

Commutative Algebra

Notes taken by Yeheli Fomberg <yp@campus.technion.ac.il>

Based on lectures by Danny Neftin

Winter 2026

These notes are not endorsed by the lecturers. I have revised them outside lectures to incorporate supplementary explanations, clarifications, and material for fun. While I have strived for accuracy, any errors or misinterpretations are most likely mine.

Contents

0	Terminology	3
1	Introduction through geometry	4
2	Categories and modules	12
2.1	Cateogries and functors	12
2.2	Modules	14
2.3	Tensor products	17
3	Localization	18
3.1	Localization of rings	18
3.2	Localization of modules	21
4	Integral dependence	23
4.1	Introduction and the Cayley–Hamilton theorem	23
4.2	The integral closure	25
4.3	Dimension of a variety	25
5	Noether’s lemma	29
5.1	Noether’s lemma	29
5.2	More nullstellensatzs	31
6	Noetherian rings	33
6.1	Noetherian rings	33
6.2	Hilbert’s basis theorem	34
6.3	Noetherian normalization	37
7	Tangent spaces	38
7.1	Introduction and Nakayama’s lemma	38
7.2	Krull’s principle ideal theorem	40
8	Schemes	44

0 Terminology

The origin of commutative algebra is found in multiple fields:

- Algebraic geometry – algebraic varieties are usually given by rings or a quotient rings of the form $K[x_1, \dots, x_n]/(f_1 \cdots f_n)$.
- Algebraic number theory – there is a correspondence with rings of the form $\mathbb{Q}[\alpha]$.

Remark 0.1 (Terminology). Some reminders and remarks on terminology:

- (1) Throughout the course all rings are commutative with unity.
- (2) Recall that a subring is required to have the same unity as its parent ring.
- (3) In order to check if a subset of a ring R is a subring it suffices to check closure under multiplication, subtraction, and that the unity element is the same.
- (4) A homomorphism of rings $f: R \rightarrow S$ is a map that preserves addition and multiplication, and we also require $f(1_R) = 1_S$.
- (5) A field is a ring $R \neq \{0\}$ in which every nonzero element is invertible.
- (6) An ideal $I \subset R$ is an additive subgroup which is closed under multiplication by R . That is, $R \cdot I \subseteq I$.
- (7) The ideal generated by elements $a_1, \dots, a_m \in R$ is $(a_1, \dots, a_m) := Ra_1 + \cdots + Ra_m$.
- (8) The quotient ring is $R/I := \{r + I \mid r \in R\}$, where $r_1 + I = r_2 + I$ if and only if $r_1 - r_2 \in I$.

Example 0.1. Let R be a ring, and let $x_1, \dots, x_n$ be variables. A polynomial a formal expression of the form:

$$\sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

such that $a_{i_1 \dots i_n} \in R$ are zero except for finitely many indices.

Example 0.2. Note that polynomials may be equivalent as functions, but different as formal expressions. For example in $R = \mathbb{Z}/2\mathbb{Z}$ we have the equivalency $x^2 + x \equiv 0$, but it is clear that these two polynomials are different as formal expressions.

1 Introduction through geometry

Definition 1.1 (Affine variety). Let k be a field. The affine n -space $\mathbb{A}_k^n$ is the set

$$\mathbb{A}_k^n := \{(x_1 \dots x_n) \mid x_i \in k \text{ s.t. } \forall i = 1, \dots, n\}.$$

For a set of polynomials $S \subseteq k[x_1, \dots, x_n]$ we define its set of zeros (also called zero locus) as:

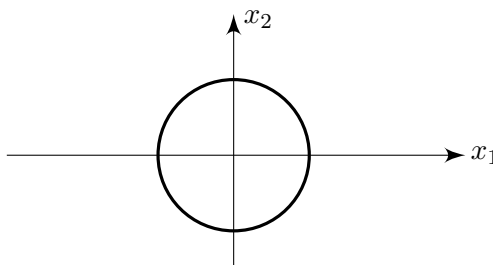
$$V(S) := \{x \in \mathbb{A}^n \mid f(x) = 0 \quad \forall f \in S\},$$

This set is called the affine (algebraic) variety associated with S .

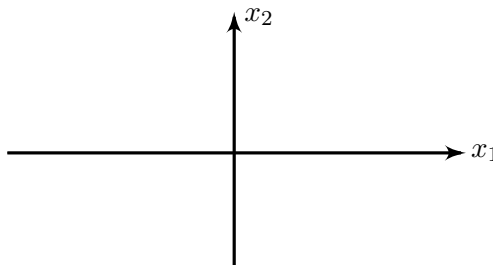
Remark 1.1. The symbol $\mathbb{A}$ stands for the word “Affine” since this space closely resembles the notion of an affine space in the theory of vector spaces.

Remark 1.2. If $S = (f_1, \dots, f_n)$ is a finite set, we sometimes will write $V(S) = V(\{f_1, \dots, f_n\})$ as $V(f_1, \dots, f_n)$.

Example 1.1. Let $k = \mathbb{R}$, and $S = \{x_1^2 + x_2^2 - 1\}$. Then $V(S) = S^1$.



If $S = \{x_1 x_2\}$ then $V(S)$ is simply the axes themselves:



If $S = \{x_1 x_2 - 1\}$ then $V(S)$ is the graph of the function $x_1 \mapsto 1/x_1$, and if $S = \{x_1^2 + x_2^2 + 1\}$ then $V(S)$ is the empty set.

Remark 1.3. A nonexample of an affine variety is $V(\sin x)$, since $\sin x$ is not a polynomial. Even though we will not discuss nonaffine varieties in this course, there is still a significant number of mathematicians working with many such abstract objects including: projective varieties, schemes, or minimal structures.

Definition 1.2 (Ideal map). Let $X \subseteq \mathbb{A}_k^n$ be an affine variety. We define a map that sends ideals to varieties $I: \{\text{Varieties}\} \rightarrow \{\text{Ideals}\}$ as follows:

$$I(X) := \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \quad \forall x \in X\}.$$

We sometimes call the ideal $I(X)$ simply “the ideal of X ”.

Remark 1.4. The ideal map $I: \{\text{Varieties}\} \rightarrow \{\text{Ideals}\}$ clearly has an inverse relation with the map $V: \{\text{Sets of polynomials}\} \rightarrow \{\text{Varieties}\}$. They are the inverse maps of each other in some sense which we will discuss soon.

Remark 1.5 (Coordinate ring). Let $X \subseteq \mathbb{A}_k^n$ be an affine variety. We define the coordinate ring (or ring of algebraic functions on X), to be the quotient $k[X] := k[x_1, \dots, x_n]/I(X)$.

Remark 1.6. Recall that $p_1, p_2 \in k[x_1, \dots, x_n]$ define the same function if and only if $p_1 - p_2 \equiv 0$ or equivalently $p_1 - p_2 \in I(X)$, or equivalently $p_1 + I(X) = p_2 + I(X)$. This implies that $k[X] := k[x_1, \dots, x_n]/I(X)$ is a ring of functions (not formal expressions). In fact, the motivation for the coordinate ring (ring of functions) is exactly this property. The intuitive way to think about $k[X]$ is as the ring of functions (that or polynomial) of the form $f: X \rightarrow k$. This intuition would be useful through this section.

Example 1.2. Let $a = (a_1, \dots, a_n) \in \mathbb{A}_k^n$. Is it a variety? Yes! since $\{a\} = V(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$. Note that this also happens to be the intersection of all the axes $\bigcap V(x_i - a_i)$.

Proposition 1.1. Let $a \in \mathbb{A}_k^n$. Then $I := I(\{a\}) = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) := M_a$, where $(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ is the ideal generated by $x_1 - a_1, x_2 - a_2, \dots, x_n - a_n$.

Proof. We will show this by double sided containment. It is clear that $M_a \subset I$.

For the other direction, consider the substitution map $\pi_a: k[x_1, \dots, x_n] \rightarrow k$ given by $g \mapsto g(a)$. Since $M_a \subseteq \ker \pi_a$ we get a surjection $k[x_1, \dots, x_n]/M_a \rightarrow k[x_1, \dots, x_n]/\ker \pi_a$, given by $g + M_a \mapsto g + \ker \pi \mapsto g(a)$, and since π_a is a surjection the first isomorphism theorem gives $k[x_1, \dots, x_n]/\ker \pi_a \cong k$.

The homomorphism (surjection) is one-to-one since

$$p(x_1, \dots, x_n) = p(a_1, \dots, a_n) \pmod{M_a}$$

(we can transfer them to constants by substitution $x_i = a_i$) for all $p \in k[x_1, \dots, x_n]$, so it follows that the map is injective, thus M_a is maximal, and $\bar{\pi}$ is an isomorphism and $\ker \pi_a = I(a)$. $\square$

Remark 1.7. We can see that the coordinate ring $k[x_1, \dots, x_n]/I(X)$ gives us a correspondence between algebraic varieties (algebraic geometry) and quotient rings (commutative algebra). In particular, by Theorem 1.1 we saw that $I(a)$ are maximal, and thus $k[x_1, \dots, x_n]/I(a)$ are fields.

Definition 1.3 (Subvarieties). Let $X \subseteq \mathbb{A}_k^n$ be a variety. Then for a set of polynomials in the coordinate ring $S \subseteq k[X]$, we say that $V(S) = V_X(S) := \{x \in X \mid f(x) = 0 \quad \forall f \in S\}$ is a subvariety of X .

Remark 1.8. It is clear that sets of the form $V_X(Y)$ are exactly the varieties in $\mathbb{A}_k^n$ contained in X . This is why they are called the subvarieties of X .

Question. Which objects in commutative algebra have a correspondence with the subvarieties of X ?

Definition 1.4 (Subideal map). Let $X \subseteq \mathbb{A}^n$ be a variety. For a subset $Y \subset X$ we define

$$I(Y) = I_X(Y) := \{f \in k[X] \mid f(y) = 0 \quad \forall y \in Y\}.$$

We call $I_X(Y)$ “the ideal of Y (in X)”.

Remark 1.9. Every variety is a subvariety. Also note that $S \subset S'$ implies $V(S) \supseteq V(S')$, and that $Y \subset Y'$ implies $I(Y) \supseteq I(Y')$.

Lemma 1.2. Let X be a variety and $k[X]$ its ring of functions. If $Y \subseteq X$ is a subvariety then $k[Y] \cong k[X]/I(Y)$. Moreover, $Y = V(I(Y))$.

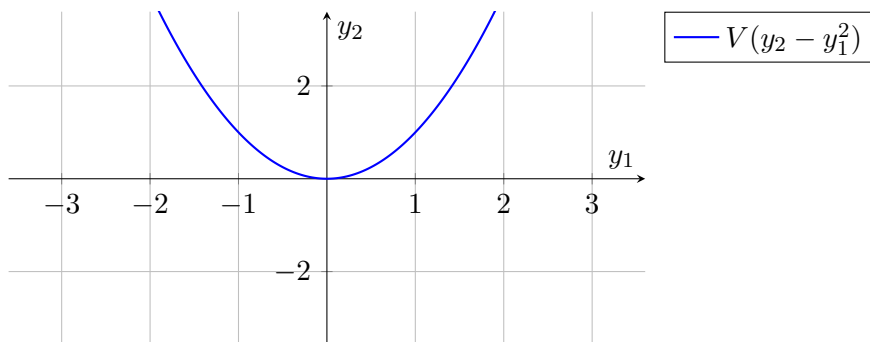
Proof. Consider the map restriction map $r: k[X] \rightarrow k[Y]$ given by $f + I(X) \mapsto f + I(Y)$. It is a ring homomorphism whose kernel is $I(Y)$, and therefore the first isomorphism theorem completes the first part of the proof.

For the second part, by definition we have $Y \subseteq V(I(Y))$. Since Y is a subvariety, we get that $Y = V(S)$ for some $S \subset k[X]$. In particular $I(Y) = I(V(S))$ and by definition $I(Y) = I(V(S)) \supseteq S$. Now by applying V on both sides and using Remark 1.9, we can conclude that $V(I(Y)) \subseteq V(S)$, which completes the proof. $\square$

Remark 1.10. By Theorem 1.2 it follows that subvarieties correspond to quotient rings.

Question. Which objects in commutative algebra have a correspondence with morphisms of subvarieties?

Exercise 1.1. Let $Y = V(y_2 - y_1^2) \subseteq \mathbb{A}_{\mathbb{R}}^2$.



We know that $I(Y) = (y_2 - y_1^2)$. Show that $K[Y] \cong K[y_1, y_2]/(y_2 - y_1^2) \cong k[y_1]$. This isomorphism of rings shows that the parabola curve is homeomorphic to the x -axis.

Definition 1.5 (Morphism of varieties). Let $X \subseteq \mathbb{A}_k^n$ and $Y \subseteq \mathbb{A}_k^m$ be varieties. A map $f: X \rightarrow Y$ is called a morphism if there exist $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ such that $f(x) = (f_1(x), \dots, f_m(x)) \in Y$ for every $x \in X$.

Definition 1.6 (Induced homomorphism). A morphism f induces a homomorphism on the coordinate rings $f^*: k[Y] \rightarrow k[X]$ by $g + I(Y) \mapsto g \circ f + I(X)$. This map is well defined since $X \xrightarrow{f} Y \xrightarrow{g} k$.

Example 1.3. Let $X = \mathbb{A}_{\mathbb{R}}^1$ and $Y = V(y_2 - y_1^2) \subseteq \mathbb{A}_{\mathbb{R}}^2$. The coordinate ring $\mathbb{R}[X]$ is simply $\mathbb{R}[x_1]$ and $\mathbb{R}[Y] = \mathbb{R}[y_1, y_2]/(y_2 - y_1^2)$.

Then the map $f: X \rightarrow Y$ given by $x \mapsto (x, x^2)$ is a morphism inducing $f^*: \mathbb{R}[Y] \rightarrow \mathbb{R}[X]$ by $g \mapsto g \circ f: x \mapsto g(x, x^2)$.

Remark 1.11. We can summarize the connections we have seen so far between geometry and algebra in the following table:

Geometry	Algebra
Variety X	The function algebra $k[X]$
Subvariety Y of X	Ideal $I(Y) \triangleleft k[X]$ of functions on X vanishing on Y
Morphism $f: X \rightarrow Y$ of varieties	Ring homomorphism $f^*: k[Y] \rightarrow k[X]$.

Remark 1.12 (Galois connection). Recall that there is a correspondence between algebraic varieties and subsets of polynomials.

$$\{X \subseteq \mathbb{A}_k^n\} \xrightleftharpoons[V]{I} \{S \subseteq k[x_1, \dots, x_n]\},$$

where $V: S \mapsto \{x \mid p(x) = 0 \ \forall p \in S\}$ and $I: X \mapsto \{p \mid p(x) = 0 \ \forall x \in X\}$.

Remark 1.13. We will call an ideal in the image of I is a *geometric ideal*. This is a temporary name until we understand these type of ideals better.

Definition 1.7 (Galois connection). Let C, D be partially ordered sets and let $V: C \rightarrow D$ and $I: D \rightarrow C$ be maps. The ordered pair (V, I) is called a Galois connection if $X \leq Y$ implies $I(X) \geq I(Y)$ and $V(I(X)) \geq X$, and similarly $S \leq T$ implies $V(S) \geq V(T)$ and $I(V(S)) \geq S$.

Remark 1.14. The correspondence in Remark 1.12 is a Galois connection with the partial order of containment.

Exercise 1.2. Suppose that (V, I) is a Galois connection. Show that:

- (1) If $X \in \text{im } V$ then $V(I(X)) = X$.
- (2) Similarly, if $J \in \text{im } I$ then $I(V(J)) = J$.

Corollary 1.3. *There is a one-to-one (invertible) correspondence:*

$$\{X \subseteq \mathbb{A}_k^n \text{ subvariety}\} \xleftrightarrow[V]{I} \{\text{Geometric ideals } I \triangleleft k[x_1, \dots, x_n]\},$$

Proof. Directly from Exercise 1.2 since we have seen that this is a Galois connection. $\square$

Corollary 1.4. *For $X \subseteq \mathbb{A}_k^n$ we have that $V(I(X))$ is the smallest subvariety containing X (this is a type of closure operation with respect to being a subvariety). Similarly, for a subset $S \subseteq k[x_1, \dots, x_n]$ we get that $I(V(S))$ is the smallest geometric ideal containing S .*

Proof. Let $X \subseteq Y \subseteq \mathbb{A}_k^n$ be a subvariety of $\mathbb{A}_k^n$ containing X . Define $Z := V(I(X))$ and replace Y by $Y \cap Z$ to obtain that $X \subseteq Y \subseteq Z$. This implies that $I(X) \supseteq I(Y) \supseteq I(Z)$, and then $Z := V(I(X)) \subseteq V(I(Y)) \subseteq V(I(Z)) = Z$ and since Y is a subvariety $V(I(Y)) = Y$, and hence $Y = Z$.

Similarly, we can let $I(V(S)) = \overline{S}$ (closure with respect to geometric ideals) and carry out the proof in the same manner. $\square$

Remark 1.15. The subvarieties of $\mathbb{A}_k^n$ are the closed subsets in a topology called the Zariski topology. (We will show this later)

Remark 1.16. The closure of a set $X \subseteq \mathbb{A}_k^n$ in the Zariski topology is $\overline{X} := V(I(X))$.

