A Self-Contained Introduction to Algebraic Geometry

Eddie Nijholt

June 4, 2023

Introduction

The goal of this text is to introduce the basics of algebraic geometry while assuming as little as possible on the part of the reader. In particular, I will not assume a strong background in commutative algebra, but rather develop the relevant topics when they become needed. Some familiarity with (polynomial) rings and ideals is useful, though a look at Wikipedia might already suffice.

The original aim was to understand zero-sets of polynomials in terms of embedded (differentiable) sub-manifolds, which in turn was motivated by studying conjugacy orbits of matrices. Even though this text will eventually touch upon these topics, they will only play a role in later chapters.

It goes without saying that I did not come up with any of the results here. Out of the various sources I have used, the most important ones are the seminal book *Algebraic Geometry* by Prof. Hartshorne [1] and the excellent lecture notes on commutative geometry by Prof. Robert B. Ash [2].

Throughout this text, a ring will always mean a commutative ring with multiplicative identity 1. An important example is given by the polynomial ring $K[X_1, \ldots, X_n]$ in n variables over some field K.

At the time of writing, this text is still under construction.

Contents

1 Basics

1.1 Zero-sets of polynomials

Let K be a field. We are interested in subsets V of K^n for some $n \in \mathbb{N}_{>0}$ that are of the form

$$V = V(\Lambda) := \{x \in K^n \mid p(x) = 0 \text{ for all } p \in \Lambda\}, \tag{1}$$

where Λ is some subset of $K[X_1, \ldots, X_n]$. The latter denotes the ring of polynomials in n variables and with coefficients in K. Of course K will in practice often be either $\mathbb{R}$ or $\mathbb{C}$. Note that Λ need not satisfy any conditions. That is, Λ is an either finite or infinite subset of $K[X_1, \ldots, X_n]$. Hence, there does not yet seem to be a reason to bring in the ring structure of $K[X_1, \ldots, X_n]$. However, Lemma 1.2 below provides strong motivation for considering rings and ideals, i.e. for turning towards commutative algebra.

Definition 1.1. Let R be a commutative ring with 1 and $\Lambda \subseteq R$ a subset. We denote by I_Λ the smallest ideal containing Λ. More precisely, we set

$$I_\Lambda := \bigcap_{\substack{I \text{ Ideal} \\ \Lambda \subseteq I}} I, \tag{2}$$

where we take the intersection of all ideals of R that contain the set Λ. Note that this collection of ideals is not empty, as it contains the whole ring R. $\triangle$

It is not hard to see that I_Λ is an ideal of its own. For, suppose we are given $r \in R$ and $x, y \in I_\Lambda$. If I is any ideal containing Λ, then necessarily $x, y \in I$. It follows that $0, x + y, -x, rx \in I$, so that likewise $0, x + y, -x, rx \in I_\Lambda$. It also follows from the construction of I_Λ that $\Lambda \subseteq I_\Lambda$.

Lemma 1.2. *The set $V(\Lambda) \subseteq K^n$ equals the set $V(I_\Lambda) \subseteq K^n$.*

Proof. Let $x \in V(\Lambda) \subseteq K^n$ be given. We consider the set

$$I_x := \{p \in K[X_1, \ldots, X_n] \mid p(x) = 0\}, \tag{3}$$

consisting of all polynomials that vanish on x. We claim that I_x is an ideal. Indeed, for $p, q \in I_x$ and $r \in K[X_1, \ldots, X_n]$ we have $(p+q)(x) = p(x) + q(x) = 0+0 = 0$ and $(rp)(x) = r(x)p(x) = r(x) \cdot 0 = 0$, so that $p+q, rp \in I_x$. Note that trivially $0 \in I_x$ and $-p \in I_x$. However, those also follow from setting $r = 0$ and $r = -1$, which works in general for rings with 1. As x is an element of $V(\Lambda)$ we have $p(x) = 0$ for all $p \in \Lambda$ (by definition). Therefore, we obtain $\Lambda \subseteq I_x$. By definition of I_Λ (as the 'smallest ideal' containing Λ), we see that $I_\Lambda \subseteq I_x$. Hence, for any $q \in I_\Lambda$ we find $q(x) = 0$. This shows that $x \in V(I_\Lambda)$.

Conversely, let $x \in V(I_\Lambda) \subseteq K^n$ be given. By definition we find $p(x) = 0$ for all $p \in I_\Lambda$. As we have $\Lambda \subseteq I_\Lambda$, we see that likewise $p(x) = 0$ for all $p \in \Lambda$. This shows that $x \in V(\Lambda)$. $\square$

Next, we will see that any set of the form $V(\Lambda)$ is the intersection of the zero-sets of only finitely many polynomials. The key idea is to show that any ideal I in $K[X_1, \ldots, X_n]$ is given by $I = I_S$ for some finite set $S = \{p_1, p_2, \ldots, p_k\}$. We also say that I is *finitely generated* (by the elements p_1 through p_k), and write $I = \langle p_1, \ldots, p_k \rangle$. It follows that for any set $\Lambda \subseteq K[X_1, \ldots, X_n]$ (so with Λ possibly infinite), there exists a finite set $S = \{p_1, p_2, \ldots, p_k\}$ such that $I_\Lambda = I_S$. Applying Lemma (1.2) twice then gives us

$$\begin{aligned} V(\Lambda) = V(I_\Lambda) = V(I_S) = V(S) &= \bigcap_{i=1}^{k} \{x \in K^n \mid p_i(x) = 0\} \\ &= \bigcap_{i=1}^{k} \text{ 'zero set of } p_i\text{'} \,. \end{aligned} \tag{4}$$

Of course the size k of S generally depends on Λ. Writing $S = \{p_1, p_2, \ldots, p_k\} \subseteq R$, note that the finitely generated ideal I_S contains all elements of the form

$$p = \sum_{i=1}^{k} r_i p_i \tag{5}$$

with $r_i \in R$ for all $i \in \{1, \ldots, k\}$. In fact, let J_S denote the set of all elements in R that can be written as Expression (5) for some $r_i \in R$. It is not hard to see that J_S is an ideal, and we have just argued that $J_S \subset I_S$. As J_S contains S, we also see that $I_S \subset J_S$ (recall the definition of I_S as the 'smallest' ideal containing S). Hence we find $I_S = J_S$, so that elements of I_S are precisely those of the form (5). To show that every ideal in $K[X_1, \ldots, X_n]$ is indeed finitely generated, we need:

Lemma 1.3 (Hilbert's basis theorem)**.** *If R is a commutative ring with 1 such that every ideal is finitely generated, then every ideal of the polynomial ring $R[X]$ is also finitely generated.*

Proof, adapted from Wikipedia. Let $\mathcal{A}$ be a given ideal of $R[X]$. We construct the set

$$\mathfrak{a} := \left\{ a \in R \;\middle|\; \begin{array}{l} a \text{ is the leading coefficient of a polynomial} \\ p(X) \in \mathcal{A} \end{array} \right\}, \tag{6}$$

where we will use the convention that 0 is the leading coefficient of the zero-polynomial, so that $0 \in \mathfrak{a}$.

We claim that $\mathfrak{a}$ is an ideal of R. Indeed, let $r \in R$ and $a, b \in \mathfrak{a}$ be given and let $p(X), q(X) \in \mathcal{A}$ be polynomials with leading coefficients a and b, respectively. Denote by $k, l \geq 0$ the degrees of $p(X)$ and $q(X)$, respectively, and assume without loss of generality that $k \geq l$. It follows that either $ra = 0$ (in which case $ra \in \mathfrak{a}$) or that ra is the leading coefficient of $rp(X) \in \mathcal{A}$. In the latter case we also find $ra \in \mathfrak{a}$. Similarly, we see that either $a + b = 0$, or that $a + b$ is

the leading coefficient of the polynomial $p(X) + X^{k-l}q(X) \in \mathcal{A}$. In either case we find that $a + b \in \mathfrak{a}$.
By the assumption of the theorem, $\mathfrak{a}$ is therefore generated by some elements $a_1, \ldots, a_m$, and there exist polynomials $p_1(X), \ldots, p_m(X) \in \mathcal{A}$ with a_i the leading coefficient of $p_i(X)$ for all $i \in \{1, \ldots, n\}$. Multiplying each $p_i(X)$ with X^{d_i} for some appropriate value of $d_i \geq 0$, we may furthermore assume that each polynomial $p_i(X)$ has the same degree $d > 0$. (We may trivially assume none of the a_i equal 0)

Similar to $\mathfrak{a}$, we define for each $c < d$ the set

$$\mathfrak{a}_c := \left\{ a \in R \;\middle|\; \begin{array}{l} a \text{ is the leading coefficient of a polynomial} \\ p(X) \in \mathcal{A} \text{ of degree } c \text{ or less} \end{array} \right\}. \tag{7}$$

As for the previous set, each $\mathfrak{a}_c$ is readily seen to be an ideal of R. The only thing to check is that the polynomials $rp(X)$ and $p(X) + X^{k-l}q(X)$ that we used to show that $\mathfrak{a}$ is an ideal have degree c or less if this holds for $p(X)$ and $q(X)$, which is clear. We may therefore write down generators $a_1^c, \ldots, a_{m_c}^c$ for $\mathfrak{a}_c$, which are the leading coefficients of polynomials $p_1^c(X), \ldots, p_{m_c}^c(X) \in \mathcal{A}$ of degree c or less. By multiplying each of these polynomials by some power of X, we may assume each $p_i^c(X)$ to be of degree precisely c.

To summarize, we now have polynomials $p_1(X), \ldots, p_m(X) \in \mathcal{A}$ of degree d whose leading coefficients generate the ideal $\mathfrak{a}$ of all leading coefficients of elements in $\mathcal{A}$. Moreover, for each $c < d$ we have polynomials $p_1^c(X), \ldots, p_{m_c}^c(X) \in \mathcal{A}$ of degree c whose leading coefficients generate the ideal $\mathfrak{a}_c$ of all leading coefficients of polynomials in $\mathcal{A}$ that have degree c or less.

We now define the ideal $\mathcal{B} \subset R[X]$, generated by the finitely many elements

$$\bigcap_{c=0}^{d-1} \{p_1^c(X), \ldots, p_{m_c}^c(X)\} \cap \{p_1(X), \ldots, p_m(X)\}. \tag{8}$$

By construction, we have $\mathcal{B} \subset \mathcal{A}$. We claim that likewise $\mathcal{A} \subset \mathcal{B}$, which we prove by induction on the degree of an element in $\mathcal{A}$. To start, let $r \in \mathcal{A}$ be a constant polynomial. As the leading coefficients of degree 0 polynomials are of course the polynomials themselves, we see that the ideal $\mathfrak{a}_0$ is precisely equal to the ideal of constant polynomials of $\mathcal{A}$. In particular, we find $r \in \mathfrak{a}_0 = \{a_1^0, \ldots, a_{m_0}^0\} = \{p_1^0(X), \ldots, p_{m_0}^0(X)\} \subseteq \mathcal{B}$, where we have used that likewise $p_i^0 = a_i^0$ for all $i \in \{1, \ldots, m_0\}$.

