.1.8. □

Theorem 1.1.11 (Hilbert's basis theorem)**.** *If A is a noetherian ring, the polynomial ring $A[x_1, \ldots, x_n]$ is noetherian.*

Proof. Since the polynomial ring $A[x_1, \ldots, x_n]$ is isomorphic to the polynomial ring $B[x_n]$, where $B = A[x_1, \ldots, x_n]$, using induction it suffices to prove the result for $n = 1$. Consider the polynomial ring $A[x]$. Let $I \subset A[x]$ be an ideal of $A[x]$. Since the cases $I = 0$ and $I = A[x]$ are trivial, we assume that $I \neq 0$ and $I \neq A[x]$. Let

$$J = \{0\} \cup \{\text{set of all leading coefficients of non-zero polynomials in } I\}.$$

Clearly J is an ideal of A, and hence is finitely generated because A is noetherian. Let $c_1, \ldots, c_r \in A$ be non-zero elements of A that generates J as an ideal of A. Each c_j is a leading coefficient of a non-zero element, say f_j, of I. Let $J' = (f_1, \ldots, f_r)$ be the ideal of $A[x]$ generated by $f_1, \ldots, f_r$. Let $m := \max\limits_{1 \leq j \leq r} \deg(f_j)$, and let

$$M := I \cap \left(A + Ax + \cdots + Ax^{m-1}\right).$$

Then M is an A-submodule of $A[x]$. We claim that $I = M + J'$. Since both M and J' are subsets of I and I is an ideal, $M + J' \subseteq I$. To show the reverse inclusion, we need to show that every $f \in I$ is in $M + J'$. We show this by induction on $d = \deg(f)$. If $d \leq m - 1$, then $f \in M \subseteq M + J'$. Suppose that $d := \deg(f) \geq m$, and assume that for given any $g \in I$ with $\deg(g) < d$ we have $g \in M + J'$. Let c be the leading coefficient of f. Since $J = (c_1, \ldots, c_r)$ and $c \in J$, we have $c = \sum\limits_{j=1}^{r} a_j c_j$, for some $a_1, \ldots, a_r \in A$. Since $g := f - \sum\limits_{j=1}^{r} a_j x^{d-\deg(f_j)} f_j \in I$ with $\deg(g) \leq d-1$, by induction hypothesis $g \in M + J'$. Then $f = g + \sum\limits_{j=1}^{r} a_j x^{d-\deg(f_j)} f_j \in M + J'$, as required. Therefore, by induction $I = M + J'$. Since A is noetherian and $A + Ax + \cdots + Ax^{m-1}$ is a finitely generated A-module, that $A + Ax + \cdots + Ax^{m-1}$ is a noetherian A-module by Corollary 1.1.10. Since M is an A-submodule of $A + Ax + \cdots + Ax^{m-1}$, M is a finitely generated A-module, generated by, say $g_1, \ldots, g_n$. Then $I = M + J'$ is generated as an $A[x]$-module by $f_1, \ldots, f_r, g_1, \ldots, g_n$. This completes the proof. $\square$

By Hilbert basis theorem, every ideal of $A = k[x_1, \ldots, x_n]$ are finitely generated. Then every generating subset E of a finitely generated ideal $\mathfrak{a}$ of A contains a finite subset that generates the ideal $\mathfrak{a}$. Therefore, for every $E \subseteq A$, there exists finitely many elements $f_1, \ldots, f_n \in E$ such that $\mathcal{Z}(E) = \mathcal{Z}(f_1, \ldots, f_n) = \bigcap\limits_{j=1}^{n} \mathcal{Z}(f_j)$. Note that, given $E_1 \subseteq E_2 \subseteq A$, we have $\mathcal{Z}(E_2) \subseteq \mathcal{Z}(E_1)$.

