

alggeo24 reading course

Matthias Frerichs

February 12, 2024

Contents

1	Hilbert basis theorem	1
2	Noether normalization theorem	4
3	Zariski topology and algebraic sets	6
4	Irreducible topological spaces	7

1 Some basic commutative algebra

This small chapter serves as a short collection on the basis theorem and the Nullstellensatz by Hilbert. This is also a collection of some commutative algebra needed to define affine varieties.

1.1 Hilbert basis theorem

Definition 1.1.1 A ring A is said to be Noetherian if it satisfies the following three equivalent conditions:

- (i) Every non-empty set of ideals in A has a maximal element.
- (ii) Every ascending chain of ideals in A is stationary.
- (iii) Every ideal in A is finitely generated.

Similarly for a R -module M we call M Noetherian if it satisfies the following three equivalent conditions:

- (i) Every non-empty set T of submodules of M has a maximal element.
- (ii) Every ascending chain of submodules of M is stationary.
- (iii) Every submodule $N \subset M$ is finitely generated.

To show the equivalence of the first two properties for rings and modules we can look at the following general result on partially ordered sets.

Proposition 1.1.2 The following conditions on a partially ordered set \mathcal{P} are equivalent:

- (i) Every increasing sequence $x_1 \leq x_2 \leq \dots$ in \mathcal{P} is stationary, i.e. there is an index $n \in \mathbb{N}$ such that for all $m \geq n$ we have $x_m = x_n$.
- (ii) Every non-empty subset of \mathcal{P} has a maximal element.

PROOF: Proposition 1.2-(i) \Rightarrow Proposition 1.2- (ii) Assume that a non-empty subset $T \subset \mathcal{P}$ and that it contains no maximal element. Then we can inductively construct an ascending sequence $(x_i)_{i \in \mathbb{N}}$ such that $x_i \leq x_{i+1}$ which is not stationary, since this would contradict the existence of a maximal element.

Proposition 1.2- (ii) \Rightarrow Proposition 1.2- (i) For an ascending sequence $(x_i)_{i \in \mathbb{N}}$ this set has a maximal element. This means that the sequence has to stabilize. \square

Now to show that the third property is also equivalent to the first two properties we just need to show that every submodule is finitely generated, as an ideal is just a special case of a submodule of the ring A considered as a module over itself.

Proposition 1.1.3 A module M over a ring A is Noetherian if and only if every submodule $N \subset M$ is finitely generated.

PROOF: Lets first consider the “if” direction. Consider a submodule $N \subset M$ and consider the set \mathcal{P} of all finitely generated submodules of N ordered by inclusion. The set \mathcal{P} is non-empty since $\{0\} \in \mathcal{P}$ and thus \mathcal{P} has a maximal element N_0 . If $N \neq N_0$ consider the submodule $N_0 \oplus \mathbf{A}x$ where $x \in N$, $x \notin N_0$. This is still finitely generated and strictly contains N_0 , which contradicts the maximality. Thus $N = N_0$ and N is finitely generated.

For the “only if” direction consider an ascending chain of submodules $T := (M_n)_{n \in \mathbb{N}}$ of M . Then the module $\cup_{n \in \mathbb{N}} M_n$ is finitely generated by assumption. Thus $T = \mathbf{A}\langle x_1, \dots, x_r \rangle$ with $x_i \in M_{n_i}$ and set $n = \max_{i=1}^r n_i$. Then each $x_i \in M_n$ and thus $M_n = M$ which means that the chain is stationary. \square

Proposition 1.1.4 *Consider a short exact sequence*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0 \quad (1.1.1)$$

then M is Noetherian if and only if M' and M'' are Noetherian.