Now suppose we have some number $s > 0$ such that all elements in $\mathcal{A}$ of degree less than s are contained in $\mathcal{B}$. Let $p(X) \in \mathcal{A}$ be an element of degree s and denote by $a \in R \setminus \{0\}$ its leading coefficient. We have to distinguish between two cases: $s < d$ and $s \geq d$.

Assume first that $s < d$. As a is the leading coefficient of $p(X) \in \mathcal{A}$, we see that $a \in \mathfrak{a}_s = \{a_1^s, \dots, a_{m_s}^s\}$. In particular, we may write

$$a = \sum_{i=1}^{m_s} r_i a_i^s \,, \tag{9}$$

for some $r_i \in R$. It follows that

$$q(X) := \sum_{i=1}^{m_s} r_i p_i^s(X) \,, \tag{10}$$

is a polynomial of degree s with leading coefficient a. By construction, we have $q(X) \in \mathcal{B} \subseteq \mathcal{A}$. As $p(X)$ and $q(X)$ both have leading coefficient a, as well as the same degree s, we see that $p(X) - q(X)$ is an element of $\mathcal{A}$ of degree strictly less than s. By the induction hypothesis, we therefore find $p(X) - q(X) \in \mathcal{B}$. As we also have $q(X) \in \mathcal{B}$, we conclude that indeed $p(X) = (p(X) - q(X)) + q(X) \in \mathcal{B}$.

Finally, assume $s \geq d$. Similar to the previous case, we may write

$$a = \sum_{i=1}^{m} r_i a_i \,, \tag{11}$$

for some $r_i \in R$. Correspondingly, we may construct the polynomial

$$u(X) := \sum_{i=1}^{m} r_i X^{s-d} p_i(X) \,. \tag{12}$$

Note that $u(X)$ has degree s and that its leading coefficient is a. As with $q(X)$, we have that $u(X) \in \mathcal{B} \subseteq \mathcal{A}$, by construction. We conclude that $p(X) - u(X)$ is an element of $\mathcal{A}$ of degree $s - 1$ or less. Hence, $p(X) - u(X) \in \mathcal{B}$ and since $u(X) \in \mathcal{B}$, we see that $p(X) \in \mathcal{B}$. By induction, we see that indeed $\mathcal{A} \subseteq \mathcal{B}$, so that $\mathcal{A} = \mathcal{B}$. It follows that $\mathcal{A}$ is finitely generated, which concludes the proof. □

Note that any field K has only two ideals: the zero ideal, which is generated by 0 (or by the empty set), and the field K itself, which is generated by 1. Hence, any ideal of K is finitely generated, and we conclude that the same holds for $K[X]$. By using Hilbert's basis theorem iteratively we find that the ring

$$K[X_1, \dots, X_n] \cong (\dots((K[X_1])[X_2])\dots)[X_n]$$

has only finitely generated ideals as well.
It turns out that having all finitely generated ideals is equivalent to another condition, which is sometimes easier to work with. We define:

Definition 1.4. A ring R is called *Noetherian* if it satisfies the *ascending chain condition*. That is, whenever we have an infinite chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq R \,,$$

there exists a number N (dependent on the particular chain), such that

$$I_N = I_{N+1} = I_{N+2} = \dots .$$

In other words, ideals 'cannot keep growing forever'. △

Lemma 1.5. *A ring R is Noetherian if and only if all of its ideals are finitely generated.*

Proof. Suppose first that R is Noetherian, and let $I \subseteq R$ be a given ideal. We will construct a growing chain of ideals as follows. We first pick an element $r_1 \in I$, and write $\langle r_1 \rangle$ for the ideal generated by this element, as usual. Then clearly $\langle r_1 \rangle \subseteq I$. If in fact $\langle r_1 \rangle = I$ then we are done; I is then finitely generated. If not, we may pick an element $r_2 \in I \setminus \langle r_1 \rangle$. It follows that $\langle r_1 \rangle \subsetneq \langle r_1, r_2 \rangle \subseteq I$. Again, either $\langle r_1, r_2 \rangle = I$ or we may pick an element $r_3 \in I \setminus \langle r_1, r_2 \rangle$, and so forth. Note that if this process terminates, then we have found elements $r_1, \dots, r_m$ such that $I = \langle r_1, \dots, r_m \rangle$. Hence, we only have to show that it indeed terminates. Suppose otherwise, then we construct a growing chain of ideals:

$$\langle r_1 \rangle \subsetneq \langle r_1, r_2 \rangle \subsetneq \langle r_1, r_2, r_3 \rangle \dots .$$

This contradicts the assumption that R is Noetherian, and we conclude that I is indeed finitely generated.

Conversely, suppose every ideal of R is finitely generated, and suppose we have an ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq R .$$

It follows that we may construct the ideal

$$I := \bigcup_{i=1}^{\infty} I_i . \tag{13}$$

Now, one has to be careful when trying to construct ideals from the union of others, as there is no guarantee the resulting set will indeed be an ideal. In our case the inclusion relations are the key: suppose we have $a, b \in I$ and $r \in R$. It follows that there exist $n, m \in \mathbb{N}$ such that $a \in I_n$ and $b \in I_m$. But then we also have $a, b \in I_{\max(n,m)}$. We conclude that $a + b \in I_{\max(n,m)} \subseteq I$, and of course $ra \in I_{\max(n,m)} \subseteq I$, so that I is indeed an ideal. By assumption, I is therefore generated by finitely many elements $r_1, \dots, r_k \in I$. Again, we may find $n_1, \dots, n_k \in \mathbb{N}$ such that $r_i \in I_{n_i}$ for all $i \in \{1, \dots, k\}$. Setting $N := \max(n_1, \dots, n_k)$, we likewise find $r_1, \dots, r_k \in I_N$, and so $\langle r_1, \dots, r_k \rangle \subseteq I_N$. However, what we have therefore found is

$$I = \langle r_1, \dots, r_k \rangle \subseteq I_N \subseteq I ,$$

so that in fact $I = I_N$. It follows that for any $j \geq 0$ we have $I = I_N \subseteq I_{N+j} \subseteq I$, so that also $I_N = I_{N+j}$. This shows that R is indeed Noetherian. □

1.2 Properties of algebraic sets

Next, we want to collect some properties of the sets

$$V(\Lambda) := \{x \in K^n \mid p(x) = 0 \text{ for all } p \in \Lambda\}\,, \tag{14}$$

which we will henceforth call *algebraic sets*. Recall that Λ may always be replaced by an ideal of $K[X_1, \ldots, X_n]$ –which is always finitely generated– without changing the algebraic set. We start with the following easy observation.

Lemma 1.6. *Let Λ_1, Λ_2 be two subsets of $K[X_1, \ldots, X_n]$. If $\Lambda_1 \subseteq \Lambda_2$ then $V(\Lambda_2) \subseteq V(\Lambda_1)$.*

Proof. Let $x \in V(\Lambda_2)$ be given, then $p(x) = 0$ for all $p \in \Lambda_2$. Hence in particular, $p(x) = 0$ for all $p \in \Lambda_1$, from which we see that $x \in V(\Lambda_1)$. We conclude that indeed $V(\Lambda_2) \subseteq V(\Lambda_1)$. □

Next, we show that algebraic sets are closed under taking intersections.

Lemma 1.7. *Let $\mathcal{S}$ be a (possibly infinite) collection of subsets of $K[X_1, \ldots, X_n]$. The corresponding algebraic sets satisfy*

$$\bigcap_{\Lambda \in \mathcal{S}} V(\Lambda) = V\left(\bigcup_{\Lambda \in \mathcal{S}} \Lambda\right). \tag{15}$$

Proof. For any fixed subset $\Lambda \in \mathcal{S}$ we have

$$\Lambda \subseteq \bigcup_{\Lambda \in \mathcal{S}} \Lambda\,,$$

so that it follows from Lemma 1.6 that

$$V\left(\bigcup_{\Lambda \in \mathcal{S}} \Lambda\right) \subseteq V(\Lambda)\,.$$

As this holds for any choice of $\Lambda \in \mathcal{S}$ we conclude that

$$V\left(\bigcup_{\Lambda \in \mathcal{S}} \Lambda\right) \subseteq \bigcap_{\Lambda \in \mathcal{S}} V(\Lambda)\,. \tag{16}$$

Conversely, let x be an element that is contained in $V(\Lambda)$ for all $\Lambda \in \mathcal{S}$. In particular, for any $\Lambda \in \mathcal{S}$ it holds that $p(x) = 0$ for all $p \in \Lambda$, so that $p(x) = 0$ for all

$$p \in \bigcup_{\Lambda \in \mathcal{S}} \Lambda\,.$$

This shows that

$$x \in V\left(\bigcup_{\Lambda \in \mathcal{S}} \Lambda\right),$$

and we conclude that

$$\bigcap_{\Lambda\in\mathcal{S}} V(\Lambda) \subseteq V\left(\bigcup_{\Lambda\in\mathcal{S}} \Lambda\right). \tag{17}$$

The result now follows from equations (16) and (17). □

Finally, we want to show that the union of finitely many algebraic sets is again an algebraic set. It turns out this will be much easier if we work with ideals. In particular, we will use the following well-known definition.

Definition 1.8. Let $I_1, I_2, \ldots, I_k$ be a finite collection of ideals of a ring R. We denote by $I_1 I_2 \ldots I_k$ the ideal generated by all products

$$r_1 r_2 \ldots r_k \text{ with } r_i \in I_i \text{ for all } i \in \{1, \ldots, k\}.$$

We sometimes call $I_1 I_2, \ldots I_k$ the *product ideal* of I_1 through I_k. △

Note that, by construction, we have $I_1 I_2 \ldots I_k \subseteq I_i$ for all $i \in \{1, \ldots, k\}$, as we see that $r_1 r_2 \ldots r_k = r_1 r_2 \ldots r_{i-1} r_{i+1} \ldots r_k r_i \in I_i$. Hence, we find

$$I_1 I_2 \ldots I_k \subseteq \bigcap_{i=1}^{k} I_i.$$

We will see below that there is in general no equality between the two ideals.