Proposition 1.1.12. *The sets $\mathcal{Z}(\mathfrak{a})$, where $\mathfrak{a}$ runs over the set of all ideals of $k[x_1, \ldots, x_n]$ satisfy axioms for closed subsets for a topology on k^n, called the Zariski topology.*

Proof. The proposition follows from the following observations.

(i) $\mathcal{Z}(1) = \emptyset$ and $\mathcal{Z}(0) = k^n$;

(ii) Given any family of ideals $\{\mathfrak{a}_j : j \in I\}$ of $k[x_1, \ldots, x_n]$, we have

$$\bigcap_{j \in I} \mathcal{Z}(\mathfrak{a}_j) = \mathcal{Z}\big(\sum_{j \in I} \mathfrak{a}_j\big);$$

(iii) given any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $k[x_1, \ldots, x_n]$, we have

$$\mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\mathfrak{a} \cap \mathfrak{b}) = \mathcal{Z}(\mathfrak{a}\mathfrak{b}).$$

The first point is obvious. To see the second, note that

$$\begin{aligned}
\bigcap_{j \in I} \mathcal{Z}(\mathfrak{a}_j) &= \bigcap_{j \in I} \{x \in k^n : f(x) = 0,\ \forall\, f \in \mathfrak{a}_j\} \\
&= \{x \in k^n : f(x) = 0,\ \forall\, f \in \mathfrak{a}_j,\ \forall\, j \in I\} \\
&= \mathcal{Z}\big(\bigcup_{j \in I} \mathfrak{a}_j\big) \\
&= \mathcal{Z}\big(\sum_{j \in I} \mathfrak{a}_j\big).
\end{aligned}$$

To see the third point, note that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, which is a subset of both $\mathfrak{a}$ and $\mathfrak{b}$. Therefore, $\mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b}) \subseteq \mathcal{Z}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathcal{Z}(\mathfrak{a}\mathfrak{b})$. Conversely, if $x \in \mathcal{Z}(\mathfrak{a}\mathfrak{b})$ and $x \notin \mathcal{Z}(\mathfrak{a})$, then there exists $f \in \mathfrak{a}$ such that $f(x) \neq 0$, and for any $g \in \mathfrak{b}$ that $f(x)g(x) = (fg)(x) = 0$, since $fg \in \mathfrak{a}\mathfrak{b}$ and $x \in \mathcal{Z}(\mathfrak{a}\mathfrak{b})$. Since k is an integral domain, we must have $g(x) = 0$, for all $g \in \mathfrak{b}$. Therefore, $x \in \mathcal{Z}(\mathfrak{b})$. This completes the proof. $\square$

Definition 1.1.13. The set k^n together with the Zariski topology on it is called the *affine n-space over k* and is denoted by $\mathbb{A}^n(k)$. A closed subspace of $\mathbb{A}^n(k)$ is called an *algebraic set*.

Given a point $a = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$, consider the evaluation map

$$ev_a : k[x_1, \ldots, x_n] \longrightarrow k$$

defined by

$$ev_a(f) = f(a_1, \ldots, a_n), \quad \forall f \in k[x_1, \ldots, x_n].$$

Note that ev_a a surjective ring homomorphism with kernel

$$\mathrm{Ker}(ev_a) = \mathfrak{m}_a := (x_1 - a_1, \ldots, x_n - a_n).$$

Therefore, $\{a\} = \mathcal{Z}(\mathfrak{m}_a)$ is a closed subset of $\mathbb{A}^n(k)$. As a result, any finite subset of $\mathbb{A}^n(k)$ is an algebraic set.

Example 1.1.14. For $n = 1$, the polynomial ring $k[x]$ is a principal ideal domain. So every ideal of $k[x]$ is generated by a single polynomial. Since a polynomial in $k[x]$ has only finite number of roots in k, any closed subset of $\mathbb{A}^1(k)$ is either finite or $\mathbb{A}^1(k)$ itself.

Example 1.1.15. For $n = 2$, the situation is more complicated. Here is an obvious list of closed subsets of $\mathbb{A}^2(k)$.