PROOF: Consider an ascending chain of submodules $(M_n)_{n \in \mathbb{N}}$ in M . This gives rise to commutative diagrams of the form

$$\begin{array}{ccccccc} 0 & \longrightarrow & \alpha^{-1}(M_n) & \xrightarrow{\alpha} & M_n & \xrightarrow{\beta} & \beta(M_n) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \alpha^{-1}(M_{n+1}) & \xrightarrow{\alpha} & M_{n+1} & \xrightarrow{\beta} & \beta(M_{n+1}) \longrightarrow 0 \end{array} \quad (1.1.2)$$

In this diagram the rows are exact by construction and since (1.1) is exact. Now assume that M is Noetherian. Then we can pick $n \in \mathbb{N}$ big enough such that the middle inclusion is an isomorphism. Then the two other inclusions are isomorphisms as well by the five lemma. Conversely, if M' and M'' are Noetherian, we can pick n big enough such that the chains in M' and M'' have stabilized. Then, again by the five lemma, the middle inclusion is also an isomorphism. \square

Now an easy corollary of this is, that direct sums of Noetherian modules are again Noetherian.

Corollary 1.1.5 *Let M_i , $i \in \{1, \dots, n\}$ be Noetherian modules. Then $\bigoplus_{i=1}^n M_i$ is also Noetherian.*

PROOF: Equation 1.2 This is an immediate consequence of Proposition 1.4 since the sequence

$$0 \longrightarrow M_k \longrightarrow \bigoplus_{i=1}^k M_i \longrightarrow \bigoplus_{i=1}^{k-1} M_i \longrightarrow 0 \quad (1.1.3)$$

is exact, the statement follows by induction. \square

Another nice feature of finitely generated modules is, that they are quotients of \mathbf{A}^n for some $n \in \mathbb{N}$.

Proposition 1.1.6 *Let M be a \mathbf{A} -module. Then M is finitely generated if and only if it is a quotient of \mathbf{A}^n for some $n \in \mathbb{N}$.*

PROOF: Let $M = \mathbf{A}\langle x_1, \dots, x_n \rangle$ be finitely generated. Then we define a \mathbf{A} -module morphism by defining

$$\phi: \mathbf{A}^n \rightarrow M, \quad \phi(a_1, \dots, a_n) := a_1 x_1 + \dots + a_n x_n.$$

This map is obviously surjective. Conversely, if we have quotient map $\phi: \mathbf{A}^n \rightarrow M$, then M is generated by $\phi(e_i)$, where $(e_i)_j = \delta_{i,j} 1$ for $i = \{1, \dots, n\}$. \square

And last but not least we can get a nice result, that all finitely generated A -modules over a Noetherian ring are also Noetherian.

Proposition 1.1.7 *Let M be a finitely generated A -module and A Noetherian. Then M is Noetherian.*

PROOF: This proof follows immediately from Proposition 1.6 since the corresponding quotient map fits into the short exact sequence

$$0 \longrightarrow \ker(\phi) \hookrightarrow A^n \xrightarrow{\phi} M \longrightarrow 0 \quad (1.1.4)$$

from which the statement follows by Proposition 1.4. \square

Now we have all tools we need to prove Hilbert basis theorem.

Theorem 1.1.8 (Hilbert basis theorem) *See [1]. Let A be a Noetherian ring, then the polynomial ring $A[x]$ is Noetherian.*

PROOF: Consider an ideal $\mathfrak{a} \subset A[x]$. We want to show that \mathfrak{a} is finitely generated. Then, by Definition 1.1, the ring $A[x]$ would be Noetherian.

We first consider the leading coefficients of polynomials p in \mathfrak{a} yield an ideal $I \subset A$. Since A is assumed to be Noetherian, this ideal is finitely generated, i.e. $I = A\langle a_1, \dots, a_n \rangle$. Now we can pick the corresponding polynomials $f_i = a_i x^{r_i} + (\text{lower terms})$. For the ideal generated by these polynomials we get $\mathfrak{a}' := A\langle f_1, \dots, f_n \rangle \subset \mathfrak{a}$.