Lemma 1.9. *Let $I_1, I_2, \ldots, I_k$ be ideals such that I_i is generated by the finitely many elements $r_1^i, \ldots, r_{m_i}^i$ for all $i \in \{1, \ldots, k\}$. Then $I_1 I_2 \ldots I_k$ is generated by the finitely many elements*

$$r_{j_1}^1 r_{j_2}^2 \ldots r_{j_k}^k \text{ with } j_i \in \{1, \ldots, m_i\} \text{ for all } i \in \{1, \ldots, k\}.$$

Proof. It is clear from the definition of $I_1 I_2 \ldots I_k$ that all elements $r_{j_1}^1 r_{j_2}^2 \ldots r_{j_k}^k$ with $j_i \in \{1, \ldots, m_i\}$ and $i \in \{1, \ldots, k\}$ are contained in $I_1 I_2 \ldots I_k$. Let us denote by J the ideal generated by such elements, so that we see that $J \subseteq I_1 I_2 \ldots I_k$. Conversely, suppose we are given elements $r_i \in I_i$ for all $i \in \{1, \ldots, k\}$. It follows that we may write

$$r_i = \sum_{j=1}^{m_i} a_j^i r_j^i, \tag{18}$$

for all $i \in \{1, \ldots, k\}$, and for some elements $a_j^i \in R$. We find

$$\begin{aligned} r_1 r_2 \ldots r_k &= \left(\sum_{j=1}^{m_1} a_j^1 r_j^1\right)\left(\sum_{j=1}^{m_2} a_j^2 r_j^2\right)\ldots\left(\sum_{j=1}^{m_k} a_j^k r_j^k\right) \\ &= \sum_{j_1=1}^{m_1}\sum_{j_2=1}^{m_2}\cdots\sum_{j_k=1}^{m_k}(a_{j_1}^1 a_{j_2}^2 \ldots a_{j_k}^k)(r_{j_1}^1 r_{j_2}^2 \ldots r_{j_k}^k). \end{aligned} \tag{19}$$

It follows that any ideal that contains all elements $r^1_{j_1} r^2_{j_2} \dots r^k_{j_k}$ also contains $r_1 r_2 \dots r_k$. Therefore the intersection of all ideals containing the elements $r^1_{j_1} r^2_{j_2} \dots r^k_{j_k}$ –that is, J– also contains $r_1 r_2 \dots r_k$. As $I_1 I_2 \dots I_k$ is defined as the smallest ideal containing all elements $r_1 r_2 \dots r_k$, we conclude that $I_1 I_2 \dots I_k \subseteq J$. We therefore find $I_1 I_2 \dots I_k = J$, so that this ideal is indeed generated by the given elements. □

Example 1.10. Consider the ring $K[X]$ with the ideal $I = \langle X \rangle$. It follows that $I^2 := II = \langle X^2 \rangle$, whereas $I \cap I = I = \langle X \rangle$. From this we see that $I^2 \subsetneq I \cap I$. △

Proposition 1.11. *Let $I_1, \dots, I_k$ be a finite collection of ideals in $K[X_1, \dots, X_n]$. The corresponding algebraic sets satisfy*

$$\bigcup_{i=1}^{k} V(I_i) = V\left(I_1 \cap I_2 \cap \dots \cap I_k\right) = V(I_1 I_2 \dots I_k)\,. \tag{20}$$

Proof. Using the fact that $I_1 I_2 \dots I_k \subset I_1 \cap I_2 \cap \dots \cap I_k$, Lemma 1.6 tells us that

$$V\left(I_1 \cap I_2 \cap \dots \cap I_k\right) \subseteq V(I_1 I_2 \dots I_k)\,. \tag{21}$$

Next, let $x \in V(I_1 I_2 \dots I_k)$ be given. As $K[X_1, \dots, X_n]$ is Noetherian, we see that each ideal I_i for $i \in \{1, \dots, k\}$ is finitely generated. We write $\{p^i_1, \dots, p^i_{m_i}\}$ for the generators of I_i, so that Lemma 1.9 tells us that $I_1 I_2 \dots I_k$ is generated by the elements $p^1_{j_1} p^2_{j_2} \dots p^k_{j_k}$ with $j_i \in \{1, \dots, m_i\}$ for all $i \in \{1, \dots, k\}$. Let us assume that for all $i \in \{1, \dots, k\}$ there exists an $l_i \in \{1, \dots, m_i\}$ such that $p^i_{l_i}(x) \neq 0$. As K is a field, it follows that $p^1_{l_1}(x) p^2_{l_2}(x) \dots p^k_{l_k}(x) \neq 0$, contradicting the assumption that $x \in V(I_1 I_2 \dots I_k)$. Hence, there exists at least one $i \in \{1, \dots, k\}$ for which $p^i_j(x) = 0$ for all $j \in \{1, \dots, m_i\}$. In other words, for that choice of i we have $x \in V(\{p^i_1, \dots, p^i_{m_i}\}) = V(I_i)$. We conclude that

$$V(I_1 I_2 \dots I_k) \subseteq \bigcup_{i=1}^{k} V(I_i)\,. \tag{22}$$

Finally, let x be an element of

$$\bigcup_{i=1}^{k} V(I_i)\,.$$

Then for at least one value of $i \in \{1, \dots, k\}$ we have $x \in V(I_i)$. Moreover, it clearly holds that $I_1 \cap I_2 \cap \dots \cap I_k \subseteq I_i$, so that Lemma 1.6 tells us that

$$x \in V(I_i) \subseteq V\left(I_1 \cap I_2 \cap \dots \cap I_k\right)\,. \tag{23}$$

We conclude that

$$\bigcup_{i=1}^{k} V(I_i) \subseteq V\left(I_1 \cap I_2 \cap \dots \cap I_k\right)\,. \tag{24}$$

The proposition now follows from combining equations (21), (22) and (24). □

Remark 1.12. Proposition 1.11 really needs ideals, and does not work for general subsets of $K[X_1, \ldots, X_n]$. Consider for instance the ring $K[X, Y]$ with sets $\Lambda_1 = \{X, Y^2\}$ and $\Lambda_2 = \{X, Y\}$. Then

$$V(\Lambda_1) \cup V(\Lambda_2) = \{(0,0)\} \cup \{(0,0)\} = \{(0,0)\},$$

whereas

$$V(\Lambda_1 \cap \Lambda_2) = V(\{X\}) = \{(X, Y) \in K^2 \mid X = 0\}.$$

For this reason we will most often work with ideals from here on out. △

Remark 1.13. Lemma 1.7 and Proposition 1.11 tell us that we may define a topology on K^n by declaring the sets $V(I)$ to be precisely the closed sets. Note also that $V(K[X_1, \ldots, X_n]) = \emptyset$ (as we have $1 \in K[X_1, \ldots, X_n]$) and $V(\{0\}) = K^n$. We call this topology the *Zariski topology*. △

1.3 The radical of an ideal

In the previous subsections we have seen that the common zero-set of any set of polynomials is also the common zero-set of an ideal of polynomials. However, there is no one-to-one relation between algebraic sets and ideals. For instance, on K we have $V(\langle X \rangle) = \{0\} = V(\langle X^2 \rangle)$. To get rid of some of this redundancy, we introduce the radical of an ideal.

Definition 1.14. Let I be an ideal of a ring R. The *radical* of I, denoted $\sqrt{I}$, is the set of all elements $x \in R$ for which a positive integer $n \in \mathbb{N}$ exists such that $x^n \in I$. Note that this number n is in general dependent on x. △

Lemma 1.15. *The set $\sqrt{I}$ is an ideal of R satisfying $I \subseteq \sqrt{I}$. Moreover, we have*

$$\sqrt{\sqrt{J}} = \sqrt{J}$$

for all ideals J. Finally, if two ideals $J_1, J_2 \subseteq R$ satisfy $J_1 \subseteq J_2$, then likewise $\sqrt{J_1} \subseteq \sqrt{J_2}$.

Proof. We begin by showing that $\sqrt{I}$ is an ideal. To this end, consider some elements $x, y \in \sqrt{I}$ and $r \in R$. Let $n, m \in \mathbb{N}$ be positive numbers such that $x^n, y^m \in I$. It follows that $(rx)^n = r^n x^n \in I$, so that likewise $rx \in \sqrt{I}$. Moreover, we have

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}, \tag{25}$$

where

$$\begin{aligned} &\binom{n+m}{k} x^k y^{n+m-k} \\ &:= x^k y^{n+m-k} + x^k y^{n+m-k} + \cdots + x^k y^{n+m-k} \quad \left(\binom{n+m}{k} \text{ times} \right). \end{aligned} \tag{26}$$

Let us fix an index $k \in \{0, \ldots, n+m\}$ and consider the term $x^k y^{n+m-k}$. If we have $k \geq n$ then we find $x^k y^{n+m-k} = (x^{k-n} y^{n+m-k}) x^n \in I$. If on the other hand we have $k < n$, then $n - k > 0$. It follows that $x^k y^{n+m-k} = (x^k y^{n-k}) y^m \in I$. Hence, for each $k \in \{0, \ldots, n+m\}$ we have $x^k y^{n+m-k} \in I$, so that in fact $(x+y)^{n+m} \in I$. Therefore, we find $x + y \in \sqrt{I}$, so that $\sqrt{I}$ is indeed an ideal. The claim that $I \subseteq \sqrt{I}$ follows from the trivial observation that $x \in I$ implies $x^1 \in I$. (So by choosing $n = 1$.)

It follows in particular that

$$\sqrt{J} \subseteq \sqrt{\sqrt{J}}\,.$$

To show the other inclusion, let

$$x \in \sqrt{\sqrt{J}}$$

be a given element. By definition, we have $x^n \in \sqrt{J}$ for some $n \in \mathbb{N}$. Again, it follows that $(x^n)^m \in J$ for some $m \in \mathbb{N}$. This shows that $x^{n+m} = (x^n)^m \in J$, so that indeed $x \in \sqrt{J}$. We conclude that taking the radical is indeed an idempotent operator on ideals.

Finally, suppose $J_1 \subseteq J_2$ and let $x \in \sqrt{J_1}$ be given. It follows that $x^n \in J_1 \subseteq J_2$ for some $n \in \mathbb{N}$, from which we immediately see that $x \in \sqrt{J_2}$. Hence we indeed have $\sqrt{J_1} \subseteq \sqrt{J_2}$. □

Definition 1.16. We call an ideal J a *radical ideal* if $\sqrt{J} = J$. Lemma 1.15 then motivates calling the ideal $\sqrt{I}$ of any ideal I the radical (ideal) of I. △

The following result motivates the radical from the point of view of algebraic sets.

Proposition 1.17. *For any ideal I of $K[X_1, \ldots, X_n]$ we have $V(I) = V(\sqrt{I})$.*

Proof. As we have $I \subseteq \sqrt{I}$, we see from Lemma 1.6 that $V(\sqrt{I}) \subseteq V(I)$. Conversely, let $x \in V(I)$ be given. It follows that $p(x) = 0$ for all polynomials $p \in I$. If q is a polynomial in $\sqrt{I}$ then necessarily $q^n \in I$ for some $n \in \mathbb{N}$. We conclude that $q^n(x) = q(x)q(x)\ldots q(x) = 0$, so that likewise $q(x) = 0$. This shows that $x \in V(\sqrt{I})$, so that $V(I) \subseteq V(\sqrt{I})$. We therefore indeed find $V(I) = V(\sqrt{I})$. □

Next, we gather some results about the radical of an ideal. The following lemma, combined with Proposition 1.17, is consistent with what we saw in Proposition 1.11.

