Lecture notes for

Commutative Algebra

Jakub Paliga

January 20, 2020

1 Preface

The following is a set of personal notes that have been taken during the lecture given by dr Joachim Jelisiejew as part of a WS2019/2020 course in commutative algebra (*Algebra przemienna*) at the faculty of Mathematics, Informatics and Mechanics, University of Warsaw.

The text of these notes was compiled by Jakub Paliga, who does not guarantee their correctness and disclaims any warranties. Indeed, he confirms any deficiency within, of which there is a nonzero number, to have been introduced by him in the process.

Contents

1 Basics

1.1 Conventions

Rings will be understood to be commutative, associative, unitary; the ring "0=1" is considered a ring. Ring homomorphism are assumed to preserve the unit.

k will denote a field, $\bar{k}$ its algebraic closure. Typically, this field will be $\mathbb{C}$ - the complex numbers - but not always.

Ideals will be denoted by I and J. Ideals satisfying additional properties will be written in fraktur and named distinctly: prime ideals are $\mathfrak{p}$, $\mathfrak{q}$; maximal ideals, $\mathfrak{m}$, $\mathfrak{n}$.

1.2 First definitions

Definition 1.1. Let A be a ring. Then an *A-algebra* is a ring B together with a fixed homomorphism

$$A \to B.$$

This homomorphism is called the *structural homomorphism*.

Definition 1.2. Let A be a ring. A *homomorphism of A-algebras* is a ring homomorphism commuting with the structural maps, that is, if

$$\phi : A \to B, \quad \psi : A \to C$$

are A-algebras, then a ring homomorphism $f : B \to C$ is an algebra homomorphism if

$$\psi = f \circ \phi.$$

Example 1.3. Let $f : \mathbb{C} \to \mathbb{C}$ be given by $z \mapsto \bar{z}$ (the complex conjugation). Then:

- f is a ring homomorphism,
- f is a real algebra homomorphism,
- f is not a complex algebra homomorphism.

Example 1.4. The polynomial ring $\mathbb{C}[x]$ becomes a $\mathbb{C}$-algebra under the inclusion map onto the zero degree component.

In this case, if I is an ideal, then the quotient map

$$\mathbb{C}[x] \to \mathbb{C}[x]/I$$

is a complex algebra homomorphism.

Definition 1.5.

1. A ring A is a domain if

$$\forall a, b \in A \ \ (ab = 0 \implies a = 0 \vee b = 0.)$$

2. An ideal I in a ring B is prime if B/I is a domain.
3. A ring A is a field if
$$\forall 0 \neq a \in A \ \exists b \in A \ ab = 1,$$
that is, every nonzero element has a multiplicative inverse.
4. An ideal I in a ring B is maximal if B/I is a field.

1.3 Motivations

Lemma 1.6. Let $f : A \to B$ be a ring homomorphism. If $\mathfrak{p} \subset B$ is prime, then $f^{-1}(\mathfrak{p}) \subset A$ is prime.

Proof. Consider the following diagram.

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A/f^{-1}(\mathfrak{p}) & \longrightarrow & B/\mathfrak{p} \end{array}$$

The preimage of an ideal is an ideal. Moreover, the lower horizontal map is injective; this is elementary, using but the definition of a quotient ring and the set-theoretical properties of preimages. Hence, $A/f^{-1}(\mathfrak{p}) \subseteq B/\mathfrak{p}$ is a subring. If then $\mathfrak{p}$ is prime, $B/\mathfrak{p}$ is a domain; its every subring is then a domain as well. Thus, $A/f^{-1}(\mathfrak{p})$ is a domain, and so $f^{-1}(\mathfrak{p}) \subseteq A$ is prime. □

Example 1.7. The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ has $f^{-1}(0) = 0$ not maximal, even though $0 \in \mathbb{Q}$ is maximal. Ergo, Lemma 1.6 does not hold with "prime" replaced by "maximal".

Example 1.8. Consider

$$S^1 = \{z \in \mathbb{C} || z| = 1\}, \quad A = C(S^1, \mathbb{R}) = \{ \text{ continuous real functions on the circle } \}.$$

Then there is a bijection between S^1 and maximal ideals in A, given by every maximal ideal being of the form
$$\mathfrak{m}_x = \{f \in A \mid f(x) = 0\}.$$
Moreover, one can recover the topology of S^1 from $A = C(S^1, \mathbb{R})$.
Indeed, for $f \in A$, consider the vanishing set

$$V(f) = \{\mathfrak{m} \text{ maximal ideal in } A \ \mid f \in m\}.$$

The topology is then generated by closed subsets with subbase

$$\{V(f) \mid f \in A\}.$$

1.4 The Spec() functor

We aim to repeat the previous considerations of Example 1.8 for an arbitrary ring.

Definition 1.9. Let A be a ring. The *spectrum* of A is its set of prime ideals:

$$\text{Spec}(A) = \{\mathfrak{p} \text{ a prime ideal in} A\}.$$

Example 1.10. $\mathrm{Spec}(\mathbb{C}[x]) = \{0\} \cup \{(x-a) | a \in \mathbb{C}\}$.

For a ring homomorphism $f\colon A \to B$, Lemma 1.6 asserts that there is a map

$$f^*\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

given by

$$B \supseteq \mathfrak{q} \mapsto f^{-1}(\mathfrak{q}) \subseteq A.$$

We will now move towards upgrading spectra of rings (which up to this point we considered as mere sets) to topological spaces in such a way that makes the maps f^* continuous. In this, we follow the previous motivation.

Definition 1.11. For $E \subseteq A$ an arbitrary subset, we define the *vanishing locus of* E as the set

$$V(E) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid E \subseteq \mathfrak{p}\}.$$

Proposition 1.12. The sets $V(E)$, $E \subseteq A$, are the closed subsets of a topology.

Proof. One sees immediately that

$$V(1) = \emptyset, \quad V(0) = \mathrm{Spec}(A).$$

Elementary set-theoretic considerations reveal that

$$\cap_{i\in I} V(E_i) = V(\cup_{i\in I} E_i).$$

It now suffices to show that

$$V(E_1) \cup V(E_2) = V(E_1 \cdot E_2), \quad E_1 \cdot E_2 \coloneqq \{e_1 \cdot e_2 \mid e_1 \in E_1, e_2 \in E_2\}.$$

The inclusion $V(E_1) \cup V(E_2) \subseteq V(E_1 \cdot E_2)$ is easy to verify. Suppose without loss of generality that $\mathfrak{p} \in V(E_1)$, that is $\mathfrak{p} \supseteq E_1$. Then

$$E_1 \cdot E_2 \subseteq \mathfrak{p} \cdot E_2 \subseteq \mathfrak{p},$$

because $\mathfrak{p}$ is an ideal.

In order to prove the other inclusion, we need to use that $\mathfrak{p}$ is prime. Suppose that

$$\mathfrak{p} \not\supseteq E_1 \quad \text{and} \quad \mathfrak{p} \not\supseteq E_2.$$

Then there exist $e_i \in E_i \setminus \mathfrak{p}$, $i = 1, 2$. For those, $e_1 \cdot e_2 \in E_1 \cdot E_2 \setminus \mathfrak{p}$ holds because $\mathfrak{p}$ is prime. □

Definition 1.13. The topology on $\mathrm{Spec}(A)$ defined by Proposition 1.12 is called the *Zariski topology.*

Question 1.14. What is the Zariski topology for $A = \mathbb{C}[x]$?

Answer. We note that

$$\begin{aligned} V(f_1, \ldots, f_r) &= \{\mathfrak{p} \text{ prime in } A \mid f_1, \ldots, f_r \in \mathfrak{p}\} \\ &= \{(x-a) \text{ maximal in } A \mid f_1, \ldots, f_r \in (x-a)\} \\ &= \{(x-a) \mid f_1(a) = \ldots = f_r(a) = 0\}. \end{aligned}$$

If any f_i is nonzero, then $0 \notin V(f_1, \ldots, f_r)$.

Hence,

$$V(f_1, \ldots, f_r) = \text{ set of common roots of } f_1, \ldots, f_r$$

and one sees that $V(f_1, \ldots, f_r)$ is finite.

In fact, all finite subsets of the set of maximal ideals are of the form $V(f_1, \ldots, f_r)$. Note that the only closed set containing the prime ideal 0 is $\operatorname{Spec}(A)$ itself; in other words, 0 lies in every nonempty open set. This yields the cofinite topology augmented by $\{0\}$.

Note 1.15. Because the closure of $\{0\} \subseteq \operatorname{Spec}(A)$ is $\operatorname{Spec}(A)$ itself, the resulting space is not T1, let alone Hausdorff. It is, however, T0.

Proposition 1.16. Let $f\colon A \to B$ be a ring homomorphism. Then the induced map

$$f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A) \quad \text{with} \quad \mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$$

is continuous.

Proof. It suffices to see that the preimage of every closed set is closed. Indeed, we claim that

$$(f^*)^{-1}(V(E)) = V(f(E)).$$

We unravel the definitions:

$$\begin{aligned}(f^*)^{-1}(V(E)) &= \{\mathfrak{p} \subseteq B \mid f^*(\mathfrak{p}) \in V(E)\} \\ &= \{\mathfrak{p} \subseteq B \mid f^{-1}(\mathfrak{p}) \in V(E)\} \\ &= \{\mathfrak{p} \subseteq B \mid E \subseteq f^{-1}(\mathfrak{p})\} \\ &= \{\mathfrak{p} \subseteq B \mid f(E) \subseteq \mathfrak{p}\} \\ &= V(f(E)).\end{aligned}$$

Note that the considerations here are purely set-theoretical. The condition that f be a ring homomorphism is only relevant for f^* to be well defined on spectra. □

The upshot is: when $k = \bar{k}$, $\operatorname{Spec}_{max}(k[x_1, \ldots, x_n])$ is well-behaved. We will see later, in the Nullstellensatz, that all maximal ideals in $k[x_1, \ldots, x_n]$ are of the form $(x_1 - a_1, \ldots x_n - a_n)$.

In fact, $\operatorname{Spec}_{max}(k[x_1, \ldots, x_n]) \cong k^n$ under $(x_1 - a_1, \ldots, x_n - a_n) \mapsto (a_1, \ldots, a_n)$.

The intuition here is: $k[x_1, \ldots, x_n]$ is the ring of regular functions on k^n.

1.5 Pictures of spectra

For any I, we get

$$V(I) = \operatorname{Spec}(A/I) \hookrightarrow \operatorname{Spec}(A)$$

with a bijection:

$$\{\bar{\mathfrak{p}} \subseteq A/I\} \cong \{\mathfrak{q} \subseteq A \mid \mathfrak{q} \supseteq I\}.$$

From

$$\pi : A \to A/I$$

we get π^*, which is injective with image $V(I)$. Hence, we identify

$$\operatorname{Spec}(A/I) \quad \text{with} \quad V(I) \subseteq \operatorname{Spec}(A).$$

Example 1.17. Consider

$$\mathrm{Spec}(k[x,y]/(xy-1)) \hookrightarrow \mathrm{Spec}(k[x,y]) \supseteq \mathrm{Spec}_{\max}(k[x,y]) = k^2.$$

A point $(a,b) \in k^2$ is seen as the maximal ideal $(x-a, y-b)$; that comes from $\mathrm{Spec}(k[x,y]/(xy-1))$ if and only if $ab - 1 = 0$.

Example 1.18. $\mathrm{Spec}(k[x,y]/xy)$ gives the "cross" $\{ab = 0\}$.

Example 1.19. In the case of

$$\mathrm{Spec}(k[x,y]/(x^2+y^2+1)) \hookleftarrow \mathrm{Spec}(k[x,y]),$$

geometric interpretations transcend our $\mathbb{R}$-intuitions.

Note 1.20. In general, $\mathrm{Spec}_{\max}$ is the set of closed points in Spec, and if the ring A be of finite type (that is, finitely generated over a field or $\mathbb{Z}$), then

$$\overline{\mathrm{Spec}_{\max}(A)} = \mathrm{Spec}(A).$$

1.6 Localization

Definition 1.21. Let A be a ring. A subset $S \subseteq A$ is called *multiplicative* if the following conditions hold:

1. $1 \in S$,
2. $\forall s,t \in S \;\; st \in S$.

We wish to obtain an initial A-algebra

$$A \xrightarrow{i} S^{-1}A$$

such that the $i(s)$ are invertible; a pseudo-

$$\{\frac{a}{s} \mid a \in A, s \in S\}.$$

Indeed, in the case that A is a domain, the preceding definition is entirely satisfactory.

Construction 1.22 (localization of a ring at a multiplicative subset)**.**
Step 1. Let

$$I = \{a \in A \mid \exists s \in S \;\; sa = 0\}.$$

Note that if $a, b \in I$, then

$$\exists s \in S \;\; sa = 0, \quad \exists t \in S \;\; tb = 0.$$

Then $(st)(a \pm b) = 0$.
Upshot: I is an ideal. We let $A \xrightarrow{\pi} A/I =: A'$.
Step 2. $\pi(S) \subseteq A'$ consists of non-zerodivisors.

Indeed, suppose that $s \in S$. If $w \in A'$ is such that $w\pi(s) = 0$, then from surjectivity of π it follows that

$$\begin{aligned} \exists a \in A \quad & w = \pi(a) \\ & \pi(s)\pi(a) = 0 \\ & \implies \pi(sa) = 0 \\ & \implies sa \in I \\ & \implies \exists t \in S tsa = 0 \\ & \implies (ts)a = 0. \end{aligned}$$

But because $ts \in S$, it follows that $a \in I$ and so $\pi(a) = 0$. This means that $\pi(s)$ is not a zero divisor.

Define $S' := \pi(S)$. We want

$$(S')^{-1}A' = \{\frac{a'}{s'} \mid a' \in A', s' \in S'\}.$$

Consider pairs

$$\{(a', s') \mid a' \in A', s' \in S'\}$$

and define their relation $\sim$ thus:

$$(a'_1, s'_1) \sim (a'_2, s'_2) \iff a'_1 s'_2 = a'_2 s'_1.$$

To prove that this is an equivalence relation, we show transitivity (exercise; use that the S' are non-zerodivisors).

Step 3.

$$(S')^{-1}A' := \{(a', s') \mid a' \in A', s' \in S'\}/\sim$$

is a well defined set. The ring operations are given by thinking about this as

$$\{\frac{a'}{s'} \mid a' \in A', s' \in S'\}.$$

This turns the set into an associative commutative ring with unity.

Lemma 1.23. Let $a, b \in A$, $s, t \in S$. Then

$$\frac{a}{s} = \frac{b}{t} \quad \iff \quad \exists u \in S \;\; u(at - bs) = 0.$$

Proof. " $\impliedby$ ":

$$\begin{aligned} u(at - bs) = 0 &\implies uta = usb \\ &\implies \frac{uta}{1} = \frac{usb}{1} \\ &\implies \frac{a}{s} = \frac{uta}{stu} = \frac{usb}{stu} = \frac{b}{t}. \end{aligned}$$

" $\implies$ ": Observe that the map $\phi : A/I = A' \to (S')^{-1}A^{-1}$ is injective. Note that

$$\forall \bar{a}, \bar{b} \in A' \;\; \frac{\bar{a}}{1} = \frac{\bar{b}}{1} \iff \bar{a} = \bar{b} \iff 1 \cdot \bar{a} = 1 \cdot \bar{b}$$

□

Corollary 1.24. A model of $S^{-1}A$ is given as the quotient

$$\{(a,s) \mid a \in A, s \in S\}/\sim$$

under

$$(a,s) \sim (b,t) \quad \iff \quad \exists s \in S \;\; u(at - bs) = 0.$$

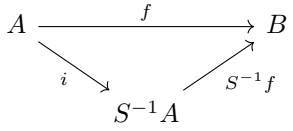
Example 1.25. For $f \in A$, let $S = \{1, f, f^2, \ldots\}$. We denote $S^{-1}A$ by A_f.

Example 1.26. $\mathfrak{p} \in \operatorname{Spec}(A)$, $S \coloneqq A \setminus \mathfrak{p}$. Then we denote $S^{-1}A$ by $A_{\mathfrak{p}}$.

Note 1.27. $S^{-1}A$ does not determine S, for instance

$$\mathbb{C}[x]_x = \mathbb{C}[x]_{x^{2019}}$$

Proposition 1.28 (universal property of localization)**.** Let $f : A \to B$ be such that $f(S)$ consists of invertible elements.



Then $\exists! S^{-1}\colon S^{-1}A \to B$ such that $f = (S^{-1}f) \circ i$.

Proof. We write $\tilde{f} \coloneqq S^{-1}f$. Suppose that $\tilde{f}$ exists. Then

$$\forall a \in A \;\; \tilde{f}(a/1) = f(a)$$

and thus

$$\forall s \in S \;\; \tilde{f}(\frac{a}{s} \cdot s) = f(\frac{a}{1}) = f(a)$$

and the formula $\tilde{f}(a/s) = f(a)/f(s)$ is recovered. One needs only to check that such a function is a homomorphism. □

Corollary 1.29. Consider the category of A-algebras whose structure maps invert S. Then Proposition 1.28 reads: $S^{-1}A$ is the initial object of this category.

Lemma 1.30. $A_f \cong A[x]/(fx - 1)$.

Proof. Note that f is invertible in $A[x]/(fx-1)$. Hence by universal property

$$\tilde{\phi}(a/f) = \phi(a)/\phi(f) = a\bar{x}.$$

Now take $\psi\colon A[x] \to A_f$ a homomorphism of A-algebras defined by $\psi(x) = 1/f$. Then

$$\psi(fx - 1) = f \cdot 1/f - 1 = 0$$

and so

$$\exists \tilde{\psi}\colon A[x]/(xf - 1) \to A_f$$

such that

$$\forall a \in A \;\; \forall n \in \mathbb{N} \;\; \tilde{\psi}(ax^n) = a/f^n.$$

The maps $\tilde{\phi}$ and $\tilde{\psi}$ are then mutual inverses. □

Corollary 1.31. A_f is a finitely generated A-algebra.