- $\emptyset$ and $\mathbb{A}^2(k)$.
- any finite subset of $\mathbb{A}^2(k)$.
- $\mathcal{Z}(f)$, where $f \in k[x_1, x_2]$ is an irreducible polynomial.

In fact, we shall see later that the no-empty closed subsets of $\mathbb{A}^2(k)$ listed above are of the form $\mathcal{Z}(\mathfrak{p})$, for some prime ideal $\mathfrak{p}$ of $k[x_1, x_2]$. Moreover, any closed subsets of $\mathbb{A}^2(k)$ is a finite union of the closed subsets of the form listed above.

Connection between affine algebraic sets and commutative algebra is established by Hilbert's Nullstellensatz and its corollaries.

Theorem 1.1.16 (Hilbert's Nullstellensatz)**.** *Let K be a field that is not necessarily algebraically closed, and let A be a finitely generated K-algebra. Then A is Jacobson; i.e., every prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$ is an intersection of all maximal ideals of A containing $\mathfrak{p}$.*

$$\mathfrak{p} = \bigcap_{\mathfrak{m} \in V_{\max}(\mathfrak{p})} \mathfrak{m},$$

where $V_{\max}(\mathfrak{p})$ is the set of all maximal ideals of A containing $\mathfrak{p}$. Moreover, if $\mathfrak{m}$ is a maximal ideal of A, then $A/\mathfrak{m}$ is a finite degree field extension of K.

Before proving Hilbert's Nullstellensatz, lets discuss some of its consequences.

Corollary 1.1.17. *Let k be an algebraically closed field, and let A be a finitely generated k-algebra.*

(i) Then $A/\mathfrak{m} = k$, for every maximal ideal $\mathfrak{m}$ of A.

(ii) Let $\mathfrak{m}$ be a maximal ideal of the polynomial ring $k[x_1, \ldots, x_n]$. Then there exists $(a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ such that $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$.

Proof. (i) Since the ring homomorphism $k \to A/\mathfrak{m}$ is a finite degree field extension of k by Hilbert's Nullstellensatz (Theorem 1.1.16), $A/\mathfrak{m}$ is an algebraic field extension of k. Since k is algebraically closed, we have $k \to A/\mathfrak{m}$ is an isomorphism of rings.

(ii) Let $\mathfrak{m}$ be a maximal ideal of $k[x_1, \ldots, x_n]$. Since $k[x_1, \ldots, x_n]$ is a finitely generated k-algebra and k is algebraically closed, by part (i) the quotient $k[x_1, \ldots, x_n]/\mathfrak{m}$ is isomorphic to the field k. Note that the quotient map

$$\varphi : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/\mathfrak{m} = k$$

is a k-algebra homomorphism. For each $i \in \{1, \ldots, n\}$, let $a_i = \varphi(x_i) \in k$. Then $\varphi(x_j - a_j) = 0, \ \forall\, j \in \{1, \ldots, n\}$. Therefore, the ideal $(x_1 - a_1, \ldots, x_n - a_n)$ is contained in the maximal ideal $\mathfrak{m}$ of $k[x_1, \ldots, x_n]$. Since $(x_1 - a_1, \ldots, x_n - a_n)$ is also maximal ideal of $k[x_1, \ldots, x_n]$, it follows that $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$. □

Corollary 1.1.18. *Let k be an algebraically closed field. Let $\mathfrak{a}$ be an ideal of $k[x_1, \ldots, x_n]$, and let $\mathcal{Z}(\mathfrak{a})$ be the algebraic subset of $\mathbb{A}^n(k)$ defined by $\mathfrak{a}$. Then there is a one-to-one correspondence between the points of $\mathcal{Z}(\mathfrak{a})$ and the set of all maximal ideals of $k[x_1, \ldots, x_n]/\mathfrak{a}$.*