Lemma 1.18. *Given ideals $I_1, I_2 \ldots, I_k$ of R, we have*

$$\sqrt{I_1 I_2 \ldots I_k} = \sqrt{I_1 \cap I_2 \cap \cdots \cap I_k} = \sqrt{I_1} \cap \sqrt{I_2} \cdots \cap \sqrt{I_k}\,. \tag{27}$$

Proof. To start, recall that we have

$$I_1 I_2 \dots I_k \subseteq I_1 \cap I_2 \cap \dots \cap I_k \,.$$

We conclude from Lemma 1.15 that

$$\sqrt{I_1 I_2 \dots I_k} \subseteq \sqrt{I_1 \cap I_2 \cap \dots \cap I_k} \,. \tag{28}$$

Next, let $x \in \sqrt{I_1 \cap I_2 \cap \dots \cap I_k}$ be given, so that a number $n > 0$ exists such that $x^n \in I_1 \cap I_2 \cap \dots \cap I_k$. Hence, for all $i \in \{1, \dots, k\}$ we see that $x^n \in I_i$, so that $x \in \sqrt{I_i}$. This shows that

$$x \in \sqrt{I_1} \cap \sqrt{I_2} \dots \cap \sqrt{I_k} \,,$$

and we conclude that

$$\sqrt{I_1 \cap I_2 \cap \dots \cap I_k} \subseteq \sqrt{I_1} \cap \sqrt{I_2} \dots \cap \sqrt{I_k} \,. \tag{29}$$

Finally, suppose that we have $x \in \sqrt{I_1} \cap \sqrt{I_2} \dots \cap \sqrt{I_k}$. It follows that for each $i \in \{1, \dots, k\}$ a number $n^i > 0$ exists such that $x^{n_i} \in I_i$. Thus we have

$$x^{n_1 + n_2 + \dots + n_k} = x^{n_1} x^{n_2} \dots x^{n_k} \in I_1 I_2 \dots I_k \,,$$

from which we see that $x \in \sqrt{I_1 I_2 \dots I_k}$. Hence we find

$$\sqrt{I_1} \cap \sqrt{I_2} \dots \cap \sqrt{I_k} \subseteq \sqrt{I_1 I_2 \dots I_k} \,. \tag{30}$$

The lemma now follows from equations (28), (29) and (30). □

Recall that a *prime ideal* P is an ideal unequal to R with the property that $xy \in P$ for elements $x, y \in R$ implies $x \in P$ or $y \in P$.

It can be shown that the quotient ring R/P by a prime ideal P is a domain. For, if we have elements $[x], [y] \in R/P$, corresponding to the classes of elements $x, y \in R$, then $[x][y] = [xy] = [0]$ implies $xy \in P$. We then find $x \in P$ or $y \in P$, so that $[x] = 0$ or $[y] = 0$. Note also that $R/P \neq \{0\}$, as $P \subsetneq R$.

Conversely, if I is an ideal of R such that R/I is a domain, then necessarily $I \neq R$. Moreover, let $x, y \in R$ satisfy $xy \in I$. We then find $[x][y] = [xy] = 0$ in R/I, so that either $[x] = 0$ or $[y] = 0$. This means that either $x \in I$ or $y \in I$, which shows that I is a prime ideal.

Hence, prime ideals are precisely those ideals I for which R/I is a domain. For such ideals we have:

Lemma 1.19. *If P is a prime ideal of a ring R then $\sqrt{P} = P$.*

Proof. By Lemma 1.15 we have $P \subseteq \sqrt{P}$, so let $x \in \sqrt{P}$ be given. It follows that $x^n \in P$ for some $n \in \mathbb{N}$. Writing $x^n = x^{n-1} x \in P$, we see that either $x \in P$ or $x^{n-1} \in P$. In the latter case we find $x \in P$ or $x^{n-2} \in P$, and so forth. Hence, we eventually find $x \in P$, so that $\sqrt{P} \subseteq P$ and so $\sqrt{P} = P$. □

1.4 Localisation of rings

It turns out the radical of an ideal I is equal to the intersection of all prime ideals that contain I, see Proposition 1.24 below. This result will prove very useful in some of the more technical arguments later on. Arguably the most natural way of proving Proposition 1.24 involves the *localization* of a ring by a multiplicative set, a concept that plays a major role throughout algebraic geometry. Hence, we first introduce localization here.

Let R be a ring and $C \subseteq R$ a subset with the following properties:

- the set C contains the identity element 1;
- the set C does not contain 0;
- if $x, y \in C$ then also $xy \in C$.

We consider the set $R \times C$, on which we put the equivalence relation: $(x, c) \sim (y, d)$ if and only if there exists an element $s \in C$ for which $sdx = scy$. To see that this is indeed an equivalence relation, note that $1cx = 1cx$ for all $x \in R$, $c \in C$. As we have $1 \in C$ it follows that $(x, c) \sim (x, c)$. Next, the implication $(x, c) \sim (y, d) \implies (y, d) \sim (x, c)$ follows directly from the definition of $\sim$. Finally, suppose we have $(x, c) \sim (y, d)$ and $(y, d) \sim (z, f)$. It follows that there exist $s, t \in C$ such that $sdx = scy$ and $tfy = tdz$. We find

$$(std)fx = tf(sdx) = tf(scy) = sc(tfy) = sc(tdz) = (std)cz\,.$$

By the third condition of C we have $std \in C$. Hence we conclude that $(x, c) \sim (z, f)$.

We will denote the class of $(x, c) \in R \times C$ under $\sim$ by $\frac{x}{c}$, and the set of all such classes by R_C. Of course the idea is to generalize the construction of fractions from integers. One observation that backs up this intuition is that

$$\frac{x}{c} = \frac{dx}{dc}$$

for all $x \in R$ and $c, d \in C$. This follows because $(x)(dc) = (dx)(c) = cdx$, where we use that $1 \in C$. (In fact, it suffices that C is non-empty.)

Next, we put a ring structure on R_C, induced by that of R. We define addition on R_C by

$$\frac{x}{c} + \frac{y}{d} = \frac{dx + cy}{cd}\,, \tag{31}$$

which makes sense as $c, d \in C$ implies $cd \in C$. To show that this is well-defined, suppose that

$$\frac{x}{c} = \frac{x'}{c'} \text{ and } \frac{y}{d} = \frac{y'}{d'}\,.$$

It follows that there exist $s, t \in C$ such that $sxc' = sx'c$ and $tyd' = ty'd$. We then obtain

$$\frac{x'}{c'} + \frac{y'}{d'} = \frac{d'x' + c'y'}{c'd'} \,.$$

However, we have

$$\begin{aligned}(st)(dx + cy)(c'd') &= stdxc'd' + stcyc'd' = tdd'(sxc') + scc'(tyd') \\ &= tdd'(sx'c) + scc'(ty'd) = std'x'cd + stc'y'cd \\ &= (st)(d'x' + c'y')(cd)\,,\end{aligned} \tag{32}$$

so that indeed

$$\frac{dx + cy}{cd} = \frac{d'x' + c'y'}{c'd'} \,.$$

To see that addition is associative, we note that on the one hand

$$\begin{aligned}\left(\frac{x}{a} + \frac{y}{b}\right) + \frac{z}{c} = \frac{bx + ay}{ab} + \frac{z}{c} &= \frac{c(bx + ay) + abz}{abc} \\ &= \frac{bcx + acy + abz}{abc} \,.\end{aligned} \tag{33}$$

On the other, we have

$$\begin{aligned}\frac{x}{a} + \left(\frac{y}{b} + \frac{z}{c}\right) = \frac{x}{a} + \frac{cy + bz}{bc} &= \frac{bcx + a(cy + bz)}{abc} \\ &= \frac{bcx + acy + abz}{abc} \,,\end{aligned} \tag{34}$$

so that equations (33) and (34) indeed agree. The zero-element of the ring is given by $\frac{0}{1}$, as clearly

$$\frac{0}{1} + \frac{0}{1} = \frac{1 \cdot 0 + 1 \cdot 0}{1^2} = \frac{0}{1} \,.$$

Note that in fact

$$\frac{0}{1} = \frac{0}{c}$$

for all $c \in C$, as $0c = 01 = 0$. It follows that the additive inverse of an element $\frac{x}{c}$ is given simply by $\frac{-x}{c}$, as we have

$$\frac{x}{c} + \frac{-x}{c} = \frac{cx - cx}{c^2} = \frac{0}{c^2} = \frac{0}{1} \,.$$

In the calculation above, we add two elements with the same 'denominator' $c \in C$. From our intuition for fractions, it stands to reason that we in fact have

$$\frac{x}{c} + \frac{y}{c} = \frac{x + y}{c}$$

for all $x, y \in R$ and $c \in C$. This is indeed true, as Equation (31) tells us that

$$\frac{x}{c} + \frac{y}{c} = \frac{cx + cy}{c^2} = \frac{c(x + y)}{c \cdot c} = \frac{x + y}{c} \,.$$

Note also that addition is clearly commutative. I.e., we have

$$\frac{x}{c} + \frac{y}{d} = \frac{dx + cy}{cd} = \frac{cy + dx}{dc} = \frac{y}{d} + \frac{x}{c}\,.$$

for all $x, y \in R$ and $c, d \in C$.

Multiplication is given by the easy formula

$$\frac{x}{c}\frac{y}{d} = \frac{xy}{cd}\,, \tag{35}$$

from which associativity and commutativity follow immediately. Of course, we first need to check that this is well-defined. As before, assume that

$$\frac{x}{c} = \frac{x'}{c'} \text{ and } \frac{y}{d} = \frac{y'}{d'}\,.$$

We see that there exist $s, t \in C$ such that $sxc' = sx'c$ and $tyd' = ty'd$. Hence we find

$$(st)(xy)(c'd') = (sxc')(tyd') = (sx'c)(ty'd) = (st)(x'y')(cd)\,, \tag{36}$$

from which it follows that

$$\frac{x}{c}\frac{y}{d} = \frac{xy}{cd} = \frac{x'y'}{c'd'} = \frac{x'}{c'}\frac{y'}{d'}\,. \tag{37}$$

We also see that the multiplicative identity is given by $\frac{1}{1} = \frac{c}{c}$ for all $c \in C$. The last thing to check is distributively. On the one hand:

$$\frac{x}{a}\left(\frac{y}{b} + \frac{z}{c}\right) = \frac{x}{a}\frac{cy + bz}{bc} = \frac{cxy + bxz}{abc}\,. \tag{38}$$

On the other:

$$\frac{x}{a}\frac{y}{b} + \frac{x}{a}\frac{z}{c} = \frac{xy}{ab} + \frac{xz}{ac} = \frac{cxy}{abc} + \frac{bxz}{abc} = \frac{cxy + bxz}{abc}\,, \tag{39}$$

by our previous observations. Distributivity then follows as equations (38) and (39) agree.

Note that any element $\frac{c}{d}$ with $c, d \in C$ has a multiplicative inverse, given by $\frac{d}{c}$.

Definition 1.20. The ring R_C constructed above is called the *localization* of R with respect to C. △

For now, our main reason for introducing the localization of a ring is to find useful ideals. To this end, let I be an ideal of R. We define the set $I_C \subseteq R_C$, consisting of all elements of the form $\frac{x}{c}$ for $x \in I$ and $c \in C$. Note that we

may still have $\frac{r}{a} \in I_C$ for some $r \notin I$. In that case $x \in I$ and $c \in C$ exist such that $\frac{r}{a} = \frac{x}{c}$. We will show that I_C is in fact an ideal of R_C. To this end, let $\frac{x}{a}, \frac{y}{b} \in I_C$ and $\frac{r}{c} \in R_C$ be given. We may assume without loss of generality that $x, y \in I$, so that we find

$$\frac{x}{a} + \frac{y}{b} = \frac{bx + ay}{ab} \in I_C \,,$$

as $bx + ay \in I$. Likewise, we have

$$\frac{r}{c}\frac{x}{a} = \frac{rx}{ca} \in I_C \,,$$

as $rx \in I$.