Question. What are the geometric ideals?

Example 1.4 (Nongeometric ideal). Let $R := k[x]$ for some field k (recall that $k[x]$ is a PID). We know that for any irreducible $f \in k[x]$, the ideal (f) is maximal. Note that $(x^2) \subsetneq (x) \triangleleft k[x]$ but $V(x^2) = V(x) = \{0\}$. Since we have seen that there is a one-to-one correspondence of geometric ideals and subvarieties, either (x) or (x^2) is a nongeometric ideal. Since we have

$$I(V(x^2)) = I(\{0\}) = (x),$$

we get that (x^2) isn't geometric.

Remark 1.17. We have seen that points are subvarieties, so by the Galois connection, intuitively, they must correspond to maximal ideals.

Remark 1.18 (Point ideals). For every point $a \in \mathbb{A}_k^n$ we have defined the evaluation map $\pi_a: k[x_1, \dots, x_n] \rightarrow k$ with $f \mapsto f(a)$, which has kernel $M_a = (x_1 - a_1, \dots, x_n - a_n)$. We notice that M_a is indeed a maximal ideal, and it is associated with the point a .

An ideal of the form $M_a = (x_1 - a_1, \dots, x_n - a_n)$ is called a *point ideal*.

Question. Is every maximal ideal a point ideal?

Answer. Not always. For example, the ideal $(x^2 + 1) \triangleleft \mathbb{R}[x]$ is maximal, but it is not a point ideal.

Lemma 1.5. *Let k be a field. Then every maximal ideal in $k[x]$ is a point ideal if and only if $k = \bar{k}$ (k is algebraically closed).*

Proof. Since $k[x]$ is a PID, its maximal ideals are generated by an irreducible polynomial $f \in k[x]$. But now all irreducible polynomials are of degree 1 if and only if k is algebraically closed, which completes the proof (the ideal is a point ideal). $\square$

Theorem 1.6 (Weak nullstellensatz). *If k is an algebraically closed field, then every maximal ideal in $k[x_1, \dots, x_n]$ is a point ideal.*

Corollary 1.7. *If k is an algebraically closed field and $X \subseteq \mathbb{A}_k^n$ is a variety, then every maximal ideal in $k[X] := k[x_1, \dots, x_n]/I(X)$ is a point ideal $(\overline{x_1 - a_1}, \dots, \overline{x_n - a_n})$ where $\overline{x_1 - a_1} = x_1 - a_1 + I(X)$.*

Proof. Follows from the weak nullstellensatz theorem and the correspondence theorem:

$$\{\text{Ideals } J \triangleleft k[x_1, \dots, x_n] \text{ containing } I\} \xleftrightarrow{\quad} \{\text{Ideals in } k[x_1, \dots, x_n]/I(X)\},$$

$\square$

Question. What are the geometric ideals?

Definition 1.8 (Radical of an ideal). Let $I \triangleleft R$ be an ideal. Then we define the radical of the ideal to be:

$$\sqrt{I} := \{f \in R \mid f^n \in I \text{ for some } n \in \mathbb{N}\}.$$

Remark 1.19. Suppose $I = I(X)$ is a geometric ideal. Then if $f^n \in I$, we get $f^n(x) = 0$ for all $x \in X$, so $f(x) = 0$ for all $x \in X$, which implies that $f \in I$. This means that any geometric ideal is necessarily radical.

Definition 1.9 (Radical ideal). A radical $I \triangleleft R$ is said to be a radical ideal if $\sqrt{I} = I$.

Example 1.5. Consider the example $(x^2 + 1) \triangleleft \mathbb{R}[x]$. It is a maximal ideal, but it is not a geometric ideal. This may seem as a contradiction to Hilbert's nullstellensatz theorem, but it is not because the field $\mathbb{R}$ is not algebraically closed.

Theorem 1.8 (Hilbert's nullstellensatz, strong form, 1893). *Let $k = \bar{k}$ be an algebraically closed field. Then I is geometric if and only if I is radical. In other words, we have the correspondence:*

$$\{X \subseteq \mathbb{A}_k^n \text{ subvariety}\} \xleftrightarrow[V]{I} \{\text{Radical ideals } I \triangleleft k[x_1, \dots, x_n]\},$$

Lemma 1.9. *The weak version of Hilbert's nullstellensatz implies its strong version.*

Proof. We know from Remark 1.19 that all geometric ideals are radical.

On the other direction, let $I = \sqrt{I}$ be a radical ideal, and write $I = (f_1, \dots, f_m)$. Assume that for every $f \in I(V(I))$ we have $f^l \in I$. Because $I = \sqrt{I}$, it follows from the claim that for every $f \in I(V(I))$ we have $f \in I$. It follows that $I(V(I)) \subseteq I$, and since from the Galois connection the opposite containment always holds we get that $I(V(I)) = I$, and therefore I is geometric. We now proceed to prove the assumption.

By Rabinowitsch's trick (Theorem 1.10), there exist $g_0, \dots, g_m \in k[x_0, \dots, x_n]$ such that $1 = g_0 f_0 + \dots + g_m f_m$. Next, substitute the expression $x_0 = \frac{1}{f(x_1, \dots, x_n)}$. This is a substitution homomorphism from $k[x_0, \dots, x_n]$ to the fraction field $k[x_1, \dots, x_n] = \text{Frac}(k[x_1, \dots, x_n])$. Then

$$1 = \underbrace{g_0(1 - 1)}_{=0} + \sum_{i=1}^m g_i \left(\frac{1}{f}, x_1, \dots, x_n \right) f_i(x_1, \dots, x_n).$$

By clearing the denominators we get:

$$f^l = \sum_{i=1}^m h_i f_i \in I$$

for some $l \in \mathbb{N}$. □

Proposition 1.10 (Rabinowitsch trick, 1929). *Consider $f, f_1, \dots, f_m \in k[x_1, \dots, x_n]$ as polynomials in the extended ring $k[x_0, x_1, \dots, x_n]$, denote $I = (f_1, \dots, f_m)$, and suppose that f vanishes whenever $f_1, \dots, f_m$ vanish. Then for $f_0 = 1 - x_0 f$, we have*

$$(f_0, f_1, \dots, f_m) = k[x_0, \dots, x_n].$$

Proof. Assume, by way of contradiction, that $(f_0, \dots, f_m)$ is contained in some maximal ideal M . By Theorem 1.6 we get that $M = I(a)$ for some point $a \in V(I)$. However, since $f \in I(V(I))$ and $a \in V(I)$ we get that $f(a) = 0$, and then $f_0(a) = 1$, which is a contradiction to $f_0 \in I(a)$. □

Remark 1.20. Intuitively, adding x_0 is like adding $1/f$ to the ring. This process is what we will later call “localization”.

Question. Why can we assume that $I = (f_1, \dots, f_m)$ is finitely generated?

Solution. Hilbert's basis theorem.

Theorem 1.11 (Hilbert's basis theorem, 1890). *Every ideal $I \triangleleft k[x_1, \dots, x_n]$ is finitely generated. More generally, every increasing chain $I_1 \subseteq I_2 \subseteq \dots$ of ideals stabilizes. Equivalently, $k[x_1, \dots, x_n]$ is Noetherian.*

Proof of Theorem 1.6, unfinished. Let $M \triangleleft k[x_1, \dots, x_n]$ be a maximal ideal. Observe that $a \in V(M)$ if and only if $I(a) = M$.

Since M is maximal, the quotient $k[x_1, \dots, x_n]/M$ is a field. We also have another field $k \subset k[x_1, \dots, x_n]$. Note that $k \cong k[x_1, \dots, x_n]/M$ implies that $x_i + M = a_i + M$ for some $a_i \in k$ and thus $x_i - a_i \in M$ for all i , and therefore $M = I((a_1, \dots, a_n))$. We have that $k \hookrightarrow k[x_1, \dots, x_n]/M$ by sending $a \mapsto a + M$. □

Remark 1.21. Let R be a ring. If $I \triangleleft R$ is an ideal then:

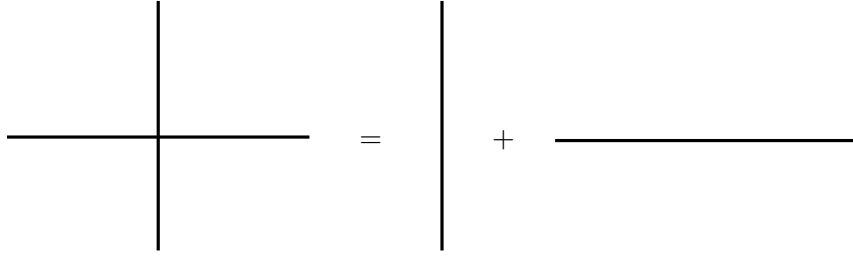
- (1) I is maximal if and only if R/I is a field.
- (2) I is prime if and only if R/I is an integral domain.
- (3) I is radical if and only if R/I is reduced (has no nilpotent elements).

In particular we have the implications:

$$I \text{ maximal} \implies I \text{ prime} \implies I \text{ radical}$$

Question. We saw that maximal ideals correspond to points. What do prime ideals correspond to geometrically?

Example 1.6. Let $X = V(x_1 \cdot x_2) \subseteq \mathbb{A}^2$. We get that:



In some sense X is reducible since we can decompose it into the sum of two varieties. Note that the ideal $(x_1 \cdot x_2) \triangleleft \mathbb{R}[x_1, x_2]$ is not a prime ideal.

Definition 1.10 (Reducible subvariety). Let $Y \subseteq X$ be a subvariety. Then Y is called reducible if and only if there exists two subvarieties $\emptyset \neq Y_1, Y_2 \subsetneq Y$ such that $Y = Y_1 \cup Y_2$. If Y is not reducible, it is called an irreducible subvariety.

Lemma 1.12. We have that $Y \subseteq X$ is irreducible if and only if $I_X(Y)$ is prime.

Proof. Note that $I_X(Y)$ is non-prime if and only if there exist $f_1, f_2 \in k[X] \setminus I_X(Y)$ such that $f_1 f_2 \in I_X(Y)$, and this happens if and only if there exists varieties $Y_1 = V_Y(f_1)$ and $Y_2 = V_Y(f_2)$, and by definition $\emptyset \neq Y_1, Y_2 \subsetneq Y$ and $Y_1 \cup Y_2 = V_Y(f_1 \cdot f_2) = Y$, which is if and only if Y is reducible (tricky), which completes the lemma. $\square$

Remark 1.22. Note that by definition we always have that $V_Y(f_1 \cdot f_2) = V(f_1) \cup V(f_2)$. Think what this means geometrically.

Exercise 1.3. Is $V(x^2 + y^2) \subseteq \mathbb{A}^2$ reducible?

Solution. The answer depends on $\mathbb{A}$. Remember the characterization of irreducible subvarieties by prime ideals. It is now easy to conclude that $V(x^2 + y^2)$ is irreducible over $\mathbb{R}$, but reducible over $\mathbb{C}$ by $x^2 + y^2 = (x + iy)(x - iy)$.

Remark 1.23 (Zariski topology). We have the following connections between varieties and ideals:

Algebra	Geometry
$V(J) \supseteq V(I)$	$J \subseteq I$
$V(I + J) = V(I) \cap V(J)$	$I + J$
$V(I \cap J) = V(I) \cup V(J)$	$I \cap J$

Note that we even have $V(\sum_{j \in J} I_j) = \bigcap_{j \in J} V(I_j)$ when J is infinite. However, the last property only holds for finite intersections. This means that $V(I)$ satisfy the basic properties of “closed sets”, and indeed, the topology generated by declaring the varieties as closed sets is a topology, and it is called the *Zariski topology*.

Remark 1.24. Recall that for a set of ideals $\{I_\alpha\}_{\alpha \in A}$ we define:

$$\sum_{\alpha \in A} I_\alpha = \left\{ \sum_{\alpha \in A} i_\alpha \mid i_k = 0 \text{ for all but finitely many } \alpha \in A \right\}.$$

Proposition 1.13. Let $I, J, I_\alpha \triangleleft k[X]$ where $\alpha \in A$. Then:

- (1) $\bigcap_{\alpha \in A} V(I_\alpha) = V(\sum_{\alpha \in A} I_\alpha)$
- (2) $V(I) \cup V(J) = V(I \cap J)$.

As a consequence, the Zariski topology is a topology.

Exercise 1.4. Deduce that $\sum_{\alpha \in A} I_\alpha$ is the smallest ideal that contains $\{I_\alpha\}_{\alpha \in A}$.

Lemma 1.14. We have that $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J} = \sqrt{I \cdot J}$.

Proof of Theorem 1.13. By the fact $V(I) = V(\sqrt{I})$ for any ideal I (since the radical of the ideal has the same set of zeros) we get that $V(I \cap J) = V(\sqrt{I \cap J})$. Then from Theorem 1.14 we conclude that:

$$V(I \cap J) = V(\sqrt{I \cap J}) = V(\sqrt{I \cdot J}) = V(I \cdot J) = \{x \mid f(x)g(x) = 0 \quad \forall f \in I \text{ and } g \in J\}.$$

where $I \cdot J = (f \cdot g \mid f \in I \text{ and } g \in J)$. Thus, from simple set theoretic arguments we have:

$$V(I \cap J) = \{x \mid f(x) = 0 \text{ or } g(x) = 0 \quad \forall f \in I \text{ and } g \in J\} = V(I) \cup V(J).$$

The proof for the infinite case and the zero locus of an intersection of ideals is left as an exercise. $\square$

2 Categories and modules

2.1 Categories and functors

Definition 2.1 (Small category). A (small) category $\mathcal{C}$ consists of:

- (1) A class $\underline{\mathcal{C}}$ whose elements are called the objects of $\mathcal{C}$,
- (2) For every $A, B \in \underline{\mathcal{C}}$ we have a set of morphisms $\text{Mor}_{\mathcal{C}}(A, B)$ whose elements are called morphisms from A to B .
- (3) For every $A \in \underline{\mathcal{C}}$ we require a distinguished element $1_A \in \text{Mor}_{\mathcal{C}}(A, A)$.
- (4) For every $A, B, C \in \underline{\mathcal{C}}$, a map $\text{Mor}(B, C) \times \text{Mor}(A, B) \rightarrow \text{Mor}(A, C)$

$$(f, g) \mapsto f \circ g$$

subject to the conditions:

- (a) $1_B \circ f = f = f \circ 1_A$ for every $A, B \in \underline{\mathcal{C}}$ and every $f \in \text{Mor}(A, B)$.
- (b) $(f \circ g) \circ h = f \circ (g \circ h)$ for every $A, B, C, D \in \underline{\mathcal{C}}$ and every $h \in \text{Mor}(A, B)$, $g \in \text{Mor}(B, C)$, and $f \in \text{Mor}(C, D)$.

Remark 2.1. When we are talking about a specific category, for example the category of **Set** (which we will soon discuss), we sometimes abuse notation and write $A \in \mathbf{Set}$ instead of $A \in \underline{\mathbf{Set}}$, and we also write $\mathbf{Set}(A, B) := \text{Mor}_{\mathbf{Set}}(A, B)$.

Example 2.1. The category **Set** is a category whose objects are sets, and for all sets $A, B, C \in \mathbf{Set}$ we have:

- (1) $\mathbf{Set}(A, B)$ are the functions from A to B .
- (2) 1_A is the identity map.
- (3) The map $\mathbf{Set}(B, C) \times \mathbf{Set}(A, B) \rightarrow \mathbf{Set}(A, C)$ is composition of functions

Remark 2.2. Similarly, we can define the categories **Grp**, **CRing** and **Ab** which are the categories of groups, commutative rings, and abelian groups respectively.

Example 2.2. Topological spaces and continuous maps form a category called **Top**. We denote the category of pointed topological spaces by **Top**_{*}.

Example 2.3. Algebraic sets over k form a category ${}_k\mathbf{Set}$ while regular maps are morphisms.

Example 2.4. Every category $\mathcal{C}$ has an opposite category which we denote by $\mathcal{C}^{\text{op}}$ which we define by “reversing arrows”. That is, $\underline{\mathcal{C}}^{\text{op}} := \underline{\mathcal{C}}$ and $\text{Mor}_{\mathcal{C}^{\text{op}}}(A, B) := \text{Mor}_{\mathcal{C}}(B, A)$.

Remark 2.3. Morphisms need not be maps between sets. For example, every poset $(X, \leq)$ defines a category $\mathcal{C}$ whose objects are the elements of X and for every $A, B \in \mathcal{C}$ we define:

$$\text{Mor}(A, B) := \begin{cases} \{f_{AB}\} & A \leq B, \\ \emptyset & \text{otherwise.} \end{cases}$$

Definition 2.2 (Covariant functor). Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A (covariant) functor $F: \mathcal{C} \rightarrow \mathcal{D}$ consists of:

- (1) A map $\underline{F}: \underline{\mathcal{C}} \rightarrow \underline{\mathcal{D}}$ denoted $C \mapsto F(C)$.

(2) For every $A, B \in \underline{\mathcal{C}}$ a map $F_{A,B}: \text{Mor}_{\mathcal{C}}(A, B) \rightarrow \text{Mor}_{\mathcal{D}}(F(A), F(B))$ denoted $f \mapsto F(f)$ such that

- (a) $F(1_A) = 1_{F(A)}$.
- (b) $F(f \circ g) = F(f) \circ F(g)$.