Proof. Let A be the quotient ring $k[x_1, \ldots, x_n]/\mathfrak{a}$. By correspondence theorem, the maximal ideals of A are in one-to-one correspondence with the maximal ideals of $k[x_1, \ldots, x_n]$ containing $\mathfrak{a}$. Let $a = (a_1, \ldots, a_n) \in \mathcal{Z}(\mathfrak{a})$ be given. Since $\mathfrak{m}_a := (x_1 - a_1, \ldots, x_n - a_n)$ is the kernel of the surjective ring homomorphism

$$ev_a : k[x_1, \ldots, x_n] \longrightarrow k$$

defined by

$$ev_a(f) = f(a), \ \ \forall\, f \in k[x_1, \ldots, x_n],$$

$\mathfrak{m}_a$ is a maximal ideal of $k[x_1, \ldots, x_n]$. Since $a \in \mathcal{Z}(\mathfrak{a})$, we have $ev_a(f) = f(a) = 0$, $\forall\, f \in \mathfrak{a}$. Therefore, $\mathfrak{a} \subseteq \mathrm{Ker}(ev_a) = \mathfrak{m}_a$. Let $\mathrm{MaxSpec}(A)$ be the set of all maximal ideals of $A = k[x_1, \ldots, x_n]/\mathfrak{a}$. Thus we get a map

$$\psi : \mathcal{Z}(\mathfrak{a}) \longrightarrow \mathrm{MaxSpec}(A)$$

defined by sending $a \in \mathcal{Z}(\mathfrak{a})$ to the maximal ideal $\overline{\mathfrak{m}_a}$ of A associated to $\mathfrak{m}_a$. Clearly ψ is injective by construction. To see ψ is surjective, note that a maximal ideal of A is given by a maximal ideal $\mathfrak{m}$ of $k[x_1, \ldots, x_n]$ containing $\mathfrak{a}$. Since k is algebraically closed, by Hilbert's Nullstellensatz (Corollary 1.1.17) we have $\mathfrak{m} = \mathfrak{m}_a$ for some $a = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$. Since $\mathfrak{a} \subseteq \mathfrak{m}_a$, given any $f \in \mathfrak{a}$, there exists $g_1, \ldots, g_n \in k[x_1, \ldots, x_n]$ such that

$f = \sum_{i=1}^{n} (x_i - a_i) g_i$. Then $f(a) = 0$. Therefore, $a \in \mathcal{Z}(\mathfrak{a})$, and hence ψ is surjective. This completes the proof. □

We now give a proof of Theorem 1.1.16 (Hilbert's Nullstellensatz). The main ingredient is Noether's normalization lemma (for a proof, see e.g. Basic Commutative Algebra book by Balwant Singh).

Definition 1.1.19. Let $\phi : A \to B$ be a ring homomorphism. An element $\beta \in B$ is said to be *integral over* A if there exists a non-constant monic polynomial $x^n + a_1 x^{n-1} + \cdots + a_n \in A[x]$ such that $\beta^n + \phi(a_1)\beta^{n-1} + \cdots + \phi(a_n) = 0$. If every element of B is integral over A, then B is called *integral* over A.

Lemma 1.1.20. *Let $\phi : A \to B$ be a ring homomorphism. Then B is a finitely generated A-algebra that is integral over A if and only if B is a finitely generated A-module.*

Theorem 1.1.21 (Noether's Normalization lemma)**.** *Let K be a field (not necessarily algebraically closed), and let $A \neq 0$ be a finitely generated K-algebra. Then there exists an integer $n \geq 0$ and $t_1, \ldots, t_n \in A$ such that the K-algebra homomorphism*

$$K[x_1, \ldots, x_n] \longrightarrow A, \quad x_j \mapsto t_j, \ \forall\, j,$$

is injective, and A is a finitely generated $K[x_1, \ldots, x_n]$-algebra that is integral over $K[x_1, \ldots, x_n]$.