Lemma 1.32. For A an algebra and S a multiplicative subset:

1. $S^{-1}A = 0 \iff 0 \in S$
2. $A \xrightarrow{i} S^{-1}A$ is injective if and only if all elements of S are non-zerodivisors in A
3. $A \to S^{-1}A$ is an isomorphism if and only if all elements of S are invertible in A

Proof. 1. By Lemma 1.30:

$$\frac{1}{1} = \frac{0}{1} \iff \exists u \in S \;\; u(1 \cdot 1 - 0 \cdot 1) = 0 \iff \exists u \in S u = 0.$$

2. i is injective if and only if
$$(\{a \in A \mid \exists s \in S \;\; sa = 0\}).$$
This happens if and only if s is a non-zerodivisor.

3. If $A \to S^{-1}A$ is iso, then $\forall s \in S \;\; s/1$ is invertible. Hence, so is s.
Conversely, if all elements of S are invertible in A, then they are non-zerodivisors. Hence $A \to S^{-1}A$ is injective by the previous point. Moreover,
$$i(as^{-1}) = \frac{as^{-1}}{a} = \frac{a}{s},$$
so i is "onto".

□

Intuitively, we think of A_f as the ring of functions on X_f, where $X = \operatorname{Spec}(A)$.
We would expect $\operatorname{Spec}(A_f)$ to be the same as X_f. Indeed, the following holds.

Proposition 1.33. Consider the maps

$$i \colon A \to S^{-1}A$$
$$i^* \colon \operatorname{Spec}(S^{-1}A) \to \operatorname{Spec}(A).$$

Then i^* is injective and
$$\operatorname{im} i^* = \{\mathfrak{p} \mid \mathfrak{p} \cap S = \emptyset\}.$$

Before presenting the proof, for which we will require some additional facts, we note the following corollaries.

Corollary 1.34. If $S = \{1, f, f^2, \ldots\}$, then
$$\operatorname{im} i^* = \{\mathfrak{p} \mid \mathfrak{p} \not\ni f\} = (\operatorname{Spec}(A))_f.$$

Corollary 1.35. For $\mathfrak{q} \in \operatorname{Spec}(A)$, $S = A \setminus q$,
$$\operatorname{im} i^* = \{\mathfrak{p} \mid \mathfrak{p} \subseteq \mathfrak{q}\} = \operatorname{Spec}(A_p).$$

Lemma 1.36. Let $I \subseteq S^{-1}A$ be an ideal. If we let
$$J = \{a \in A \mid \frac{a}{1} \in I\},$$
then
$$I = \{\frac{j}{s} \mid j \in J, s \in S\}.$$

Proof. "$\supseteq$":

$$\forall j \in J \ \frac{j}{i} \in I \implies \frac{j}{s} = \frac{j}{1} \cdot \frac{1}{s} \in I$$

"$\subseteq$":

$$\frac{a}{s} \in I \implies \frac{a}{1} = \frac{a}{s} \cdot \frac{s}{i} \in I \implies a \in J \implies \frac{a}{s} \in \{\frac{j}{s} \mid j \in J, s \in S\}$$

□

Proposition 1.33. Let $\mathfrak{q} \in \operatorname{Spec}(S^{-1}A)$. We let

$$\mathfrak{p} = i^*(\mathfrak{q}) = i^{-1}(\mathfrak{q}) = \{a \in A \mid f \in \mathfrak{q}\}.$$

By Lemma 1.36 we can recover $\mathfrak{q}$ from $\mathfrak{p}$ alone, and so i^* is injective.

Let $\mathfrak{p} = i^*(\mathfrak{q})$. Suppose $\mathfrak{p} \cap S \neq \emptyset$. This means that

$$\frac{s}{1} \in \mathfrak{q} \text{ and } \frac{s}{t} \text{ is invertible } \implies \mathfrak{q} = (1).$$

Suppose $\mathfrak{p} \in \operatorname{Spec}(A)$, $\mathfrak{p} \cap S = \emptyset$. We wish to find $\mathfrak{q}$. We guess that

$$q \coloneqq \{\frac{p}{s} \mid p \in \mathfrak{p}, s \in S\} \subseteq S^{-1}A$$

does the job. This $\mathfrak{q}$ is an ideal, we want to see that it is prime.

Suppose that

$$\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{q}.$$

Then $ab/1 \in \mathfrak{q}$ and so □

Corollary 1.37. For $f \in A$, the following are equivalent:

1. f is nilpotent (that is, $\exists n > 0 \ \ f^n = 0$),
2. $f \in \bigcap\{\mathfrak{p} \mid p \in \operatorname{Spec}(A)\}$,
3. $V(f) = \operatorname{Spec}(A)$.

Proof. The equivalence between 2 and 3 is checked formally.

"$1 \implies 2$": $\forall \mathfrak{p} \ \ f^n = 0 \in \mathfrak{p} \implies f \in \mathfrak{p}$.

"$\neg 1 \implies \neg 2$": let $0 \notin \{1, f, f^2, \dots\}$ so $A_f \neq 0$ by Lemma 1.36. Hence, $\operatorname{Spec}(A_f) \neq \emptyset$, so by Proposition 1.33

$$\operatorname{Spec}(A_f) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid f \notin \mathfrak{p}\} \neq \emptyset.$$

□

Definition 1.38. The nilradical of a ring A is defined as

$$\operatorname{nil}(A) = \bigcap\{\mathfrak{p} \mid p \in \operatorname{Spec}(A)\} = \{f \in A \mid \exists n > 0 \ \ f^n = 0\}.$$

2 Modules

2.1 Modules

Definition 2.1. Let A be a ring. An A-module M is an abelian group M together with a ring homomorphism $A \to \mathrm{End}_{\mathbb{Z}}(M)$.

Equivalently, M is an abelian group together with a map

$$A \times M \to M, \quad (a, m) \mapsto am,$$

such that:

1. $\forall a \in A, \ \ m_1, m_2 \in M \ \ a(m_1 + m_2) = am_1 + am_2$
2. $(a_1 + a_2)m = a_1 m + a_2 m$
3. $1 \cdot m = m$
4. $a_1(a_2 m) = (a_1 a_2)m$

Definition 2.2. A homomorphism of A-modules $\phi\colon M \to N$ is a homomorphism of abelian groups such that

$$\forall a \in A \ \ \forall m \in M \ \ a\phi(m) = \phi(am).$$

Example 2.3. For A a ring, A is an A-module; in fact, any ideal $I \subseteq A$ is an A-module.

Example 2.4. For any A-algebra B, B is an A-module under the action $a.b \coloneqq f(a) \cdot b$, where f is the structural homomorphism. In particular, A/I is an A-module for any ideal $I \subseteq A$.

Definition 2.5. If M is an A-module and $m_1, \ldots, m_k \in M$ its elements, then the submodule generated by $m_1, \ldots, m_k$ is

$$Am_1 + Am_2 + \ldots + Am_k = \{\sum_{i=1}^{k} a_i m_i \mid a_i \in A\}.$$

Proposition 2.6. The set

$$\hom_A(M, N) = \{\phi : M \to N \text{ an } A\text{-module homomorphism}\}$$

is an A-module under

$$(a.\phi)(m) \coloneqq \phi(am) = a\phi(m).$$

Definition 2.7. An A-module is finitely generated if $\exists k \in \mathbb{N}, \ \ m_1, \ldots, m_k \in M$ such that

$$M = A_1 + \ldots + A_{m_k}.$$

Definition 2.8. An A-module is free if it is isomorphic to an A-module of the form

$$\bigoplus_{i \in I} A.$$

Example 2.9. All k-vector spaces are free k-modules. Not all abelian groups are free.

Lemma 2.10. An A-module M is finitely generated if and only if there exists a surjective homomorphism

$$\phi : \bigoplus_{i=1}^{k} A \to M.$$

2.2 More on modules

Note 2.11. In the following, when we write $I \cdot M$, we will mean the linear span of elements of the form $i \cdot m$.

Lemma 2.12 (adjugate matrix)**.** Let $X \in M_{n\times n}(A)$. Then

$$\exists Y \in M_{n\times n}(A) \quad \text{such that} \quad Y \cdot X = \operatorname{diag}(d), \;\; d = \det(X).$$

Concretely, Y is given by the formula

$$Y \coloneqq [(-1)^{i+j} \det X_{ji}]_{ij},$$

where X_{ij} is the submatrix of X formed by excluding the i-th row and the j-th column.

We skip the proof of Lemma 2.12.

Theorem 2.13 (Cayley-Hamilton)**.** Let M be an A-module. Let $\phi : M \to M$ be a homomorphism of A-modules such that

$$\phi(m) = IM = \{\sum i_k m_k \mid i_k \in I, m_k \in M\}.$$

Then there exist elements

$$a_{n-1} \in I, a_{n-2} \in I^2, \ldots, a_0 \in I^n$$

such that

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0 = \text{ the zero morphism.}$$

Proof. Let

$$\pi \colon A^{\oplus n} \to M \quad \text{via} \quad e_i \mapsto m_i.$$

Then

$$\forall i \;\; \exists u_{ij} \in I \;\; \phi(m_i) = \sum_j u_{ij} m_j$$

in face of the assumptions. Define the lift of ϕ to a self-map $\tilde{\phi}$ of the free module $A^{\oplus n}$ by

$$\tilde{\phi} \colon A^{\oplus n} \to A^{\oplus n} \quad \text{via} \quad \tilde{\phi}(e_i) = \sum_j u_{ij} e_j.$$

This can be fitted inside a commutative diagram

$$\begin{array}{ccc} A^{\oplus n} & \xrightarrow{\tilde{\phi}} & A^{\oplus n} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ M & \xrightarrow{\phi} & M \end{array}$$

Let $B \coloneqq A[x]$ and make $A^{\oplus n}$ into a B-module by

$$\forall f \in A^{\oplus n} \quad x.f \coloneqq \tilde{\phi}(f).$$

Now,

$$X \coloneqq [u_{ij}]_{ij} - \mathrm{diag}(x) \in M_{n\times n}(B).$$

View X as an endomorphism of $A^{\oplus n}$. Then

$$X.e_i = \sum_j u_{ij}e_j - x \cdot e_i = \sum_j u_{ij}e_j - \tilde{\phi}(e_j) = 0.$$

Hence X acts on $A^{\oplus n}$ as the zero endomorphism.
Now, use Lemma 2.12 to see that

$$\exists Y \;\; Y \cdot X = \mathrm{diag}(d).$$

Hence

$$\forall i \;\; 0 = Y \cdot X \cdot e_i = \mathrm{diag}de_i = d \cdot e_i.$$

Expand the determinant by columns:

$$d = \det(X) = x^n + a_1x^{n-1} + \ldots + a_n, \quad a_k \in I^k.$$

So as an endomorphism of $A^{\oplus n}$,

$$\tilde{\phi}^n + a_1\tilde{\phi}^{n-1} + \ldots + a_n = 0.$$

But

$$\phi \circ \pi = \pi \circ \tilde{\phi}.$$

So for all i

$$\begin{aligned}(\phi^n + a_1\phi^{n-1} + \ldots + a_n)(m_i) &= \pi((\tilde{\phi}^n + a_1\tilde{\phi}^{n-1} + \ldots + a_n)(e_i)) \\ &= \pi(0) \\ &= 0.\end{aligned}$$

□

Lemma 2.14 (Nakayama)**.** Let M be an A-module, $I \cdot M = M$. If M is finitely generated, then

$$\exists i \in I \;\; (1 - i) \cdot M = 0.$$

Proof. Consider $\mathrm{id}_M \colon M \xrightarrow{\simeq} M$. By Section 2.2,

$$\exists a_i \;\; \mathrm{id}^n + a_1\mathrm{id}^{n-1} + \ldots + a_n = 0$$

and then

$$\forall m \in M(1 + a_1 + \ldots + a_n) \cdot m = 0.$$

We now let

$$-i \coloneqq a_1 + \ldots + a_n.$$

□

Corollary 2.15 (local Nakayama)**.** Let A be a local ring, $\mathfrak{m}$ the maximal ideal of A, M an A-module, M finitely generated, $M = \mathfrak{m} \cdot M$. Then

$$M = 0.$$

Proof. Apply Lemma 2.14:

$$\exists a \in \mathfrak{m} \ (1-a) \cdot M = 0, \quad (1-a) \notin \mathfrak{m}.$$

But $(1-a)$ is invertible; let its inverse be b. Then

$$M = 1 \cdot M = b(1-a)M = b \cdot 0 = 0.$$

□

Corollary 2.16. Let $N \subseteq M$, M finitely generated, A local, $\mathfrak{m}$ maximal. Let

$$M = N + \mathfrak{m} \cdot M.$$

Then $M = N$.

Proof. Write $N + M = M = N + \mathfrak{m}M$ and so $M/N = \mathfrak{m}M/N$. By Corollary 2.15, $M/N = 0$. □

Corollary 2.17. Let M be a finitely generated A-module, $(A, \mathfrak{m})$ a local ring. Suppose

$$m_1, \ldots, m_k \in M$$

be such that their images in $M/\mathfrak{m} \cdot M$ generate $M/\mathfrak{m} \cdot M$. Then $m_1, \ldots, m_k$ generate M.

Proof. Let

$$N \coloneqq \sum_{i=1}^{k} A \cdot m_i \subseteq M.$$

Then the map

$$N \to M/\mathfrak{m} \cdot M$$

is surjective by assumption, so by Corollary 2.16:

$$M = \mathfrak{m} \cdot M + N \implies M = N = \sum_{i=1}^{k} A \cdot m_i.$$

□

Example 2.18. Consider $\mathbb{Q} \in \mathbb{Z}_{\text{mod}}$. Consider $I = (2019) \subseteq \mathbb{Z}$. Certainly $\mathbb{Q} = I \cdot \mathbb{Q}$, but there does not exist an $i \in I$ such that

$$(1-i) \cdot \mathbb{Q} = 0,$$

so $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.

Example 2.19. Another counterexample (this time local) is given by $\mathbb{Z}_{(2)}$.

Note 2.20. Localizing is a typical way of finding non-finitely generated modules.

Example 2.21. Let $X = S^1$, $A = C(S^1, \mathbb{R})$. Consider

$$\mathfrak{m}_x = \{f \mid f(x) = 0\}.$$

Then $\mathfrak{m}_x^2 = \mathfrak{m}_x$, hence $\mathfrak{m}_x$ is not a finitely generated ideal.

2.3 Tensor product

Fix A-modules M, N. We will construct their tensor product $M \otimes N$ - another A-module whose definition demands that it in some way classify "A-multiplications" with domain $M \times N$.

Definition 2.22. Let P be an A-module. A function (not a homomorphism!)

$$f\colon M \times N \to P$$

is called A-bilinear if:

1. $\forall a \in A, m \in M, n \in N \;\; af(m,n) = f(am,n) = f(m,an)$,
2. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$,
3. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$.

The set of such functions will be denoted by

$$\mathrm{Bilin}_{M\times N}(P).$$

Proposition 2.23. For a homomorphism of A-modules $\phi\colon P \to R$ one gets a map

$$\phi^*\colon \mathrm{Bilin}_{M\times N}(P) \to \mathrm{Bilin}_{M\times N}(R) \quad \text{via} \quad f \mapsto \phi \circ f.$$

Theorem 2.24. There exists a unique (up to isomorphism) pair

$$T \in A_{\mathrm{mod}}, \quad g \in \mathrm{Bilin}_{M\times N}(T)$$

such that

$$\forall P \in A_{\mathrm{mod}} \;\; \forall f \in \mathrm{Bilin}_{M\times N}(P) \;\; \exists! f'\colon T \to P \;\; f = f' \circ g.$$

Note 2.25. One can rephrase Theorem 2.24 as the existence of a natural isomorphism

$$\hom(T, -) \simeq \mathrm{Bilin}_{M\times N}(-).$$

Definition 2.26. The A-module T of Theorem 2.24 is denoted by

$$M \otimes_A N$$

and called the tensor product of M and N. The map g is written as

$$m \otimes n \coloneqq g(m,n).$$

Proof. (Theorem 2.24) Let

$$T_0 = A^{M\times N}.$$

Then

$$\forall P \;\; \hom(T_0, P) \simeq \mathrm{Set}(M \times N, P) \quad \text{via} \quad f \mapsto \sum a_i f(e_i)$$

as the free module functor is adjoint to the forgetful functor to Set. Denote the generator of T_0 corresponding to (m,n) by $e(m,n)$. Now define

$$T = T_0/\!\sim,$$

where $\sim$ describes the relations given in Definition 2.22. We now claim that T together with the quotient of e satisfies the universal property.

Uniqueness up to isomorphism does follow from this very universal property. □

Question 2.27. Do all representable functors have left adjoints?

Answer. Yes, provided the category considered has all coproducts, as then for functors into Set the two conditions are in fact equivalent; the same holds in the case of corepresentability and having a right adjoint.

Concretely, the left adjoint to a functor represented by X is given by

$$Y \mapsto \bigsqcup_Y X.$$

Note that this does not agree with our definition of a tensor product. Indeed, while the representable functors considered in this question are Set-valued, the one right adjoint to the tensor product is an endofunctor of the category of A-modules.

2.4 Localization of modules

Definition 2.28. The rank of a free module F is

$$\operatorname{rk}(F) \coloneqq \dim_{A/\mathfrak{m}}(F/\mathfrak{m}F).$$

This does not depend on the choice of $\mathfrak{m}$.