We want to show that $\mathfrak{a} = \mathfrak{a}'$. For this we pick some $f = ax^m + (\text{lower terms})$ for $a \in I$, i.e. $f \in \mathfrak{a}$. If $m \geq r$ for $r = \max_{i=1}^n r_i = \max_{i=1}^n \deg(f_i)$ we can write $a = \sum_{i=1}^n u_i a_i$ with $u_i \in A$, $i = 1, \dots, n$ since $a \in I$ and I is finitely generated. We can thus consider

$$f - \sum_{i=1}^n u_i f_i x^{m-r_i}.$$

This is an element in \mathfrak{a} and has degree $< m$.

We can thus write $f = g + h$ for a polynomial g with $\deg(g) < r$ and $h \in \mathfrak{a}'$.

Now consider $M = A\langle 1, x, x^2, \dots, x^{r-1} \rangle$, then we have shown that $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$. Since M is finitely generated as a A -module, it is quotient of A^n which means that it is Noetherian as well by Proposition 1.7. Since $\mathfrak{a} \cup M$ is a submodule of M it is thus also finitely generated. Finally if we have generators $\{f_i\}_{i=1, \dots, n}$ of \mathfrak{a}' and generators $\{g_i\}_{i=1, \dots, m}$ of $\mathfrak{a} \cup M$ they generate \mathfrak{a} together.

This shows that any ideal \mathfrak{a} is finitely generated, even as a A -module and hence $A[x]$ is Noetherian. \square

Corollary 1.1.9 *For a Noetherian ring A the polynomials $A[x_1, \dots, x_n]$ is Noetherian.*

PROOF: This is just an inductive application of Hilbert basis theorem on $A[x, y] = (A[x])[y]$. \square

1.2 Noether normalization theorem

In this section we prove the Noether normalization theorem. This is needed in [2, Thm 1.7] for the proof of Hilberts Nullstellensatz. Since there is a proof given for Hilberts Nullstellensatz starting from Noether normalization theorem, we will only prove the latter and state the first.

Definition 1.2.1 (Ring extension) *Consider rings A, B . Then we define the following:*

(i) *If $A \subset B$ we call B an extension ring of A . We also call $A \subset B$ a ring extension.*

- (ii) Let $A \subset B$ be a ring extension. We call $b \in B$ integral over A if there is a monic polynomial $p \in A[x] \subset B[x]$ such that $p(b) = 0$.
- (iii) For a ring extension $A \subset B$ we call B integral over A if every $b \in B$ is integral over A . In this case we say that $A \subset B$ is an integral ring extension.
- (iv) A morphism $f: A \rightarrow B$ is called integral if $f(A) \subset B$ is an integral ring extension.
- (v) A ring extension $A \subset B$ is called finite if B is finitely generated as a A -module.

Proposition 1.2.2 Let $A \subset B \subset C$ be ring extensions. Then $A \subset C$ is also an integral extension. This means that being an integral ring extension is a transitive property.

PROOF: This follows immediately from Definition 2.1. □

Lemma 1.2.3 Given a vector $a = (a_1, \dots, a_n)$ and a multiindex $\beta = (\beta_1, \dots, \beta_n)$ we set $a \cdot \beta = \sum_{i=1}^n a_i \beta_i$.

Consider a finite set of multiindices $I := \{\beta_i\}_{i=1, \dots, m} \subset \mathbb{N}_0^n$ and define

$$M_i = \max_{j=1, \dots, n} (\beta_i)_j - \min_{j=1, \dots, n} (\beta_i)_j.$$

If a fulfills $a_{i-1} > \sum_{k=i}^n M_k a_k$ for $i = 2, \dots, n$ with $a_n \geq 0$, we have the following equivalence:

$$(a \cdot \beta = a \cdot \alpha) \Leftrightarrow (\alpha = \beta) \tag{1.2.1}$$

for all $\beta, \alpha \in I$.

PROOF: Suppose that $a \cdot (\beta - \beta')$ for $\beta, \beta' \in I$. Then we have

$$a_1((\beta)_1 - (\beta')_1) = \sum_{k=2}^n a_k((\beta')_k - (\beta)_k) := \hat{a} \cdot (\hat{\beta}' - \hat{\beta})$$

for $\hat{a} = (a_2, \dots, a_n)$ and $\hat{\beta} = (\beta_2, \dots, \beta_n), \hat{\beta}' = (\beta'_2, \dots, \beta'_n)$ being the original vectors without the first component in \mathbb{R}^{n-1} and \mathbb{N}_0^{n-1} respectively.