Remark 2.4. In slightly less formal words, a covariant functor is a function between categories that preserves their structure, or simply, a “homomorphism of categories”.

Definition 2.3 (Contravariant functor). A contravariant functor $F: \mathcal{C} \rightarrow \mathcal{D}$ is a covariant functor from $\mathcal{C}^{\text{op}} \rightarrow \mathcal{D}$.

Remark 2.5. Note that a functor $F: \mathcal{C} \rightarrow \mathcal{D}$ such that for every $f \in \text{Mor}(A, A')$ and $g \in \text{Mor}(A', A'')$ satisfies $F(f \circ g) = F(g) \circ F(f)$ is still a contravariant functor.

Remark 2.6. Small categories and functors between them constitute a category.

Example 2.5 (Forgetful functor). The forgetful functor is a functor $F: \mathbf{Grp} \rightarrow \mathbf{Set}$ sending all groups their underlying sets, and preserving morphisms.

Example 2.6. The map $\pi_1: \mathbf{Top}_* \rightarrow \mathbf{Grp}$ that sends a pointed topological space to its fundamental group is a functor.

Example 2.7. The functor $F: \mathbf{Vect}_k \rightarrow \mathbf{Vect}_k$ sends a vector space V to its double-dual space V^{**} , and now we need to find a way to send a map $f: V \rightarrow W$ to a map $f^{**}: V^{**} \rightarrow W^{**}$. Note that if $\lambda \in W^*$ then $f^*(\lambda) := \lambda \circ f \in V^*$. Now given $\psi \in V^{**}$ we define $f^{**}(\psi) \in W^{**}$ by (for every $\lambda \in W^*$) $f^{**}(\psi)(\lambda) := \psi(f^*(\lambda))$.

Example 2.8 (Representable functor). Every object $A \in \underline{\mathcal{C}}$ defines a functor into the category of sets $\text{Mor}(A, -): \mathcal{C} \rightarrow \mathbf{Set}$ called the functor represented by A . Since all families of morphisms $\text{Mor}_{\mathcal{C}}(A, B)$ are sets, the functor maps any $B \in \underline{\mathcal{C}}$ to $\text{Mor}_{\mathcal{C}}(A, B) \in \mathbf{Set}$.

We now have to think how to send an arrow from $B \xrightarrow{f} B'$ to an arrow in the category of sets. That is, we need to send an arrow $B \xrightarrow{f} B'$ to a function $\text{Mor}_{\mathcal{C}}(A, B) \rightarrow \text{Mor}_{\mathcal{C}}(A, B')$, and we can do this by function composition. More precisely, the mapping is $f \mapsto f \circ$, where $f \circ: \text{Mor}_{\mathcal{C}}(A, B) \rightarrow \text{Mor}_{\mathcal{C}}(A, B')$ is the map $(f \circ)(h) = f \circ h \in \text{Mor}_{\mathcal{C}}(A, B')$.

We also have the contravariant functor $\mathcal{C} \rightarrow \mathbf{Set}$ denoted $\text{Mor}(-, A): \mathcal{C} \rightarrow \mathbf{Set}$ which sends B to $\text{Mor}(B, A)$ and f to $\circ f$.

Remark 2.7. The map $f \circ$ is sometimes denoted f_* and is called the pushforward map, while the map $\circ f$ is denoted f^* and is called the pullback map.

Definition 2.4 (Isomorphism). A morphism $A \xrightarrow{f} B$ in a category $\mathcal{C}$ is called an isomorphism if there exists $B \xrightarrow{g} A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

Definition 2.5 (Product). A product of two objects $A, B \in \underline{\mathcal{C}}$ is an object $A \amalg B$ together with two morphisms $A \xleftarrow{P_A} A \amalg B \xrightarrow{P_B} B$ such that for every object C and all morphisms $A \xleftarrow{Q_A} C \xrightarrow{Q_B} B$ there exists a unique map $\tau: C \rightarrow A \amalg B$ such that the following diagram is commutative:

$$\begin{array}{ccccc}
 & & C & & \\
 & \swarrow Q_A & \downarrow \exists! \tau & \searrow Q_B & \\
 A & \xleftarrow{P_A} & A \amalg B & \xrightarrow{P_B} & B
 \end{array}$$

Exercise 2.1. If (C, P_A, P_B) , (D, Q_A, Q_B) are products of A and B then there exists a unique isomorphism $\tau: C \rightarrow D$ such that the following diagram commutes:

$$\begin{array}{ccccc}
 & & C & & \\
 & P_A \swarrow & \downarrow \exists! \tau & \searrow P_B & \\
 A & \xleftarrow{Q_A} & D & \xrightarrow{Q_B} & B
 \end{array}$$

Definition 2.6 (Coproduct). A coproduct of A and B is a triple $(A \amalg B, i_A, i_B)$ where i_A and i_B are maps to $A \amalg B$ such that for any object C and all maps $j_A: A \rightarrow C$ and $j_B: B \rightarrow C$ there exists a unique map $f: A \amalg B \rightarrow C$ such that the following diagram commutes:

$$\begin{array}{ccccc}
 A & \xrightarrow{i_A} & A \amalg B & \xleftarrow{i_B} & B \\
 & \searrow j_A & \downarrow \exists! f & \swarrow j_B & \\
 & & C & &
 \end{array}$$

Remark 2.8. The coproduct is also unique up to isomorphism.

Remark 2.9. Note that the coproduct is defined exactly like we defined product, except we reversed the arrows. This is a common theme in category theory, and pretty much everything we define, we can define in the same way but also reverse the arrows.

Remark 2.10 (Existence of products and coproducts). Products and coproducts do not always exist.

Example 2.9. The following table shows what are the products and coproducts in **Set**, **Grp**, and **Ab**.

Category	Product	Coproduct
Set	$\times$	$\sqcup$
Grp	direct product	free product
Ab	direct product	direct sum

2.2 Modules

The goal of this subsection is to introduce the category of modules.

Definition 2.7 (R -module). An R -module is an abelian group M with an action $R \times M \rightarrow M$ written $(r, m) \mapsto r \cdot m$ such that for every $r, s \in R$ and $m, n \in M$:

- (1) $1 \cdot m = m$.
- (2) $r \cdot (s \cdot m) = (rs) \cdot m$.
- (3) $(r + s) \cdot m = r \cdot m + s \cdot m$ and $r \cdot (m + n) = r \cdot m + r \cdot n$.

Remark 2.11. A submodule $N \leq M$ is an abelian subgroup preserved by the action of R .

Remark 2.12. In particular M/N is an abelian group with an R -module structure. That is, the multiplication $r \cdot (m + N) = r \cdot m + N$ is well defined.

Example 2.10. If $R = k$ is a field, then an R -module M is a k -vector space.

Example 2.11. If A is an abelian group, it has a $\mathbb{Z}$ -module structure under the action $\mathbb{Z} \times A \rightarrow A$ defined by $(n, a) \mapsto n \cdot a$, where multiplication is just repetitive addition for $\mathbb{Z}_{\geq 0}$, and similarly for $\mathbb{Z}_{< 0}$ except we multiply by -1 .

Example 2.12. Every ideal $I \triangleleft R$ is an R -module. It is a submodule of R as an R -module.

Similarly, every submodule of R corresponds to an ideal.

Remark 2.13. Recall that a group action $G \curvearrowright S$ defines a homomorphism $\varphi: G \rightarrow \text{Sym}(S)$ which we write as $\varphi: g \mapsto \varphi_g \in \text{Sym}(S)$ such that $\varphi_g(s) = g \cdot s$.

Similarly, for every R -module M , we get a homomorphism $\varphi: R \rightarrow \text{End}(M)$, which is given by $\varphi: r \mapsto \varphi_r \in \text{End}(M)$ defined by $\varphi_r: m \mapsto r \cdot m$.

Remark 2.14. The objects in the category of R -modules are obviously modules. The arrows in the category are R -modules homomorphisms.

Definition 2.8 (Module homomorphism). Let M, N be R -modules. A map $f: M \rightarrow N$ is called a homomorphism of R -modules if it is a homomorphism of abelian groups which preserves the action $f(r \cdot m) = r \cdot f(m)$.

Remark 2.15. Homomorphism of an R -module for R which is a field are linear transformation. Homomorphism of an R -module for $R = \mathbb{Z}$ are homomorphisms of abelian groups.

Remark 2.16. The category of modules is denoted $R\text{-mod}$. The category of right modules is sometimes denoted $\text{mod-}R$.

Remark 2.17. For a commutative ring R , a left R -module defines a right R -module.

Remark 2.18. In fact, $\text{Hom}_{R\text{-mod}}(M, N)$ is an R -module by:

$$(f + g)(m) := f(m) + g(m) \quad \text{and} \quad (r \cdot f)(m) = f(r \cdot m) = r \cdot f(m).$$

Remark 2.19. Let N and M be R -modules, and let $f: N \rightarrow M$ be a homomorphism. Then $\text{im}(f)$ and $\ker(f)$ are submodules, and we define $\text{coker}(f) := M/\text{im}(f)$.

Remark 2.20. We have that $\text{Hom}_{R\text{-mod}}(M, N)$ is an R -module by:

$$(f + g)(m) := f(m) + g(m) \quad \text{and} \quad (r \cdot f)(m) = f(r \cdot m) = r \cdot f(m).$$

Remark 2.21. The isomorphism theorems from group theory also work similarly for modules.

Definition 2.9 (Universal property of the kernel). Let $f: M \rightarrow N$ be a module homomorphism. Then $\ker f$ makes the following diagram commute:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \uparrow i & \searrow 0 & \\ \ker(f) & & \end{array}$$

The universal property of the kernel, is that for any other object K in the category of R -modules that makes the previous diagram commute, there exists a unique $\varphi: K \rightarrow \ker(f)$ such that the following diagram commute:

$$\begin{array}{ccc} & M & \xrightarrow{f} N \\ & \uparrow i & \\ K & \xrightarrow{\exists! \varphi} \ker(f) & \searrow 0 \\ & \uparrow \alpha & \end{array}$$

Definition 2.10 (Universal object). A universal object is an initial or terminal object in some category.

Remark 2.22. The product is a universal objects in the cateogry of pairs (C, P_A, P_B) , and similarly the coproduct is also a universal object in its cateogry.

Remark 2.23. In the cateogry of modules the product is direct product, and the coproduct is the direct sum. Note that this is the same as in the category of abelian groups. In particular, in the category $R\text{-mod}$ the product and coproduct coincide in the finite case, and when they coincide we call that element a *universal object*.

Definition 2.11 (Preadditive category). A preadditive cateogry $\mathcal{C}$ is a cateogry that is enriched over the cateogry of abelian groups $\mathbf{Ab}$. That is, every $\text{Hom}(A, B)$ set in $\mathcal{C}$ has the structure of an abelian groups, and composition of morphisms is bilinear, which means that we have that $f \circ (g + h) = (f \circ g) + (f \circ h)$ and $(f + g) \circ h = (f \circ h) + (g \circ h)$.

Definition 2.12 (Additive cateogry). An additive cateogry is a preadditive cateogry which admits all finite biproducts.

Definition 2.13 (Normal morphism). A monomorphism is normal if it is the kernel of some morphism, and an epimorphism is conormal if it is the cokernel of some morphism.

Definition 2.14 (Abelian category). An abelian category is a preadditive category which has a zero object, all binary biproducts, all kernels and cokernels, and all monomorphisms and epimorphisms are normal.

Example 2.13. The cateogry $\mathbf{Ab}$ is an abelian category.

Example 2.14 (Exact functor). Let M, N_1, N_2, N_3 be R -modules such that the sequence:

$$0 \longrightarrow N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \longrightarrow 0$$

is a short exact sequence. Apply the representable functor $\text{Hom}(M, -)$ on the sequence and get:

$$0 \longrightarrow \text{Hom}(M, N_1) \xrightarrow{f_*} \text{Hom}(M, N_2) \xrightarrow{g_*} \text{Hom}(M, N_3) \longrightarrow 0$$

and we can verify that this is also an exact sequence.

Definition 2.15 (Exact covariant functor). Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a commutative diagram for objects $A, B, C \in \mathcal{C}$. A covariant functor $F: \mathcal{C} \rightarrow \mathcal{D}$ is called left exact if

$$0 \longrightarrow FA \xrightarrow{f} FB \xrightarrow{g} FC$$

is a short exact sequence, and similarly it is called right exact if

$$FA \xrightarrow{f} FB \xrightarrow{g} FC \longrightarrow 0$$

is a short exact sequence. Finally, a functor $F: \mathcal{C} \rightarrow \mathcal{D}$ is called an exact functor if it is left exact and right exact. Equivalently, a functor $F: \mathcal{C} \rightarrow \mathcal{D}$ is called exact if it preserves short exact sequences.

Remark 2.24. The same definitions from Definition 2.15 also apply except we need to reverse the arrows.

Remark 2.25. Recall that we can construct a functor $F: \mathbf{Set} \rightarrow \mathbf{Vect}_k$ which sends a set X to the vector space generated by that set which is:

$$F(X) = \left\{ \sum_{x \in X} a_x \cdot x : a_x \in k \text{ and } a_x = 0 \text{ for all but finitely many } x \in X \right\}.$$

This functor satisfies the universal property that for every map $\varphi: X \rightarrow V$ where X is a set and V is a k -vector space, there exists a unique linear map $\tilde{\varphi}: F(X) \rightarrow V$ which extends φ and makes the following diagram commute:

$$\begin{array}{ccc} X & \xrightarrow{i} & FX \\ & \searrow \varphi & \downarrow \exists! \tilde{\varphi} \\ & & V \end{array}$$

2.3 Tensor products

Definition 2.16 (R -modules). Let M, N, L be R -modules. A map $\varphi: M \times N \rightarrow L$ is called R -bilinear if the induced maps $\varphi(m, \cdot)$ and $\varphi(\cdot, n)$ are linear for any $n \in N$ and $m \in M$.

Definition 2.17 (Tensor product). A tensor product of R -modules is a module $M \otimes_R N$ with a map $i: M \times N \rightarrow M \otimes_R N$ making the following diagram commute:

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & M \otimes_R N \\ & \searrow \varphi & \downarrow \exists! \tilde{\varphi} \\ & & L \end{array}$$

In other words, for every R -bilinear map $\varphi: M \times N \rightarrow L$ there exists a unique homomorphism $\tilde{\varphi}: M \otimes_R N \rightarrow L$ such that $\tilde{\varphi} \circ i = \varphi$.

Remark 2.26. The tensor product is unique up to isomorphism.

Proposition 2.1. Every pair of R -modules has a tensor product.

Proof. We consider the formal sums of elements of $M \times N$ and divide by the desired relations. The full proof is found in the notes. $\square$

Remark 2.27. The tensor product $M \otimes_R N$ is generated as an R -module by the elements $i(m, n) = m \otimes n$ for all $m \in M$ and $n \in N$. Put simply, we have $M \otimes_R N = \sum R(m \otimes n)$.

Remark 2.28. In $M \otimes_R N$ one has $r \cdot (m \otimes n) = (rm) \otimes n = m \otimes (rn)$.

Example 2.15. Let $R = k$ be a field, and let V and W be any two finitely generated k -vector fields, with corresponding bases $\{v_1, \dots, v_m\}$ and $\{w_1, \dots, w_n\}$. Then $\{v_i \otimes w_j\}$ is a spanning set for $V \otimes W$. We claim that it is also a basis.

Example 2.16. We have that $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = \sum \mathbb{Z}(m \otimes n)$, but since:

$$1 \otimes q = 2(1 \otimes \frac{q}{2}) = 2 \otimes \frac{q}{2} = 0 \otimes \frac{q}{2} = 0,$$

we get that $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = \sum \mathbb{Z}(m \otimes n) = 0$.

missing lecture

3 Localization

3.1 Localization of rings

Definition 3.1. Let $X \subset \mathbb{A}_n^k$ be a variety. A rational function on X has the form $\varphi: X \rightarrow k$ by $\varphi(x) = \frac{f(x)}{g(x)}$ on the open subset $S = \{x \mid g(x) \neq 0\}$.

Definition 3.2 (Rational functions around a point). Pick $a \in X$. The ring of polynomials $\{\frac{f}{g} \mid g(a) \neq 0\}$ defined on a is called the ring of rational functions around a .

Definition 3.3 (Multiplicatively closed set). A subset $S \subseteq R$ is called multiplicatively closed if $1 \in S$ and $a, b \in S$ implies $ab \in S$.

Definition 3.4 (Localization relation). Let $S \subseteq R$ be a multiplicatively closed set. Define an equivalence relation on $R \times S$ by:

$$(a, s) \sim (a', s') \iff u(as' - a's) = 0,$$

for some $u \in S$.

Exercise 3.1. Check that the localization relation is an equivalence relation.

Definition 3.5 (Localization). Denote by $\frac{a}{s}$ the equivalence class of (a, s) . We define the localization of R with respect to S by

$$S^{-1}R = \left\{ \frac{a}{s} \mid a \in R \text{ and } s \in S \right\}.$$

Then, $S^{-1}R$ is a ring under the operations:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{and} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Exercise 3.2. Verify that the operation in the ring $S^{-1}R$ are well defined.