Example 2.29. $\operatorname{rk}(A^{\oplus I}) = |I|$.

Definition 2.30. Let $S \subseteq A$ be a multiplicative subset, $M \in A_{\text{mod}}$. The one forms an $S^{-1}A$-module $S^{-1}M$ analogously to $S^{-1}A$ itself. That is,

$$S^{-1}M \coloneqq \{m/s \mid m \in M, s \in S\}$$

with

$$m/s = m'/s' \iff \exists t \in S \;\; t(s'm - sm') = 0.$$

Example 2.31. If $S = \{1, f, f^2, \dots\}$, then we denote $M_f = S^{-1}M$. Analogously, for $S = A \setminus \mathfrak{p}$, we will write $M_{\mathfrak{p}} = S^{-1}M$.

Lemma 2.32. Let $S \subseteq A$ be a multiplicative subset, M an A-module. Then

$$S^{-1}A \otimes_A M \cong S^{-1}M$$

under the map

$$(a/s) \otimes m \mapsto am/s.$$

Proof. The given map $f\colon S^{-1}A \otimes M \to S^{-1}M$ is linear by the universal property of the tensor product. We show that it is an isomorphism.

1. f is "onto":
$$f(1/s \otimes m) = m/s,$$
2. f is "into": take an element
$$n \in S^{-1}A \otimes_A M.$$
We write
$$n = \sum_{k=1}^{r} a_k/s_k \otimes m_k = \sum_{k=1}^{r} \tilde{a}_k/s \otimes \tilde{m}_k.$$

If we let

$$s = \prod_{k=1}^{r} s_k,$$

we can write

$$\sum_{k=1}^{r} 1/s \otimes \tilde{a}_k m_k = 1/s \otimes (\sum_{k=1}^{r} \tilde{a}_k m_k) =: 1/s \otimes m.$$

Since any n is of the form, we may proceed as follows. Assume $0 = f(n)$; we will show $n = 0$. Have:

$$0 = f(n) = m/s \iff \exists t \in S \ \ tm = 0.$$

Then

$$n = 1/s \otimes m = 1/(st) \otimes tm = 1/(st) \otimes 0 = 0.$$

□

Corollary 2.33.

$$S^{-1}(\oplus_{i \in I} M_i) = \oplus_{i \in I} S^{-1} M_i.$$

Proof. Since the tensor product is left adjoint, it is coexact in that it commutes with colimits (essentially by Yoneda); in particular, with the direct sum. □

2.5 Exactness

Definition 2.34. Let M_i be A-modules, $i = 1, 2, 3$.

1. The sequence
$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$$
is exact if
$$\operatorname{im} f_1 = \ker f_2.$$

2. The sequence
$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$
is exact if and only if
$$M_1 \to M_2 \to M_3$$
is exact and f_2 is surjective.

3. The sequence
$$0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$
is a short exact sequence if:
   - f_1 is injective,
   - $\operatorname{im} f_1 = \ker f_2$,
   - f_2 is surjective.

Proposition 2.35 (right-exactness of the tensor product)**.** For all exact sequences

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$

and for all $N \in \mod A$, the induced sequence

$$M_1 \otimes_A N \xrightarrow{f_1 \otimes_A \mathrm{id}} M_2 \otimes_A N \xrightarrow{f_2 \otimes \mathrm{id}} M_3 \otimes N \to 0$$

is exact.

Proof. First, we need to check that

$$M_2 \otimes_A N \to M_3 \otimes_A N$$

is "onto". This is checked on elements: $M_3 \otimes_A N$ is generated by elements of the form

$$m_3 \otimes n \quad \text{such that} \quad m_3 \in M_3, n \in N.$$

The claim then follows by surjectivity of f_2 itself.

Exactness in the middle means that

$$M_2 \otimes N/(f_1 \otimes \mathrm{id})(M_1 \otimes N) \to M_3 \otimes N$$

is an isomorphism. We already checked that it is "onto"; now we need to know that there exists a section, that is, a one-sided inverse.

Have

$$M_2/f_1(M_1) \cong M_3 \times N \to M_2 \otimes_A N/(f_1 \otimes \mathrm{id})(M_1 \otimes_A N) \text{ via } (m_3, n) \mapsto \overline{m_2 \otimes n}.$$

This is bilinear if it is well-defined. Hence, it yields a map

$$s \colon M_3 \otimes_A N \to M_2 \otimes N$$

and indeed, the equality

$$s \circ \pi = \mathrm{id}_{M_3 \otimes N}$$

holds, and so π is injective and further, an isomorphism. □

Note 2.36. We have shown that

$$M_3 \cong M_2/f_1(M_1).$$

Hence, we get

$$M_2/(f_1(M_1) \otimes N \cong M_2 \otimes_A N/(f_1(M_1) \otimes_A N).$$

Example 2.37. $A/I \otimes_A N \cong N/IN$.

And in fact, quotients and localizations of modules can be computed by means of the tensor product.

Note 2.38. The notions of right-exactness as defined above in Proposition 2.35 coincide with the preserving of colimits. The definition of Proposition 2.35 is valid in the case of preadditive categories.

2.6 Fibers

In the following, we justify the hardships endured in the process of developing a theory of tensor products of modules.

Proposition 2.39. Tensoring with an A-algebra B is left adjoint to the forgetful functor

$$B_{\text{mod}} \to A_{\text{mod}}.$$

Proposition 2.40. Suppose A-algebras B, C are given. Then $B \otimes_A C$ is an A-algebra with multiplication

$$(b_1 \otimes c_1) \cdot (b_2 \otimes c_2) = (b_1 b_2) \otimes (c_1 c_2).$$

We claim that $B \otimes_A C$ is in fact the coproduct of B and C.

Note 2.41. Under application of the Spec() functor, Proposition 2.40 leads to the pullback diagram

$$\begin{array}{ccc} \operatorname{Spec}(B \otimes_A C) & \longrightarrow & \operatorname{Spec}(C) \\ \downarrow & & \downarrow \\ \operatorname{Spec}(B) & \longrightarrow & \operatorname{Spec}(A) \end{array}$$

Note that in general,

$$\operatorname{Spec}(B \otimes_A C) \neq \operatorname{Spec}(B) \times \operatorname{Spec}(C).$$

In the case that B, C are polynomial rings over the field A, this holds as an equality of sets, but not of topological spaces. Indeed, if $B = C = A[x]$, the diagonal $\{x = y\}$ is a closed subset of $\mathbb{A}^2$, while not being closed in $\mathbb{A}^1 \times \mathbb{A}^1$ (as the opposite would expose $\mathbb{A}^1$ as a Hausdorff space).

We note the following special cases of Proposition 2.40.

Corollary 2.42. Let $A = k$ a field,

$$B = k[x_1, \ldots, x_s], \quad C = k[y_1, \ldots, y_k].$$

Then

$$B \otimes_k C \cong k[x_1, \ldots, x_s, y_1, \ldots, y_t].$$

Proof. Note that B and C are free k-modules, so $B \otimes_k C$ is a free k-module with basis

$$x_1^{a_1} \otimes \ldots \otimes x_s^{a_s} \otimes y_1^{b_1} \otimes \ldots \otimes y_t^{b_t}.$$

One checks that the obvious map defined by the universal property is an isomorphism. □

Corollary 2.43. Suppose

$$B = k[x_1, \ldots, x_s]/I,$$
$$C = k[y_1, \ldots, y_t]/J.$$

Then

$$B \otimes_k C \cong k[x_1, \ldots, x_s, y_1, \ldots, y_t]/(I + J).$$

In differential geometry, the fiber $f^{-1}(x)$ of a map $f\colon X \to Y$ over a point $x \in Y$ is not typically a manifold. In contrast, in the algebraic case, we have the following.

Definition 2.44. Let $f\colon A \to B$ be a homomorphism, $\mathfrak{m} \subseteq A$ a maximal ideal. Then the *fiber* of f over $\mathfrak{m}$ is

$$B/\mathfrak{m}B.$$

Proposition 2.45. In the above setting,

$$\operatorname{Spec}(B/\mathfrak{m}B) \cong \{\mathfrak{p} \subseteq B \mid f^*(\mathfrak{p}) = \{\mathfrak{m}\}\}.$$

Recall that

$$\operatorname{Spec}(A_\mathfrak{p}) = \{\mathfrak{q} \subseteq \mathfrak{p}\}, \quad \operatorname{Spec}(A/\mathfrak{p}) = \{\mathfrak{q} \supseteq \mathfrak{p}\}.$$

Definition 2.46. More generally, if $f\colon A \to B$ is a homomorphism, $\mathfrak{p} \subseteq A$ a prime ideal, then the *fiber* of f (corresponding on the level of spectra to a fiber of f^*) over $\mathfrak{p}$ is given by

$$B \otimes_A \kappa(\mathfrak{p}),$$

where

$$\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$$

is called the *residue field*.

Proposition 2.47. For any prime ideal $\mathfrak{p} \subseteq B$, $\kappa(\mathfrak{p})$ is a field.

Note 2.48. If $\mathfrak{m}$ is maximal, then

$$\kappa(\mathfrak{m}) \cong A/\mathfrak{m}.$$

Proposition 2.49. A ring homomorphism $f\colon A \to B$ together with choice of a prime ideal $\mathfrak{p} \subseteq A$ leads to a pullback diagram

$$\begin{array}{ccc} \operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})) & \longrightarrow & \operatorname{Spec}(B) \\ \downarrow & & \downarrow{\scriptstyle f^*} \\ \operatorname{Spec}(\kappa(\mathfrak{p})) & \longrightarrow & \operatorname{Spec}(A) \end{array}$$

2.7 Derivations and Kaehler differentials

Definition 2.50. Let $R \to S$ be a ring homomorphism and M an S-module. A map of abelian groups $\mathrm{d}\colon S \to M$ is a *derivation* if it satisfies the *Leibniz formula* $\forall f, g \in S \;\; \mathrm{d}(fg) = f\mathrm{d}(g) + g\mathrm{d}(f)$. If in addition, d is a homomorphism of R-modules, it is called *R-linear*. The set of R-linear derivations $S \to M$ is then denoted by $\operatorname{Der}_R(S, M)$.

Note 2.51. That the map d of Definition 2.50 is R-linear means that $\mathrm{d}(rs) = r\mathrm{d}(s)$. Under the Leibniz rule, this is equivalent to $\mathrm{d}(R) = 0$.

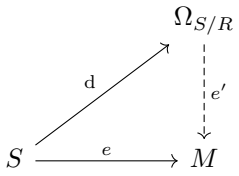
Proposition 2.52. The set $\operatorname{Der}_R(S, M)$ is an S-module under $(s.d)(f) = s.(\mathrm{d}(f))$.

Much like in the case of bilinear maps, derivations are also represented by an S-module.

Theorem 2.53. There exists an S-module $\Omega_{S/R}$ together with a k-derivation $\mathrm{d}\colon S \to \Omega_{S/R}$ such that

$$\forall M \in S_{\mathrm{mod}} \;\; \forall e \in \operatorname{Der}_R(S, M) \;\; \exists! e'\colon \Omega_{S/R} \to M \;\; e = e' \circ \mathrm{d},$$

e' being an S-module homomorphism.



Proof. Take $\Omega_{S/R}$ to be generated freely by $\{\mathrm{d}(f) \mid f \in S\}$ (that is to say, a quotient of S^S, whose S-generators are denoted by $\mathrm{d}(f)$) subject to relations

$$\forall a, a' \in R, b, b' \in S \;\; \mathrm{d}(bb') = b\mathrm{d}(b') + b'\mathrm{d}(b), \;\; \mathrm{d}(ab + a'b') = a\mathrm{d}(b') + a'\mathrm{d}(b').$$

If, as was assumed, $e\colon S \to M$ is a function, then e' must necessarily send $d(f)$ to $e(f)$, which proves uniqueness of e'. It remains to see that it is well defined (as then it is clearly an S-module homomorphism). But indeed, because e is a derivation, the map defined factors through the relations placed on free generators of $\Omega_{S/R}$. □

Note 2.54. One can rephrase Theorem 2.53 as stating the existence of an S-module isomorphism, natural in M :

$$\hom_S(\Omega_{S/R}, M) \simeq \mathrm{Der}_R(S, M).$$

Definition 2.55. The S-module $\Omega_{S/k}$ is called the module of *Kaehler differentials*.

The generators $\mathrm{d}(f), f \in S$, are frequently abbreviated as $\mathrm{d}f$.

Proposition 2.56. If S is generated as an R-algebra by elements f_i, then $\Omega_{S/R}$ is generated as an S-module by the $\mathrm{d}f_i$.

Proof. That the f_i generate S as an R-algebra means that any element $f \in S$ is equal to an R-polynomial in the f_i. But then, R-linearity together with the Leibniz formula give an S-linear formula for $\mathrm{d}f$ in terms of the $\mathrm{d}f_i$. □

Proposition 2.57. Let $S = R[x_1, \ldots, x_n]$ be a polynomial ring over R. Then $\Omega_{S/R}$ is a free S-module on n generators $\mathrm{d}x_1, \ldots, \mathrm{d}x_n$.

Proof. Consider for $i = 1, \ldots, n$ the differentiation map $\frac{\partial}{\partial x_i}\colon S \to S$. Clearly, those maps are derivations, and so is their direct sum, which is the derivation gradient

$$\nabla = (\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n})\colon S \to S^n.$$

By universal property of $\Omega_{S/R}$, an S-linear map $\partial\colon \Omega_{S/R}$ is induced, taking $\mathrm{d}x_i$ to the sequence of length n having 1 in its i-th term and only 0s elsewhere. But then ∂ is exactly the inverse of the surjection $S^n \twoheadrightarrow \Omega_{S/R}$ of Proposition 2.56. □

Note 2.58. Kaehler differentials are closely related to differential forms as known from smooth geometry, capturing their algebraic aspects.

More precisely, let M be a real smooth manifold, $A = C^\infty(M)$ - the ring of smooth functions on A. One considers the module of Kaehler differentials $\Omega_{A/\mathbb{R}}$. By Note 2.54, there is a natural isomorphism of A-modules

$$\mathrm{Der}_{\mathbb{R}}(A, A) \cong \hom_A(\Omega_{A/\mathbb{R}}, A).$$

Those adept in differential geometry will recognize $\mathrm{Der}_{\mathbb{R}}(A, A)$ as the vector fields, or global sections of the tangent bundle TM. If we should be inclined to denote, for $X \in A_{\mathrm{mod}}$, $X \coloneqq \hom_A(X, A)$, then we may well write $\Omega^*_{A/\mathbb{R}} \cong TM$. Consequently, $\Omega^*_{A/\mathbb{R}} \cong (TM)^* = T * M$ is identified with (global sections of) the cotangent bundle, its sections the differential forms on M.

It is not true that $\Omega_{A/\mathbb{R}} \to T^*M$ is an isomorphism of A-modules. It is not surjective as it only has the exact forms in its image; it is not injective, as $\mathrm{d}(e^x)$ and $e^x \mathrm{d}x$ are not equal in $\Omega_{A/\mathbb{R}}$, at least if one assumes the Axiom of Choice. [Spe]

3 Properties of rings and modules

3.1 Noetherian modules

Proposition 3.1. Let $M \in \mod A$. Then the following conditions are equivalent:

1. every submodule of M is finitely generated,
2. every sequence of submodules
$$M_1 \subseteq M_2 \subseteq \ldots \subseteq M$$
stabilises, that is,
$$\exists n_0 \in \mathbb{N} \ \forall n \geq n_0 M_n - M_{n_0},$$
3. every family of submodules of M has a maximal element with respect to inclusion.

Proof. (Proposition 3.1): The implication "2 $\implies$ 3" follows from Kuratowski-Zorn.

For "3 $\implies$ 2", take $\{M_i\}_{i\in\mathbb{N}}$ as the family in statement of 3; then the maximal element is also necessarily the one on which the sequence stabilises.

"2 $\implies$ 1": choose $N \subseteq M$ a submodule. Further, take

$$n_1 \in N \setminus \{0\}, \ \ n_2 \in N \setminus A_{n_1}, \ \ n_3 \in N \setminus A_{n_2} \oplus A_{n_3}, \ \ \ldots.$$

Either one can do this for all $k \in \mathbb{N}$ or not. In the latter case, N is necessarily finitely generated. In the former, we get the sequence

$$A_{n_1} \subseteq A_{n_1} + A_{n_2} \subseteq A_{n_1} + A_{n_2} + A_{n_3} \subseteq \ldots$$

that does not stabilize.

"1 $\implies$ 2": take a sequence
$$M_1 \subseteq M_2 \subseteq \ldots;$$
we want to stabilise it. To that end, consider

$$N = \bigcup_{n\in\mathbb{N}} M_n.$$

Since the sequence is increasing, this is a submodule of M.

By 1, this is finitely generated, and by a finite set of elements from N. Then this very set is already contained in one of the M_k, and then for $n > k$, $M_n = M_k$. □

Definition 3.2. An A-module M is called Noetherian if it satisfies the equivalent conditions of Proposition 3.1.

Definition 3.3. A ring A is Noetherian if and only if the A-module A is Noetherian.

Proposition 3.4. Let A be a ring. The following conditions are equivalent:

1. A is Noetherian,

2. every ideal of A is finitely generated,
3. every prime ideal of A is finitely generated.

■

The implication "3 $\implies$ 1" of Proposition 3.4 is due to Cohen, 1950.