Now we assume that $((\beta)_1 - (\beta')_1) \geq 0$, otherwise just switch the two multiindices. If $((\beta)_1 - (\beta')_1)$ is not zero we get the following by our assumption on the entries of a :

$$a_1((\beta)_1 - (\beta')_1) \geq a_1 > \sum_{k=2}^n M_k a_k \geq \sum_{k=2}^n |(\beta')_k - (\beta)_k| a_k \geq \sum_{k=2}^n ((\beta)_1 - (\beta')_1) a_k.$$

This strict inequality is a contradiction, yielding $(\beta)_1 = (\beta')_1$ since $a_1 \neq 0$. Now we can consider the vector \hat{a} with multiindices $\hat{I} = \{\hat{\beta}_i\}_{i=1, \dots, m} \subset \mathbb{N}_0^{n-1}$ and proceed inductively, since \hat{a} fulfills an analogous condition for the multiindices $\{\hat{\beta}_i\}_{i=1, \dots, m} \subset \mathbb{N}_0^{n-1}$. Thus $(\beta)_k = (\beta')_k$ for $k = 1, \dots, n$ follows. □

Definition 1.2.4 Consider a \mathbb{k} -algebra \mathcal{A} . We call a subset of elements $\{x_1, \dots, x_n\} \subset \mathcal{A}$ algebraically independent if there exists no non-zero polynomial $p \in \mathbb{k}[t_1, \dots, t_n]$ such that $p(x_1, \dots, x_n) = 0$ in \mathcal{A} holds.

In this case $\mathbb{k}\langle x_1, \dots, x_n \rangle \cong \mathbb{k}[t_1, \dots, t_n]$, i.e. the subalgebra generated by the x_i is isomorphic to a polynomial algebra.

Theorem 1.2.5 (Noether normalization theorem) *Let \mathbb{k} be a field and \mathcal{A} a finitely generated \mathbb{k} -algebra. Then there are elements $z_1, \dots, z_m \in \mathcal{A}$ such that $B = \mathbb{k}[z_1, \dots, z_m]$ is isomorphic to a polynomial ring in m variables and \mathcal{A} is integral over B . This means that \mathcal{A} is a finitely generated B -module.*

PROOF: Suppose \mathcal{A} is generated by x_1, \dots, x_n over \mathbb{k} . If the x_i are algebraically independent over \mathbb{k} , then we may take $m = n$ and $B = \mathcal{A}$.

Otherwise there is a non trivial polynomial $f = \sum_{\beta \in I_f \subset \mathbb{N}_0^n} \alpha_\beta t^\beta$ in $\mathbb{k}[t_1, \dots, t_n]$, i.e.

$$\sum_{\beta \in I_f \subset \mathbb{N}_0^n} \alpha_\beta \prod_{i=1}^n t_i^{\beta_i}$$

such that $f(x_1, \dots, x_n) = 0$. Given positive integers a_1, \dots, a_{n-1} we may define $y_i = x_i - x_n^{a_i}$ for $i < n$ and $a_n = 1$. Substituting into f and writing $\underline{a} = (a_i)_{i=1, \dots, n}$ we obtain

$$f(y_1 + x_n^{a_1}, \dots, y_{n-1} + x_n^{a_{n-1}}, x_n) = \sum_{\beta \in I_f} \alpha_\beta x_n^{\beta \cdot \underline{a}} + g(y_1, \dots, y_n) = 0. \quad (1.2.2)$$

For the set $I_f \subset \mathbb{N}_0^n$ we can choose \underline{a} as in Lemma 2.3 such that $\beta \cdot \underline{a} \neq \beta' \cdot \underline{a}$ whenever $\beta \neq \beta'$ and α_β and $\alpha_{\beta'}$ are non-zero. Thus the powers of x_n on both sides of (2.2) have to cancel and x_n is thus integral over $\mathbb{k}[y_1, \dots, y_{n-1}]$.