Example 3.1. Let R be an integral domain. Then $S = R \setminus \{0\}$ is multiplicatively closed, and $S^{-1}R$ is the field of fractions of R .

Example 3.2. Given a prime ideal $P \subsetneq R$, the set $S = R \setminus P$ is multiplicatively closed. The localization:

$$R_P := S^{-1}R = \left\{ \frac{r}{s} \mid r \in R \text{ and } s \in S \right\},$$

is called the localization at P .

Remark 3.1. A special case of Example 3.2 when we consider a ring of functions $k[X]$, and a point ideal $M_a \subset k[X]$ which gives the localization:

$$k[X]_{M_a} = \left\{ \frac{f}{g} \in k[X] \mid g(a) \neq 0 \right\},$$

which is simply the ring of rational functions around a .

Example 3.3. Let $f \in R$. The set $\{1, f, f^2, \dots\}$ is multiplicatively closed. Then

$$R_f := S^{-1}R = \left\{ \frac{r}{f^i} \mid r \in R \text{ and } i \geq 0 \right\},$$

is called the localization at f .

Remark 3.2. A special case of Example 3.3 is $R = \mathbb{Z}$ and $f = p \in \mathbb{Z}$ for a prime $p \in \mathbb{Z}$. Then:

$$R_p = S^{-1}R = \left\{ \frac{r}{p^k} \mid r \in \mathbb{Z} \text{ and } k \geq 0 \right\} = \bigcup_{k \geq 0} \frac{1}{p^k} \mathbb{Z}.$$

Warning: This is NOT the same as $R_{(p)} = \left\{ \frac{r}{s} \mid (s, p) = 1 \right\}$.

Remark 3.3. In Example 3.3, $R_S = S^{-1}R = \{0\}$ if and only if f is nilpotent. This is because

$$S^{-1}R = \{0\} \iff \frac{x}{1} = 0, \forall x \in R \iff f^k x = 0 \text{ for some } k \geq 0, \forall x \in R \iff f \text{ is nilpotent.}$$

Remark 3.4. The map $\varphi: R \rightarrow S^{-1}R$ given by $r \mapsto \frac{r}{1}$ is homomorphism which gives $S^{-1}R$ the structure of an R -algebra. Moreover, φ is injective if and only if S doesn't contain a zero divisor.

Remark 3.5. For every $S^{-1}R$ -algebra T with a homomorphism $\eta: S^{-1}R \rightarrow T$, we have that $\eta(S) \subseteq T^\times$. In particular, T is an R -algebra

$$R \xrightarrow{\varphi} S^{-1}R \xrightarrow{\eta} T$$

such that $\eta \circ \varphi(S) \subseteq T^\times$.

Definition 3.6 (Universal property of localization). For every homomorphism $f: R \rightarrow T$ of R -algebras such that $f(S) \subseteq T^\times$ there exists a unique homomorphism $\tilde{f}: S^{-1}R \rightarrow T$ of $S^{-1}R$ -algebras such that $\tilde{f} \circ \varphi = f$. In fact,

$$\tilde{f}\left(\frac{r}{s}\right) = f(s)^{-1}f(r).$$

The associated commutative diagrams are:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S^{-1}R \\ & \searrow f & \downarrow \tilde{f} \\ & & T \end{array} \quad \begin{array}{c} S^{-1}R \\ \downarrow \exists! \tilde{f} \\ T \end{array}$$

In the category of R -algebras and $S^{-1}R$ -algebras respectively.

Proposition 3.1. Let $S \subseteq R$ be a multiplicatively closed set, and let $\varphi: R \rightarrow S^{-1}R$ with $r \mapsto \frac{r}{1}$ be the natural homomorphism. Then:

(1) For every $I \triangleleft R$,

$$\varphi(I) \cdot S^{-1}R = \left\{ \frac{a}{s} \mid a \in I \text{ and } s \in S \right\}.$$

(2) For every $J \triangleleft S^{-1}R$,

$$\varphi\left(\varphi^{-1}(J)\right) \cdot S^{-1}R = J.$$

(3) There is a one-to-one correspondence:

$$\left\{ \text{Prime ideals } I \triangleleft R \text{ such that } I \cap S = \emptyset \right\} \xrightleftharpoons[B]{A} \left\{ \text{Proper prime ideals in } S^{-1}R \right\},$$

where $A: I \mapsto \varphi(I) \cdot S^{-1}R$ and $B: J \mapsto \varphi^{-1}(J)$.

Proof.

- (1) The $\supseteq$ direction is immediate since $\frac{1}{s} \in S^{-1}$ and $\frac{a}{1} \in \varphi(I)$ and thus $\frac{a}{s} \in \varphi(I) \cdot S^{-1}R$. The $\subseteq$ direction follows since $\{\frac{a}{s} \mid a \in I \text{ and } s \in S\}$ is an ideal which contains $\varphi(I)$.
- (2) By (1) we have that

$$\varphi\left(\varphi^{-1}(J)\right) S^{-1}R = \left\{ \frac{a}{s} \mid a \in \varphi^{-1}(J) \text{ and } s \in S \right\} = J,$$

where the last transition follows from

$$a \in \varphi^{-1}(J) \iff \varphi(a) = \frac{a}{1} \in J \iff \frac{a}{s} \in J, \quad \forall s.$$

- (3) It suffices to check that the maps are inverses of each other. We have seen that

$$\varphi\left(\varphi^{-1}(J)\right) S^{-1}R = J.$$

It remains to show that $\varphi^{-1}\left(\varphi(I)\right) S^{-1}R = I$ for $I \triangleleft R$ such that $I \cap S = \emptyset$. The $\supseteq$ direction is clear since $\varphi^{-1}\left(\varphi(I)\right) \supseteq I$. On the other direction we have that $a \in \varphi^{-1}\left(\varphi(I) S^{-1}R\right)$ implies that $\frac{a}{1} = \varphi(a) \in \varphi(I) S^{-1}R$. And by (1) this implies $\frac{a}{1} = \frac{b}{s}$ for some $b \in I$ and $s \in S$. In other words $u(as - b) = 0$ for some $u \in S$. Then since $b \in I$ we get $us \cdot a \in I$, and $us \in S$, I is prime so $a \in I$.

□

Example 3.4. Let $P \triangleleft R$ be a prime ideal, and let $S = R \setminus P$. We get a correspondence

$$\{\text{Prime ideals } I \triangleleft R \text{ such that } I \subseteq P\} \xleftrightarrow[B]{A} \{\text{Proper prime ideals in } R_P\}.$$

In particular, $S^{-1}P$ is the only maximal ideal in R_P . In particular, R_P is called a *local ring* (has a unique maximal ideal). For example, if $R = k[X]$ for a variety $X \subset \mathbb{A}_k^n$ and $a \in X$, then the ring of rational functions around a

$$k[X]_{M_a} = \left\{ \frac{f}{g} \in k[X] \mid g(a) \neq 0 \right\},$$

is a local ring with maximal ideal

$$M_a \cdot k[X]_{M_a} = \left\{ \frac{f}{g} \in k[X] \mid f(a) = 0 \right\}.$$

Example 3.5. Let $X \subseteq \mathbb{A}^n$ be a variety and $f \in k[X]$. The open subset

$$X_f = \{x \in X \mid f(x) \neq 0\}$$

is then a variety as follows: Consider the zeros $\widehat{X_f}$ of

$$(I(X), f(x)x_{n+1} - 1) \triangleleft k[x_1, \dots, x_n, x_{n+1}].$$

This is a variety with a one-to-one correspondence $X_f \longleftrightarrow \widehat{X_f}$ as follows:

$$\{x \in X \mid f(x) \neq 0\} \longleftrightarrow \left\{ (x, x_{n+1}) \mid x_{n+1} = \frac{1}{f(x)} \text{ and } x \in X \right\}.$$

Proposition 3.2 (Rabinowitch trick, revisited). *The weak nullstellensatz implies the strong nullstellensatz. Recall that the strong nullstellensatz says that for any ideal I in $\mathbb{C}[x_1, \dots, x_n]$ we have:*

$$I(V(I)) = \sqrt{I}.$$

That is, $I(V(I))$ is the closure of I with respect to the property of being radical.

Proof. We will show this with double sided containment.

If $f \in \sqrt{I}$, then $f^k \in I$ for some $k \geq 1$. Therefore $f^k(p) = (f(p))^k = 0$ for all $p \in Z(I)$. This implies that $f(p) = 0$ for all $p \in Z(I)$, which implies that $f \in I(Z(I))$.

In order to prove the other side of the containment, we will use localization. Consider $0 \neq f \in I(Z(I))$. In $\mathbb{C}[x_1, \dots, x_n, t]$ we claim that the ideal

$$\hat{I} = (ft - 1) + (I) \subseteq \mathbb{C}[x_1, \dots, x_n, t]$$

has no zeros, where (I) denotes the ideal in the ring $\mathbb{C}[x_1, \dots, x_n, t]$ generated by I . Indeed, for any $(a_1, \dots, a_n, b) \in Z(\hat{I})$ there must exist $g \in I$ such that $g(a_1, \dots, a_n) = 0$, and in particular $f(a_1, \dots, a_n) = 0$, so we get that $(ft - 1)$ has to vanish at $(a_1, \dots, a_n, b)$, or in other words that $0 = f(a_1, \dots, a_n)b - 1 = -1$ which is a contradiction to $f(a_1, \dots, a_n) = 0$.

By the weak nullstellensatz we have that $Z(\hat{I}) = \emptyset$ if and only if $\hat{I} = (1) = \mathbb{C}[x_1, \dots, x_n, t]$, and thus the ideal the ideal $\hat{I}$ must be the whole ring, and in particular it contains $1 \in \hat{I}$. This means that there exist $f_i \in I$ such that:

$$1 = (f(x_1, \dots, x_n)t - 1)g_0(x_1, \dots, x_n, t) + \sum_i f_i(x_1, \dots, x_n)g_i(x_1, \dots, x_n, t).$$

Consider the image of this equality in the field of rational functions in n variables $\mathbb{C}(x_1, \dots, x_n)$ under the algebra map which sends x_i to x_i and t to $f(x_1, \dots, x_n)^{-1}$. Then the equation becomes:

$$1 = 0 + \sum_i f_i(x_1, \dots, x_n) \frac{h_i(x_1, \dots, x_n)}{f_i(x_1, \dots, x_n)^{k_i}},$$

for some polynomials h_i and some $k_i \geq 0$. After clearing the denominators we conclude that f^k lies in I , which proves the other side of the inclusion and concludes the proof. $\square$

3.2 Localization of modules

Definition 3.7 (Localization of modules). Let $S \subseteq R$ be a multiplicative subset and let M be an R -module. For $m \in M$, $s \in S$ let $\frac{m}{s}$ be the equivalence class in $M \times S$ under

$$(m, s) \sim (m', s') \iff k \cdot (s' \cdot m - m' \cdot s) = 0$$

for some $k \in S$. The set:

$$S^{-1}M = \left\{ \frac{m}{s} \mid s \in S \text{ and } m \in M \right\}$$

is the localization of M . It is an abelian group with:

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s' \cdot m + s \cdot m'}{ss'}.$$

Moreover, $S^{-1}M$ is a $S^{-1}R$ -module via the scalar multiplication map $S^{-1}R \times S^{-1}M \rightarrow S^{-1}M$ defined by:

$$\frac{r}{s} \cdot \frac{m}{s'} = \frac{r \cdot m}{ss'}.$$

Lemma 3.3. *Let $S \subseteq R$ be a multiplicatively closed set, and let M be an R -module. Then $S^{-1}M \cong S^{-1}R \times_R M$.*

Proof. First, we define the map $\tilde{\varphi}: S^{-1}R \times M \rightarrow S^{-1}M$ by:

$$\left(\frac{r}{s}, m\right) \rightarrow \frac{r \cdot m}{s}.$$

(you may check that it is well defined). Note that $\tilde{\varphi}$ is R -bilinear and hence by the universal property it induces a homomorphism $\varphi: S^{-1}R \otimes_R M \rightarrow S^{-1}M$ by

$$\frac{r}{s} \otimes m \mapsto \frac{r \cdot m}{s}.$$

We define an inverse map $\psi: S^{-1}M \rightarrow S^{-1}R \otimes_R M$ by

$$\frac{m}{s} \mapsto \frac{1}{s} \otimes m.$$

This map is also well defined (we can simply check), and it is clear that the maps are inverses of each other since we have that:

$$(\psi \circ \varphi) \left(\frac{r}{s} \otimes m \right) = \psi \left(\frac{r \cdot m}{s} \right) = \frac{1}{s} \otimes rm = \frac{r}{s} \otimes m,$$

and vice versa. □

Remark 3.6. Notice the similarity of Theorem 3.3 to extension of scalars.

Proposition 3.4. *The functor $S^{-1} \equiv S^{-1}R \otimes$ which sends M to $S^{-1}M$ and φ to $S^{-1}\varphi$ is exact.*

Proof. Let

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence. We claim that the short sequence:

$$0 \longrightarrow S^{-1}M_1 \xrightarrow{S^{-1}\varphi} S^{-1}M_2 \longrightarrow S^{-1}M_3 \longrightarrow 0$$

is exact. Since localization is given by tensoring with $S^{-1}R$, and since tensoring from the left is a right exact functor, the sequence is exact, except possibly at $S^{-1}M_1$. In order to show exactness at $S^{-1}M_1$ let $m/s \in \ker(S^{-1}\varphi)$. We then have that $S^{-1}\varphi(m/s) = \varphi(m)/s = 0$. This implies that $\varphi(um) = u\varphi(m) = 0$ for some $u \in S$, and since φ is injective $um = 0$, and thus $m/s = 0$, which completes the proof. □

Corollary 3.5. *If $N \subseteq M$ is an R -submodule and $S \subseteq R$ is multiplicatively closed, then $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.*

Proof. We start by applying localization to

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$$

where i and π are the natural injection and projection maps. We get that the sequence:

$$0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}i} S^{-1}M \xrightarrow{S^{-1}\pi} S^{-1}(M/N) \longrightarrow 0$$

is exact by Theorem 3.4, and thus $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$, which completes the proof. □

Remark 3.7 (On localization of algebras). Recall that $S^{-1}R$ is an R -algebra.

- (1) If R' is an R -algebra then $S^{-1}R' \cong S^{-1}R \otimes_R R'$ is an isomorphism of R -algebras, giving $S^{-1}R'$ the structure of an $S^{-1}R$ algebra.
- (2) From the universal property we have that $\text{Hom}_{R\text{-mod}}(R, R') \cong \text{Hom}_{S^{-1}R\text{-mod}}(S^{-1}R, R')$. These are adjoint functors.

4 Integral dependence

4.1 Introduction and the Cayley–Hamilton theorem

Definition 4.1 (Integral element). An element s in a ring extension S/R is called integral if there exists a monic polynomial $f \in R[x]$ such that $f(s) = 0$.

Remark 4.1. Note that an integral element is different than an algebraic element. For example, there may exist a nonmonic polynomial $p(x) \in R[x]$ such that $p(s) = 0$, but s is not integral, since the leading coefficient of p is not invertible.

Definition 4.2 (Integral extension). A ring extension S/R is called an integral extension if every $s \in S$ is integral over R .

Definition 4.3 (Finite ring extension). A ring extension S/R is finite if S is finitely generated as an R -module.

Remark 4.2. If S/R is a field extension, then it is algebraic if and only if it is integral as a ring extension.

Proposition 4.1. Let R be a UFD, and let S be its field of fractions. Then $a \in S$ is integral over R if and only if $a \in R$.

Proof. Indeed if $a \in R$ then it is integral by $x - a$. On the other hand, if $s = \frac{p}{q} \in S$ is integral for p, q without a common factor, then:

$$\left(\frac{p}{q}\right)^n + c_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + c_0 = 0$$

for some $c_{n-1}, \dots, c_0 \in R$. Thus,

$$p^n = -q \left(c_{n-1} p^{n-1} + c_{n-2} p^{n-2} q + \cdots + c_0 q^{n-1} \right)$$

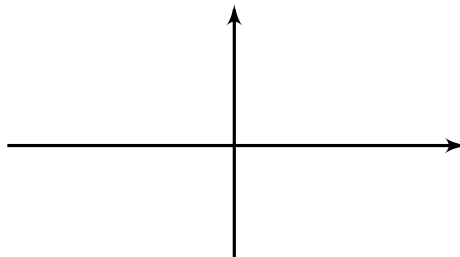
in R and hence $q \mid p^n$. Since p and q have no common factors, q must be a unit, and hence $a = \frac{p}{q} \in R$. $\square$

Example 4.1. Let $R = \mathbb{Z}$ and $S = \mathbb{Q}$. Then the R -integral elements in S are only elements in R .

Remark 4.3. The situation could be different when S is not the field of fractions of R . For example, let $R = \mathbb{Z}$ and $S = \mathbb{Q}[\sqrt{2}]$. Then every element in $\mathbb{Z}[\sqrt{2}]$ is integral over $\mathbb{Z}$ (this can be verified by setting $x = a + b\sqrt{2}$ and noticing that $(x - a)^2 = 2b^2$ and both sides are in $\mathbb{Z}[x]$).