Proposition 3.5. Let $N \subseteq M$ be A-modules. Then the following conditions are equivalent:

1. M is Noetherian,
2. N and M/N are Noetherian.

Proof. We start with "1 $\implies$ 2". First, we show that N is Noetherian; indeed, if

$$N_1 \subseteq N_2 \subseteq \ldots \subseteq N \subseteq M$$

is a sequence of submodules of N, it is also a sequence of submodules of M and the claim follows.

To show that M/N is Noetherian, consider a sequence of submodules

$$P_1 \subseteq P_2 \subseteq M/N.$$

If then $\pi\colon M \to M/N$ denotes the quotient map, then the sequence

$$\pi^{-1}(P_1) \subseteq \pi^{-1}(P_2) \subseteq \ldots \subseteq M$$

stabilizes, and since π is surjective, we have

$$\pi(\pi^{-1}(P_n)) = P_n,$$

ending the proof of "1 $\implies$ 2".

For "2 $\implies$ 1", pick a sequence of submodules

$$M_1 \subseteq M_2 \subseteq \ldots \subseteq M$$

and define

$$N_k = M_k \cap N, \quad P_k = \pi(M_k).$$

The sequences defined by the N_k and P_k stabilize, say at common n_0.

We will show that

$$\forall n > n_0 \;\; M_n = M_{n_0}.$$

First, show $M_n \subseteq M_{n_0}$. Take $m \in M_n$, then

$$\pi(m) \in P_n = P_{n_0} = M_{n_0}/\ker \pi \cap M_{n_0}$$

Pick $\tilde{m} \in M_{n_0}$ such that $\pi(m) = \pi(\tilde{m})$. Then we have

$$m - \tilde{m} \in \ker(\pi) \cap M_n = N_n = N_{n_0} \subseteq M_{n_0}.$$

Since $m - \tilde{m} \in M_{n_0}$, we have that in fact

$$m = \tilde{m} + m - \tilde{m} \in M_{n_0}$$

and the claim follows since m was arbitrary in M_n. □

Note that this translates to the claim that in the short exact sequence

$$0 \to N \to M \to M/N \to 0$$

the middle term is Noetherian if and only if the other ones are.

Corollary 3.6. If A is a Noetherian ring, then all finitely generated A-modules are Noetherian.

Proof. First, we show that all finitely generated free modules are Noetherian. This follows easily by induction since we get short exact sequences

$$0 \to A \to A^{\oplus n} \to A^{\oplus(n-1)} \to 0.$$

If then K is a finitely generated A-module, say generated by k elements, we get a short exact sequence

$$0 \to \ker \alpha \to A^{\oplus k} \xrightarrow{\alpha} K \to 0,$$

and the claim follows from Proposition 3.5 again. □

Example 3.7. Some Noetherian rings include:

1. fields,
2. principal ideal domains (e.g. $\mathbb{Z}$, $k[x]$, $\mathbb{Z}[x]$).

Theorem 3.8 (Hilbert basis theorem)**.** If A is Noetherian, then

$$A[x_1, \ldots, x_n]$$

is also a Noetherian ring.

Note the difference: when considered as a $\mathbb{C}$-module, $\mathbb{C}[x]$ is not Noetherian, as it is not finitely generated. However, Theorem 3.8 states that as a module over itself, it is Noetherian.

Corollary 3.9. If A is Noetherian and B is a finitely generated A-algebra, then B is also Noetherian.

Proof. Immediate, since

$$B = A[x_1, \ldots, x_n]/I.$$

□

Question 3.10. Are tensor products of Noetherian modules also Noetherian?

Answer. No, since

$$\bar{\mathbb{Q}} \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$$

is not Noetherian. In fact,

$$\operatorname{Spec}(\bar{\mathbb{Q}} \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}) \simeq \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

is a natural isomorphism of sets (and not of groups).

Lemma 3.11. If the ring A is Noetherian, then so is A/I for all ideals $I \subseteq A$.

Lemma 3.12. If A is Noetherian, then for any multiplicative subset $S \subseteq A$, the localization $S^{-1}A$ is also Noetherian.

Proof. Consider $I \subseteq S^{-1}A$, $J = i^{-1}(I) \subseteq A$. Write

$$I = \{\frac{j}{s} \mid j \in J, s \in S\}.$$

The ideal $J \subseteq A$ is finitely generated, say

$$J = A(j_1, \dots, j_r).$$

Then

$$\forall j \in J \ \exists a_1, \dots, a_r \ \ j = \sum_{k=1}^{r} a_k j_k.$$

We then have

$$\frac{j}{s} = \sum_{k=1}^{r} \frac{a_k}{s} \cdot \frac{j_k}{1},$$

and so I is generated by

$$\frac{j_1}{1}, \dots, \frac{j_r}{1}.$$

□

Note that we have used the previous characterization of Proposition 3.1; indeed, as the submodules of a ring are exactly the ideals.

Proof. (Hilbert basis theorem) Let $I \subseteq A[x]$. Write

$$J = \{a \in A \mid \exists f \in I \ \ f = ax^n + a_1 x^{n-1} + \dots\},$$

that is, J is the set of polynomials with leading term ax^n.

One claims that J is an ideal: indeed, let $j_1, j_2 \in J$. Put

$$r = j_1 - j_2.$$

If $r = 0$, we are done; in the other case, proceed. Take $f_1, f_2 \in I$ with leading term $f_i = j_i x^{n_i}$. Then the leading term of

$$x^{n_2} f_1 - x^{n_1} f_2$$

is

$$(j_1 - j_2) x^{n_1 + n_2}.$$

Hence, J is an abelian subgroup.

If $j \in J, a \in A$, and so J is an ideal.

Since $J \subseteq A$ is an ideal of a Noetherian ring, it is finitely generated, say by elements

$$j_1, \dots, j_r.$$

One then has

$$\exists f_1, \dots, f_r \in I$$

with leading terms of f_i equal to $j_i x^{n_i}$.

If we let $n = \max(n_i)$, one can modify the f_i to get leading term $f_i = j_i x^n$.

Let

$$SP = I \cap A[x]_{<n}.$$

This is not an ideal, but an A-module; it is isomorphic to $A^{\oplus n}$, and so finitely generated, we write

$$SP = Ag_1 + \ldots + Ag_t.$$

We claim that

$$I = (f_1, \ldots, f_r, g_1, \ldots, g_t)$$

as an ideal in $A[x]$.

Clearly,

$$I \supseteq (f_1, \ldots, f_r, g_1, \ldots, g_t).$$

For the other inclusion, we pick $h \in I$ and proceed by induction on degree.

Write the leading term of h as

$$bx^{\deg(h)}.$$

Now, if $\deg(h) < n$, h must necessarily be an element of SP.

In the other case,

$$\deg(h) \geq n$$

and we can divide with remainder. Write

$$b = \sum_{s=1}^{r} a_s j_s$$

and consider

$$h' = h - \sum a_s f_s x^{\deg(h)-n}.$$

Then

$$\deg(h') < \deg(h) \implies h' \in (f_1, \ldots, f_r, g_1, \ldots, g_t)$$

and so also

$$h \in (f_1, \ldots, f_r, g_1, \ldots, g_t).$$

This ends the proof. □

3.2 Finite and integral ring extensions

Consider B an A-algebra.

Definition 3.13. An element $b \in B$ is *integral* over A if

$$\exists a_{n-1}, \ldots, a_0 \in A \;\; b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0.$$

B is integral over A if all its elements are integral over A.

Definition 3.14. An A-algebra B is *finite* over A if it is finitely generated as an A-module, that is,

$$\exists b_1 \ldots, b_k \;\; B = Ab_1 + \ldots + Ab_k.$$

Example 3.15. The following hold:

1. $\mathbb{Z} \to \mathbb{Z}[i]$ is finite,
2. $\mathbb{Z} \to \mathbb{Z}/n$ is finite,
3. more generally, $A \to A/I$ is finite,

4. $\mathbb{Z} \to \mathbb{Z}[x]$ is not finite.

Lemma 3.16. If $A \to B$ is finite, then it is integral.

Proof. Let $b \in B$ and consider the multiplication map

$$\phi\colon B \to B, \quad \phi(a) = a \cdot b.$$

This is an A-module homomorphism. By Cayley-Hamilton with $I = (1)$, one has

$$\exists a_{n-1}, \ldots, a_0 \in A \;\; b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0.$$

□

Lemma 3.17. If $A \to B$ is integral and B is a finitely generated A-algebra, then $A \to B$ is finite.

Proof. Let

$$B = A[x_1, \ldots, x_n]/I.$$

Then every $x_i \in B$ is integral over A and so

$$\exists n \;\; \forall i \;\; \exists a_0^{(i)} \;\; x_i^n + a_{n-1}^{(i)} + \ldots + a_0^{(i)} = 0.$$

We check that B is generated as an A-module by the finitely many monomials

$$\{x_1^{c_1}, \ldots, x_n^{c_n}, 0 \leq c_i \leq n\}.$$

□

Example 3.18. The extension

$$\mathbb{Q} \to \bar{\mathbb{Q}}$$

is integral, but not finite.

Definition 3.19. For B and A-algebra, $b \in B$ an element, $A[b]$ will denote the smallest A-algebra contained in B and containing $b \in B$.

Proposition 3.20. Let $A \to B$ be an A-algebra, $b \in B$. The following conditions are equivalent:

1. v is integral over A,
2. $A[b]$ is a finitely generated A-module,
3. $A[b]$ is contained in a finitely generated A-module.

Proof. "1 $\implies$ 2 $\implies$ 3" is formal: the first one uses the same trick as in Lemma 3.17.
For "3 $\implies$ 1, fix a finitely generated A-module $A[b] \subseteq C$. Then the multiplication map

$$\phi_b\colon C \to C$$

is an $A-$module homomorphism, so Cayley-Hamilton implies

$$\exists n \exists a_{n-1}, \ldots, a_0 \in A \;\; b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0.$$

□

Definition 3.21. Let B be an A-algebra. Then the *integral closure* of A in B is

$$\bar{A} = \{b \in B \mid b \text{ is integral in } A\}.$$

The *normalization* of a domain A is its integral closure in the field of fractions $\mathrm{Frac}(A)$.

Corollary 3.22. $\bar{A}$ is an A-algebra.

Proof. Consider $x, y \in \bar{A}$. By Proposition 3.20, $A[x]$ and $A[y]$ are finitely generated A-modules. In fact, by the proof of Lemma 3.17, $A[x, y]$ is a finitely generated A-module.

One has

$$A[x - y] \subseteq A[x, y], \quad A[xy] \subseteq A[x, y],$$

so by Proposition 3.20, point 3,

$$x - y, xy \in \bar{A}.$$

Hence, $\bar{A}$ is a ring. One has also the map

$$A \to \bar{A}$$

which makes $\bar{A}$ an A-algebra; indeed, an A-subalgebra of B. □

Example 3.23. Let $\mathbb{Z} \to \mathbb{Q} \to K$ with $\mathbb{Q} \to K$ finite. Then one has also

$$O_K = \bar{Z} \to K$$

- the ring of algebraic integers in K. This is Noetherian.

Theorem 3.24 (Nagata)**.** If A is finitely generated over k, then the normalization of A is as well. Moreover,

$$A \to \bar{A}$$

is finite.

3.3 Further properties of integral extensions

Recall that we have talked about the fiber and noted an isomorphism of A-algebras $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ and $\mathrm{Frac}(A/\mathfrak{p})$; we denoted this result by $\kappa(\mathfrak{p})$.

As motivation for the following, consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{\text{integral}} & B \\ \downarrow & & \downarrow \\ A/\mathfrak{p} & \xrightarrow{\text{integral}} & B/\mathfrak{q} \end{array}$$

with $\mathfrak{p}$, $\mathfrak{q}$ prime.

Lemma 3.25. Let $f\colon A \hookrightarrow B$ be an integral extension and let f be injective. Suppose that A and B are domains. Then A is a field if and only if B is a field.

Proof. Assume that A is a field. Take $0 \neq b \in B$ and minimum n such that

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

Then a_0 cannnot be zero since n is minimal. Thus, it is invertible (as A is a field). One can then write

$$b(b^{n-1} + \cdots + a_2 b + a_1) = -a_0,$$

so that b is invertible. Hence, A is a field.

Conversely, supose B is a field. Let $a \in A \setminus \{0\}$, so that for some $b \in B$, $ab = 1$ holds. Let

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

and multiply both sides by a^{n-1}. We then have

$$b(ab)^{n-1} + a_{n-1}(ab)^{n-1} + \cdots + a_1(ab)a^{n-2} + a_0 a^{n-1} = 0.$$

Thus, for some $a' \in A$, one has $b + a = 0$. Thus $b \in A$ and so a is invertible in A. □

Proposition 3.26. Suppose $f\colon A \hookrightarrow B$ is integral with f injective. Then

$$f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$$

is surjective.

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(A)$, $S = A \setminus \mathfrak{p}$. An exercise shows that

$$S^{-1}f\colon S^{-1}A \hookrightarrow S^{-1}B$$

is integral and injective. In particular, $S^{-1}B$ is nonzero. Thus, there exists a maximal ideal $\mathfrak{m} \subseteq S^{-1}B$. If we now let $\mathfrak{p}'$ be the preimage of $\mathfrak{p}$, then by Lemma 3.25, $S^{-1}A/\mathfrak{p}'$ is a field.

In particular, $A_\mathfrak{p} = S^{-1}A$ has only one maximal ideal $\mathfrak{p}A_\mathfrak{p}$ and we get $\mathfrak{p}' = mathfrakpA_\mathfrak{p}$.

If we now tahe $\mathfrak{m} \subseteq B$ to be the preimage of $\mathfrak{m} \subseteq S^{-1}B$, then $f^*(\mathfrak{m}) = \mathfrak{p}$. □

Note 3.27. For $f\colon A \to A/\mathfrak{p}$ integral, $\operatorname{Spec}(A) \leftarrow \operatorname{Spec}(A/\mathfrak{p}$ is not usually surjective.

Proposition 3.28 (incomparability)**.** Suppose $f\colon A \to B$ is integral, $\mathfrak{p} \in \operatorname{Spec}(A)$. Let $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, $\mathfrak{q}_i \in \operatorname{Spec}(B)$ such that $f^*(\mathfrak{q}_1) = f^*(\mathfrak{q}_2) = \mathfrak{p}$. Then $\mathfrak{q}_1 = \mathfrak{q}_2$.

Proof. Take $D \coloneqq \kappa(\mathfrak{p}) \otimes_A B$. Consider the integral extensions

$$\kappa(\mathfrak{p}) \to D \to D/\mathfrak{q}_i D.$$

By Lemma 3.25, from $\kappa(\mathfrak{p})$ being a field it follows that $D/\mathfrak{q}_i D$ is also a field, and hence $\mathfrak{q}_i D \subseteq D$ is maximal. But $\mathfrak{q}_1 D \subseteq \mathfrak{q}_2 D$ and so $\mathfrak{q}_1 D = \mathfrak{q}_2 D$.

Then the claim follows, as $\mathfrak{q}_i = g^{-1}(\mathfrak{q}_i D)$, where $g\colon B \to D$ is the natural map. □

3.4 Krull dimension

Definition 3.29. Let A be a ring. A *chain of prime ideals* in A is a sequence of proper inclusions

$$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_s$$

of prime ideals.

The *length* of such a chain is the number of those inclusions, that is, a number smaller by one than the number of ideals in the chain.

Definition 3.30. The *Krull dimension* of A is

$$\dim A = \sup\{ \text{ length of a chain of prime ideals in } A\}.$$

Example 3.31.

1. If k is a field, then $\dim k = 0$.
2. If A is a principal ideal domain, then $\dim A = 1$, since nonzero prime ideals are maximal.

The following result is more difficult to prove.

Theorem 3.32. If k is a field, then

$$\dim(k[x_1, \ldots, x_n]) = n.$$

A chain of length n is given as

$$(0) \subseteq (x_1) \subseteq (x_1, x_2) \subseteq \ldots \subseteq (x_1, \ldots, x_n).$$

However, $k[x_1, \ldots, x_n]$ has many more prime ideals than those.

Example 3.33. Let $f = x_n^3 + x_n^2 x_1$. One can take $x_i' = x_i$ for $i = 1, 2, \ldots, n-1$. Then

$$x_n^3 + x_1' x_n^2 - f = 0$$

and the extension $k[x_1', \ldots, x_{n-1}', x_n \cdot f] \subseteq k[x_1, \ldots, x_n]$ is finite.

This approach can be extended in a way allowing us to prove Theorem 3.32.

Lemma 3.34 (Nagata's trick)**.** Let $f \in S = k[x_1, \ldots, x_n]$, $f \notin k$. Then there exist

$$x_1', \ldots, x_{n-1}' \in S$$

such that

$$k[x_1', x_2', \ldots, x_{n-1}' \cdot f] \subseteq k[x_1, \ldots, x_n]$$

is a finite extension.

Proof. Fix $e > \deg(f)$ and assume without loss of generality that x_n appears in f. Consider a k-algebra homomorphism

$$\phi \colon S \to S \quad \text{via} \quad x_i \mapsto x_i - x_n^{e^{n+1-i}}, \;\; x_n \mapsto x_n.$$

We claim that ϕ is an isomorphism with inverse

$$\phi^{-1} \colon S \to S \quad \text{via} \quad x_i \mapsto x_i + x_n^{e^{n+1-i}} \;\; x_n \to x_n.$$

Moreover, $\phi(f) = \pm x_n^D +$ monomials of a smaller total degree.

Indeed, one sees that distinct monomials are mapped by ϕ to polynomials with different top degree of x_n. More specifically, if $m = x_1^{a_1} \cdot \cdots \cdot x_n^{a_n}$ is such that $a_n > 0$ and m is lexicographically the greatest possible of all monomials in f, then

$$D = \sum_{i=0}^{n} a_i e^{n-i}.$$

The process is akin to coding the variables in base e, and our claim is that decoding remains possible.