On the other hand $\mathbb{k}[x_1, \dots, x_{n-1}]$ is integral over $\mathbb{k}[y_1, \dots, y_{n-1}, x_n]$. Thus by the transitivity of integral extensions, see Proposition 2.2, \mathcal{A} is integral over $\mathbb{k}[y_1, \dots, y_{n-1}]$. By the induction on the number of generators on \mathcal{A} we may find $z_1, \dots, z_m \in \mathbb{k}[y_1, \dots, y_n]$ such that z_1, \dots, z_m are algebraically independent over \mathbb{k} and $\mathbb{k}[y_1, \dots, y_{n-1}]$ is integral over $\mathbb{k}[z_1, \dots, z_m]$. By transitivity of the integral extensions we get that \mathcal{A} is integral over $\mathbb{k}[z_1, \dots, z_m]$ as required. \square

Now we state Hilberts Nullstellensatz, see [2, Thm. 1.7].

Theorem 1.2.6 (Hilberts Nullstellensatz) *Let \mathbb{k} be a (not necessarily algebraically closed) field and let \mathcal{A} be a finitely generated \mathbb{k} -algebra. Then \mathcal{A} is Jacobson, i.e. for every prime ideal $\mathfrak{p} \subset \mathcal{A}$ we have*

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \supset \mathfrak{p} \\ \text{maximal ideal}}} \mathfrak{m}.$$

If $\mathfrak{m} \subset \mathcal{A}$ is a maximal ideal, the field extension $\mathbb{k} \subset \mathcal{A}/\mathfrak{m}$ is finite.

2 Algebraic varieties

We collect some basic results from the first chapter of [2].

2.1 Zariski topology and algebraic sets

Definition 2.1.1 Consider a subset $M \subset \mathbb{k}[T_1, \dots, T_n] =: \mathbb{k}[\underline{T}]$. We call define the vanishing set, or set of common zeros, of the polynomials in M by

$$V(M) := \{(t_1, \dots, t_n) \in \mathbb{k}^n \mid \forall f \in M ; f(t_1, \dots, t_n) = 0\}.$$

Definition 2.1.2 The sets $V(\mathfrak{a})$ where \mathfrak{a} runs through the set of ideals of $\mathbb{k}[\underline{T}]$, are the closed sets of a topology on \mathbb{k}^n , called the Zariski topology.

Exercise 2.1.1 Prove that this is a well defined topology, or alternatively read the proof in [2, Prop. 1.3].

Definition 2.1.3 We call the topological space $(\mathbb{k}^n, \{V(\mathfrak{a})\}_{\mathfrak{a} \text{ is ideal}})$ of the space \mathbb{k}^n with the Zariski topology the affine space of dimension n and denote it with $\mathbb{A}^n(\mathbb{k})$.

Closed subspaces of $\mathbb{A}^n(\mathbb{k})$ are called affine algebraic sets.

Sets consisting of one point $x = (x_1, \dots, x_n) \in \mathbb{A}^n(\mathbb{k})$ are closed because $\{x\} = V(\mathfrak{m}_x)$, where $\mathfrak{m}_x = (T_1 - x_1, \dots, T_n - x_n)$ is the kernel of the evaluation homomorphism $\mathbb{k}[\underline{T}] \rightarrow \mathbb{k}$ which sends f to $f(x)$. As finite unions of closed sets are again closed, we see that all finite subsets of $\mathbb{A}^n(\mathbb{k})$ are close.

Definition 2.1.4 Let A be a ring. For an ideal $\mathfrak{a} \subset A$ we call $\text{rad } \mathfrak{a} := \{f \in A \mid \exists r \text{ in } \mathbb{N}_0 \text{ such that } f^r \in \mathfrak{a}\}$ the radical of \mathfrak{a} .