Hence, out of an ideal $I \subseteq R$ we may form an ideal $I_C \subseteq R_C$. Conversely, given an ideal $J \subseteq R_C$, we may form the set $N(J) \subseteq R$, consisting of all $r \in R$ for which an element $c \in C$ exists such that $\frac{r}{c} \in J$. (the letter N is chosen to convey the notion of all 'numerators' of J.) Note that, if some value $c \in C$ exists for which $\frac{r}{c} \in J$, then also

$$\frac{c}{d}\frac{r}{c} = \frac{cr}{cd} = \frac{r}{d} \in J \,,$$

for any value $d \in C$. In particular we have: $\frac{r}{c} \in J$ for some $c \in C$, if and only if $\frac{r}{c} \in J$ for all $c \in C$, if and only if $\frac{r}{1} \in J$.

Again we show that $N(J)$ is an ideal. To this end, let $x, y \in N(J)$ and $r \in R$ be given. It follows that $\frac{x}{1}, \frac{y}{1} \in J$, from which we see that

$$\frac{x}{1} + \frac{y}{1} = \frac{x + y}{1} \in J \,.$$

We conclude that $x + y \in N(J)$. Likewise, we have

$$\frac{r}{1}\frac{x}{1} = \frac{rx}{1} \in J \,,$$

so that $rx \in N(J)$. This shows that $N(J)$ is indeed an ideal of R.

The following lemmas establish some connections between the two constructions $I \mapsto I_C$ and $J \mapsto N(J)$.

Lemma 1.21. *Given two ideals I, I' of R such that $I \subseteq I'$, we also have $I_C \subseteq I'_C$.*
Likewise, given two ideals J, J' of R_C such that $J \subseteq J'$, we have $N(J) \subseteq N(J')$. For any ideal $I \in R$ we have $I \subseteq N(I_C)$ and for any ideal $J \in R_C$ we have $J = (N(J))_C$.

Proof. We start by considering two ideals $I \subseteq I'$ of R. Let $\frac{x}{c} \in I_C$ be given, and assume without loss of generality that $x \in I$. Then $x \in I'$, so that by definition $\frac{x}{c} \in I'_C$. This shows that indeed $I_C \subseteq I'_C$.

Next, suppose that $J \subseteq J'$ are ideals of R_C and let $x \in N(J)$ be given. It follows that $\frac{x}{1} \in J$. Hence we have $\frac{x}{1} \in J'$, so that $x \in N(J')$. This shows that indeed $N(J) \subseteq N(J')$.
To show that $I \subseteq N(I_C)$ for any ideal I of R, let $x \in I$ be given. It follows that $\frac{x}{c} \in I_C$ for any $c \in C$, and so that $x \in N(I_C)$. Hence, we indeed find $I \subseteq N(I_C)$.
Next, let $\frac{x}{c}$ be a given element of an ideal J of R_C. By definition of $N(J)$, we have $x \in N(J)$. Hence we find $\frac{x}{c} \in N(J)_C$, so that $J \subseteq (N(J))_C$. Finally, let $\frac{x}{c}$ be an element of $N(J)_C$. We may assume without loss of generality that $x \in N(J)$, so that $\frac{x}{d} \in J$ for all $d \in C$. In particular we find $\frac{x}{c} \in J$, so that $N(J)_C \subseteq J$. This shows that indeed $J = (N(J))_C$, which completes the proof. □

The following lemma may help explain why we do not in general have equality between I and $N(I_C)$.

Lemma 1.22. *Given an ideal $I \subseteq R$, we have $I_C = R_C$ if and only if $I \cap C \neq \emptyset$.*

Proof. Suppose we have $I_C = R_C$. It follows that $\frac{1}{1} \in I_C$, from which we see that elements $c \in C$ and $x \in I$ exist such that

$$\frac{x}{c} = \frac{1}{1}\,.$$

We conclude that an element $d \in C$ exists such that $dx = dc$. As I is an ideal and C is closed under multiplication, we find $dx = dc \in I \cap C \neq \emptyset$.
Conversely, if $I \cap C \neq \emptyset$ we pick an element $c \in I \cap C$. It follows that I_C contains the element

$$\frac{c}{c} = \frac{1}{1}\,,$$

and so $I_C = R_C$. □

When dealing with prime ideals we can say more than what Lemma 1.21 tells us.

Lemma 1.23. *Let P be a prime ideal of R that is disjoint from C, then P_C is a prime ideal of R_C and we have $N(P_C) = P$. Conversely, let Q be a prime ideal of R_C, then $N(Q)$ is a prime ideal of R that is disjoint from C.*

Proof. We begin with P a prime ideal of R satisfying $P \cap C = \emptyset$. It follows from Lemma 1.22 that $P_C \neq R_C$. Now let $\frac{x}{a}, \frac{y}{b} \in R_C$ be elements such that

$$\frac{x}{a}\frac{y}{b} = \frac{xy}{ab} \in P_C\,.$$

It follows that an element $p \in P$ exists together with an element $u \in C$ such that

$$\frac{xy}{ab} = \frac{p}{u}\,.$$

Therefore, an element $v \in C$ exists such that $vuxy = vabp$. As we have $p \in P$, we find $vabp = vuxy = (vux)(y) \in P$. Therefore, we either have $y \in P$, from which we find $\frac{y}{b} \in P_C$, or $vux \in P$, from which we find

$$\frac{x}{a} = \frac{vux}{avu} \in P_C \,.$$

This shows that P_C is indeed a prime ideal of R_C.
To show that $N(P_C) = P$, note that by Lemma 1.21 we have $P \subseteq N(P_C)$. For the reverse inclusion, let $x \in N(P_C)$ be given. It follows that $\frac{x}{1} \in P_C$, so that there are elements $p \in P$ and $c \in C$ such that

$$\frac{x}{1} = \frac{p}{c} \,.$$

From this we see that $acx = ap$ for some $a \in C$. In particular, it follows that $acx \in P$. As ac is an element of C, and because we have $P \cap C = \emptyset$, we see that necessarily $x \in P$. Hence we find $N(P_C) \subseteq P$, and so $N(P_C) = P$.

Now let Q be a prime ideal of R_C. We start with the claim that $N(Q)$ is disjoint from C. Suppose otherwise, then we find $N(Q)_C = R_C$ by Lemma 1.22. However, Lemma 1.21 tells us that $Q = N(Q)_C$, so that $Q = R_C$. This directly contradicts the assumption that Q is a prime ideal. Hence we indeed have $C \cap N(Q) = \emptyset$.
Next is the claim that $N(Q)$ is a prime ideal. Note that by the foregoing, $N(Q) \neq R$. Therefore, let $x, y \in R$ be elements such that $xy \in N(Q)$. It follows that $\frac{xy}{1} \in Q$. Writing

$$\frac{xy}{1} = \frac{x}{1}\frac{y}{1} \,,$$

we see that either $\frac{x}{1} \in Q$ or $\frac{y}{1} \in Q$. We therefore find $x \in N(Q)$ or $y \in N(Q)$, which shows that $N(Q)$ is indeed prime. □

Lemmas 1.21 and 1.23 tell us that the map $P \mapsto P_C$ induces a bijection from

$$\{P \text{ prime ideal of } R \mid P \cap C = \emptyset\}$$

to

$$\{Q \text{ prime ideal of } R_C\} \,,$$

with inverse given by $Q \mapsto N(Q)$.

Recall that an ideal $\mathcal{M}$ in a ring R is called *maximal* if it satisfies $\mathcal{M} \neq R$ and if the only ideals J satisfying $\mathcal{M} \subseteq J \subseteq R$ are $J = \mathcal{M}$ and $J = R$.

If $\mathcal{M}$ is a maximal ideal, then the quotient ring $R/\mathcal{M}$ is a field. One way of seeing this is as follows: let $x \in R$ be given, and consider the corresponding class $[x] \in R/\mathcal{M}$. We construct the ideal $\mathcal{M} + \langle x \rangle$, consisting of all elements of the form $m + rx$, with $m \in \mathcal{M}$ and $r \in R$. One easily verifies that $\mathcal{M} + \langle x \rangle$ is indeed an ideal. Clearly $\mathcal{M} \subseteq \mathcal{M} + \langle x \rangle$, so either $\mathcal{M} + \langle x \rangle = \mathcal{M}$ or $\mathcal{M} + \langle x \rangle = R$.

In the former case, we find $x \in \mathcal{M} + \langle x \rangle = \mathcal{M}$, and so $[x] = [0] \in R/\mathcal{M}$. In the latter we have $1 \in \mathcal{M} + \langle x \rangle$, so that we may write $1 = m + rx$ for some $m \in \mathcal{M}$ and $r \in R$. It follows that $[1] = [m + rx] = [m] + [r][x] = [r][x]$ in $R/\mathcal{M}$, as $[m] = 0$. We therefore see that $[x]$ is a unit. Note also that $1 \notin \mathcal{M}$, as otherwise $\mathcal{M} = R$, and so $[1] \neq [0] \in R/\mathcal{M}$. This shows that $R/\mathcal{M}$ is indeed a field.

Conversely, if I is an ideal of R such that R/I is a field, then necessarily $[1] \neq [0] \in R/I$. This shows that $I \subsetneq R$. If we have an ideal J of R such that $I \subsetneq J$, then let $x \in J \setminus I$ be given. It follows that $[x] \neq [0] \in R/I$, and so an element $y \in R$ exists such that $[x][y] = [1]$. In the ring R this means that $xy - 1 \in I \subseteq J$. As we also have $x \in J$, and so $xy \in J$, we conclude that $1 = (xy) - (xy - 1) \in J$ and therefore $J = R$. This shows that I is a maximal ideal.

Hence, maximal ideals are precisely those ideals $\mathcal{M} \subseteq R$ for which the quotient $R/\mathcal{M}$ is a field.

As any field is also a domain, we see that any maximal ideal is also a prime ideal. This is a particularly useful observation, as any ideal $I \subsetneq R$ is contained in at least one maximal ideal. We will not prove this here, but it is a well-known result that relies on Zorn's lemma. In the proof of Proposition 1.24 below, we will construct a prime ideal in R by finding a corresponding maximal ideal in R_C.

Proposition 1.24. *Let $I \subseteq R$ be an ideal unequal to R. We have*

$$\sqrt{I} = \bigcap_{\substack{P \text{ prime} \\ \text{ideal, } I \subseteq P}} P \,. \tag{40}$$

That is, $\sqrt{I}$ equals the intersection of all prime ideals containing I.

Recall that any ideal $I \subsetneq R$ is contained in a maximal ideal, which is prime. Hence, the set of prime ideals containing I is not empty. Of course for $I = R$ the set of such prime ideals is empty. In that case we have $\sqrt{I} = R$, so that Proposition 1.24 still holds if we use the convention that the empty intersection is the whole ring.