One takes $x_i' = \phi^{-1}(x_i)$. Then all x_i are integral over $k[x_1', \dots, x_{n-1}', \phi(f)$. One may look at the diagram

$$\begin{array}{ccc} k[x_1, \dots, x_{n-1}, \phi(f)] & \xrightarrow{\text{integral}} & k[x_1, \dots, x_n] \\ \downarrow{\scriptstyle \phi^{-1}} & & \downarrow{\scriptstyle \phi^{-1}} \\ k[x_1', \dots, x_{n-1}', f] & \longrightarrow & k[x_1, \dots, x_n] \end{array}$$

The horizontal inclusions are integral, and because B is finitely generated over A, the extension must be finite by Lemma 3.17. □

Proposition 3.35. If $A \hookrightarrow B$ is integral, then $\dim A = \dim B$.

Proof. First, we show $\dim A \leq \dim B$. Take a chain of prime ideals in A

$$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \dots \subseteq \mathfrak{p}_s.$$

We will lift it to a chain in B. We shall proceed by induction:

- The base case follows from surjectivity of $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$.
- For the induction step, consider a partial lift

  $$\mathfrak{q}_0 \subseteq \dots \subseteq \mathfrak{q}_k.$$

  We wish to find $\mathfrak{q}_{k+1}$ such that $\mathfrak{q}_{k+1} \cap A = \mathfrak{p}_{k+1}$. Consider $A/\mathfrak{p}_k \to B/\mathfrak{q}_k$; this is injective, and so it is surjective by . Then one picks a preimage of p_{k+1} in $B/\mathfrak{q}_k$.

For $\dim A \geq \dim B$, take

$$\mathfrak{q}_0 \subseteq \dots \subseteq \mathfrak{q}_s$$

a chain in B; take $p_i = \mathfrak{q}_i \cap A$. Then

$$\mathfrak{p}_0 \subseteq \dots \subseteq \mathfrak{p}_s$$

is a chain in A, as if $\mathfrak{p}_i = \mathfrak{p}_{i+1}$, $\mathfrak{q}_i \cap A = \mathfrak{q}_{i+1} \cap A$ and then by incomparability $\mathfrak{q}_i = \mathfrak{q}_{i+1}$. □

Proof. (Theorem 3.32) Proceed by induction on n. Base $n = 0$ is fine.

Now assume that we have shown the claim for $n-1$ want to prove for n. Suppose that this is false, and so we get a chain of length $n+1$. For $i \geq 1$, pick $f \in \mathfrak{p}_i$. Use Nagata's trick to get a finite extension

$$A = k[x_1', \dots, x_{n-1}' \cdot f] \subseteq k[x_1, \dots, x_n].$$

Take a preimage of a chain on the right side in the left side. Consider a quotient map

$$k[y_1, \dots y_{n-1}] \to k[x_1', \dots, x_n' \cdot f]/(f).$$

Put $\bar{\mathfrak{q}}_i = \mathfrak{q}_i/f$. If we let $\mathfrak{r}_i$ to be the preimage of $\bar{\mathfrak{q}}_i$ in $k[y_1, \dots, y_{n-1}]$, then $\mathfrak{r}_1 \subseteq \mathfrak{r}_2 \subseteq \dots \subseteq \mathfrak{r}_{n+1}$ is a chain of length n, in contradiction of the inductive assumption. □

Corollary 3.36. If $A = k[x_1, \dots, x_d]/I$ with $I \neq 0$, then $\dim(A) < d$.

Proof. Suppose $\dim(A) \geq d$. Choose a chain of prime ideals

$$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_d$$

in A and consider their preimages in $k[x_1, \ldots, x_d]$, that is,

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ldots \subseteq \mathfrak{q}_d.$$

This is again a chain of prime ideals. Then by considering I one gets a chain of length $d+1$ in $k[x_1, \ldots, x_d]$, contradicting Theorem 3.32. □

Example 3.37. Take $A = k[x_1, \ldots, x_d]/(f)$. What is the dimension of A?

1. $f = 0 \implies \dim(A) = d$,
2. $f \in k \setminus 0 \implies A = 0$, whose dimension may be taken to be -1 or $-\infty$,
3. If $f \notin k$, then by Nagata's coordinate change there exists a finite extension

   $$k[x_1', \ldots, x_{d-1}', f] \subseteq k[x_1, \ldots, x_d].$$

   Now, $k[x_1', \ldots, x_{d-1}', f]$ is a polynomial ring, since its dimension is d and thus Corollary 3.36 implies that there are no relations.

   Because of this, there exists a chain

   $$0 \subseteq (f) \subseteq (f, x_1') \subseteq (f, x_1', x_2') \subseteq \ldots \subseteq (f, x_1', x_2', \ldots, x_{d-1}')$$

   Now, by Proposition 3.35 this chain lifts to a chain

   $$0 \subseteq \mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_{d-1}.$$

   Because $f \in \mathfrak{p}_0$, we get a chain in $k[x_1, \ldots, x_n]/(f)$, giving the dimension of $k[x_1, \ldots, x_d]/(f)$ as $d-1$.

Proposition 3.38. If $I \subseteq k[x_1, \ldots, x_d]$ and $x_d \in I$, then

$$k[x_1, \ldots, x_d]/I \cong k[x_1, \ldots, x_d]/I \cap k[x_1, \ldots, x_{d-1}].$$

3.5 Noether Normalization

Theorem 3.39. (Noether normalization; cf. [Eis95, §13]) Let A be a finitely generated k-algebra. Assume that A is a domain. Consider

$$\mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_m$$

a chain in A. Then, there exists a finite extension

$$k[x_1, \ldots, x_d] \subseteq A, \quad \dim(A) = d, \quad \dim(A/\mathfrak{p}_i) =: d_i,$$

such that

$$\forall i \;\; \mathfrak{p}_i \cap k[x_1, \ldots, x_d] = (x_{d_i+1}, x_{d_i+2}, \ldots, x_d)$$

and with $k[x_1, \ldots, x_{d_i}] \subseteq A/\mathfrak{p}_i$ a finite extension.

Intuitively, this lets us think of ideals in a chain as if they were exactly the planes, curves and points, with their respective interplay preserved by a "coordinate map", leading from the variety into an affine space of equal dimension. That the algebraic extension is finite corresponds to fibers of this morphism being finite.

Note 3.40. In the case that the prime ideal chain consists only of the zero ideal, Theorem 3.39 states that A is a finite extension of a polynomial ring.

Theorem 3.41 (weak Nullstellensatz)**.** If A is a finitely generated k-algebra, $\mathfrak{m} \subseteq A$ a maximal ideal, then $k \hookrightarrow A/\mathfrak{m}$ is finite. In particular, if $k = \bar{k}$, then $k \cong A/\mathfrak{m}$.

Proof. Since $A/\mathfrak{m}$ is a finitely generated k-algebra, we have $\dim(A/\mathfrak{m}) = 0$. Apply Theorem 3.39 to get a finite extension $k[x_1, \ldots, x_d] \subseteq A/\mathfrak{m}$ wth $\dim(A/\mathfrak{m}) = 0$. Then $k \subseteq A/\mathfrak{m}$ is finite. Suppose that $k = \bar{k}$. Should $k \hookrightarrow A/\mathfrak{m}$ not be an equality, then there exists $\alpha \in A/\mathfrak{m} \setminus k$ together with its minimal polynomial over k :

$$\alpha^r + k_{r-1}\alpha^{r-1} + \ldots + k_0 = 0, \quad k_i \in k.$$

By Bezout, there exists a $\beta \in k$ such that

$$\beta^r + k_{r-1}\alpha^{r-1} + \cdots + k_0 = 0.$$

Then

$$\alpha^r + k_{r-1}\alpha^{r-1} + \cdots + k_0 = (\alpha - \beta)(\ldots) = 0.$$

Either $\alpha = \beta$ or $(\ldots)$ is satisfied. □

Corollary 3.42. If k is algebraically closed, then $\mathrm{Spec}_{max}(k[x_1, \ldots, x_d]) = k^d$.

Proof. Take $\mathfrak{m} \subseteq k[x_1, \ldots, x_d]$ a maximal ideal. By Theorem 3.41, the map $k \to k[x_1, \ldots, x_d]/\mathfrak{m}$ is an isomorphism. If one considers the quotient map $k[x_1, \ldots, x_d] \twoheadrightarrow k[x_1, \ldots, x_d]/\mathfrak{m}$, this means that $\forall x_i - \alpha_i \in \mathfrak{m}$ and so $(x_1 - \alpha_1, \ldots, x_d - \alpha_d) \subseteq \mathfrak{m}$. Since both ideals are maximal, there must be an equality. □

We will now move towards a proof of the Noether normalization theorem. First, we give some intuitions.

Even if $A = k[x_1, \ldots, x_d]$ and each $\mathfrak{p}_i$ is generated by linear forms, there is a coordinate change involved. We will claim that solving this problem guides us towards the general solution.

Proof. (Noether normalization) *Case 1.* Let $A = k[y_1, \ldots, y_d]$ a polynomial ring. We claim that there exist $x_1, \ldots, x_d \in A$ such that

1. $k[x_1, \ldots, x_d] \subseteq A$ is finite,
2. $(x_{d_i+2}, x_{d_i+2}, \ldots, x_d) \subseteq \mathfrak{p}$ and $d_i = \dim(A/\mathfrak{p}_i)$.

Indeed: let $x_1' \coloneqq y_1, \ldots, x_d' \coloneqq y_d$. We find $x_1, \ldots, x_d$ by downward induction. Suppose that we found $x_d, \ldots, x_{e+1}, x_e', \ldots, x_1'$ so that:

1. $k[x_1', \ldots, x_e', x_{e+1}, \ldots, x_d] \subseteq A$ is finite,
2. $\mathfrak{p}_i \supseteq (x_n, \ldots, x_d)$, $h = \max(d_i + 1, e + 1)$.

For the base of induction, point 1. is true and point 2. - vacuous. *Induction step*: we want to find x_e. Let i be the smallest index such that x_e lies in $\mathfrak{p}_i$, that is, the smallest i such that $d_i \leq e-1$. Put $S_e \coloneqq k[x'_1, \ldots, x'_e, x_{e+1}, \ldots, x_d]$. We have

$$d_i = \dim(A/\mathfrak{p}_i) = \dim(S_e/S_e \cap \mathfrak{p}_i).$$

Point 2. implies that $x_{e+1}, \ldots, x_d \in \mathfrak{p}_i$, and so in fact $d_i = \dim(k[x'_1, \ldots, x'_e]/\mathfrak{p}_i \cap k[x'_1, \ldots, x'_e]) \leq e-1$. Hence, $\mathfrak{p}_i \cap k[x'_1, \ldots, x'_e] \neq 0$. Choose $x_e \in \mathfrak{p}_i \cap k[x'_1, \ldots, x'_e]$. Now, perform Nagata's coordinate change to get a finite extension

$$k[x''_1, \ldots, x''_{e-1}, x_e] \subseteq k[x'_1, \ldots, x'_e].$$

We replace $x_1, \ldots, x'_e$ by $x''_1, \ldots, x''_{e-1}, x_e$. For those, point 1. holds because the extension is finite; point 2, because $x_e \in \mathfrak{p}_i$. We have finished the induction step, and so the first claim of *Case 1* is proved.

Now, what follows is that:

1. $\dim(k[x_1, \ldots, x_d]) = \dim(A) = d$, so there are no relations among x_i,
2. One has

$$\begin{aligned} d_i = \dim(A/\mathfrak{p}_i) &= \dim(k[x_1, \ldots, x_d]/\mathfrak{p}_i \cap k[x_1, \ldots, x_d]) \\ &= \dim(k[x_1, \ldots, x_{d_i}]/\mathfrak{p}_i \cap k[x_1, \ldots, x_{d_i}]), \end{aligned}$$

so $\mathfrak{p}_i \cap k[x_1, \ldots, x_{d_i}] = 0$. Hence, $\mathfrak{p}_i \cap k[x_1, \ldots, x_d] = (x_{d_i+1}, x_{d_i+2}, \ldots, x_d)$ and the proof of *Case 1* is finished.

Case 2 (of the general ring A). Write $A = k[y_1, \ldots, y_r]/I$ as A is finitely generated. I is prime, because A is a domain. W now lift $\mathfrak{p}_1 \subseteq \ldots, \mathfrak{p}_m$ to $k[y_1, \ldots, y_r]$, adding also I: $I \subseteq \mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$. We now get $k[x_1, \ldots, x_r] \subseteq k[y_1, \ldots, y_r]$ finite, and so

$$I \cap k[x_1, \ldots, x_r] = (x_{d+1}, x_{d_2}, \ldots, x_r),$$

$\mathfrak{q}_i \cap k[x_1, \ldots, x_r] = (x_{d_i+1}, x_{d_i+2}, \ldots, x_r)$, $d = \dim(A) = \dim(k[y_1, \ldots, y_r])/I$. We get a diagram

$$\begin{array}{ccc} k[x_1, \ldots, x_r] & \xrightarrow{\text{finite}} & k[y_1, \ldots, y_r] \\ \downarrow & & \downarrow \\ k[x_1, \ldots, x_d] & \xrightarrow{\text{finite}} & k[y_1, \ldots, y_r]/I = A \end{array}$$

In this, the vertical maps are surjective. Then $\mathfrak{p}_i \cap k[x_1, \ldots, x_d]$ is the image of $\mathfrak{q}_i \cap k[x_1, \ldots, x_r]$ so $\mathfrak{p}_i \cap k[x_1, \ldots, x_d] = (x_{d_i+1}, x_d)$. □

Note 3.43. Let A be a ring. Then

$$\mathrm{Nil}(A) = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p} = \{f \mid \exists n \;\; f^n = 0\}.$$

Take $I \subseteq A$, $\pi \colon A \twoheadrightarrow A/I$. Then

$$\pi^{-1}(\mathrm{Nil}(A/I)) = \{f \in A \mid \exists n \;\; f^n \in I\} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}.$$

Definition 3.44. The *radical* of I is

$$\sqrt{I} = \{f \in A \mid \exists n \ \ f^n \in I\} = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

In particular, $\sqrt{I}$ can be recovered from $V(I)$.

Proposition 3.45. For $\mathfrak{p}$ prime, $\sqrt{\mathfrak{p}} = \mathfrak{p}$.

Theorem 3.46 (Nullstellensatz)**.** If A is a finitely generated k-algebra, $k = \bar{k}$, $I \subseteq A$, then

$$\sqrt{I} = \bigcap \{\mathfrak{m} \mid \mathfrak{m} \text{ maximal in } A, I \subseteq \mathfrak{m}\}.$$

Proof. Case 1, $A = k[x_1, \ldots, x_d]$ a polynomial ring. If I is prime, denote $I =: \mathfrak{p}$. $\sqrt{\mathfrak{p}} = \mathfrak{p}$, so we want $\mathfrak{p} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}$. Obviously, $LHS \subseteq RHS$. Take $f \in \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}$. Then

$$(k[x_1, \ldots, x_d]/\mathfrak{p})_{\mathfrak{p}} \cong k[x_1, \ldots, x_d, y]/(\mathfrak{p} + (fy - 1)) \neq 0.$$

Take a maximal ideal in $k[x_1, \ldots, x_d, y]/(\mathfrak{p}) + (fy - 1)$. It is te image of some maximal ideal in $k[x_1, \ldots, x_d, y]$. By Theorem 3.41, this maimal ideal is $(x_1 - \alpha_1, \ldots, x_d - \alpha_d, y - \beta)$, where $\alpha, \ldots, \alpha_d, \beta \in k$. Now,

$$(x_1 - \alpha_1, \ldots, x_d - \alpha_d, y - \beta) \cap k[x_1, \ldots, x_d] = (x_1 - \alpha_1, \ldots, x_d - \alpha_d),$$

so $\mathfrak{p} \subseteq (x_1 - \alpha_1, \ldots, x_d - \alpha_d)$. Suppose that $f \in (x_1 - \alpha_1, \ldots, x_d - \alpha_d)$. Then

$$f \in (x_1 - \alpha_1, \ldots, x_d - \alpha_d, y - \beta),$$

$$fy - 1 \in (x_1 - \alpha_1, \ldots, x_d - \alpha_d, y - \beta),$$

so $1 \in (x_1 - \alpha_1, \ldots, x_d - \alpha_d, y - \beta)$. Hence, $f \notin (x_1 - \alpha_1, \ldots, x_d - \alpha_d) =: \mathfrak{m}$. Now, $m \supseteq \mathfrak{p}, f \notin \mathfrak{p}, f \notin \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}$. Thus, $\bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m} = \mathfrak{p}$. Case 1 is finished, thus:

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \bigcap_{\mathfrak{p} \supseteq I} \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m} = \bigcap_{\mathfrak{m} \supseteq I} \mathfrak{m}.$$

The general case is $A = k[x_1, \ldots, x_r]/I$; one lifts everything to $k[x_1, \ldots, x_r]$. □

Example 3.47. If $A = k[x]_{(x)}$, then $0 \in A$ is prime, so $\sqrt{0} = 0$, but

$$0 \neq \bigcap_{m \subseteq A \text{ maximal}} \mathfrak{m} = xA.$$

3.6 Other notions of dimension for rings

Definition 3.48. Let $k \subseteq K$ be fields. We say that $x_1, \ldots, x_b \in K$ are *algebraically independent* over k if there is no nonzero polynomial $0 \neq f \in k[X_1, \ldots, X_b]$ such that $f(x_1, \ldots, x_b) = 0$. One says that $\{x_1, \ldots, x_b\} \subseteq K$ is a *transcendence basis* of K over k if $x_1, \ldots, x_b$ are algebraically independent and the extension $k(x_1, \ldots, x_b) \subseteq K$ is integral.