Remark 4.4 (Geometric meaning). Set $R = \mathbb{R}[\mathbb{A}^1]$ and $S = \mathbb{R}[X']$, where $X' = V(f)$ for some $f \in \mathbb{R}[x, y]$. Then the projection $\pi: X' \rightarrow \mathbb{A}^1$ defined $(x, y) \mapsto x$ induces a function ring homomorphism $\pi^*: R \rightarrow S$, defined by $h \mapsto h \circ \pi: X' \rightarrow \mathbb{R}$. This is the map $(x, y) \mapsto h(x)$ which is in $\mathbb{R}[X']$ as wanted. We identify R with its image under π^* . More concretely, we identify $R = \mathbb{R}[x]$ and $R' = \mathbb{R}[x, y]/(f(x, y))$, and $\pi^*: \mathbb{R}[x] \rightarrow \mathbb{R}[x, y]/(f)$ is the embedding $h \mapsto h + (f)$. We will see the geometric meaning in the following examples.

Example 4.2. Let $f(x, y) = xy$.



Remark 4.5. Recall that for a field extension L/K we have that L/K is algebraic and finite if and only if it is finitely generated by algebraic elements.

Proposition 4.2. *A ring extension S/R is integral and finite if and only if $S = R[a_1, \dots, a_n]$ for integral elements $a_1, \dots, a_n$.*

Proof. One side requires linear algebra, and the other side requires the following generalized version of the classic Cayley–Hamilton theorem. We never use the details in this proposition in order to compute something, so we will just take it as a result (though a proof was shown in class). $\square$

Theorem 4.3 (Cayley–Hamilton theorem for modules). *Let M be a finitely generated R -module, let $I \triangleleft R$ and let $\varphi: M \rightarrow M$ be a homomorphism satisfying $\varphi(M) \subseteq I \cdot M := \langle i \cdot m \rangle$. Then*

$$\varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_0 = 0$$

for some $a_0, \dots, a_{n-1} \in I$.

Proof. Since M is finitely generated, we can write $M = Rm_1 + \dots + Rm_k$ for $m_1, \dots, m_k \in M$. We can now write:

$$\varphi(m_i) = \sum_{j=1}^k a_{ij}m_j$$

with $a_{ij} \in I$ for all $1 \leq i \leq k$. Define an $R[x]$ -module structure (recall that this is simply an R -module structure with an extra linear map $x: M \rightarrow M$) on M by

$$x \cdot m = \varphi(m),$$

and then we get:

$$\sum_{j=1}^k (x\delta_{ij} - a_{ij}) m_j = 0$$

(for all j ?) where δ_{ij} is Kronecker's delta. We then have that:

$$\underbrace{\begin{pmatrix} x - a_{11} & -a_{12} & \dots & -a_{1k} \\ -a_{21} & x - a_{22} & \dots & -a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{k1} & -a_{k2} & \dots & x - a_{kk} \end{pmatrix}}_{A \in \text{Mat}(R[x])} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

We can then multiply by the adjugate matrix A^{adj} of A using the identity $A^{\text{adj}}A = \det(A) \cdot I$ to get $\det(A) \cdot m_j = 0$. But we have

$$\det(A) = x^k + \sum_{j=0}^k a_{ij}x^j \in R[x],$$

for $a_{ij} \in I$. We now have that

$$0 = \left(x^k + \sum_{j=0}^k a_{ij}x^j \right) \cdot m_j = \left(\varphi^k + \sum_{j=0}^k a_{ij}\varphi^j \right) \cdot m_j$$

for all j and hence

$$\varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_0 = 0,$$

which completes the proof. $\square$

Remark 4.6. If $R = k$ is a field we recover the classic Cayley–Hamilton theorem.

4.2 The integral closure

Definition 4.4 (Integral closure). Let S/R be a ring extension. The integral closure of R in S is defined by

$$\overline{R} := \{a \in S \mid a \text{ is integral over } R\}.$$

Corollary 4.4. The integral closure $\overline{R}$ is a subring of S since by Theorem 4.2 if $a, b \in \overline{R}$ then $a \pm b, a \cdot b \in \overline{R}$.

Example 4.3. Let $R = \mathbb{Z}$ and $S = \mathbb{C}$. Then $\overline{R} = O$ is the ring of algebraic integers (roots of monic polynomials over $\mathbb{Z}$). It contains all kind of weird numbers, such as $\mathbb{Z}, i, \sqrt[m]{m}, e^{2\pi i/m}, \frac{1+\sqrt{5}}{2}$.

missing lecture

4.3 Dimension of a variety

Our goal in this subsection is to define the (Krull) dimension of a variety. For example, clearly the dimension of the affine space $\mathbb{A}_k^3$ should be 3. We will also define the Krull dimension of a ring, in a very analogical way to how we define the Krull dimension of a variety.

Remark 4.7. We see that we can define the (Krull) dimension of $\mathbb{A}_k^n$ to be the length of the longest increasing (with respect to containment) sequence of irreducible varieties (varieties such that their associated ideals are prime). For example, in the case of $\mathbb{A}^3$ the longest chain (there are different chains of irreducible varieties of this length), we can take $a_1 = V(x_1x_2x_3)$ to be the origin, $a_2 = V(x_2x_3)$ to be a line, and $a_3 = (x_3)$ to be the plane (note we could also add $a_0 = \emptyset$ and $a_4 = \mathbb{A}^3$ to the sequence, but we don't care about the edges).

Equivalently, this sequence of increasing subvarieties induces a rising sequence of *prime* ideals in $k[x_1, x_2, x_3]$, which is:

$$k[x_1, x_2, x_3] \supseteq (x_1, x_2, x_3) \supseteq (x_2, x_3) \supseteq (x_3) \supseteq \emptyset.$$

Note that (excluding the edges) this is a sequence of length 3, indeed the maximal increasing chain of prime ideals in $k[x_1, x_2, x_3]$ is 3, and so we define the Krull dimension of $k[x_1, x_2, x_3]$ to be 3.

Remark 4.8 (The term lying over). In a ring extension S/R we say that for a prime ideal $P_R \triangleleft R$, there exists a prime ideal lying over it if there exists a prime ideal $P_S \triangleleft S$ such that $P_S \cap R = P_R$. We say that P_S is the ideal lying over P_R .

Theorem 4.5 (Lying over). Let S/R be a ring extension and let $P_R \triangleleft R$ be a prime ideal. Then:

- (1) There exists a prime ideal $P_S \triangleleft S$ lying over P_R if and only if $(P_RS) \cap R \subseteq P_R$.
- (2) Moreover, if S/R is integral, then for any prime $P_R \triangleleft R$ we have $(P_RS) \cap R = P_R$, and in particular there exists a prime ideal $P_S \triangleleft S$ lying over P_R .

Proof. We did the left to right direction of (1) last time.

Suppose that $P_RS \cap R \subseteq P_R$. Define $M = R \setminus P_R$ (since P_R is prime, M is multiplicatively closed). Then $(P_RM) \cap M = P_RM \cap R \setminus P_R = \emptyset$. Let $P_R \subseteq P_S \triangleleft S$ be maximal such that $P_S \cap M = \emptyset$. Then:

$$P_S \cap M = \emptyset \implies P_S \cap R \setminus P_R = \emptyset \implies P_S \cap R \subseteq P_R,$$

and hence $P_S \cap R \subseteq P_R$, and P_S is prime by Exercise 4.1.

We proceed to prove (2) using the Cayley–Hamilton theorem. Assume that S/R is integral. Let $a := p_1^R r_1^S + \cdots + p_m^R r_m^S \in P_RS \cap R$, where $p_1^R, \dots, p_m^R \in R$ and $r_1^S, \dots, r_m^S \in S$. Consider $N = R[r_1^S, \dots, r_m^S]$ (N is finitely generated since $r_1^S, \dots, r_m^S$ are integral, which allows us to use

Cayley–Hamilton). Since M is finitely generated, by Cayley–Hamilton for the map $\varphi: N \rightarrow P_R N \subseteq N$ defined by $x \mapsto ax$ gives:

$$\varphi^n + c_{n-1}\varphi^{n-1} + \cdots + c_0 \equiv 0,$$

for some $c_1, \dots, c_n \in P_R$. Substitue $x = 1$ to get:

$$a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0,$$

or equivalently,

$$a^n = -c_{n-1}a^{n-1} + \cdots - c_0 \in P_R,$$

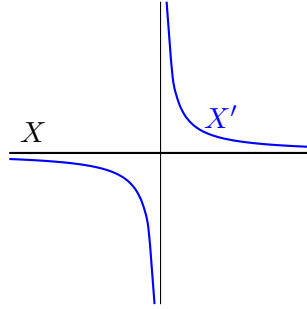
and since P_R is prime $a \in P_R$, which completes the proof. $\square$

Exercise 4.1. Let $M \subseteq R$ be a multiplicatively closed subset disjoint from $I \triangleleft R$. Let $I \subseteq P \triangleleft R$ be maximal such that $P \cap M = \emptyset$. Then P is prime.

Proof. Left to us, the readers. $\square$

Remark 4.9. We mainly use the result from Theorem 4.5 (and the result from Theorem 4.6) in order to find out if a given ring extension S/R is integral or not.

Example 4.4. Let $X = \mathbb{A}^1$ and $X' = V(xy - 1) \subseteq \mathbb{A}^2$, and let $\pi: X' \rightarrow X$ be the projection map defined by $(x, y) \mapsto x$.



Let $S = k[X'] = k[x, y]/(xy - 1)$ (recall that this is the coordinate ring of the variety X' . we may also assume $k = \mathbb{C}$). By definition, $R = \pi^*(k[X])$ (where π^* is the pullback map of rings induced by the map π on the varieties), so that S/R is a ring extension. Note that π^* is not an isomorphism (since π is not an isomorphism of varieties), however, it is injective, so by restricting it to its image we get that $\tilde{\pi}^*: k[X] \rightarrow R$ is an isomorphism.

Next, we want to figure out if S/R is an integral extension. The point $0 \in X$ has no source in X' (geometrically, “it has no point above it”). Algebraically, the fact 0 has no source, or that the ideal at 0 (which is (x)) has no ideal lying over it follows from Theorem 4.5 by the fact the equation

$$\begin{array}{ccc} \square & \triangleleft & S \\ \uparrow & & \uparrow \\ (x) & \triangleleft & R \cong k[X] \end{array}$$

has no prime solution for $\square$, and no solution in maximal ideas. Thus S/R is not an integral extension.

Theorem 4.6 (Going up). *Let R'/R be an integral extension. Let $P, Q \triangleleft R$ be prime ideals such that $P \subseteq Q$ and let $P' \triangleleft R'$ be a prime ideal lying over P . Then there exists a prime ideal $Q' \triangleleft R'$ which is lying over Q such that $P' \subseteq Q'$.*

Proof. The kernel of the projection $R \rightarrow R' \rightarrow R'/P'$ given by $x \mapsto x \mapsto x + P'$ is $R \cap P' = P$. Thus $R/P \hookrightarrow R'/P'$ given by $x + P \mapsto x + P'$ identifies R/P with its image in R'/P' . Since R'/R is integral so is $(R'/P')/R/P$. Thus, by Theorem 4.5, there exists a prime $Q'/P' \triangleleft R'/P'$ lying over Q/P , such that $Q'/P' \cap R/P = Q/P$, or equivalently $Q' \cap R = Q$. The proof is finished, but we add that the “lying over” diagram for convenience.

$$\begin{array}{ccc} \boxed{Q'/P'} & \triangleleft & R'/P' \\ \uparrow & & \uparrow \\ Q/P & \triangleleft & R/P \end{array}$$

□

Example 4.5. Let $k = \mathbb{C}$, let $R = k[\mathbb{A}^1] = k[x]$ be identified with its image in $R' = k[x, y]/(xy - 1) \cap (x, y)$. Let $X = \mathbb{A}^1$ and $X' = V(xy - 1) \cup V(x, y) = V((xy - 1) \cap (x, y))$. If the extension were integral, by the “going up” theorem, the “going up diagram equation”

$$\begin{array}{ccc} R' & (xy - 1) & \subseteq \quad \square \\ \downarrow & \downarrow & \downarrow \\ R & (0) & \subseteq \quad (x) \end{array}$$

has no solution, that is because $P' = (xy - 1) \triangleleft R'$ is a prime lying over (0) , and (x, y) is the only prime ideal lying over $Q = (x)$, but $(xy - 1) \subsetneq (x, y)$. Hence R'/R is not an integral extension.

Example 4.6. Let $X = \mathbb{A}^1$ and $X' = \mathbb{A}^1 \cup \{(0, 1)\} \subset \mathbb{A}^2$, with the projection map $\pi: X' \rightarrow X$ defined by $\pi(x, y) = x$. Let $Q' := (x, y - 1)$ be the point ideal corresponding to $(0, 1)$. On the level of rings, R is the image of $k[x]$ in $R' = k[x, y]/(y) \cap (x, y - 1)$. The corresponding ideals are $P = (0)$ and $Q = (x)$, and $Q' = (x, y - 1)$. Then, the diagram equation:

$$\begin{array}{ccc} R' & \square & \subseteq \quad Q' \\ \downarrow & \downarrow & \downarrow \\ R & P & \subseteq \quad Q \end{array}$$

has no solution since:

- $Q' \cap R = (x) = Q$
- there is no $P' \subseteq Q'$ prime such that $P' \cap R = (0)$.

It follows that R'/R is not an integral extension.

Theorem 4.7 (Going down). *Let R'/R be an integral extension such that R is normal (has no nilpotent elements) and R' is an integral domain. Let $P \subseteq Q$ be primes in R and $Q' \triangleleft R'$ be a prime lying over Q . Then there exists a prime $P' \triangleleft R'$ such that $P' \subseteq Q'$ lying over P . Equivalently, we have a prime solution for the following equation:*

$$\begin{array}{ccc} R' & \square & \subseteq \quad Q' \\ \downarrow & \downarrow & \downarrow \\ R & P & \subseteq \quad Q \end{array}$$

Proof. Since R' is an integral domain, we may identify it with its image in the localization $R'_{Q'}$.

Claim: There exists a prime $P'_{Q'} \triangleleft R'_{Q'}$ such that $P'_{Q'} \cap R = P$.

If this claim is correct, then $P'_{Q'}$ is of the form $P'R'_{Q'}$ (by characterization of ideals in localized rings any ideal is of this form) for a prime $P' \subseteq Q'$ of R' and

$$P' \cap R = (P'_{Q'} \cap R') \cap R = P'_{Q'} \cap R = P,$$

which completes the proof.

Proof of claim: In order to prove the claim, it suffices to verify that the conditions for the lying over theorem (Theorem 4.5) are satisfied, and then result follows from it immediately. The main condition we need to show is:

$$PR'_{Q'} \cap R \subseteq P.$$

Suppose $a \in PR' \cap R$. Then $a = \frac{p}{s}$ for $p \in PR'_{Q'}$ and $s \in R' \setminus Q'$. In order to verify the condition, we will use the following version of Gauss' lemma:

Lemma 4.8 (Gauss' lemma). *Let R'/R be an integral extension of integral domains such that R is normal and $P \triangleleft R$ is prime. Let $a \in PR'$ and let $f \in F[x]$ be the minimal polynomial of a over $F = \text{Frac}(R)$. Then $f \in R[x]$ and all of its coefficients but the leading coefficient are in P .*

By Gauss' lemma the minimal polynomial of p is:

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in R[x],$$

for $c_i \in P$. Then

$$\frac{1}{a^n} f(ax) = x^n + \frac{c_{n-1}}{a} x^{n-1} + \cdots + \frac{c_0}{a^n}$$

is the minimal polynomial of $s \in R'$ over F . By the lemma, $c'_i := \frac{c_i}{a^{n-i}} \in R$ or $a^{n-i}c'_i = c_i \in P$. Assume, by way of contradiction, that $a \notin P$, and the $c'_i \in P$ for all i . Thus,

$$s^n = -c'_{n-1}s^{n-1} - \cdots - c'_0 \in P,$$

hence $s \in P$ which is a contradiction. This contradiction completes the proof. $\square$

Exercise 4.2 (Gauss' lemma, slightly weaker version). Let R be a normal domain and $F = \text{Frac}(R)$ be its fraction field. If $g \in R[x]$ is monic, and $g = f \cdot h \in F[x]$ for a monic h , then $f, h \in R[x]$.

Proof of Theorem 4.8. Write:

$$p = p_1a_1 + \cdots + p_ka_k \in PR',$$

for $p_i \in P$ and $a_i \in R'$. Replace R' by $R[a_1, \dots, a_k]$, a finite extension of R .

Since R'/R is a finite extension, we can apply the Cayley–Hamilton theorem on $\varphi: R' \rightarrow R$ defined by:

$$\varphi(x) := px \in PR',$$

and get that:

$$\varphi^n + c_{n-1}\varphi^{n-1} + \cdots + c_0 = 0,$$

for some $c_i \in P$. We can now plug in 1 to get

$$g(p) := p^n + c_{n-1}p^{n-1} + \cdots + c_0 = 0.$$

Since $g = f \cdot h$, and g is monic, and h is a minimal polynomial and hence monic, so by Exercise 4.2, $f, h \in R[x]$.