Proof of Proposition 1.24. Let P be a prime ideal containing I. It follows from Lemma 1.15 that $\sqrt{I} \subseteq \sqrt{P}$. Lemma 1.19 then tells us that $\sqrt{P} = P$, and we conclude that $\sqrt{I} \subseteq P$. Hence, $\sqrt{I}$ is contained in the intersection of all such prime ideals.
Conversely, let x be an element of all prime ideals containing I. If $x^n = 0$ for some integer $n > 0$, then clearly $x^n \in I$ and so $x \in \sqrt{I}$. Suppose therefore that the set

$$C := \{1, x, x^2, x^3, \dots, \}$$

does not contain 0. It does contain 1, and it is also clear that C is closed under multiplication. We may therefore consider the corresponding localized

ring R_C, and in there the localized ideal I_C. Suppose first that $I_C \neq R_C$. Then a maximal ideal $\mathcal{M} \subseteq R_C$ exists such that $I_C \subseteq \mathcal{M}$. It follows from Lemma 1.21 that

$$I \subseteq N(I_C) \subseteq N(\mathcal{M}) .$$

Moreover, $\mathcal{M}$ is a maximal ideal, and therefore prime. It follows from Lemma 1.23 that $N(\mathcal{M})$ is a prime ideal such that $N(\mathcal{M}) \cap C = \emptyset$. However this is a contradiction, as x was chosen to lie in every prime ideal containing I, and so in particular $x \in N(\mathcal{M})$, so that $x \in N(\mathcal{M}) \cap C$.
We arrived at this contradiction by assuming that $I_C \neq R_C$, so apparently $I_C = R_C$. By Lemma 1.22 we find $I \cap C \neq \emptyset$, and so I either contains 1 or a positive power of x. The former gives us $I = R$, which contradicts our assumption on I. Hence, we get $x^n \in I$ for some $n > 0$, from which we see that $x \in \sqrt{I}$. This completes the proof. □

1.5 Ideals from algebraic sets

We continue our investigation of the relation between ideals and algebraic sets by introducing a means of associating an ideal to a subset of K^n. Specifically, for a set $S \subset K^n$ we define

$$I(S) := \{p \in K[X_1, \ldots, X_n] \mid p(x) = 0 \,\forall\, x \in S\} .$$

We then have:

Lemma 1.25. *The set $I(S)$ is a radical ideal of $K[X_1, \ldots, X_n]$.*

Proof. Let $p, q \in I(S)$ be given, and let $r \in K[X_1, \ldots, X_n]$ be any polynomial. It follows that $(p + q)(x) = p(x) + q(x) = 0$ and $(rp)(x) = r(x)p(x) = 0$ for all $x \in S$, showing that $I(S)$ is indeed an ideal. To see that it is radical, let $p \in \sqrt{I(S)}$ be given. It follows that $p^n \in I(S)$ for some $n > 0$, and so $p^n(x) = p(x)p(x) \ldots p(x) = 0$ for all $x \in S$. We therefore see that $p(x) = 0$ for all $x \in S$, and so $p \in I(S)$. This shows that $\sqrt{I(S)} \subseteq I(S)$. As the reverse inclusion always holds, we conclude that indeed $\sqrt{I(S)} = I(S)$. □

We gather some more results on $I(S)$. To this end, it will be useful to write $p|_S$ for the restriction of a function $p \in K[X_1, \ldots, X_n]$ to the set $S \subseteq K^n$. We then have $p \in I(S)$ if and only if $p|_S = 0$.

Lemma 1.26. *For S, T subsets of K^n we have $S \subseteq T \implies I(T) \subseteq I(S)$.*

Proof. Let $p \in I(T)$ be given, so that $P|_T = 0$. It follows that $P|_S = 0$ and so $p \in I(S)$. □

Given an ideal $J \subset K[X_1, \ldots, X_n]$, recall that $V(J)$ denotes the set of points in K^n on which every element of J vanishes.

Lemma 1.27. *For any subset $S \subseteq K^n$ we have $S \subseteq V(I(S))$. Likewise, for any ideal $J \subseteq K[X_1, \ldots, X_n]$ we have $J \subseteq I(V(J))$.*

Proof. We start with the claim that $S \subseteq V(I(S))$. Let $x \in S$ be given, and let p be any element of $I(S)$. It follows that $p(x) = 0$ by definition of $I(S)$. As this holds for any $p \in I(S)$, we conclude that $x \in V(I(S))$. Hence we indeed find $S \subseteq V(I(S))$.
As for the claim that $J \subseteq I(V(J))$, let $p \in J$ be given. For any $x \in V(J)$ we have $p(x) = 0$, so that $p|_{V(J)} = 0$. We therefore see that $p \in I(V(J))$, so that indeed $J \subseteq I(V(J))$. □

Note that $J \subseteq I(V(J))$ gives $\sqrt{J} \subseteq \sqrt{I(V(J))} = I(V(J))$. Hence, for any ideal J we in fact have $\sqrt{J} \subseteq I(V(J))$. If the set $S \subset K^n$ is itself an algebraic set, then we can do better than Lemma 1.27:

Proposition 1.28. *For any algebraic set $W \subseteq K^n$ we have $W = V(I(W))$.*

Proof. Lemma 1.27 tells us that $W \subseteq V(I(W))$. Conversely, as W is an algebraic set we see that an ideal J exists such that $W = V(J)$. Lemma 1.27 then tells us that $J \subseteq I(V(J))$. From Lemma 1.6 we obtain $V(I(V(J))) \subseteq V(J)$, which gives $V(I(W)) \subseteq W$. Hence we indeed find $W = V(I(W))$. □

Next we show how the assignment $S \mapsto I(S)$ behaves with respect to unions of sets.

Lemma 1.29. *Let $\mathcal{S}$ be a collection of subsets of K^n. We have*

$$I\left(\bigcup_{S\in\mathcal{S}} S\right) = \bigcap_{S\in\mathcal{S}} I(S)\,.$$

Proof. Given

$$p \in I\left(\bigcup_{S\in\mathcal{S}} S\right)$$

we see that $p|_S = 0$ for all $S \in \mathcal{S}$. Hence we indeed see that $p \in I(S)$ for all $S \in \mathcal{S}$. Conversely, if p is contained in $I(S)$ for all $S \in \mathcal{S}$, then p vanishes on all these sets. In particular, p then vanishes on the union of all these sets, and we conclude that

$$p \in I\left(\bigcup_{S\in\mathcal{S}} S\right)\,.$$

This completes the proof. □

Summarizing some of our results so far, given an ideal $I \subseteq K[X^1, \ldots, X^n]$, we may form the algebraic set $W = V(I) \subseteq K^n$. By Lemma 1.2 this assignment reaches all algebraic sets, i.e. all sets of the form

$$V(\Lambda) := \{x \in K^n \mid p(x) = 0\,\forall\, p \in \Lambda\}$$

with Λ any subset of $K[X^1, \ldots, X^n]$. In fact, it suffices to restrict the assignment $I \mapsto V(I)$ to the radical ideals, as we have $V(\sqrt{I}) = V(I)$ by Proposition 1.17.

Given an algebraic set W, we may form the radical ideal $I(W)$ of all polynomials that vanish on W. Proposition 1.28 then tells us that $W = V(I(W))$. We would therefore get a full correspondence between algebraic sets and radical ideals if we had $J = I(V(J))$ for all radical ideals J.
Unfortunately this is not true over all fields K. Consider for instance the ideal generated by $X^2 + 1$ in the ring $\mathbb{R}[X]$. It is not hard to see that $\langle X^2 + 1\rangle$ is a prime ideal in $\mathbb{R}[X]$. In fact, we have $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$, so that $\langle X^2 + 1\rangle$ is even maximal. It follows from Lemma 1.19 that $\langle X^2 + 1\rangle$ is radical. However, we have $V(\langle X^2 + 1\rangle) = V(\{X^2 + 1\}) = \emptyset$, as $X^2 + 1$ has no roots in $\mathbb{R}$. We thus find $I(V(\langle X^2 + 1\rangle)) = I(\emptyset) = \mathbb{R}[X] \neq \langle X^2 + 1\rangle$.
In case K is algebraically closed (i.e. when every non-constant polynomial $p \in K[X]$ has a zero in K), then we do have $J = I(V(J))$ for any radical ideal $J \subseteq K[X^1, \ldots, X^n]$. Hence in this case a one-to-one correspondence between radical ideals and algebraic sets exists. More generally, for any ideal $J \subseteq K[X^1, \ldots, X^n]$ we then have $I(V(J)) = \sqrt{J}$. This is known as *Hilbert's Nullstellensatz*, and its proof will be the goal of the following section. Note that for a radical ideal J Hilbert's Nullstellensatz indeed implies $I(V(J)) = \sqrt{J} = J$.

2 Hilbert's Nullstellensatz

2.1 Modules over rings

To prove Hilbert's Nullstellensatz, it will be convenient to develop some machinery regarding polynomial rings and field extensions. In particular, we want to understand the so-called *transcendency degree*, as well as the *Noether normalization lemma*. To this end, we first need to know about integral extensions, which in turn requires introducing (Noetherian) modules over rings.

Definition 2.1. A module M over a ring R is an Abelian group (with addition denoted '+'), together with a map $\cdot : R \times M \to M$ satisfying

- $r \cdot (s \cdot m) = rs \cdot m$ for all $r, s \in R$ and $m \in M$;
- $(r + s) \cdot m = r \cdot m + s \cdot m$ for all $r, s \in R$ and $m \in M$;
- $r \cdot (m + n) = r \cdot m + r \cdot n$ for all $r \in R$ and $m, n \in M$;
- $1 \cdot m = m$ for all $m \in M$. △

Note that in a module M we always have

$$0 \cdot m = (0 + 0) \cdot m = 0 \cdot m + 0 \cdot m$$

for all $m \in M$, so that necessarily $0 \cdot m = 0$. Likewise, we find

$$r \cdot 0 = r \cdot (0 \cdot m) = (r0) \cdot m = 0 \cdot m = 0$$

for all $r \in R$ and $m \in M$, so that $r \cdot 0 = 0$. Note also that

$$0 = 0 \cdot m = (1 + -1) \cdot m = m + -1 \cdot m\,,$$

so that we find $-1 \cdot m = -m$. In light of these properties, we will often simply write rm for $r \cdot m$ if $r \in R$ and $m \in M$. Note that a module over a field $R = K$ is just a vector space. Hence, modules can be thought of as generalizations of these. Examples of modules over a general ring R are given by the ring R itself, as well as any ideal $I \subseteq R$. The action $\cdot$ is then simply defined by $r \cdot s = rs$ for $r, s \in R$ (or $s \in I$). Likewise any quotient ring R/I is a module over R, with the action given by $r \cdot [s] = [rs]$ for $r, s \in R$.

These last examples are instances of more general constructions. Given a module M over R, a *submodule* is a subgroup $N \subseteq M$ satisfying $n \in N \implies rn \in N$ for all $r \in R$. It is easy to see that N is then a module over R in its own right. To check if a non-empty subset P of a module M is a submodule, one only has to verify that $p, q \in P$ implies $p + q \in P$ and that $p \in P$, $r \in R$ implies $rp \in N$. If these two conditions hold, then immediately $0 = 0 \cdot p \in P$ and $-p = -1 \cdot p \in P$ for all $p \in P$. In practice, we may demonstrate that P is non-empty by showing that $0 \in P$. Note that the submodules of R (seen as a module over itself) are

precisely its ideals.