Lemma 3.49. Every two transcendence bases have the same cardinality, provided K is finitely generated over k.

Definition 3.50. The number of elements in a transcendence basis is called the *transcendence degree* of K over k and denoted by $\mathrm{trdeg}_k(K)$.

Theorem 3.51. Ket A be a finitely generated k-algebra. Assume that A is a domain with $\mathrm{Frac}(A) = K$. Then $\dim(A) = \mathrm{trdeg}_k(K)$.

Proof. Noether normalization implies that there exists a finite extension

$$k[x_1, \ldots, x_d] \subseteq A, \quad d = \dim(A).$$

Let $S = k[x_1, \ldots, x_n] \setminus \{0\}$. Then, the extension $K = S^{-1}k[x_1, \ldots, x_d] \subseteq S^{-1}A$ is finite, and because $S^{-1}A$ is a domain, it follows that $S^{-1}A = \mathrm{Frac}(A)$ is a field; that is, $\mathrm{Frac}(S^{-1}A) = \mathrm{Frac}(A)$.

Hence, we have a finite extension $k(x_1, \ldots, x_d) \subseteq \mathrm{Frac}(A)$, so $\{x_1, \ldots, x_d\}$ is a transcendence basis. The claim follows. □

Example 3.52. $\dim(k[x, y]/y^2 - x^3 - x) = 1$.

4 Algebraic sets

4.1 Algebraic sets

In the following, we will consider an algebraically closed field $k = \overline{k}$.

Definition 4.1. An *algebraic set* in k^n is a subset of the form

$$V(E) = \{\alpha \in k^n \mid \forall f \in E \;\; f(\alpha) = 0\},$$

where $E \subseteq S = k[x_1, \ldots, x_n]$ is some subset. $V(E)$ is then also called the *vanishing locus* of E.

Proposition 4.2. $V(E) = V(I)$, where $I = (E)$ is the ideal generated by E.

Proof. Indeed: if $f, g \in k[x_1, \ldots, x_n]$ and $f(\alpha) = 0$, then also $(f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha) = 0 \cdot g(\alpha) = 0$. □

Lemma 4.3. The sets $\{V(E) \subseteq k^n \mid E \subseteq k[x_1, \ldots, x_n]\}$ are closed subsets of a topology.

Proof. One needs to check that:

1. $\exists E \subseteq k[x_1, \ldots, x_n] \;\; V(E) = k^n$,
2. $\exists E \subseteq k[x_1, \ldots, x_n] \;\; V(E) = \emptyset$,
3. $\forall I \;\; \forall (E_i)_{i \in I} \subseteq (k[x_1, \ldots, x_n])^I \;\; \exists E \subseteq k[x_1, \ldots, x_n] \;\; V(\bigcap_{i \in I} E_i) = V(E)$,
4. $\forall E_1, E_2 \subseteq k[x_1, \ldots, x_n] \;\; \exists E \subseteq k[x_1, \ldots, x_n] \;\; V(E_1) \cup V(E_2) = V(E)$.

One inevitably finds that:

1. $E = \emptyset$ does the job since any point satisfies an empty set of conditions,
2. $E = \{(1\}$ does the job,
3. if one puts $E = \bigcup_{i \in I} E_i$, then, for any $\alpha \in k^n$:

$$\begin{aligned} \alpha \in V(E) &\iff \forall f \in \bigcup_{i \in I} \; f(\alpha = 0) \\ &\iff \forall i \in I \;\; \forall f \in E_i \;\; f(\alpha) = 0 \\ &\iff \forall i \in I \;\; \alpha \in V(E_i) \\ &\iff \alpha \in \bigcap_{i \in I} V(E_i), \end{aligned}$$

4. if we put $E = E_1 \cdot E_2 = \{f_1 \cdot f_2 \mid f_1 \in E_1, f_2 \in E_2\}$, then for any $\alpha \in k^n$ the following holds:

$$\begin{aligned}
\alpha \in V(E) &\iff \forall f \in E_1 \cdot E_2 \;\; f(\alpha = 0) \\
&\iff \forall f_1 \in E_1, f_2 \in E_2 \;\; (f_1 \cdot f_2)(\alpha) = f_1(\alpha) \cdot f_2(\alpha) = 0 \\
&\iff \forall f_1 \in E_1, f_2 \in E_2 \;\; f_1(\alpha) = 0 \;\; \vee f_2(\alpha) = 0 \\
&\iff \alpha \notin V(E_1) \implies \alpha \in V(E_2) \;\; \wedge \;\; \alpha \notin V(E_2) \implies \alpha \in V(E_1) \\
&\iff \alpha \in V(E_1) \;\; \vee \alpha \in V(E_2) \\
&\iff \alpha \in V(E_1) \cup V(E_2)
\end{aligned}$$

□

Definition 4.4. The topology defined by Lemma 4.3 is called the *Zariski topology* on k^n.

Definition 4.5. For $Z \subseteq k^n$ one defines $I(Z) = \{f \in k[x_1, \ldots, x_n] \mid f(Z) = \{0\}\}$.

Example 4.6. Suppose $\alpha = (\alpha_1, \ldots, \alpha_n) \in k^n$ and $Z = \{\alpha\}$. Then

$$I(\{\alpha\}) = \{f \in k[x_1, \ldots, x_n] \mid f(\alpha) = 0\} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n).$$

Lemma 4.7. If $Z \subseteq k^n$ is any subset, then

$$I(Z) = \bigcap_{\alpha \in Z} I(\{\alpha\}) = \bigcap_{\alpha \in Z} (x_1 - \alpha_1, \ldots, x_n - \alpha_n).$$

Proof. Straightforward. □

Definition 4.8. An ideal $I \subseteq R$ is called radical if $\sqrt{I} = I$.

If $J = \sqrt{I}$, then $\sqrt{J} = J$, and so J is radical.

Lemma 4.9. For any subset $Z \subseteq k^n$, $I(Z) \subseteq k[x_1, \ldots, x_n]$ is a radical ideal.

Proof. If $f^n \in I(Z)$, then $f^n(Z) = \{0\}$. This happens if and only if $f(Z) = \{0\}$, hence exactly when $f \in I(Z)$. □

Theorem 4.10 (Nullstellensatz, algebraic set version)**.** For any ideal $J \subseteq k[x_1, \ldots, x_n]$ and subset $Z \subseteq k^n$, one has

$$I(V(J)) = \sqrt{J} \text{ and } V(I(Z)) = \overline{Z}.$$

Proof. Pick any $\alpha \in k^n$. Then

$$\begin{aligned}
\alpha \in V(J) &\iff \forall f \in J \;\; f(\alpha) = 0 \\
&\iff \forall f \in J \;\; f \in I(\alpha) \\
&\iff J \subseteq I(\alpha) = (x_1 - \alpha_1, \ldots, x_n - \alpha_n).
\end{aligned}$$

Then

$$I(V(J)) = \bigcap_{\alpha \in V(J)} I(\alpha) = \bigcap_{J \subseteq I(\alpha)} I(\alpha) = \bigcap_{J \subseteq \mathfrak{m}} \mathfrak{m} = \sqrt{J},$$

in which the second to last equality is implied by the weak Nullstellensatz (Theorem 3.41) and the last - by the strong Nullstellensatz (Theorem 3.46).

For the other equality, we consider

$$\overline{Z} = \bigcap_{Z \subseteq V} V = \bigcap_{Z \subseteq V(J)} V(J) = \bigcap_{J \subseteq \bigcap_{\alpha \in Z} I(\alpha)} V(J) = \bigcap_{J \in I(Z)} V(J) = V(I(Z)).$$

□

Corollary 4.11. The functions $I(-)$ and $V(-)$ give a bijective (inclusion-reversing) correspondence

$$\{Z \subseteq k^n, Z \text{ closed}\} \cong \{J \subseteq S \mid \sqrt{J} = J\}.$$

Note 4.12. If k is not algebraically closed, then the weak Nullstellensatz and the related results may well fail. For example, one can produce a polynomial $f \in k[x_1, \ldots, x_n]$ such that $V(f) = \{(0, \ldots, 0)\} \subseteq k^n)$.

Definition 4.13. An algebraic set V is irreducible if it is irreducible in the Zariski topology; that is, if for any pair of algebraic sets V_1, V_2, the equality $V = V_1 \cup V_2$ implies that either $V_1 = V$ or $V_2 = V$.

Proposition 4.14. The bijection of Corollary 4.11 restricts to

$$\{Z \subseteq k^n \mid Z \text{ irreducible closed}\} \cong \{\mathfrak{p} \subseteq k[x_1, \ldots, x_n] \mid \mathfrak{p} \text{ prime}\}.$$

Proof. Take a radical ideal $J = \sqrt{J}$. We state two claims:

1. If J is prime, then $V(J)$ is irreducible.
2. If J is not prime, then $V(J)$ is reducible.

For the first, one writes $V(J) = V_1 \cup V_2$. By Theorem 4.10,

$$J = I(V(J)) = I(V_1 \cup V_2) = I(V_1) \cap I(V_2).$$

Hence, $I(V_1) \cdot I(V_2) \subseteq J$. Because J is prime, it follows that either $I(V_1) \subseteq J$ or $I(V_2) \subseteq J$; indeed, in general, $J_1 \cdot J_2 \subseteq \mathfrak{p}$ with $\mathfrak{p}$ prime implies that one of the J_i is contained in $\mathfrak{p}$, as a pair of elements exposing the contrary would deny that $\mathfrak{p}$ is prime. It follows that $V_1 = V(J)$ or $V_2 = V(J)$, and so $V(J)$ is irreducible since V_1, V_2 were arbitrary.

For the second claim, pick $a, b \notin J$ such that $ab \in J$. We let $V_1 = V((a) + J)$, $V_2 = V((b) + J)$. Now, we write

$$V_1 \cup V_2 = V((a) + J) \cup V((b) + J) = V(J) \subseteq V(((a) + J) \cdot ((b) + J)).$$

In particular, $V(J) \subseteq V_1 \cup V_2)$. Suppose that $V_1 = V(J)$. Then $I(V_1) = I(V(J)) = J$. But $a \in I(V_1)$ and $a \notin J$. Analogously, $V_2 = V(J)$ leads to contradiction. □

Example 4.15. Let $n = 1$, $S = k[x]$. Then the irreducible subsets of k^1 are:

- $k^1 = \overline{V(0))}$,
- $V(x - \lambda)$, $\lambda \in k$.

Example 4.16. Let $n = 2$, $S = k[x_1, x_2]$. This is a unique factorization domain. The prime ideals are:

- (0),

- (f) such that f is irreducible,
- $(x_1 - \alpha_1, x_2 - \alpha_2)$ such that $(\alpha_1, \alpha_2) \in k^2$, that is, the maximal ideals.

Recall that $\dim(S) = 2$. One sees easily that the points above make up all chains of prime ideals; indeed, if $\mathfrak{p}$ is a prime ideal that is not zero and not maximal, then one may pick a nonzero element $f \in \mathfrak{p}$ along with its decomposition into primes $f = f_1 \cdot \cdots \cdot f_r$. Then one of the f_i is irreducible, $(f_i) \subseteq \mathfrak{p}$, and if $\mathfrak{p} \neq (f_i)$, this would expose a chain of length 3, which is absurd.

As we had remarked previously, considerations like this make precise the intuition that the dimension k components of an algebraic set are the k-dimensional surfaces inside the algebraic set.

Lemma 4.17. k^n equipped with the Zariski topology is a Noetherian topological space.

Proof. Consider a descending sequence $V_1 \supseteq V_2 \supseteq \ldots$ of closed sets; this leads to an ascending sequence of ideals

$$I(V_1) \subseteq I(V_2) \subseteq \ldots \subseteq k[x_1, \ldots, x_n].$$

This stabilizes, because $k[x_1, \ldots, x_n]$ is Noetherian. Suppose is stabilizes at k; then for all $l \geq k$, $V(I(V_l) = V(I(V_k)))$. But $V(I(V_i)) = V_i$ by the Nullstellensatz (Theorem 4.10), since V_i are closed, and so the claim is proved. □

Corollary 4.18. For any ideal $J \subseteq k[x_1, \ldots, x_n]$, there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq k[x_1, \ldots, x_n]$ such that $\sqrt{J} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. In other words, any radical is an intersection of finitely many prime ideals.

Proof. $V(J) = V(\sqrt{J}) = V_1 \cup \cdots \cup V_r$ with V_i irreducible algebraic sets. Then

$$\sqrt{J} = I(V(J)) = I(V_1 \cup \cdots \cup V_r) = I(V_1) \cap \cdots \cap I(V_r),$$

and the $I(V_i) = \mathfrak{p}_i$ are in fact prime ideals, because V_i are irreducible. □

4.2 Noetherian rings of dimension one

Example 4.19. The following are examples of Noetherian local rings of dimension one:

1. $k[[x]]$,
2. $k[x]_{(x)}$,
3. $\mathbb{Z}_{(p)}$.

Definition 4.20. A *valuation* on a field R is a function $V \colon R \to \mathbb{Z} \cup \{\infty\}$ satisfying:

- $\forall a, b \in R \;\; V(ab) = V(a) + V(b)$,
- $\forall a, b \in R \;\; V(a + b) \geq \min(V(a), V(b))$,
- $V(0) = \infty$,
- V is surjective.

The *valuation ring* of R is $A = \{x \in R \mid V(x) \geq 0\}$.

Example 4.21. One can introduce a "mock valuation" on $k[[x]]$ by considering $k((x)) = k[[x]]_x$.

Proposition 4.22. The valuation ring of any field k is a local ring with maximal ideal

$$\mathfrak{m} = \{x \in k \mid V(x) > 0\}.$$

Proof. $\mathfrak{m}$ is an ideal. Let $a \in A \setminus \mathfrak{m}$. $V(a) = 0$, so

$$V(a^{-1}) = -V(a) = 0,$$

so $a^{-1} \in A$, hence a is invertible in A. Now, $V(1 \cdot 1) = V(1) + V(1)$, so $V(1) = 0$. In particular, all invertible elements (and so, all elements of the complement of $\mathfrak{m}$ in A) are mapped to 0 under V. This concludes the proof. □

Lemma 4.23. If A is a valuation ring, $a, b \in A$, then

$$(a) \subseteq (b) \implies V(a) \geq V(b).$$

Proof. $(a) \subseteq (b) \iff \exists c \in A \;\; a = bc$. For such a c, $V(a) = V(c) + V(b) \geq V(b)$. □

Corollary 4.24. With notation of Lemma 4.23,

$$V(a) = V(b) \iff (a) = (b).$$

Definition 4.25. A *local parameter* or *uniformizer* of a valuation ring A is any element $t \in A$ such that $V(t) = 1$.

Proposition 4.26. If t_1 and t_2 are uniformizers of a valuation ring A and n is a natural number, then $(t_1^n) = (t_2^n)$.

Proof. This follows from Lemma 4.23 and the property $V(ab) = V(a) + V(b)$. □

Corollary 4.27. The principal ideals of a valuation ring A are totally ordered by inclusion.

Proof. It suffices to show that if $a, b \in A$ and $(a) \not\subseteq (b)$, $(b) \subseteq (a)$ follows. □

Lemma 4.28. The only ideals of a valuation ring A are (0) and (t^n) for $n = 0, 1, \ldots$ and t a uniformizer of A.

Proof. Let $I \subseteq A$ be an ideal, $0 \neq I$. Let

$$n = \min\{V(i) \mid i \in I\} < \infty.$$

Pick $i \in I$, $V(i) = n$. From Corollary 4.24 it follows that $(i) = (t^n)$. □

Corollary 4.29. A valuation ring is a principal ideal domain (in particular Noetherian) of dimension 1, local.

Definition 4.30. A valuation ring is called a *discrete valuation ring* (DVR).

Lemma 4.31. A DVR is normal (that is, integrally closed in $\mathrm{Frac}(A)$).

Proof. Let $A \subseteq \mathrm{Frac}(A) \ni \alpha$, $V(\alpha) = v$. Let

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0, \quad \alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0).$$

From this, it follows that $n \cdot bV(\alpha^n) = V(a_{n-1}\alpha^{n-1} + \cdots + a_0)$. ... If $v < 0$, then $nv \geq (n-1)v \iff v \geq 0$. Hence $v = V(\alpha) \geq 0$ and so A is normal. □

Theorem 4.32. Let A be a ring. The following conditions are equivalent:

1. A is a DVR,
2. A is a Noetherian local domain, $\dim(A) = 1$, normal.

Proof. The implication $1 \implies 2$ has already been proved. For the other implication, let us consider $\mathfrak{m}$ the maximal ideal. Nakayama implies $\mathfrak{m} \neq \mathfrak{m}^2$, since $\mathfrak{m} \neq 0$. Pick $t \in \mathfrak{m} \setminus \mathfrak{m}^2$. We wish to show that $(t) = \mathfrak{m}$. Suppose not; then

$$\operatorname{Spec}(A/(t)) = V(t) = \{\mathfrak{m}\} \subseteq \operatorname{Spec}(A).$$

In particular,

$$\operatorname{Nil}(A/(t)) = \bigcap \mathfrak{p} = \mathfrak{m}/(t).$$

Now, there exists an n such that $\operatorname{Nil}(A/(t))^n = 0$. Hence, $(\mathfrak{m}/(t))^n = 0$ and so $\mathfrak{m}^t \subseteq (t)$. Let k be a number one less than the smallest such n. If we now choose $y \in \mathfrak{m}^k \setminus (t)$, then $y\mathfrak{m} \subseteq (t)$. Hence, because A is a domain, $y/t \cdot \mathfrak{m} \subseteq A$. Now, $y/t \cdot \mathfrak{m}$ is an A-module as a subset of A and so it is an ideal of A.