Note that $(\text{mod } P)$ we have that:

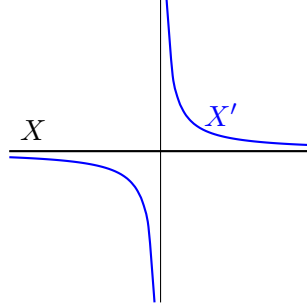
$$g(x) = x^n \pmod{P}.$$

Thus $f \equiv x^k \pmod{P}$, and $h \equiv x^{n-k} \pmod{P}$, and hence the nonleading coefficients of f are in P , which completes the proof. $\square$

5 Noether's lemma

5.1 Noether's lemma

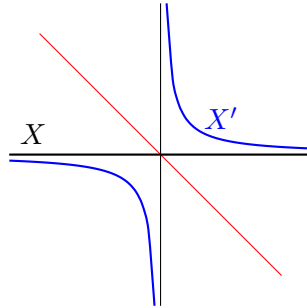
Example 5.1. Let $R' := \mathbb{C}[x_1, x_2]/(x_1x_2 - 1)$ be the coordinate ring of functions on $X' = V(x_1x_2 - 1)$, and let $R = \mathbb{C}[x_1]$ be identified with its image in R' .



We have seen in Example 4.4 that R'/R is not an integral extension, by the lying over theorem. We will show that by a change of coordinates we *could* get an integral extension. The change of coordinates is:

$$\begin{aligned} x_1 &= y_1 + y_2 \\ x_2 &= y_2 - y_1 \end{aligned}$$

In these coordinates we get $R'[y_1, y_2]/(y_2^2 - y_1^2 - 1)$, which is integral over $R[y_1]$, not only because geometrically see that this is actually a projection of X' over the following red line:



in which every point has a “point over it”, but also because we see that it is simply the ring extension we get by adjoining the root of the monic polynomial $x^2 - y_1^2 - 1 \in \mathbb{C}[y_1][x]$.

Remark 5.1 (Goal). Given a finitely generated k -algebra R' , our next goal is to find a subring R such that $R \cong k[z_1, \dots, z_r]$ and R'/R is finite.

Definition 5.1 (Total degree of a monomial). Let $x_1^{a_1}x_2^{a_2} \cdots x_r^{a_r}$ be a monomial. We define its total degree to be

$$\text{td}(x_1^{a_1}x_2^{a_2} \cdots x_r^{a_r}) = a_1 + a_2 + \cdots + a_r.$$

Definition 5.2 (Total degree of a polynomial). The total degree of a polynomial is defined to be the maximal total degree of its monomials.

Definition 5.3 (Homogeneous polynomial). A polynomial $p \in k[x_1, \dots, x_r]$ is called homogeneous if all of its monomials have the same total degree.

Remark 5.2.

Lemma 5.1. *Let $0 \neq f \in k[x_1, \dots, x_n]$ be homogeneous polynomial over an infinite field k . Then there exist $a_1, \dots, a_{n-1}$ such that $f(a_1, \dots, a_{n-1}, 1) \neq 0$.*

Proof. We simply prove this by induction on n . In the base case $n = 1$ we have $f(x_1) = cx_1^k$, for $c \neq 0$, and then $f(1) = c \neq 0$. Next we suppose the claim holds for all $n > k \geq 1$, and show the claim for n . Write f as a “polynomial in x_1 ” as follows:

$$f(x_1, \dots, x_n) = \sum_{i=0}^d f_i(x_2, \dots, x_n) x_1^i,$$

where f_i is homogeneous of degree $d - i$ or $f_i \equiv 0$. Since $f \neq 0$, we get $f_m \neq 0$ for some $0 \leq m \leq d$. By induction, there exist $a_2, \dots, a_{n-1} \in k$ such that its dehomogenization in the last coordinate is nonzero:

$$f_m(a_2, \dots, a_{n-1}, 1) \neq 0,$$

and hence the polynomial

$$0 \neq f(x, a_2, \dots, a_{n-1}, 1) \in k[x]$$

is a polynomial, with finitely many roots (and it is not the zero polynomial). Since k is infinite, there exists $a_1 \in k$ such that

$$f(a_1, a_2, \dots, a_{n-1}, 1) \neq 0,$$

which completes the proof. $\square$

Lemma 5.2. *Let $0 \neq f \in k[x_1, \dots, x_n]$ be a polynomial over an infinite field. Then there exists $a_1, \dots, a_{n-1}, \lambda \in k$ and a change of coordinates such that:*

$$\lambda f(y_1 + a_1 y_n, y_2 + a_2 y_n, \dots, y_{n-1} + a_{n-1} y_n, y_n) \in k[y_1, \dots, y_n],$$

is monic in y_n .

Proof. Let d be the total degree of f and write:

$$f = \sum_{k_1, \dots, k_n} c_{k_1, \dots, k_n} x_1^{k_1} \cdots x_n^{k_n},$$

such that $c_{k_1, \dots, k_n} \in k$. Then:

$$\begin{aligned} \lambda f(y_1 + a_1 y_n, y_2 + a_2 y_n, \dots, y_{n-1} + a_{n-1} y_n, y_n) \\ = \sum_{k_1, \dots, k_n} c_{k_1, \dots, k_n} (y_1 + a_1 y_n)^{k_1} \cdots (y_{n-1} + a_{n-1} y_n)^{k_{n-1}} y_n^{k_n}. \end{aligned}$$

The leading coefficient is:

$$\lambda \sum_{k_1 + \dots + k_n = d} c_{k_1, \dots, k_n} a_1^{k_1} \cdots a_{n-1}^{k_{n-1}} \cdot y_n^{k_1 + \dots + k_n} \cdot 1^{k_n} = \lambda f_d(a_1, \dots, a_{n-1}, 1) y_n^d,$$

for a homogeneous polynomial $f_d \neq 0$ of degree d . By Theorem 5.1 we can pick $a_1, \dots, a_{n-1} \in k$ (remember they were free variables so far) such that $f_d(a_1, \dots, 1) \neq 0$, and the claim follows by picking $\lambda = 1/f_d(a_1, \dots, a_{n-1}, 1)$. $\square$

Lemma 5.3 (Noether's lemma). *Let R be a finitely generated k -algebra. Then there exists an injective homomorphism $i: k[z_1, \dots, z_r] \rightarrow R$ such that $R/\text{im}(i)$ is a finite extension.*

Proof. Suppose that R is generated over k by $x_1, \dots, x_n$. We prove this lemma by induction on n . In the base case $n = 0$ we have $R = k$ and the claim is immediate. Suppose $n > 0$.

Case I: $x_1, \dots, x_n$ are algebraically independent. In this case $i: k[z_1, \dots, z_n] \rightarrow R$ defined by $i(z_i) = x_i$ is an isomorphism, which completes the proof.

Case II: $x_1, \dots, x_n$ are not algebraically independent. In this case suppose $f \neq 0$ is a polynomial in n variables such that $f(x_1, \dots, x_n) = 0 \in R$. As in Theorem 5.2, we pick $a_1, \dots, a_{n-1}, \lambda$ such that if:

$$\begin{aligned} y_1 &= x_1 - a_1 y_n \\ &\vdots \\ y_{n-1} &= x_{n-1} - a_{n-1} y_n \\ y_n &= x_n, \end{aligned}$$

then $R = k[y_1, \dots, y_n]$ and now:

$$\lambda f(y_1 + a_1 y_n, y_2 + a_2 y_n, \dots, y_{n-1} + a_{n-1} y_n, y_n) \in k[y_1, \dots, y_n],$$

is a monic polynomial in y_n . Thus, $R = k[y_1, \dots, y_n]$ is a finite extension of $k[y_1, \dots, y_{n-1}]$. By induction, $k[y_1, \dots, y_{n-1}]/k[z_1, \dots, z_r]$ is a finite extension, for some subalgebra $k[z_1, \dots, z_r]$ isomorphic to a polynomial ring. Since both the first extension $k[y_1, \dots, y_n]/k[y_1, \dots, y_{n-1}]$ and the second extension $k[y_1, \dots, y_{n-1}]/k[z_1, \dots, z_r]$ are finite, then we conclude that $R/k[z_1, \dots, z_r]$ is finite, which completes the proof. $\square$

5.2 More nullstellensatzs

Corollary 5.4 (Algebraic version of the weak nullstellensatz). *Let R be a finitely generated k -algebra. If R is a field, then R/k is a finite field extension.*

Proof. By Noether's lemma, R is a finite extension of a polynomial ring $k[z_1, \dots, z_r]$ in variables $z_1, \dots, z_r$. The following diagram is just for visual aid for the following and last part of the proof:

$$\begin{array}{ccc} R & & \square \\ \downarrow & & \\ k[z_1, \dots, z_r] & & p \\ \parallel & & \\ k & & \end{array}$$

Since $R/k[z_1, \dots, z_r]$ is finite, by the lying over theorem, there is no nontrivial prime ideal in $k[z_1, \dots, z_r]$. But $k[z_1, \dots, z_r]$ is a polynomial ring! This implies that $r = 0$ and R/k is finite. $\square$

Remark 5.3. If $k = \bar{k}$, then R/k cannot be finite unless $R = k$, and thus we get $R = k$.

Corollary 5.5 (Nullstellensatz, weak version). *Let $k = \bar{k}$ be an algebraically closed field. Then every maximal ideal M in a polynomial ring $R = k[x_1, \dots, x_n]$ is a point ideal $M = I(\mathbf{a}) = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$, for some $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{A}_k^n$.*

Proof. Let $M \triangleleft k[x_1, \dots, x_n]$ be a maximal ideal. Then R/M is a field. But R/M is also a finitely generated k -algebra with the homomorphism $\varphi: k \rightarrow R/M$ defined by $\varphi(\alpha) = \alpha + M$. (then R/M is generated by the finitely many $\bar{x}_i = x_i + M$).

Since $k = \bar{k}$, by the algebraic version of the nullstellensatz and Remark 5.3 we have $R/M \cong \text{im}(\varphi)$, so φ is an isomorphism. Let $a_i \in k$ be $\varphi^{-1}(\bar{x}_i)$. Then $\bar{x}_i = \bar{a}_i$, which equivalently means that $x_i - a_i \in M$ for all i , and hence $I(\mathbf{a}) = (x_1 - a_1, \dots, x_n - a_n) \subseteq M$. We have seen that $I(\mathbf{a})$ is maximal, and hence $M = I(\mathbf{a})$. $\square$

Remark 5.4. We have seen before that I is geometric if and only if it is radical. The strong formulation of the nullstellensatz is as follows.

Theorem 5.6 (Nullstellensatz strong form). *Let $X \subseteq \mathbb{A}_k^n$ be a variety and $I \triangleleft k[X] = R$. Then $I(V(I)) = \sqrt{I}$. In particular, if I is radical, it is geometric.*

Theorem 5.7 (Algebraic version of the strong nullstellensatz). *Let R be a finitely generated k -algebra, and $I \triangleleft R$. Then $\sqrt{I} = \bigcap_{P \supseteq I} P$.*

Remark 5.5. Recall that the algebraic form of the strong nullstellensatz implies the strong nullstellensatz. We will show this under the additional assumption of the strong nullstellensatz which is $k = \bar{k}$.

Let $f \in \sqrt{I}$. This implies that $f^n \in I$ for some $n \geq 1$ so $f^n(a) = 0$ for all $a \in V(I)$, and then $f \equiv 0$ on $V(I)$ so $f \in I(V(I))$.

On the other hand if $f \notin \sqrt{I}$, by the algebraic version of the nullstellensatz there exists a maximal ideal $I \subseteq P \triangleleft R$ such that $f \notin P$. By the weak nullstellensatz (which we can use since $k = \bar{k}$),

$$P = I(a) = (x_1 - a_1, \dots, x_n - a_n),$$

for some $a = (a_1, \dots, a_n) \in X \subseteq \mathbb{A}^n$. Since $I \subseteq I(a)$, we have $a \in V(I)$. Since $f \notin I(a)$, we have $f(a) \neq 0$ and $f \notin I(V(I))$.

Proof of Theorem 5.6. Recall that we need to show that $\sqrt{I} = \bigcap_{P \supseteq I} P$.

First let $f \in \sqrt{I}$, we get $f^n \in I$ so $f^n \in P$ but $P \supseteq I$ max is prime so $f \in P$ for all such P , so $f \in \bigcap_{P \supseteq I} P$.

On the other hand (we use the Rabinowich trick), suppose $f \in R \setminus \sqrt{I}$. Let:

$$S := \{1, f, f^2, \dots\}$$

be a multiplicative set, and let $R_f = S^{-1}R$ be the localization at S . Since $f \notin \sqrt{I}$, we have $I \cap S = \emptyset$, and by an exercise from the homework, there exists a prime $I \subseteq P \triangleleft P$ such that $P \cap S = \emptyset$ and:

$$P_f = S^{-1}P = \left\{ \frac{p}{f^i} \mid p \in P \text{ and } i \geq 0 \right\}$$

is a maximal ideal in R_f . Since P is a prime, R/P is an integral domain. Thus R/P can be identified with its image in $(R/P)_f$ since $(R/P)_f \cong R_f/P_f$ and $P_f \triangleleft R_f$ is maximal, $(R/P)_f$ is a field.

Since R/P and hence $(R/P)_f$ is a finitely generated k -algebra, the algebraic version of the weak nullstellensatz (Theorem 5.4) implies that $(R/P)_f/k$ is a finite extension. Thus, $(R/P)/k$ is a finite extension and hence R/P is a field. $\square$

6 Noetherian rings

6.1 Noetherian rings

Definition 6.1 (Noetherian module). Let M be an R -module. Then M is called Noetherian if every chain:

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq \cdots$$

of submodules of M stabilizes, that is, $M_i = M_{i+1}$ for all $i > i_0$ for some i_0 .

Definition 6.2 (Noetherian ring). A ring is R is called Noetherian if R is Noetherian as an R -module.

Remark 6.1. R is Noetherian if and only if every ascending chain of ideals stabilizes.

Example 6.1. The following are Noetherian modules:

- (1) All fields k .
- (2) A vector space V over k is Noetherian if and only if $\dim V < \infty$.

Example 6.2. The ring $R[x_1, x_2, \dots] := \bigcup_{n \in \mathbb{N}} k[x_1, \dots, x_n]$ is not Noetherian. We have the infinite chain:

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots$$

Lemma 6.1. Let M be an R -module. Then the following are equivalent:

- (1) M is Noetherian.
- (2) Every nonempty family of submodules has a maximal element.
- (3) Every submodule of M is finitely generated.

Proof. It is clear that (1) $\rightarrow$ (2) is just Zorn's lemma. In order to show (2) $\rightarrow$ (3), Let $N \leq M$ be a submodule. If $N \neq 0$, pick $0 \neq x_1 \in N$ and define $N_1 = \langle x_1 \rangle$. If $N_1 \neq N$, pick $x_2 \in N \setminus N_1$, and define $N_2 = \langle x_1, x_2 \rangle$. If the process doesn't stop, we will get an infinite increasing chain of submodules with no maximal element, in contradiction to our assumption (2). Thus, the process must eventually stop, which implies that $N = N_i$ for some i , and hence M is finitely generated. In order to show (3) $\rightarrow$ (1), let

$$M_1 \subsetneq M_2 \subsetneq \cdots$$

the union $M_\infty = \bigcup_{i=1}^\infty M_i$ is a submodule, and hence it is finitely generated. Since each x_i is contained somewhere in the chain, there exists some i_0 such that all generators are in M_{i_0} , hence $M_i = M_\infty$, hence the sequence stabilizes eventually so M is Noetherian. $\square$

Remark 6.2.

- (1) If R is Noetherian, every $I \triangleleft R$ is finitely generated.
- (2) If R is Noetherian and $J \triangleleft R$, then R/J is Noetherian (Ideals in R/J are of the form I/J for $J \subseteq I \triangleleft R$).

6.2 Hilbert's basis theorem

Theorem 6.2 (Hilbert's basis theorem, 1890). *Let R be a Noetherian ring. Then any polynomial ring $R[x]$ is also Noetherian.*

Proof. Assume, by way of contradiction, that $R[x]$ is not Noetherian. Thus, there exists an ideal $I \subsetneq R[x]$ which is not finitely generated. Pick a sequence $f_1, f_2, \dots$ such that f_{k+1} is a polynomial of minimal degree in I but not in $(f_1, \dots, f_k)$ for all k . In particular, the sequence of degrees:

$$d_1 = \deg f_1 \leq d_2 = \deg f_2 \leq d_3 \leq \dots$$

is not decreasing. Write:

$$f_k = a_k x^{d_k} + (\text{lower term}).$$

Since R is Noetherian, the sequence:

$$(a_1) \subseteq (a_1, a_2) \subseteq \dots$$

stabilizes from some index $s \in \mathbb{N}$. Thus, $a_{s+1} = c_1 a_1 + \dots + c_s a_s$ for some $c_i \in R$. Then the leading coefficient of $x^{d_{s+1}}$

$$c_1 f_1 x^{d_{s+1}-d_1} + \dots + c_s f_s x^{d_{s+1}-d_s} \in I$$

is $c_1 a_1 + \dots + c_s a_s = a_{s+1}$. Thus,

$$f'_{s+1} := f_{s+1} - c_1 f_1 x^{d_{s+1}-d_1} - \dots - c_s f_s x^{d_{s+1}-d_s} \in I$$

is of smaller degree but $f'_{s+1} \notin (f_1, \dots, f_s)$ since $f_{s+1} \notin (f_1, \dots, f_s)$. □

Corollary 6.3. *Every finitely generated ring S over a Noetherian ring R is Noetherian. In particular, the polynomial ring $R[x_1, \dots, x_n]$ is Noetherian.*

Proof. Suppose $S = R[z_1, \dots, z_k]$ with some relations between the z_i . Then there exists an epimorphism $\pi: R[x_1, \dots, x_k] \rightarrow R[z_1, \dots, z_k] = S$ defined $x_i \mapsto z_i$, and $S \cong R[x_1, \dots, x_k] / \ker \pi$. Now since $R[x_1, \dots, x_k]$ (the variables have no relations) is Noetherian (by applying Hilbert's basis theorem k times), so is its quotient S . □

Corollary 6.4. *Every finitely generated k -algebra is Noetherian. In particular $k[X]$ is Noetherian for $X \subseteq \mathbb{A}_k^n$ a variety. Moreover, any subvariety $Y \subseteq X$ is the zero locus of finitely many functions in $k[X]$. Equivalently, we have $I_X(Y) = (f_1, \dots, f_r)$. In fact every sequence of subvarieties:*

$$Y_0 \supseteq Y_1 \supseteq \dots$$

stabilizes since it corresponds to $I(Y_0) \subseteq I(Y_1) \subseteq \dots$.