Given a module M together with a submodule N, we may form the *quotient module* in much the same way one defines a quotient ring for a given ideal. Namely, we put an equivalence relation $\sim_N$ on M by stating that $m \sim_N m'$ if and only if $m - m' \in N$ for $m, m' \in M$. We then define M/N as the set of equivalence classes of M under $\sim_N$. As N is a subgroup of the Abelian group M, the set M/N naturally inherits an Abelian group structure from M. The action of R on a class $[m]$ for $m \in M$ is then given by $r \cdot [m] = [rm]$ for all $r \in R$. One easily verifies that this is well-defined, and that it makes M/N into an R module.

Given two R-modules M and P, a map $\psi : M \to P$ is called a *morphism of R modules* (or simply a morphism) if for all $m, m' \in M$ and all $r \in R$ we have $\psi(m + m') = \psi(m) + \psi(m')$ and $r\psi(m) = \psi(rm)$. Note that automatically $\psi(-m) = \psi(-1 \cdot m) = -1 \cdot \psi(m) = -\psi(m)$ for all $m \in M$ and that $\psi(0) = \psi(0 \cdot 0) = 0 \cdot \psi(0) = 0$. If a morphism $\psi : M \to P$ is invertible, then its inverse $\psi^{-1} : P \to M$ is again a morphism. To see why, let $p, q \in P$ be given. It follows that

$$\psi(\psi^{-1}(p) + \psi^{-1}(q)) = \psi(\psi^{-1}(p)) + \psi(\psi^{-1}(q)) = p + q = \psi(\psi^{-1}(p + q)) \,.$$

By injectivity of ψ we conclude that indeed $\psi^{-1}(p) + \psi^{-1}(q) = \psi^{-1}(p + q)$. Likewise, for $r \in R$ we get

$$\psi(r\psi^{-1}(p)) = r\psi(\psi^{-1}(p)) = rp = \psi(\psi^{-1}(rp)) \,,$$

so that by injectivity of ψ we have $r\psi^{-1}(p) = \psi^{-1}(rp)$. We say that the two modules M and P are *isomorphic* if an invertible morphism exists between them.

Morphisms give rise to submodules in a number of ways. For instance, let $\psi : M \to P$ be a morphism and N a submodule of M, its image

$$\psi(N) = \{\psi(n) \mid n \in N\}$$

is easily seen to be a submodule of P. In particular, the image $\mathrm{Im}(\psi)$ of M under ψ is a submodule. Likewise if Q is a submodule of P, then its pre-image

$$\psi^{-1}(Q) = \{m \in M \mid \psi(m) \in Q\}$$

is a submodule of M. To see why, note that $\psi(0) = 0 \in Q$, so that $0 \in \psi^{-1}(Q)$. If $m, n \in M$ are element of $\psi^{-1}(Q)$ then by definition $\psi(m), \psi(n) \in Q$. It follows that $\psi(m + n) = \psi(m) + \psi(n) \in Q$ and likewise $\psi(rm) = r\psi(m) \in Q$ for all $r \in R$, which shows that $m + n, rm \in \psi^{-1}(Q)$. An important example of this construction is given by the kernel

$$\mathrm{Ker}(\psi) := \psi^{-1}(\{0\}) = \{m \in M \mid \psi(m) = 0\} \,.$$

Note that $\{0\}$ is indeed a submodule of any module P.

Given a module M together with a submodule N, one verifies that the inclusion $\iota : N \to M$, $n \mapsto n$ is a morphism. Likewise, we have the projection morphism $\pi : M \to M/N$, given by $\pi(m) = [m]$ for all $m \in M$. The following result is very useful for proving that two modules are isomorphic:

Lemma 2.2 (The First Isomorphism Theorem for Modules)**.** *Given a morphism ψ between two R-modules M and P, there exists an isomorphism between $M/\mathrm{Ker}(\psi)$ and $\mathrm{Im}(\psi)$.*

Proof. We define a map $[\psi]$ from $M/\mathrm{Ker}(\psi)$ to $\mathrm{Im}(\psi)$ by setting $[\psi]([m]) = \psi(m)$ for all $m \in M$. Of course we need to verify that this is well-defined. To this end, suppose $[m] = [m'] \in M/\mathrm{Ker}(\psi)$ for some $m, m' \in M$. It follows that $m'-m \in \mathrm{Ker}(\psi)$, so that $\psi(m') = \psi(m+(m'-m)) = \psi(m)+\psi(m'-m) = \psi(m)$. Hence we may indeed write $[\psi]([m]) = \psi(m)$. Note also that $\mathrm{Im}([\psi]) = \mathrm{Im}(\psi)$, so that $[\psi]$ indeed sends elements to $\mathrm{Im}(\psi)$ and does so surjectively.
As for injectivity, suppose we have $[\psi]([m]) = [\psi]([m'])$ for certain classes $[m], [m'] \in M/\mathrm{Ker}(\psi)$. It follows that $\psi(m) = \psi(m')$ and so $\psi(m) - \psi(m') = \psi(m - m') = 0$. Thus we have $m - m' \in \mathrm{Ker}(\psi)$, and so $[m] = [m']$.
Finally, we show that $[\psi]$ is a morphism. Given $[m], [m'] \in M/\mathrm{Ker}(\psi)$ and $r \in R$ we have

$$[\psi]([m]+[m']) = [\psi]([m+m']) = \psi(m+m') = \psi(m)+\psi(m') = [\psi]([m])+[\psi]([m'])$$

and likewise

$$[\psi](r[m]) = [\psi]([rm]) = \psi(rm) = r\psi(m) = r[\psi]([m])\,.$$

This shows that $M/\mathrm{Ker}(\psi)$ and $\mathrm{Im}(\psi)$ are indeed isomorphic as R-modules. □

Another construction that will be useful is that of the *direct sum module* of a collection of modules $(M_i)_{i\in\mathcal{I}}$. We denote this module by

$$\bigoplus_{i\in\mathcal{I}} M_i$$

and its elements are given by expressions $(m_i)_{i\in\mathcal{I}}$ with $m_i \in M_i$ for all $i \in \mathcal{I}$ and where $m_i = 0$ for all but a finite number of $i \in \mathcal{I}$. Addition is given by $(m_i)_{i\in\mathcal{I}} + (n_i)_{i\in\mathcal{I}} = (m_i + n_i)_{i\in\mathcal{I}}$ and the action of R by $r \cdot (m_i)_{i\in\mathcal{I}} = (rm_i)_{i\in\mathcal{I}}$ for all $r \in R$. We will mostly be interested in the direct sum of finitely many modules M_1 through M_k, which we may denote by $M_1 \oplus \cdots \oplus M_k$.

Just as with ideals, it is easy to show that the intersection of any collection of submodules of a module M is again a submodule of M. In particular, we may define the smallest submodule M_S containing a given subset $S \subseteq M$ as the intersection of all submodules that contain S. (Note that M is trivially a submodule of itself.) Of particular importance is again the case where S is finite. We call a module M *finitely generated* if $M = M_S$ for some finite set

$S = \{x_1, \ldots, x_k\} \subseteq M$. In that case elements of M_S are precisely those that can be written as

$$\sum_{i=1}^{k} r_i x_i \tag{41}$$

with $r_1, \ldots, r_k \in R$. To see this, let $P \subseteq M$ denote the set of all expressions of the form (41), which is easily seen to form a submodule of M. As P contains all elements in S, we conclude that $M = M_S \subseteq P \subseteq M$, and so $M = P$.

The following definition will prove very useful in showing that (sub)modules are finitely generated.

Definition 2.3. A module M is called *Noetherian* if for any sequence of submodules

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq M\,,$$

we have

$$N_k = N_{k+1} = N_{k+2} = \ldots$$

for some number k. △

As ideals of a ring R are precisely the submodules of R seen as a module over itself, we see that a ring is Noetherian if and only if it is Noetherian as a module. As with Noetherian rings, we have:

Lemma 2.4. *A module is Noetherian if and only if every submodule is finitely generated.*

Proof. Assume M is Noetherian and let N be any submodule of M. Pick an element $x_1 \in N$, so that $M_{\{x_1\}} \subseteq N$. If in fact $M_{\{x_1\}} = N$ then we are done. If not, pick an element $x_2 \in N \setminus M_{\{x_1\}}$, so that $M_{\{x_1\}} \subsetneq M_{\{x_1,x_2\}} \subseteq N$, and so forth. This process has to terminate at some point, as otherwise we get an infinite sequence

$$M_{\{x_1\}} \subsetneq M_{\{x_1,x_2\}} \subsetneq M_{\{x_1,x_2,x_3\}} \subsetneq \cdots \subseteq N \subseteq M\,.$$

Hence we find that N is indeed finitely generated.
Conversely, if every submodule of M is finitely generated, suppose we are given a sequence of submodules

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq M\,.$$

Just as with an increasing sequence of ideals, we may form

$$N := \bigcup_{i=0}^{\infty} N_i\,,$$

which is easily seen to be a submodule of M. In particular, finitely many elements $\{x_1, \ldots, x_l\}$ exist such that $N = M_{\{x_1,\ldots,x_l\}}$. As clearly $x_i \in N$ for all

$i \in \{1, \ldots, l\}$, we see that numbers $n_i \geq 0$ exist such that $x_i \in N_s$ whenever $s \geq n_i$. We therefore find $\{x_1, \ldots, x_l\} \subseteq N_s$ for all $s \geq \max(n_1, \ldots, n_l)$. For such s we see that $N = M_{\{x_1,\ldots,x_l\}} \subseteq N_s \subseteq N$, which shows that $N_s = N$. This completes the proof. □

Note that Lemma 2.4 does not tell us that every finitely generated module is Noetherian. In fact, every ring is generated by 1 as a module over itself, and a ring is Noetherian if and only if it is a Noetherian module over itself. This seems to imply that more can be said about modules over Noetherian rings, which is what Proposition 2.7 below confirms. First we make some useful observations.

Lemma 2.5. *Let M be an R-module and $N \subseteq M$ a submodule. Then, M is Noetherian if and only if both N and the quotient M/N are Noetherian.*

Proof. Assume first that M is Noetherian, and suppose we have a sequence

$$N_0 \subseteq N_1 \subseteq \cdots \subseteq N$$

of submodules of N. Then this is also a sequence of submodules of M, and we conclude that $N_k = N_{k+1} = \ldots$ for some $k \geq 0$. Likewise, suppose we have a sequence

$$P_0 \subseteq P_1 \subseteq \cdots \subseteq M/N$$

of submodules of M/N. Consider the submodules $\pi^{-1}(P_i)$ of M for all $i \geq 0$, where $\pi : M \to M/N$ is the quotient morphism. It follows that $\pi^{-1}(P_i) \subseteq \pi^{-1}(P_{i+1})$ for all $i \geq 0$ and we conclude that $\pi^{-1}(P_k) = \pi^{-1}(P_{k+1}) = \ldots$ for some $k \geq 0$.
Now let $s \geq k$ be given, and let $[x]$ be an element of P_{s+1}. It follows that $x \in \pi^{-1}(P_{s+1}) = \pi^{-1}(P_s)$, and so $[x] = \pi(x) \in P_s$. We see that $P_{s+1} \subseteq P_s$, and so $P_s = P_{s+1}$ for all $s \geq k$. This shows that M/N is Noetherian.