A is a local ring, and so either $y/t \cdot \mathfrak{m} = A$ or $y/t \cdot \mathfrak{m} \subseteq \mathfrak{m}$.

In the first case, one gets $y\mathfrak{m} = (t)$, $y \in \mathfrak{m}^k$ and $k \geq 1$, so $y \cdot \mathfrak{m} \subseteq \mathfrak{m}^{k+1} \subseteq \mathfrak{m}^2$, so $t \in \mathfrak{m}^2$. This is absurd.

In the other case, by Cayley-Hamilton we get y/t integral over A and by normality, $y/t \in A$. Hence, $y \in (t)$, which is absurd.

Hence, we have $\mathfrak{m} = (t)$.

Now, we claim that

$$\bigcap_{n \in \mathbb{N}} (t^n) = 0.$$

Suppose that there is a nonzero $x \in \bigcap_{n\in\mathbb{N}}(t^n)$. Then

$$\forall i \ \ \exists a_i \ \ x = a_i t^i$$

This gives a ... so t is invertible, which is absurd.

We now construct a valuation. For each nonzero $x \in A$, one has a number $n \geq 0$ such that $x \in (t^n)$ and $x \notin (t^{n+1})$. One puts $\mathcal{V}(x) = n$. Further, define

$$\mathcal{V}(\frac{x}{y}) = \mathcal{V}(x) - \mathcal{V}(y) \text{ for } \frac{x}{y} \in \operatorname{Frac}(A).$$

One checks that this in fact defines a valuation.

That A is a valuation ring is now tautological in terms of the previous considerations. □

We now explore various ways in which DVRs arise.

Lemma 4.33. Let A be a domain with fraction field K and integral closure $\overline{A} \subseteq K$. Let $S \subseteq A$ be a multiplicatively closed subset. Then $S^{-1}\overline{A} = \overline{S^{-1}A}$.

Proof. $A \subseteq S^{-1}A \implies \overline{A} \subseteq \overline{S^{-1}A}$. Moreover, $S^{-1}A \subseteq \overline{S^{-1}A}$, so $S^{-1}A \subseteq \overline{S^{-1}A}$. Take $x \in \overline{S^{-1}A}$, so that $x^n + (\frac{a_{n-1}}{s_{n-1}})x^{n-1} + \cdots + \frac{a_0}{s_0}$, $\quad a_i \in A, \ \ s_i \in S$. Take $s = s_0 \cdot \cdots \cdot s_n - 1$. Then ... so $xs \in \overline{A}$, so $x \in S^{-1}\overline{A}$. The claim follows. □

Corollary 4.34. Let A be a normal domain and $S \subseteq A$ a multiplicative subset. Then $S^{-1}A$ is also normal.

Proof. $A = \overline{A}$, so

$$\overline{S^{-1}A} = S^{-1}\overline{A} = S^{-1}A.$$

□

Proposition 4.35. Let A be a Noetherian normal domain. Let $\mathfrak{p}$ be a minimal nonzero prime ideal. Then $A_\mathfrak{p}$ is a DVR.

Proof. $A_\mathfrak{p}$ is a Noetherian domain and normal. By Corollary 4.34,

$$\operatorname{Spec}(A_\mathfrak{p}) = \{\mathfrak{q} \subseteq \mathfrak{p}\} = \{0, \mathfrak{p}\},$$

so $\dim(A) = 1$ and $A_\mathfrak{p}$ satisfies the assumptions of Theorem 4.32. □

Definition 4.36. A Noetherian normal domain of dimension one is called a *Dedekind domain.*

Example 4.37. $\mathbb{Z}$ and $k[x]$ are Dedekind domains.

Theorem 4.38 (cf. Milne)**.** Let $\mathbb{Q} \subseteq K$ be a finite field extension. Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K. Then $\mathcal{O}_K$ is a Dedekind domain.

Corollary 4.39. If A is Dedekind, $\mathfrak{m} \subseteq A$ is a maximal ideal, then $A_\mathfrak{m}$ is a DVR.

Lemma 4.40. Let A be a domain. Then

$$A = \bigcap_{\mathfrak{m} \text{ maximal}} A_\mathfrak{m} \subseteq \operatorname{Frac}(A).$$

Proof. Trivially, $A \subseteq \cap A_\mathfrak{m}$. We wish to show the converse inclusion.
Pick $x/y \in \operatorname{Frac}(A)$, $x/y \in \cap A_\mathfrak{m}$. Then,

$$\forall \mathfrak{m} \subseteq A \text{ maximal } \exists s \in A \setminus \mathfrak{m}, a \in A \ \frac{x}{y} = \frac{a}{s} \ (\iff s \cdot \frac{x}{y} \in A).$$

Consider the ideal $D \coloneqq \{a \in A \mid a \cdot \frac{x}{y} \in A\} \subseteq A$. Now, if $D = (1)$, we get what we want; in the other case, a contradiction. □

Proposition 4.41. Let A be a Noetherian domain such that for all maximal ideals $\mathfrak{m} \subseteq A$, $A_\mathfrak{m}$ is a DVR. Then A is a Dedekind domain.

Proof. We want A to satisfy $\dim(A) = 1$ and normality. Recall that in general $\dim(A) = \sup \dim(A_\mathfrak{m})$. In our case, the RHS is equal to 1. Now, by Lemma 4.40, we get $A = \cap A_\mathfrak{m}$. Pick $\alpha \in \operatorname{Frac}(A)$, α integral over A. Then for all maximal ideals $\mathfrak{m} \subseteq A$, α is integral over $A_\mathfrak{m}$. By normality of $A_\mathfrak{m}$, $\alpha \in A_\mathfrak{m}$. Hence,

$$\alpha \in \cap A_\mathfrak{m} = A$$

and thus A is normal. □

Example 4.42. If one takes $A = \mathbb{Z} \times \mathbb{Z}$, then for any maximal ideal $\mathfrak{m} \subseteq A$, $A_\mathfrak{m}$ is a DVR. However, A is not a domain. In fact, $\operatorname{Spec}(A) = \operatorname{Spec}(\mathbb{Z}) \sqcup \operatorname{Spec}(\mathbb{Z})$.

Lemma 4.43. Let A be a ring, $M, N \in \mod A$. Let $\phi\colon M \to N$ be an A-module homomorphism. Then the following hold:

1. $M = 0 \iff \forall \mathfrak{m} \subseteq A M_\mathfrak{m} = 0$,
2. ϕ is onto if and only if for any $\mathfrak{m} \subseteq A$ $M_\mathfrak{m} \to N_\mathfrak{m}$ is onto,

3. into if and only if into,
4. iso if and only if iso.

Proof. 1. Take a nonzero $m \in M$ and consider its annihilator $ann(m)$. Because $1 \notin ann(m)$, there exists a maximal ideal $\mathfrak{m}$ containing $ann(m)$. But if $m/1 \in M_{\mathfrak{m}}$ is zero, then there exists $s \in A \setminus \mathfrak{m}$ with $s \cdot m = 0$. But then $s \in ann(m) \subseteq \mathfrak{m}$, which makes a contradiction.

2. Consider $C = N/\phi(M)$. Then $C = 0$ if and only if ϕ is onto. But the same holds in localizations:
$$C_{\mathfrak{m}} = N_{\mathfrak{m}}/\phi(M)_{\mathfrak{m}} = N_{\mathfrak{m}}/\phi(M_{\mathfrak{m}}).$$
Now, $\phi_{\mathfrak{m}}$ is onto if and only if $C_{\mathfrak{m}} = 0$; by 1. this happens for all $\mathfrak{m}$ if and only if $C = 0$. This ends the proof.

3. Same as 2. but with $K = \ker(\phi)$.

4. Follows from 2. and 3.

□

Theorem 4.44. Let A be a Dedekind domain, $0 \neq I \subseteq A$ an ideal. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq A$ and $e_1, \ldots, e_r \in \mathbb{Z}_{\geq 1}$ such that
$$I = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r}.$$
The $\mathfrak{p}_i$ and e_i are unique.

Proof. Let $\mathfrak{p} \in \mathrm{Spec}(A)$ be a maximal ideal. For any I, $IA_{\mathfrak{p}} = \mathfrak{p}^e A_{\mathfrak{p}}$ for some $e \in \mathbb{Z}_{\geq 0}$ (because $A_{\mathfrak{p}}$ is a DVR). Let $e =: \mathcal{V}_{\mathfrak{p}}(I)$.

One defines $\prod_{\mathfrak{p} \text{ maximal}} \mathfrak{p}^{\mathcal{V}_{\mathfrak{p}}(I)}$. One notes that the definition is correct. One then considers localizations of such product in maximal ideals to check that it is equal to I; this uses Lemma 4.43. □

Note 4.45. In a Dedekind domain, the map $I \otimes J \hookrightarrow I \cdot J$ is an isomorphism.

In the following, we use that a zero-dimensional Noetherian ring is the same as an Artinian ring; moreover, in an Artinian ring all prime ideals are maximal and there are only finitely many of those. [AM94]

Lemma 4.46. Let A be an Artinian ring, $\mathrm{Spec}(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$. Then $A = A_{\mathfrak{m}_1} \times \cdots \times A_{\mathfrak{m}_r}$.

Proof. Consider the homomorphism of modules $A \to A_{\mathfrak{m}_1} \times \cdots \times A_{\mathfrak{m}_r}$ given by $a \mapsto (a, \ldots, a)$. For any maximal $\mathfrak{m} \subseteq A$ this gives $A_{\mathfrak{m}} \to (A_{\mathfrak{m}_1})_{\mathfrak{m}_1}) \times \cdots \times (A_{\mathfrak{m}_r})_{\mathfrak{m}}$. If $\mathfrak{m} \neq \mathfrak{m}_i$, then $(A_{\mathfrak{m}_i})_{\mathfrak{m}} = 0$. On the other hand, $\mathrm{Spec}(A_{\mathfrak{m}}) = \{\mathfrak{m} \cdot A_{\mathfrak{m}}\}$. We get the claim by Lemma 4.43. □

Theorem 4.47. Let A be a Dedekind domains. Let $0 \neq I \subseteq A$. Then there exist $f, g \in A$ such that $I = (f, g)$. In fact, for any nonzero f there exists a $g \in A$ such that $I = (f, g)$.

Proof. Let $0 \neq f \in I$. One has $V(f) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Then $A/(f)$ is Noetherian and 0-dimensional, and so Artinian.
$$A/(f) \cong \prod_{i=1}^{s} (A/(f))_{\mathfrak{p}_i} = \prod_{i=1}^{r} \frac{A_{\mathfrak{p}_i}}{f A_{\mathfrak{p}_i}}.$$
From Theorem 4.44 we know that
$$I = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r}, \;\; e_i \geq 0.$$
If we fix $t_i \in A$ for $i = 1, \ldots, r$, we are free to put $g = t_1^{e_1} \cdot \cdots \cdot t_s^{e_s}$.

We then get $I/(f) = (g, f) = (g, f)/(f)$, so $I = (g, f)$.

The proof is incorrect. □

4.3 Local theory

One wonders what the dimension of $k[x_1, \dots, x_n]/(f_1, \dots, f_r)$ may be.

For instance, $\dim(k[x_1, \dots, x_n]/(f))$ may be n if $f = 0$; -1 if $f \in k^*$; $n-1$ otherwise.

In general, $\dim(k[x_1, \dots, x_n]/(f_1, \dots, f_r))$ may be -1 if $(f_1, \dots, f_r) = (1)$ and otherwise it is no smaller than $n - r$.

Example 4.48.

$$\dim(k[x_1, x_2, x_3]/(x_1^2, x_1x_2, x_2^2)) = \dim(k[x_1, x_2, x_3]/(x_1, x_2)) = 1.$$

Theorem 4.49 (Krull's principal ideal theorem)**.** Let A be a Noetherian ring, $f \in A$. If $\mathfrak{p} \in V(f)$ is minimal, then $\dim(A_\mathfrak{p}) \leq 1$.

Corollary 4.50. Let A be a Noetherian ring, $f_1, \dots, f_r \in A$. If $\mathfrak{p} \in V(f_1, \dots, f_r)$ is minimal, then $\dim(A_\mathfrak{p}) \leq r$.

Corollary 4.51. Let $\mathfrak{m} \subseteq A$ be a maximal ideal. Then

$$\dim(A_\mathfrak{m}) \leq \dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2).$$

Definition 4.52. A maximal ideal $\mathfrak{m} \in \operatorname{Spec}(A)$ is *regular* if

$$\dim(A_\mathfrak{m}) = \dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2).$$

Theorem 4.53. If $\mathfrak{m}$ is regular, then $A_\mathfrak{m}$ is a unique factorization domain (UFD).

Proof. See Eisenbud. □

Note 4.54. Being regular is a property of $A_\mathfrak{m}$.

Example 4.55. All DVRs are regular.

Note 4.56. By Nakayama, $\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ is equal to the number of generators of $\mathfrak{m}A_\mathfrak{m}$, provided A is Noetherian.

Indeed, suppose that $f_1, \dots, f_d \in \mathfrak{m}A_\mathfrak{m}$ are such that $\tilde{f}_1, \dots, \tilde{f}_d$ span $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m}A_\mathfrak{m}/\mathfrak{m}^2A_\mathfrak{m}$.

Then,

$$(f_1, \dots, f_d)A_\mathfrak{m} + \mathfrak{m}^2A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$$

and by Nakayama, $(f_1, \dots, f_d)A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$.

4.4 Regular points

Example 4.57. Consider the elliptic curve $V(y^2 - x^3 - x) \subseteq \operatorname{Spec}(k[x, y])$. The Jacobian has constant rank 1 (on the zero locus).

We will aim to show existence of regular points. We recall a fact.

Note 4.58. If $f\colon A \to B$ is a ring homomorphism, M is an A-module and N a B-module, then there is a natural bijection

$$\hom_A(M, N) \cong \hom_B(B \otimes_A M, N)$$

that generalizes to an adjunction between tensoring by B and forgetting the structure of a B-module.

Theorem 4.59 (Krull's principal ideal theorem)**.** Let A be Noetherian, $f \in A$, $\mathfrak{p} \in V(f)$ minimal. Then $\dim(A_\mathfrak{p}) \leq 1$.

Proof. Let $\mathfrak{q} \subseteq \mathfrak{p}$ be distinct prime ideals. We wish to have $\operatorname{Spec}(A_\mathfrak{q}) = \{\mathfrak{q}A_\mathfrak{q}\}$. We replace A by $A_\mathfrak{p}$ and write further on A instead of $A_\mathfrak{p}$. Now, because $\mathfrak{p}$ is minimal over f, we have $V(f) = \{\mathfrak{p}A_\mathfrak{p}\}$. Because $\dim(A/(f)) = 0$, $A/(f)$ is Artinian. Let $\pi\colon A \to A_\mathfrak{q}$. Now, a sequence

$$\mathfrak{q}A_\mathfrak{q} \supseteq \mathfrak{q}^2 A_\mathfrak{q} \supseteq \ldots \supseteq \mathfrak{q}^n A_\mathfrak{q}$$

leads to a sequence

$$I_1 \coloneqq \pi^{-1}(\mathfrak{q}A_\mathfrak{q}) \supseteq$$

Then $I_n + (f)/(f)$ stabilizes, because $A/(f)$ is Artinian. Hence, $I_n + (f)$ stabilizes. In particular, there exists an n such that $I_n + (f) = I_{n+1} + (f)$. Hence, if we choose $i \in I_n$, there will be an $\tilde{i} \in I_{n+1}$ and an $a \in A$ such that $i = \tilde{i} + af$.

We deduce that $I_n = I_{n+1} + f \cdot I_n$. By Nakayama, we get $I_n = I_{n+1}$. Since we have

$$\mathfrak{q}^n A_\mathfrak{q} = \pi(I_n)A_\mathfrak{q} = \pi(I_{n+1})A_\mathfrak{q} = \mathfrak{q}^{n+1}A_\mathfrak{q},$$

another use of Nakayama implies that $\mathfrak{q}^n A_\mathfrak{q} = 0$ and so $\mathfrak{q}A_\mathfrak{q}$ is nilpotent. This finishes the proof. □

Corollary 4.60. Let A be Noetherian, $f_1, \ldots, f_r \in A$, $\mathfrak{p} \in V(f_1, \ldots, f_r)$ minimal. Then $\dim(A_\mathfrak{p}) = 1$.

Proof. We proceed by induction on r, seeing that the case $r = 1$ is correct. In the following, replace A by $A_\mathfrak{p}$.

For the induction step, consider a proper inclusion $\mathfrak{q} \subseteq \mathfrak{p}$ of prime ideals, with no prime ideals between. We claim that $\dim(A_\mathfrak{q}) \leq r - 1$. We have $\{f_1, \ldots, f_r\} \not\subseteq \mathfrak{q}$, for example $f_1 \notin \mathfrak{q}$.

Then $\mathfrak{p} \in V(\mathfrak{q} + (f_1))$ is a minimal element; if not, then $\mathfrak{q} = \mathfrak{r} \subseteq \mathfrak{p}$ is a proper inclusion, $f_1 \in \mathfrak{p}$.

Now,

$$\operatorname{Spec}(A/(\mathfrak{q} + (f_1))) = \{\mathfrak{p}\} \implies \operatorname{Nil}(A/\mathfrak{q} + (f_1)) = \mathfrak{p}$$

and so $f_2, \ldots, f_r \in \operatorname{Nil}(A/\mathfrak{q} + (f_1))$, hence

$$\exists n \forall i = 2, \ldots, r \;\; \exists g_i \in \mathfrak{q} \;\; \exists a_i \in A \;\; f_i^n = g_i + f_1 a_i.$$

Consider now $\tilde{f_1} \in A/(g_2, \ldots, g_r)$, and $\tilde{\mathfrak{p}}$ a minimal element of $V(f_1)$.