Remark 6.3 (Artinian ring). An Artinian ring is a notion equivalent to a Noetherian ring where the chains are decreasing instead of increasing. This is a much stronger condition and not as many rings are Artinians. In commutative algebra we even have that any Artinian ring is also Noetherian. This notion is less relevant in this course, and is studied more thoroughly in noncommutative algebra.

Remark 6.4. Recall definitions of dimension discussed in the previous sections.

Example 6.3. If $R = k$ is a field, then $\dim R = 0$ since the longest sequence of primes is (0) .

Example 6.4. If R is a PID (for example $k[x]$ but not $k[x, y]$) but not a field, then $\dim R = 1$. The maximal chain is $(0) \subsetneq M$ where M is maximal. We also have that $\dim R[x_1, \dots, x_n] = n$ and $\dim \mathbb{A}_k^n = n$, and the following theorem will show this.

Theorem 6.5. *Every maximal chain of primes:*

$$C := (P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_m)$$

in $k[x_1, \dots, x_n]$ is of length $m = n$. In particular $\dim k[x_1, \dots, x_n] = n$.

Exercise 6.1. In a Noetherian UFD R every minimal prime ideal is principle.

Exercise 6.2. Given an integral extension of finitely generated k -algebras and prime ideals P_1, P_2, P_3, Q_1, Q_2 as in (diagram to be added), then there exists $Q_1 \subsetneq Q_2 \subsetneq Q_3$.

Lemma 6.6 (Incomparability lemma). *If R'/R is integral and $P \triangleleft R$ and $P', Q' \triangleleft R'$ are ideals lying over P . Then $P' \not\supsetneq Q'$.*

Proof of Theorem 6.5. By induction on n . For $n = 0$ or $n = 1$ see examples from earlier. We claim that in the chain C we have $m = n$. Since C is maximal, $P_0 = (0)$ and P_1 is a minimal prime, and P_m is maximal.

By Exercise 6.1, we have $P_1 = (f)$ for some $0 \neq f \in k[x_1, \dots, x_n]$. Let $R' := k[x_1, \dots, x_n]/P_1$, and $R := k[x_1, \dots, x_{n-1}]$. Then the chain of primes:

$$(0) = P_1/P_1 \subsetneq P_2/P_1 \subsetneq P_m/P_1$$

is lying over

$$(0) = P_1/P_1 \cap R \subsetneq P_2/P_1 \cap R \subsetneq P_m/P_1 \cap R.$$

By a change of variables using Noether's lemma we can assume f is monic in x_n . Thus we get that R'/R is integral and the map from R to R' is injective, so we can use the incomparability lemma to get that P_i/P_1 and P_{i+1}/P_1 are not lying over the same prime, so $R \cap P_i/P_1 \subsetneq R \cap P_{i+1}/P_1$ for all i . Now we can conclude that

$$(0) = P_1/P_1 \cap R \subsetneq P_2/P_1 \cap R \subsetneq P_m/P_1 \cap R$$

is a maximal chain by the second exercise plus the going up theorem (note that the length of this chain is $m - 1$ not m since earlier we defined m to be the length of C which going from P_0 to P_m). Thus by induction we conclude that $m - 1 = n - 1$, so $m = n$ which completes the proof. $\square$

Proof of Theorem 6.6. Assume on the contrary that $P' \subseteq Q'$, and $a \in Q' \setminus P'$. Since R'/P' is integral over R/P , the element $\bar{a} \in R'/P'$ satisfies:

$$\bar{a}^n + \bar{c}_{n-1}\bar{a}^{n-1} + \cdots + \bar{c}_0 = 0,$$

for some $c_i \in R$. Assume that this polynomial that vanishes on $\bar{a}$ has minimal degree. Since $\bar{a} \in Q'/P'$,

$$\bar{c}_0 = -\bar{a}^n - \cdots - \bar{c}_1\bar{a} \in Q'/P',$$

and hence $c_0 \in Q' \cap R = P$, so $\bar{c}_0 = 0$. Since R/P is an integral domain we get that:

$$\bar{a}^{n-1} + \cdots + \bar{c}_1 = 0,$$

which contradicts the minimality we assumed previously, and completes the proof. $\square$

Exercise 6.3. Let $R = \mathbb{C}[x]$ and $R' = \mathbb{C}[x, y, z]/(z^2 - y^3)$. Check if R'/R is integral.

Solution. We have that both (x) and (x, y, z) are lying over (x) , and thus by the incomparability lemma R'/R cannot be integral.

Remark 6.5. Our next goal is to find the dimension of $k[x_1, \dots, x_n]/P$ for any prime ideal P .

Definition 6.3 (Height of an ideal). The codimension (or height) of a prime ideal $P \triangleleft R$ is:

$$\text{codim}_R(P) := \sup \{n \mid \text{there exists } P = P_n \supsetneq \cdots \supsetneq P_0 \text{ of length } n\}.$$

Remark 6.6. The height of an ideal could potentially be ∞ .

Definition 6.4 (Codimension of a subvariety). For an irreducible subvariety $Y \subseteq X$, we define the codimension of Y by:

$$\text{codim } Y := \text{codim}_{k[X]} I_X(Y).$$

Remark 6.7. This is the maximal length of a chain of irreducible subvarieties:

$$Y = Y_n \subsetneq \cdots \subsetneq Y_0 \subseteq X.$$

Proposition 6.7. Let R be a ring of dimension n such that every maximal chain of prime ideals is of length n . Let $P \triangleleft R$ be a prime. Then:

$$\dim R = \text{codim}_R P + \dim R/P.$$

Moreover, every maximal chain of primes in R/P is of length $\dim R - \text{codim } P$.

Proof. Every maximal chain of prime ideals in R/P corresponds to a maximal chain of primes:

$$P = Q_0 \subsetneq \cdots \subsetneq Q_r \subseteq R,$$

in R . By definition of $s = \text{codim}_R P$, there exists a maximal chain:

$$P = P_s \supsetneq \cdots \supsetneq P_0.$$

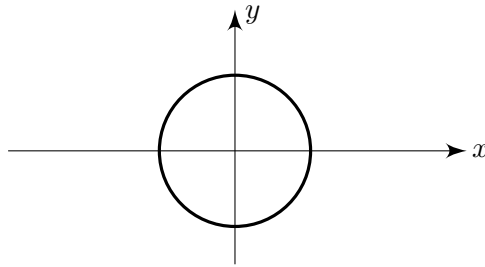
Thus,

$$\underbrace{P_0 \subsetneq \cdots \subsetneq P_s}_{\text{codim}_R P} = P = \underbrace{Q_0 \subsetneq \cdots \subsetneq Q_r}_{\dim R/P} \subseteq R$$

is a maximal chain in R . Thus, its length is $n = \dim R = r + s$. In total, we have that $\dim R \geq \dim R/P + \text{codim}_R P \geq r + s = \dim R$. Thus all inequalities are actually equalities, and every maximal chain in R/P is of length $\dim R/P$. $\square$

Exercise 6.4. Let $X = V(x^2 + y^2 - 1) \subseteq \mathbb{A}_k^2$ for an algebraically closed field $k = \bar{k}$. Show that $\dim k[X] = 1$.

Solution. Our variety is of the shape:



Since $P = (x^2 + y^2 - 1) \triangleleft k[x, y]$ is prime, thus,

$$\{0\} \subsetneq P = (x^2 + y^2 - 1) \subsetneq (y, x - 1) =: m$$

is a maximal chain of primes in $k[x, y]$. Thus,

$$\{0\} = P/P \subsetneq m/p$$

is a maximal chain in R/P , and we conclude that $\dim R/P = 1$. We then compute using Theorem 6.7 that:

$$\text{codim } P = \dim R - \dim R/P = 2 - 1 = 1.$$

Corollary 6.8. *For every finitely generated k -algebra R , which is an integral domain, all maximal chains of primes are of the same length $\dim R$.*

Proof. If $R = k[z_1, \dots, z_n]$ (where the z_i may have relations), there exists $\varphi: k[x_1, \dots, x_n] \rightarrow R$ given by $x_i \mapsto z_i$ whose kernel $P = \ker \varphi$ is a prime (since $k[x_1, \dots, x_n]/P \cong R$ which is an integral domain). Now the claim follows from the proposition (add reference). $\square$

Example 6.5. In $R = k[x, y]/(y) \cap (x, y - 1)$ both $(x, y - 1)$ and $(y) \subsetneq (x, y)$ are maximal chains.

6.3 Noetherian normalization

Definition 6.5 (Noetherian normalization). Given $\dim X = \dim k[x_1, \dots, x_n]/I(X)$ we find $k[X]/k[y_1, \dots, y_m]$ finite then $\dim X = m$.

Example 6.6. Let $X = V(y^2 - x^2) \subseteq \mathbb{A}^2$ and $R' = k[X] = k[x, y]/(y^2 - x^2)$ and $R = k[\mathbb{A}^1]$ is the coordinate projection of the variety onto $\mathbb{A}^1$. The resulting R'/R is an integral extension with $\dim R' = \dim R$.

Proof $\dim R' \geq \dim R$: Given a maximal chain $P_0 \subsetneq \dots \subsetneq P_n$ of primes in R , we may pick Q_0 to be a prime over P_0 by “lying over”. By going up we may choose primes $Q_1, \dots, Q_n$ lying over $P_1, \dots, P_n$ respectively such that $Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_n$, which completes the first direction of the proof.

In order to show the other direction let $Q_0 \subsetneq \dots \subsetneq Q_n$ be a chain of primes in R' . We define $P_i := Q_i \cap R$ a chain of rising ideals in R below Q_i . By the incomparability lemma $P_{i+1} \neq P_i$ for all i so $P_0 \subsetneq \dots \subsetneq P_n$ is a chain of primes of length at least n , which completes the second direction and completes the proof.

Corollary 6.9. *Let R be a finitely generated k -algebra, and $i: k[x_1, \dots, x_n] \hookrightarrow R$ a Noetherian normalization. Then $\dim R = n$.*

Proof. In a Noetherian normalization $R/i(k[x_1, \dots, x_n])$ is integral and hence by the previous proposition $\dim R = \dim k[x_1, \dots, x_n] = n$. $\square$

Remark 6.8. In particular, the number of variables in any two Noetherian normalizations is the same.

Recall: (definition of transcendence degree) For a finitely generated field extension E/K we define $\text{tr. deg.}_K E$ to be the maximal number of algebraically independent elements over K .

Corollary 6.10. *Let R be a finitely generated k -algebra such that R is an integral domain, and $F = \text{Frac}(R)$ its fraction field. Then $\dim R = \text{tr. deg.}_K F$.*

Proof. Let $k[x_1, \dots, x_n] \hookrightarrow R$ be a Noetherian normalization. From the second to last corollary $\dim R = n$. Since $R/k[x_1, \dots, x_n]$ is integral, $F/k(x_1, \dots, x_n)$ is algebraic and hence $\text{tr. deg. } F = \text{tr. deg. } k(x_1, \dots, x_n) = n = \dim R$. $\square$

7 Tangent spaces

7.1 Introduction and Nakayama's lemma

Let $X \subseteq \mathbb{A}^n$ be a variety and $\bar{a} = (a_1, \dots, a_n) \in X$. For $f \in k[x_1, \dots, x_n]$, we can define the *formal derivative* with respect to x_i just like we did in field theory (the definition coincide with standard polynomial differentiation).

We also define the formal differential $d: k[x_1, \dots, x_n]$ by:

$$f \mapsto d_a f := \sum \frac{\partial f}{\partial x_i}(\bar{a}) y_i$$

where $y_i = x_i - a_i$ for $i = 1, \dots, n$. The tangent space at $\bar{a}$ is

$$T_a X = V\left(\{d_a f \mid f \in I(a)\}\right).$$

Remark 7.1. Writing $I(X) = (f_1, \dots, f_r)$ one has $T_a X = V(df_1, \dots, df_r)$. This follows since for any $f, g \in I(X)$ and $h \in k[X]$ we have $d_a(f + g) = d_a f + d_a g$ and $d_a(hf) = h(\bar{a})d_a f + f(\bar{a})d_a h = h(\bar{a})d_a f$.

Lemma 7.1. Set $P = I_X(a)$. Then $\text{Hom}(T_a X, k)$ (in the category $\mathbf{Vect}_k$) which is $(T_a X)^*$ is isomorphic to P/P^2 as a vector space over $k[X]/P \cong k$.

Proof. Consider $\varphi: P \rightarrow \text{Hom}(T_a X, k)$ by $f \mapsto d_a f|_{T_a X}$. φ is well defined (exercise) and surjective (d is surjective). It is left to show that $\ker \varphi = P^2$.

For any $h_1, h_2 \in I_X(a)$ we clearly have $\frac{\partial(h_1 h_2)}{\partial x_i} = 0$ which shows $\ker \varphi \supseteq P^2$.

In the other direction for $\bar{f} \in P \subseteq k[X]$ such that $d_a f|_{T_a X} = 0$. We claim that $df = dg$ for some $g \in I(X)$, □

Remark 7.2. Recall that if $V(f_1, \dots, f_r) = X \subseteq \mathbb{A}^n$ is a variety, we define the tangent space by $T_a X = V(df_1, \dots, df_r)$.

We have seen that $\text{Hom}(T_a X, k) = P/P^2$ where P is the maximal ideal at the point a , that is, $P = I_X(a) \triangleleft k[X]$.

Proposition 7.2. Let R be a ring (for example $k[X]$ for some variety X), with a maximal $P \triangleleft R$ (for example $I_X(a)$). Set $R_p = S^{-1}R$ where $S = R \setminus P$. Similarly, we can consider $S^{-1}P/S^{-1}P^2 \in R_p\text{-mod}$. We claim that $S^{-1}P/S^{-1}P^2 \cong P/P^2$ as k -vector spaces where $k = R/P$.

Proof. We know that $M = P/P^2$ is an R -module, with a trivial P -action and hence a module over $R/P = k$, or since k is a field, a vector space. Since the image of S in $k = R/P$ consists of invertible elements,

$$S^{-1}M = \underbrace{S^{-1}k}_{=k} \otimes M \cong M,$$

as a k -vector space (the equality $S^{-1}k = k$ follows from the fact k is a field). Thus,

$$M \cong S^{-1}M \cong S^{-1}P/S^{-1}P^2,$$

as k -vector spaces. □

Definition 7.1 ((co)tangent spaces). For a Noetherian local ring R with a maximal ideal $P \triangleleft R$ and residue field $k = R/P$, its cotangent space is $\text{Hom}(T_a X, k) \cong P/P^2$, and its tangent space is the dual $\text{Hom}(P/P^2, k)$, and its dimension is $\dim_k P/P^2$.

Proposition 7.3. For a local Noetherian ring R with a maximal $P \triangleleft R$ and residue field $k = R/P$ with have the following:

- (1) $\dim_K P/P^2$ is the minimal size of a set of generators of P .
- (2) $\dim R \leq \dim_k P/P^2$.

Definition 7.2 (Frattini subgroup). Mentioned by name, to be added.

Lemma 7.4 (Nakayama's lemma). *Let $R \neq 0$ be a local ring with maximal $P \triangleleft R$ and let M be a finitely generated R -module. Then:*

- (1) $M = PM$ implies $M = (0)$.
- (2) Furthermore, if $M = N + PM$ for $N \leq M$, then $M = N$.
- (3) Furthermore, if $M/PM = \langle \overline{m_1}, \dots, \overline{m_r} \rangle = \text{span}_k \{ \overline{m_1}, \dots, \overline{m_r} \}$ for the images $\overline{m_i} \in M/PM$ of some $m_i \in M$, then $M = \langle m_1, \dots, m_r \rangle$.

Theorem 7.5 (Burnside basis theorem). *Mentioned by name.*

Proof of Theorem 7.4.