If $\text{rad } \mathfrak{a} = \mathfrak{a}$ we call \mathfrak{a} a radical ideal.

Proposition 2.1.5 Let A be a ring and \mathfrak{a} an ideal.

(i) We have $\text{rad } \mathfrak{a} = \text{rad } (\text{rad } \mathfrak{a})$.

(ii) If A is finitely generated as a \mathbb{k} algebra for a field (not necessarily algebraically closed), we have

$$\text{rad } \mathfrak{a} = \bigcap_{\substack{\mathfrak{a} \subset \mathfrak{p} \subset A \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{p} = \bigcap_{\substack{\mathfrak{a} \subset \mathfrak{m} \subset A \\ \mathfrak{m} \text{ maximal ideal}}} \mathfrak{m}$$

(iii) We have $V(\text{rad } \mathfrak{a}) = V(\mathfrak{a})$.

(iv) The ring A/\mathfrak{a} is reduced, i.e. it contains no non-zero idempotent elements.

(v) Every prime ideal is radical.

Definition 2.1.6 For $Z \subset \mathbb{A}^n(\mathbb{k})$ we define the vanishing ideal of the subset Z by

$$I(Z) := \{f \in \mathbb{k}[\underline{T}] \mid \forall x \in Z \text{ we have } f(x) = 0\} \subset \mathbb{k}[\underline{T}].$$

Proposition 2.1.7 *Consider the affine space $\mathbb{A}^n(\mathbb{k})$. We have the following results:*

(i) *For a subset Z we have*

$$I(Z) = \bigcap_{x \in Z} \mathfrak{m}_x.$$

(ii) *For an ideal $\mathfrak{a} \subset \mathbb{k}[\underline{T}]$ we have*

$$I(V(\mathfrak{a})) = \text{rad } \mathfrak{a}$$

(iii) *For a subset $Z \subset \mathbb{A}^n(\mathbb{k})$ we have*

$$V(I(Z)) = \overline{Z}$$

Corollary 2.1.8 *The maps*

$$\{\text{radical ideals } \mathfrak{a} \text{ of } \mathbb{k}[\underline{T}]\} \xrightleftharpoons[I(Z) \leftrightarrow Z]{\mathfrak{a} \mapsto V(\mathfrak{a})} \{\text{closed subsets } Z \text{ of } \mathbb{A}^n(\mathbb{k})\} \quad (2.1.1)$$

are mutually inverse bijections, whose restrictions define a bijection

$$\{\text{maximal ideals of } \mathbb{k}[\underline{T}]\} \longleftrightarrow \{\text{points of } \mathbb{A}^n(\mathbb{k})\}. \quad (2.1.2)$$

2.2 Irreducible topological spaces

Definition 2.2.1 *A non-empty topological space X is called irreducible if X cannot be expressed as the union of two proper closed subsets.*

A non-empty subset Z of X is called irreducible if Z is irreducible when we endow it with the induced topology.

Proposition 2.2.2 *Let X be a non-empty topological space. The following assertions are equivalent.*

- (i) *X is irreducible.*
- (ii) *Any two non-empty open subsets of X have a non-empty intersection.*
- (iii) *Every non-empty open subset is dense in X .*
- (iv) *Every non-empty open subset is connected.*
- (v) *Every non-empty open subset is irreducible.*

Corollary 2.2.3 *Let $f: X \rightarrow Y$ be a continuous map of topological spaces. If $Z \subset X$ is an irreducible subspace, its image $f(Z)$ is irreducible.*

Bibliography

- [1] M.F. Atiyah and I.G. Macdonald. *Introduction to commutative algebra*. Vol. 1. Addison-Wesley Reading, Mass, 1969.
- [2] U. Görtz and T. Wedhorn. *Algebraic Geometry: Part I: Schemes. With Examples and Exercises*. Advanced Lectures in Mathematics. Vieweg+Teubner Verlag, 2010. ISBN: 9783834897220. URL: <https://books.google.de/books?id=XEiLudn6sq4C>.