By Theorem 4.59, we get $\dim(A/(g_2, \ldots, g_r)) \leq 1$, $\operatorname{Spec}(A/(g_2, \ldots, g_r)) = \{\tilde{\mathfrak{q}}, \tilde{\mathfrak{p}}\}$, with $\tilde{\mathfrak{q}}$ a minimal element of the spectrum.

$\mathfrak{q} \in V(g_2, \ldots, g_r)$ is minimal, so by induction $\dim(A_\mathfrak{q}) \leq r - 1$. Then $\dim(A_\mathfrak{p}) \leq r$. □

Corollary 4.61. Let A be Noetherian, $\mathfrak{m}$ a maximal ideal. Then

$$\dim(A_\mathfrak{m}) \leq \dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2).$$

Proof. Let $r = \dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. Choose $f_1 \ldots, f_r$ that span $\mathfrak{m}/\mathfrak{m}^2$. Nakayama implies that $\mathfrak{m}A_\mathfrak{m} = (f_1, \ldots, f_r)A_\mathfrak{m}$, $\mathfrak{m}A_\mathfrak{m} \in V(f_1, \ldots, f_r)$, and we use the Corollary 4.60 to derive the result. □

Note 4.62. In the above,

$$\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m}A_\mathfrak{m}/\mathfrak{m}^2 A_\mathfrak{m}.$$

For some time, we will consider the following setup: A is a finitely generated algebra over $k = \overline{k}$, as well as a domain. Then the set of regular points is open (does not need the domain assumption) and we will claim that A has regular points. For technical reasons, we will consider the case of characteristic zero, though our results carry over to arbitrary characteristic.

Example 4.63. If A is not a domain, then $A = k[\varepsilon]/\varepsilon^2$ has no regular points.

Definition 4.64. The *cotangent space* at $\mathfrak{m}$ is $\mathfrak{m}/\mathfrak{m}^2$.

Recall that $\Omega = \Omega_{A/\mathfrak{m}}$ is defined by the universal property $\hom_A(\Omega, M) \cong \mathrm{Der}_k(A, M)$.
For now, we use the following two facts without proof.

Lemma 4.65. $\forall \mathfrak{m}$

$$\Omega/\mathfrak{m}\Omega \cong \mathfrak{m}/\mathfrak{m}^2.$$

Lemma 4.66. Let $K = \mathrm{Frac}(A)$. Then $\Omega \otimes_A K = K^{\oplus \dim(A)}$.

We also require a nontrivial result.

Theorem 4.67. If A is a domain, then for any maximal ideal $\mathfrak{m} \subseteq A$, $\dim(A) = \dim(A_{\mathfrak{m}})$.

Those allow us to derive the following.

Proposition 4.68. The following are equivalent, where $d = \dim(A)$.

1. $\mathfrak{m}$ is regular,
2. $\dim_k(\Omega/\mathfrak{m}\Omega) = d$,
3. $\dim_k(\Omega/\mathfrak{m}\Omega) \leq d$,
4. $\Omega_{\mathfrak{m}}$ is a free A-module.

Proof. $3 \implies 2$, because otherwise,

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\Omega/\mathfrak{m}\Omega) < d,$$

contradicting a corollary from Krull and Theorem above. For $2 \iff 4$, use a result from the exercise sheet. □

Proposition 4.69 (smearing out)**.** Let M be a finitely generated A-module. If $\mathfrak{p} \in \mathrm{Spec}(A)$ is such that

$$\dim_{\kappa(\mathfrak{p})}(M \otimes_A \kappa(\mathfrak{p})) \leq d,$$

then there exists $f \in A \setminus \mathfrak{p}$ such that M_f is generated by no more than d elements.

Corollary 4.70. With assumptions on A as before, there exists $f \in A \setminus \{0\}$ such that Ω_f is generated by at most d elements. Hence, every point outside $V(f)$ is regular.

Proof. Apply Proposition 4.69 to $\mathfrak{p} = (0) \subseteq A$, $M = \Omega$. We get f such that Ω_f is generated by no more than d elements. By Proposition 4.68,

$$\forall f \notin \mathfrak{m} \;\; \Omega/\mathfrak{m}\Omega \cong \Omega_f/\mathfrak{m}\Omega_f$$

which is generated by no more than d elements, which is equivalent to $\dim_k(\Omega/\mathfrak{m}\Omega) \leq d$. By Proposition 4.68, $\mathfrak{m}$ is regular. □

5 Back to rings and modules

5.1 Graded rings and modules

Let $(\Lambda, +, 0)$ denote a commutative monoid.

Example 5.1. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}^n, +)$, $(\mathbb{Z}/n, +)$ are all commutative monoids.

Definition 5.2. A Λ-*graded abelian group* A is a direct sum of abelian groups $\oplus_{l\in\Lambda} A_l$. A Λ-*graded ring* is a Λ-graded abelian group such that $1 \in A_0$ and

$$\forall l_1, l_2 \in \Lambda \;\; A_{l_1} \cdot A_{l_2} \subseteq A_{l_1+l_2}.$$

Definition 5.3. For every nonzero element $a \in A_l$ the *degree* of a is defined as $\deg(a) \coloneqq l$. The element a is then called *homogeneous* of degree $\deg(a)$.

Example 5.4. The polynomial ring $k[x]$ is graded by $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Z}/n$ for any n.

Definition 5.5. A Λ-*graded module* M is over a Λ-graded ring A is a Λ-graded abelian group M such that $\forall l_1, l_2 \in A \;\; A_{l_1} \cdot M_{l_2} \subseteq M_{l_1+l_2}$.

Not every module over a graded ring is a graded module; consider for example a non-homogeneous ideal (that is, one that is not generated by homogeneous elements).

Definition 5.6. A homomorphism of Λ-graded rings is a ring homomorphism $f\colon A \to B$ such that $\forall l \in \Lambda \;\; f(A_l) \subseteq B_l$.

In the following, we will mostly consider $\Lambda = \mathbb{Z}, \mathbb{N}$.

Definition 5.7. For $n \in \mathbb{Z}$, M a $\mathbb{Z}$-graded module, the *n-shifted module* $M(n)$ is defined by $M(n)_d = M_{n+d}$.

Example 5.8. The multiplication by x on $k[x]$ is not a graded self-homomorphism of $k[x]$ with the usual grading, but it is a graded homomorphism $k[x](-1) \to k[x]$.

One may consider the categories of graded groups and graded A-modules.

Proposition 5.9. Let A be an $\mathbb{N}$-graded ring. The following are equivalent:

1. A is Noetherian,
2. A_0 is Noetherian and $A_+ \coloneqq \oplus_{n\geq 1} A_n$ is a finitely generated ideal of A,
3. A_0 is Noetherian and A is a finitely generated A_0-algebra.

Proof. ($1 \implies 2$): $A_0 = A/A_+$ is Noetherian, A_+ is a finitely generated ideal. ($2 \implies 3$): Let $A_+ = (f_1, \ldots, f_r)$ with f_i homogeneous. We then claim that $A = A_0[f_1, \ldots, f_r]$; this is proved by induction on n with $A_n = (A_0[f_1, \ldots, f_r])_n$. Indeed, if we let $d_i = \deg(f_i)$, then

$$A_{n+1} = (A_+)_{n+1} = (f_1, \ldots, f_r)_{n+1} = \sum_{i=1}^{k}$$

($3 \implies 1$): Hilbert basis theorem. □

Definition 5.10. Let M be a finitely generated $\mathbb{Z}$-graded A-module, with A a Noetherian $\mathbb{N}$-graded ring and $A_0 = k$. Then the *Poincare characteristic* of M is a function $\chi_M \colon \mathbb{Z} \to \mathbb{N}$ given by $\chi_M(n) = \dim_k M_n$.

One needs to check that the definition is proper:

Lemma 5.11. For any n, the dimension of M_n is finite.

Proof. M is finitely generated and graded, so there exist homogeneous generators $m_1, \ldots, m_r \in M$; that is, the map $\oplus_{i=1}^r A(-\deg(m_i)) \to M$ is a graded surjection. □

Example 5.12. Let $A = k[x]$, $M = A$. Then

$$\chi_M(n) = \begin{cases} 1, & n \geq 0, \\ 0, & n < 0. \end{cases}$$

Example 5.13. Let $A = k[x_1, \ldots, x_d]$, $M = A$. If we put $\deg(x_i) = 1$, then

$$\chi_M(n) = \begin{cases} \binom{d+n-1}{d-1}, & n \geq 0, \\ \text{polynomial in } n \text{ of degree } d-1, \end{cases}$$

Note 5.14. If

$$0 \to V_1 \to V_2 \to \ldots \to V_n \to 0$$

is an exact sequence of vector spaces over k, then $\sum_{i=1}^n (-1)^i \dim(V_i) = 0$.

Corollary 5.15. If

$$0 \to M_1 \to \ldots \to M_n \to 0$$

is an exact sequence of graded A-modules, then $\forall j \ \ \sum_{i=1}^r (-1)^i \dim_k((M_i)_j) = 0$.

Definition 5.16. The *Poincare series* is $P_M(T) = \sum_{n=-\infty}^{\infty} \chi_M(n) T^n$.

Note 5.17. Corollary 5.15 is then restated as

$$\sum_{i=1}^{r} (-1)^i P_{M_i} = 0.$$

Theorem 5.18. Let $A = k[x_1, \ldots, x_r]$, $\deg(x_i) = d_i \geq 1$. Let M be a finitely generated A-module. Then

$$P_M = \frac{W}{\prod_{i=1}^r (1 - T^{d_i})}, \quad W \in \mathbb{Z}[T].$$

Proof. Induction on r. In $r = 0$, let $A = k$, M a finitely generated vector space. For large enough n, $M_n = 0$ and so P_M is a polynomial in T.

For the induction step, consider

$$0 \to K \to M(-d_r) \xrightarrow{x_r} M \to M/x_r M \to 0,$$

$K = \ker(x_r)$. $x_r \cdot K = 0$, so K is a finitely generated $k[x_1, \ldots, x_{r-1}]$-module. One then has $P_K - P_{M(-d_r)} + P_M - P_{M/x_r M} = 0$ and hence $P_{M(-d_r)} = \sum \chi_{M(-d_r)}(n) T^n = \sum \chi_M(n - d_r) T^n = P_M(1 - T^{d_r}) = P_{M/x_r M} - P_K$. Thus, $P_m = \frac{1}{1 - T^{d_r}} (P_{M/x_r M - P_K})$. □

Corollary 5.19. If $d_1 = d_2 = \cdots = d_r = 1$, then

$$\exists h_M \in \mathbb{Q}[t] \ \ \forall n >> 0 \ \ h_M(n) = \chi_M(n).$$

Proof. Combinatorics. □

Proposition 5.20 (graded Nagata trick)**.** Let k be algebraically closed, $\deg(x_i) = 1$, $f \in k[x_1, \ldots, x_r]$ a homogeneous element. Then there exist homogeneous elements $x'_1, \ldots, x_{r-1'}$ such that $k[x'_1, \ldots, x'_{r-1}, f] \subseteq k[x_1, \ldots, x_r]$ is a finite extension.

Corollary 5.21 (graded Noether normalization)**.** If $A = k[x_1, \ldots, x_N]/I$ is graded, then there exist homogeneous elements $y_1, \ldots, y_d \in A$ of degree 1 such that $k[y_1, \ldots, y_r] \subseteq A$ is finite, $d = \dim(A)$.

Proof. [Eis95] □

Theorem 5.22. Let k be algebraically closed. $P_A = \frac{W}{(1-T)^d}$, where $d = \dim(A)$. Consequently, $\deg(h_A) = d - 1$.

Proof. Fix $y_1, \ldots, y_d \in A$ as above, $S = k[y_1, \ldots, y_d] \subseteq A$ a graded submodule such that A is a finitely generated S-module.

For all n, one then obtains

$$\sum_{i=1}^{N} \chi_S(n - e_i) \geq \chi_A(n) \geq \chi_S(n).$$

It follows that $\deg(h_A) = \deg(h_S) = d - 1$. By arguments combinatorial, the claim follows. □

We will consider an action of k^* on $M = \oplus_{i \in \mathbb{Z}} M_i$ by $t.m_= t^{-i} m$ when $m \in M_i$.

Proposition 5.23 (homogeneous Nullstellensatz)**.** Let k be algebraically closed, $S = k[x_1, \ldots, x_r]$ be graded with $\deg(x_r) = 1$, $\sqrt{I} = I \subseteq S$. Then the following are equivalent:

1. I is homogeneous,
2. $k^* \cdot I \subseteq I$,
3. $V = V_{max}(I)$, $k^* \cdot V \subseteq V$.

Consider the action of k^* on k^n by $t \cdot (v_1, \ldots, v_n) = (tv_1, \ldots, tv_n)$. Moreover, denote $\mathrm{Proj}(S) = \{\mathfrak{p} \subseteq S\} \setminus S_+$.

Corollary 5.24. Maximal elements of $\mathrm{Proj}(S)$ are the closures of orbits of k^* on k^n, that is, lines through 0 in k^n, which is the same as the projective space $k\mathbb{P}^{n-1}$.

Lemma 5.25. Let A be a graded ring, $I \subseteq A$ an additive subgroup (resp. an ideal). The following are equivalent:

1. I is generated as an additive subgroup (respectively, as an ideal) by homogeneous elements,
2. $\forall i \in I \ \ i = \sum_j i_j, \ \ i_j \in A_j$.

Definition 5.26. If I satisfies the conditions of Lemma 5.25, it is called *homogeneous*.

Note 5.27. If I, J are homogeneous, then so are $I + J$, $I \cap J$ and many other "usual" constructions on ideals.

Lemma 5.28. Let A be an $\mathbb{N}$-graded k-algebra, k infinite. Let $I \subseteq A$ be a vector subspace. Then the following are equivalent:

1. I is homogeneous,
2. $k^*.I \subseteq I$, where k^* acts by the *torus action* $t.a_i = t^{-i} \cdot a_i$ for $a_i \in A_i$.

Proof. For the implication 1 $\implies$ 2, take $a \in I$, $a_i = \sum a_j$, $a_j \in I_j$. Then

$$t.a = t.\sum a_j = \sum t^{-j} a_j.$$

For the converse, take $a \in A$ with $a = \sum_{j=0}^{r} a_j$, $a_j \in A_j$. For any $t \in k^*$, one has $t.a \in I$. We choose r different elements $t_0, \ldots, t_r \in k^*$; this is possible because k is infinite. We consider the action of the Vandermonde matrix $\mathrm{Vdm}(t_0^{-1}, \ldots, t_r^{-1})$ on the vector $(a_0, \ldots, a - r)$. The Vandermonde matrix is invertible in the vector space A/I and at the same time, it acts on $(a_0, \ldots, a_r)$ by zero. Hence, we get the condition 2, as it is equivalent to every a_i being zero in A/I. □

Corollary 5.29 (of Proposition 5.23)**.** The standard Nullstellensatz bijection for $S = k[x_1, \ldots, x_n]$ restricts to

$$\{I = \sqrt{I} \subseteq S \text{ homogeneous}\} \cong \{k^*\text{-stable algebraic subsets}\}.$$

For the following note that the k^*-action on k^n is by coordinate multiplication, while on S it is the torus action.

Proof. (of Proposition 5.23) Let $V = V_{\max}(I)$. We begin by showing 2 $\implies$ 1. Assume $k^*.V \subseteq V$. Lines through 0 are then closures of k^*=orbits in k^n. V is the sum of all lines in V through 0. Apply Nullstellensatz to get

$$I = I(V) = \cap\{I(l) \mid l \subseteq V \text{ a line}\}.$$

We now claim that for any line l through 0, $I(l)$ is homogeneous. Indeed, if we take $(\alpha_1, \ldots, \alpha_n) \in l$, $\alpha_i \neq 0$, then $I(l) = (\alpha_1 x_i - x_1 \alpha_i)_{i=2,\ldots,n}$ is homogeneous as it is generated by homogeneous elements. I is then the intersecton of homogeneous ideals and so it is homogeneous.

We now show 1 $\implies$ 2. Let $f \in S$, $t \in k^*$, $\alpha \in k^n$. Then the actions of k^* on k^n and on S are related by

$$f(t^{-1}.\alpha) = (t.f)(\alpha).$$

We claim that $\alpha \in V_{\max}(I)$ if and only if $\forall f \in I \ f(\alpha) = 0$. This is further equivalent to $t^{-1}.\alpha \in V_{\max}(I)$. □

Note 5.30. Closed subsets of $k^n \setminus 0/k^* = k\mathbb{P}^{n-1}$ with the quotient topology correspond to the k^*-stable closed subsets of $k^n \setminus 0$. This is not the same as the k^*-stable algebraic subsets of k^n, as that space is missing $\{0\}$.

The space $k\mathbb{P}^{n-1}$ is Hausdorff, unlike the affine spaces.

Bibliography

[AM94] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Avalon Publishing, 1994. ISBN: 9780813345444.

[Eis95] David Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995. ISBN: 9780387942698.

[Mil17] James S. Milne. *Algebraic Geometry (v6.02)*. Available at www.jmilne.org/math/. 2017.

[Spe] David E Speyer. *Kahler differentials and Ordinary Differentials*. MathOverflow. URL:https://mathoverflow.net/q/9723 (version: 2009-12-25). eprint: `https://mathoverflow.net/q/9723`. URL: `https://mathoverflow.net/q/9723`.