- (1) By the Cayley–Hamilton theorem for $\text{id}: M \rightarrow M = PM$, we have

$$\text{id}^n + a_{n-1} \text{id}^{n-1} + \dots + a_0 \text{id} \equiv 0$$

for some $a_i \in P$, which implies

$$(1 + \underbrace{a_{n-1} + \dots + a_0}_{:= -a}) \text{id} \equiv 0,$$

therefore $1 - a \in \text{Ann}_R(M) := \{r \in R \mid r \cdot m = 0 \text{ for all } m \in M\} \triangleleft R$. Hence $1 - a \in P$ which implies $1 \in P$, but by assumption $M \neq (0)$, so we get a contradiction, which completes the proof.

- (2) Since $M = N + PM$ implies that $M/N = P(M/N)$, by (1) we get $M/N = (0)$, hence $M = N$ which completes the proof.
- (3) Set $N = \langle m_1, \dots, m_r \rangle$, so that $M = N + PM$ and $M = N$ by (2).

□

Theorem 7.6 (Krull's theorem). *Let $I = (a_1, \dots, a_r) \triangleleft R$, and let $P \supseteq I$ be a minimal prime. Then $\text{codim } P \leq r$.*

Proof of Theorem 7.3.

- (1) Immediately follows by applying Nakayama's lemma (part (3)) to $M = P$.
- (2) By Krull's theorem, if $P = (a_1, \dots, a_r)$, then $\text{codim } P \leq r$, so by picking r to be the minimal number of generators we get $r = \dim_k P/P^2$ by (1). Since a maximal chain:

$$P_0 \subsetneq \dots \subsetneq P_{m-1} \subsetneq P_m = 0$$

of primes in R starts/ends (depending how you look at it) with P , we have $\text{codim } P = \dim R \leq \dim_k P/P^2$, which completes the proof.

□

Example 7.1. Let $X_1 = V(f_1) \subsetneq \mathbb{A}_{\mathbb{R}}^2$ and $X_2 = V(f_2) \subsetneq \mathbb{A}_{\mathbb{R}}^2$ for $f_1(x_1, x_2) = x_2 - x_1^2$ and $f_2(x_1, x_2) = x_2^2 - x_1^3 - x_1^2$.

Then we have that $d_{(0,0)}(f_1) = (-2x_1)|_0 \cdot y_1 + 1 \cdot y_2 = y_2$, but in this case $y_2 = x_2 - 0 = x_2$ so $d_{(0,0)}(f_1) = x_2$, and therefore $T_{(0,0)}X_1 = V(x_2) = x_1$ -axis, which is exactly what we would expect. If we compute the Jacobian we see that it is $J = \begin{pmatrix} 0 & 1 \end{pmatrix}$, which has dimension equal to the dimension of the tangent space (just like in smooth manifolds) $\dim T_{(0,0)}X_1 = \dim \ker J = n - \text{rank } J = 2 - 1 = \dim X_1$.

We also have that $d_{(0,0)}f_2 \equiv 0$ and so $T_{(0,0)}X_2 = V(0) = \mathbb{R}^2$, the kernel of the Jacobian is everything, and so $\dim T_{(0,0)}X_2 = n - \text{rank } J = 2$, which is strictly greater than $\dim X_2 = n - m = 2 - 1 = 0$.

Remark 7.3. If the Jacobian is of full degree, then we actually have an equality $\dim R \leq \dim_{R/P} P/P^2$.

Definition 7.3 (Regular point). Let R be a local Noetherian ring with maximal ideal $P \triangleleft R$. Let $k = R/P$ be the residue field. We say that R is regular (or sometimes smooth) at P if $\dim R = \dim P/P^2$. If $R = k[X]$ and $a \in X$, we say that $a \in X$ is a regular (or smooth) point if $\dim T_a X = \dim X$.

7.2 Krull's principle ideal theorem

Theorem 7.7 (Krull's principle ideal theorem, geometric version). Let $X \subseteq \mathbb{A}^n$ be an irreducible variety, and $f \in k[X]$. Then $\dim V(f) \geq \dim X - 1$.

Theorem 7.8 (Krull's principle ideal theorem, algebraic version). Let R be a Noetherian ring and let $a \in R$. Then a minimal prime $P \supseteq (a)$ has codimension $\text{codim } P \leq 1$.

Remark 7.4 (Algebraic implies geometric). For $R = k[X]$ and $a = f$ we have $\dim X = \dim R = \dim R/P + \text{codim } P \leq \dim V(f) + 1$ for P such that $\dim R/P = \dim V(f)$.

Corollary 7.9. Let R be a Noetherian ring and $a_1, \dots, a_n \in R$. Then a minimal prime $P \supseteq (a_1, \dots, a_n)$ has $\text{codim}(P) \leq n$.

Proof. We prove the theorem by induction on n . In the base case $n = 1$ the statement is immediate from Krull's theorem. Let $n \geq 2$, and take a maximal chain:

$$P_0 \subsetneq \dots \subsetneq P_s = P$$

of primes.

Exercise 7.1. Change the sequence of primes so that $a_n \in P_1$.

Using this exercise we can quotient the sequence by (a_n) and get that

$$P_1/(a_n) \subsetneq \dots \subsetneq P_s/(a_n) = P/(a_n)$$

is a maximal chain in $R/(a_n)$. Since $P/(a_n)$ is minimal over $(\overline{a_1}, \dots, \overline{a_n}) \triangleleft R/(a_n)$, we get that by induction that:

$$s - 1 \leq \text{codim } P/(a_n) \leq n - 1,$$

therefore $s \leq n$ which completes the proof. $\square$

Corollary 7.10. Let $R = k[X]$, and let $I = (f_1, \dots, f_r)$ for $X \subseteq \mathbb{A}^n$ a variety and $f_1, \dots, f_r \in R$. Then every irreducible component of $V(I)$ is of codimension $\leq r$.

Definition 7.4 (Primary ideal). An ideal $Q \triangleleft R$ is called primary if $ab \in Q$ implies $a \in Q$ or $b^n \in Q$ for some $n \geq 1$. Equivalently, $Q \triangleleft R$ is called a primary ideal if all zero divisors are nilpotent.

Remark 7.5. Let $Q \not\subseteq R$ be a primary ideal. Then $P = \sqrt{Q}$ is prime and equivalently R/P is an integral domain. In this case we say that Q is P -primary.

Example 7.2. Let R be a principle ideal domain. Then $(q) = Q$ is P -primary if and only if $Q = P^n$ for some n . That is, if $q = ap^n$ for $a \in R^\times$.

Definition 7.5 (Symbolic power). The symbolic power of a ideal $P \triangleleft R$ is denoted by $P^{(n)}$ and defined by:

$$P^n \subseteq P^{(n)} := \{a \in R \mid ab \in P^n \text{ for some } b \in R \setminus P\} \subseteq P.$$

Remark 7.6. If P is a prime ideal then $P^{(n)}$ is P -primary:

$$P = \sqrt{P^n} \subseteq \sqrt{P^{(n)}} \subset \sqrt{P} = P,$$

where the last equality follows from the fact P is radical (all primes are radical). From this follows that $\sqrt{P^{(n)}} = P$, so $P^{(n)}$ is P -primary.

In order to show that $P^{(n)}$ is primary, suppose that $ab \in P^{(n)}$, and suppose that $b \notin P = \sqrt{P^{(n)}}$.

Remark 7.7. Recall that R is called Artinian if every decreasing chain of ideals eventually stabilizes.

Theorem 7.11 (Hopkins). *A ring R is Artinian if and only if R is Noetherian of dimension zero.*

Proof of Theorem 7.8. Let $Q' \subseteq Q \subsetneq P$ be a chain of primes. By replacing R by $(R/Q')_{P/Q'}$, we may assume the following:

- (1) $Q' = (0)$ and R is an integral domain.
- (2) R is a local ring with a maximal ideal P .

Consider the chain of symbolic powers:

$$Q^{(0)} \supseteq Q^{(1)} \supseteq \dots$$

Recall that Hopkins theorem states that a ring is Artinian if and only if it is Noetherian and of dimension zero. Since $R/(a)$ is Noetherian and of dimension zero, by Hopkins theorem it is Artinian, and therefore:

$$Q^{(0)} + (a)/(a) \supseteq Q^{(1)} + (a)/(a) \supseteq \dots$$

eventually stabilizes, but this implies that the numerator eventually stabilizes. This means that from a certain point we have $Q^{(n)} + (a) = Q^{(n+1)} + (a)$.

Claim: If from a certain point we have $Q^{(n)} + (a) = Q^{(n+1)} + (a)$ then from some point we also have $Q^{(n)} = Q^{(n+1)} + PQ^{(n)}$.

By the claim and Nakayama's lemma we get that $Q^{(n)} = Q^{(n+1)}$ from some point. However, $Q^{(n)}R_Q = Q^nR_Q$ and hence:

$$Q^nR_Q = Q^{n+1}R_Q = (QR_Q) \cdot (Q^nR_Q),$$

and so by applying Nakayama part (1) we get $Q^nR_Q = 0$. However, since R is an integral domain we get that $Q = 0$, which completes the proof.

Proof of Claim: The direction $\supseteq$ is clear, so we will only show the other direction. Suppose that $b \in Q^{(n)}$. This implies that $b = c + ar$ for some $c \in Q^{(n+1)}$ and $r \in R$. Thus $ar = b - c \in Q^{(n)}$, and so $r \in Q^{(n)}$ (since $a \notin Q$ by minimality of P nad $Q^{(n)}$ is P -primary). Thus $b = c + ar \in Q^{(n+1)} + PQ^{(n)}$. $\square$

Remark 7.8. Recall that R is Artinian if and only if (under the assumption of Zorn's lemma) every set $\Sigma \neq \emptyset$ of ideals in R has a minimal element.

Lemma 7.12. *Let $R \neq 0$ be an Artinian ring. It has only finitely many maximal ideals $P_1, \dots, P_r$ and $P_1^{e_1} \cdots P_r^{e_r} = 0$ for some $e_i \geq 0$. Moreover, every prime is maximal.*

Proof. Let I be a minimal ideal of the form:

$$I = Q_1 \cdots Q_s$$

for some maximal $Q_i \triangleleft R$. By minimality of I , we get that $I^2 = I$ and that $P \cdot I = I$ for all maximal $P \triangleleft R$. We now want to show that $I = 0$. Assume, by way of contradiction, that $I \neq 0$. Then there exists a minimal $J \triangleleft R$ such that $IJ \neq 0$ (by Remark 7.8). By minimality of J we have that $IJ = J$, and J is principle, that is, $J = (b)$ for some $b \in J$, and hence finitely generated.

We conclude from Exercise 7.2 that $1 - a \notin R^\times$ and hence $(1 - a) \subseteq Q$ for some maximal $Q \triangleleft R$. Thus,

$$1 = \underbrace{(1 - a)}_{\in Q} + \underbrace{a}_{\in I \subseteq Q} \in Q$$

so $I = (0)$. Let $P \triangleleft R$ be a prime. Then $Q_i \subseteq P$ for some i (otherwise $a_i \in Q_i \setminus P$ for all i , hence $a_1 \cdots a_s \in Q_1 \cdots Q_s = (0) \subseteq P$, so $\prod a_i \in P$ but $a_i \notin P$ which is a contradiction), and hence $P = Q_i$. $\square$

Exercise 7.2. Show that as in the proof of Nakayama's lemma, there exists $a \in I$ such that $(1 - a)J = 0$.

Remark 7.9. We have shown that R is Artinian implies that $\dim R = 0$ and that there exist finitely many maximal ideals $Q_1, \dots, Q_s \triangleleft R$ such that $Q_1 \cdots Q_s = 0$, where there may be repetitions, that is, we may have $Q_i = Q_j$ for $i \neq j$.

Exercise 7.3. If $N \leq M$ is an R -submodule, then M is Noetherian/Artinian if and only if M/N and N are Noetherian/Artinian.

Proof of Theorem 7.11. Using Remark 7.9 we can conclude the theorem from the following claim: Assuming $\dim R = 0$ we need to show that R is Artinian if and only if it is Noetherian.

First suppose that R is Artinian. Consider the sequence:

$$R \supseteq Q_1 \supseteq Q_1 Q_2 \supseteq \cdots \supseteq Q_1 \cdots Q_s = (0).$$

Then we get that $M_i := Q_1 \cdots Q_{i-1} / Q_1 \cdots Q_i$ is an R -module, which is annihilated by Q_i , and hence it is an R/Q_i -module. Since R/Q_i is a field, we get that M_i is a vector space, and since R is Artinian, it is finite dimensional and therefore it is also Noetherian. Since each of M_i is Noetherian, the result follows from Exercise 7.3.

Next suppose that R is Noetherian. Assume, by way of contradiction, that $\Sigma \neq \emptyset$. By this assumption,

$$\Sigma := \{I \triangleleft R \mid R/I \text{ is not Artinian}\} \neq \emptyset$$

and since R is Noetherian Σ has a maximal element $P \in \Sigma$. We claim that P is prime. Since $\dim R = 0$, this gives that P is maximal, so R/P is a field and thus Artinian which completes the proof.

In order to show that P is prime, it suffices to show that $S := R/P$ is an integral domain. For $a \in S$ consider the exact sequence:

$$0 \longrightarrow S / \text{Ann}_S(a) \xrightarrow{a} S \longrightarrow S/(a) \longrightarrow 0$$

Since S is not Artinian, either $S / \text{Ann}_S(a)$ or $S/(a)$ is not Artinian. By maximality of P , we get that either $\text{Ann}(a) = 0$ or $(a) = 0$, which completes the proof. $\square$

Theorem 7.13. *Let R be a Noetherian local ring of $\dim R = 1$. Then the following are equivalent:*

- (1) *R is regular/smooth.*
- (2) *R is normal.*
- (3) *R is a PID.*
- (4) *R is a UFD.*
- (5) *R is a valuation ring.*

8 Schemes

Definition 8.1 (Presheaf). Let X be a topological space. A presheaf $\mathcal{F}$ of abelian groups is a contravariant functor from the category of open subsets (with inclusions as morphisms) of X to $\mathbf{Ab}$.

Remark 8.1. We think of $\mathcal{F}(U)$ as functions on U (indeed elements in $\mathcal{F}(U)$ are elements in a group, but indeed they are thought of as functions), so the intuition of why $\mathcal{F}$ is contravariant functor should be clear.

Definition 8.2 (Restriction maps). Given $V \subseteq U \subseteq X$, we have an arrow $\mathcal{F}(V \hookrightarrow U) = \rho_{U,V}: \mathcal{F}(U) \rightarrow \mathcal{F}(V)$ which is called the restriction map.

Definition 8.3 (Section). The elements of $\mathcal{F}(U)$ are called sections.

Remark 8.2. We have that $\mathcal{F}(\emptyset) = (0)$.

Definition 8.4 (Sheaf). A presheaf $\mathcal{F}$ on a topological space X is called a sheaf if $U = \bigcup_{\alpha} U_{\alpha}$ for open U_{α} and $S_{\alpha} \in \mathcal{F}(U_{\alpha})$ sections such that $S_{\alpha}|_{U_{\alpha} \cap U_{\beta}} = S_{\beta}|_{U_{\alpha} \cap U_{\beta}}$, then there exists a unique $s \in \mathcal{F}(U)$ such that $S|_{U_{\alpha}} = S_{\alpha}$ for all α .

Example 8.1. If X is a real manifold we can set take the functor we know very well from topology C , which sends an open subset $U \subseteq X$ to all continuous maps on it $C(U)$. In this case C is a sheaf.

Definition 8.5 (Spec). Let R be a ring we define the topological space $\text{Spec } R$ to be the set:

$$\text{Spec } R = \{I \triangleleft R \mid I \text{ is prime}\}.$$

with the Zariski topology, which is the topological defined by declaring $V(I) = \{P \in \text{Spec } R \mid P \supseteq I\}$ to be the closed sets.

Definition 8.6. For an open subset $U \subseteq \text{Spec } R$, we define

$$\mathcal{O}(U) = \left\{ (\alpha_p)_{p \in U} \left| \begin{array}{l} \alpha_p \in R_p \text{ for all } p \in U, \\ \text{and for every } p \in U \text{ there exists an open} \\ \text{neighborhood } D(f) \subseteq U \text{ of } p \\ \text{and elements } a, f \in R \text{ with } f \notin q \text{ for all } q \in D(f), \\ \text{such that } \alpha_q = \frac{a}{f} \in R_q \text{ for all } q \in D(f) \end{array} \right. \right\}.$$

Remark 8.3. Note that $\mathcal{O}(U)$ is a ring and $R \cong \mathcal{O}(\text{Spec } R)$ is a ring isomorphism.

Definition 8.7 (Induced morphisms). Let $f: R \rightarrow S$ be a ring homomorphism. We can defined the induced morphism $f^*: \text{Spec } S \rightarrow \text{Spec } R$ by $Q \mapsto f^{-1}(Q)$.

Exercise 8.1. Let $f: R \rightarrow S$ be a ring homomorphism. Show that f^* is continuous.

Definition 8.8 (Schemes). A scheme is a topological space X with a sheaf $\mathcal{O}_X$ that locally look like $(\text{Spec } R, \mathcal{O})$.

Example 8.2. Let k be a field. Then $\text{Spec } k = \{0\}$. The sections over 0 are the field k .

Example 8.3.

Example 8.4.

Example 8.5.

Example 8.6.