To deduce Hilbert's Nullstellensatz from Noether's normalization lemma, we need the following two lemmas.

Lemma 1.1.22. *Let A and B be integral domains and let $A \to B$ be an injective ring homomorphism. If B is integral over A, then A is a field if and only if B is a field.*

Proof. Suppose that A is a field. Let $b \in B \setminus \{0\}$. Since b is integral over A, $A[b]$ is a finite dimensional A-vector space. Since B is an integral domain, the multiplication by b map

$$\mu_b : A[b] \to A[b], \ \ f(b) \mapsto bf(b)$$

is injective. Clearly μ_b is A-linear, and hence is bijective. Then $bf(b) = 1$, for some $f(b) \in A[b]$, and hence b is a unit in $A[b]$. Thus B is a field.

Conversely, suppose that B is a field. Let $a \in A \setminus \{0\}$. Let $b = a^{-1}$ in B. Since B is integral over A, there exists $a_1, \ldots, a_n \in A$ such that $b^n + a_1 b^{n-1} + \cdots + a_n = 0$. Multiplying both sides by $a^{n-1} \neq 0$ and using the fact that $ab = 1$, we see that

$$b = -(a_1 + a_2 b + \cdots + a_n a^{-1}) \in A.$$

Therefore, A is a field. □

Lemma 1.1.23. *Let K and L be a fields such that L is a finitely generated K-algebra. Then L is a finite degree field extension of K.*

Proof. Since L is a finitely generated K-algebra, by Noether's normalization lemma (Theorem 1.1.21) there exists an injective K-algebra homomorphism $\varphi : K[x_1, \ldots, x_n] \to L$ that makes L integral over $K[x_1, \ldots, x_n]$, for some integer $n \geq 0$. Since L is a field, by Lemma 1.1.22 we conclude that $n = 0$. Then L is a finitely generated K-algebra that is integral over K, and hence L is a finitely generated K-vector space. Therefore, L is a finite degree field extension of K. $\square$

Proof of Hilbert's Nullstellensatz (Theorem 1.1.16). Let A be a finitely generated K-algebra. To see the second part, let $\mathfrak{m}$ be a maximal ideal of A. Since the composite map

$$K \longrightarrow A \xrightarrow{\pi} A/\mathfrak{m}$$

is a non-zero K-algebra homomorphism, $A/\mathfrak{m}$ is a field extension of K. Since $A/\mathfrak{m}$ is a finitely generated K-algebra, it follows from Lemma 1.1.23 that $A/\mathfrak{m}$ is a finite degree field extension of K.

For the first part, we begin with the following remark. If L is a finite degree field extension of K and $\varphi : A \to L$ is a K-algebra homomorphism, the image of φ is an integral domain that is finitely generated K-vector space. Then $\varphi(A)$ is a field by Lemma 1.1.23. Therefore, $\mathrm{Ker}(\varphi)$ is a maximal ideal of A.

Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Replacing A by $A/\mathfrak{p}$, if required, it suffices to show that if A is an integral domain that is a finitely generated K-algebra then intersection of all maximal ideals of A is the zero ideal. For this we show that, given any $\alpha \in A \setminus \{0\}$ there is a maximal ideal $\mathfrak{m}$ of A such that $\alpha \notin \mathfrak{m}$. Note that, for $\alpha \neq 0$ in A, the ring $A[\alpha^{-1}] \subseteq Q(A)$ is a non-zero finitely generated K-algebra. Let $\mathfrak{n}$ be a maximal ideal of $A[\alpha^{-1}]$. Then $L := A[\alpha^{-1}]/\mathfrak{n}$ is a finite degree field extension of K by the second assertion. Then the kernel of the composite map

$$\varphi : A \to A[\alpha^{-1}] \to L$$

is a maximal ideal, say $\mathfrak{m}$, of A by above remark. Clearly $\alpha \notin \mathfrak{m}$. $\square$