Assume next that both N and M/N are Noetherian, and suppose we have a sequence

$$N_0 \subseteq N_1 \subseteq \cdots \subseteq M$$

of submodules. It follows that we get the sequence of modules

$$(N_0 \cap N) \subseteq (N_1 \cap N) \subseteq \cdots \subseteq N\,,$$

as well as

$$\pi(N_0) \subseteq \pi(N_1) \subseteq \cdots \subseteq M/N\,.$$

We conclude that $k_1, k_2 \geq 0$ exist such that

$$(N_{k_1} \cap N) = (N_{k_1+1} \cap N) = \ldots \text{ and } \pi(N_{k_2}) = \pi(N_{k_2+1}) = \ldots$$

Setting $k = \max(k_1, k_2)$, we may simply conclude that

$$(N_s \cap N) = (N_{s+1} \cap N) \text{ and } \pi(N_s) = \pi(N_{s+1})$$

for all $s \geq k$. Fix such a value of s and let $x \in N_{s+1}$ be given. It follows that $\pi(x) = [x] \in \pi(N_{s+1}) = \pi(N_s)$, and so $y \in N_s$ exists such that $[y] = [x]$. This means that $x - y \in N$, and as we have $x \in N_{s+1}$ and $y \in N_s \subseteq N_{s+1}$, we conclude that in fact $x - y \in N \cap N_{s+1} = N \cap N_s$. In particular, we see that $x - y \in N_s$. As we also have $y \in N_s$, we conclude that $x = (x - y) + y \in N_s$. Hence we find $N_{s+1} \subseteq N_s$ and so $N_{s+1} = N_s$ for all $s \geq k$, which shows that M is indeed Noetherian. □

Lemma 2.6. *The direct sum of a finite number of Noetherian modules is itself Noetherian.*

Proof. It suffices to show that the direct sum $M_1 \oplus M_2$ of two Noetherian modules M_1 and M_2 is Noetherian. To this end, consider the function

$$\begin{aligned} \psi : M_1 \oplus M_2 &\to M_2 \\ (x, y) &\mapsto y \,. \end{aligned} \tag{42}$$

This is clearly a surjective morphism, and its kernel is given by

$$\mathrm{Ker}(\psi) = \{(x, 0) \mid x \in M_1\} \,, \tag{43}$$

We may identify this kernel with M_1 using the obvious morphism $M_1 \ni x \mapsto (x, 0) \in \mathrm{Ker}(\psi)$, and so we will simply write $\mathrm{Ker}(\psi) = M_1$. The first isomorphism theorem for modules (Lemma 2.2) now tells us that

$$(M_1 \oplus M_2)/M_1 \cong M_2 \,. \tag{44}$$

Hence, we see that both the submodule $M_1 \subseteq M_1 \oplus M_2$ and the corresponding quotient $(M_1 \oplus M_2)/M_1$ are Noetherian. We conclude by Lemma 2.5 that $M_1 \oplus M_2$ is indeed Noetherian, which completes the proof. □

Proposition 2.7. *A module over a Noetherian ring is Noetherian if and only if it is finitely generated.*

Proof. As any module is a submodule of itself, it follows from Lemma 2.4 that a Noetherian module is finitely generated (whether the ring is Noetherian or not). Conversely, suppose R is a Noetherian ring and let M be a finitely generated module over R. Suppose M is generated by the elements $x_1, \ldots, x_k$ and consider the map

$$\begin{aligned} \psi : \oplus^k R := R \oplus R \oplus \cdots \oplus R \ (k \text{ times}) &\to M \\ (r_1, \ldots, r_k) &\mapsto \sum_{i=1}^{k} r_i x_i \,. \end{aligned} \tag{45}$$

It is easy to see that ψ is a morphism between the modules $\oplus^k R$ and M. As M is generated by the elements $x_1, \ldots, x_k$, we see that ψ is surjective. Let us write $N = \mathrm{Ker}(\psi) \subseteq \oplus^k R$, so that the first isomorphism theorem (Lemma 2.2) tells us that

$$M \cong (\oplus^k R)/N \,. \tag{46}$$

Now, R is a Noetherian ring and is therefore Noetherian as a module over itself. By Lemma 2.6 we see that $\oplus^k R$ is Noetherian as well, and so by Lemma 2.5 we conclude that $(\oplus^k R)/N$ is Noetherian. Finally, Equation (46) shows that M is indeed Noetherian. □

2.2 Integral extensions

Next, we want to study integral extensions. It will turn out that finitely generated modules play an important role, see Proposition 2.10 below.

Definition 2.8. Let S be a ring and $R \subseteq S$ a *subring* of R. That is, R is a subset of S containing 0 and 1, such that for any two elements $x, y \in R$ we have $-x, x+y, xy \in R$. It follows that R is a ring in its own right. Recall that a polynomial $p \in R[X]$ is called *monic* if it is non-zero with leading coefficient 1. An element $s \in S$ is called *integral* over R if a monic polynomial $p \in R[X]$ exists such that $p(s) = 0$. In other words, if a number $k \geq 1$ exists together with elements $r_0, r_1, \ldots, r_{k-1} \in R$ such that

$$r_0 + r_1 s + r_2 s^2 + \ldots r_{k-1} s^{k-1} + s^k = 0\,.$$

Note that any element $r \in R$ is integral over R, as we have $p(r) = 0$ for the polynomial $p(X) = X - r$.

We say that S is an *integral extension* of R, or simply that S is integral over R, if every element of S is integral over R. △

Whenever we have an inclusion of rings $R \subseteq S$ (i.e. when R is a subring of S), then we may also view S as a module over R. Addition in S is the same as the one from its ring structure, and the action of R is induced by the product in S, by simply setting $r \cdot s = rs$ for all $r \in R$ and $s \in S$.

Given an element $s \in S$, we may form the polynomial ring $R[s] \subseteq S$ consisting of all elements that may be written as polynomial expressions

$$\sum_{i=0}^{k} r_i s^i = r_0 + r_1 s + r_2 s^2 + \cdots + r_{k-1} s^{k-1} + r^k s^k \tag{47}$$

for some $k \geq 0$ and with $r_0, \ldots, r_k \in R$. This is a subring of S because it is closed under addition and multiplication, and because it contains R as a subset (namely as the constant polynomials). It follows as well that R is a subring of $R[s]$.
More general, given finitely many elements $s_1, \ldots, s_l \in S$, we may define $R[s_1, \ldots, s_l] \subseteq S$ as the subset of all elements in S that may be written as

$$\sum_{I \in \mathcal{I}} r_I s^I = \sum_{I \in \mathcal{I}} r_I s_1^{I_1} s_2^{I_2} \ldots s_l^{I_l}\,. \tag{48}$$

Here $\mathcal{I}$ is a finite collection of multi-indices $I = (I_1, I_2, \ldots, I_l) \in (\mathbb{N}_{\geq 0})^l$, and we have $r_I \in R$ for all $I \in \mathcal{I}$. It can again be seen that $R[s_1, \ldots, s_l]$ is a subring of

S containing R as a subring itself.
Just as with ideals and submodules, one can show that the intersection of any collection of subrings of S is again a subring of S. Hence, we may form the smallest subring $T_{\{s_1,\ldots,s_l\}}$ of S containing R and the elements s_1 through s_l. By definition we have $T_{\{s_1,\ldots,s_l\}} \subseteq R[s_1,\ldots,s_l]$. Conversely, any subring containing R and the elements s_1 through s_l necessarily also contains all elements of the form (48). It follows that $R[s_1,\ldots,s_l] \subseteq T_{\{s_1,\ldots,s_l\}}$ and so $R[s_1,\ldots,s_l] = T_{\{s_1,\ldots,s_l\}}$. In conclusion, we see that we may also characterize $R[s_1,\ldots,s_l]$ as the smallest subring of S containing R and the elements s_1 through s_l.
By the foregoing, $R[s_1,\ldots,s_l]$ is also a module over R. Adopting this point of view, we have:

Lemma 2.9. *Let R be a subring of S and suppose the elements $s_1,\ldots,s_l \in S$ are each integral over R. Then $R[s_1,\ldots,s_l]$ is a finitely generated module over R.*

Proof. As each s_i for $i \in \{1,\ldots,l\}$ is integral over R, there exist monic polynomials p_i with coefficients in R such that $p_i(s_i) = 0$. Suppose the degree of p_i is k_i, so that it follows from $p_i(s_i) = 0$ that $k_i > 0$. We claim that $R[s_1,\ldots,s_l]$ is generated by the finite set of elements

$$C := \{s_1^{i_1} s_2^{i_2} \ldots s_l^{i_l} \mid 0 \leq i_1 < k_1, 0 \leq i_2 < k_2, \ldots, 0 \leq i_l < k_l\},$$

as a module over R. Let us denote by $M_C \subseteq S$ the module over R generated by C, so that we have to show that $R[s_1,\ldots,s_l] = M_C$. Clearly $M_C \subseteq R[s_1,\ldots,s_l]$, and so it remains to show that any element $s_1^{j_1} s_2^{j_2} \ldots s_l^{j_l}$ with $j_1,\ldots,j_l \in \mathbb{N}_{\geq 0}$ is contained in M_C, as this would imply $R[s_1,\ldots,s_l] \subseteq M_C$ by linearity. We will do so by induction on $J := j_1 + j_2 + \cdots + j_l$.
For $J = 0$ we necessarily have $j_1 = j_2 = \cdots = j_l = 0$ and so clearly $0 \leq j_1 < k_1, \ldots, 0 \leq j_l < k_l$. It follows that $s_1^{j_1} s_2^{j_2} \ldots s_l^{j_l} = s_1^0 s_2^0 \ldots s_l^0 = 1 \in M_C$. Therefore, let $\mathbf{k} > 0$ be given such that $s_1^{i_1} s_2^{i_2} \ldots s_l^{i_l} \in M_C$ whenever $i_1 + i_2 + \cdots + i_l < \mathbf{k}$. Suppose we have j_1 through j_l such that $j_1 + j_2 + \cdots + j_l = \mathbf{k}$. If it holds that $0 \leq j_1 < k_1, \ldots, 0 \leq j_l < k_l$ then by definition $s_1^{j_1} s_2^{j_2} \ldots s_l^{j_l} \in M_C$. Suppose therefore that $j_t \geq k_t$ for some $t \in \{1,\ldots,l\}$. We will write the corresponding polynomial p_t as

$$p_t(X) = r_0 + r_1 X + r_2 X^2 + \ldots r_{k_t-1} X^{k_t-1} + X^{k_t}.$$

From $p_t(s_t) = 0$ we get

$$0 = r_0 + r_1 s_t + r_2 s_t^2 + \cdots + r_{k_t-1} s_t^{k_t-1} + s_t^{k_t},$$

so that

$$s_t^{k_t} = -r_0 - r_1 s_t - r_2 s_t^2 - \cdots - r_{k_t-1} s_t^{k_t-1}. \tag{49}$$

Multiplying both sides of Equation (49) by $s_1^{j_1} s_2^{j_2} \dots s_t^{j_t - k_t} \dots s_l^{j_l}$ then gives us

$$\begin{aligned} s_1^{j_1} s_2^{j_2} \dots s_t^{j_t} \dots s_l^{j_l} = &- r_0(s_1^{j_1} s_2^{j_2} \dots s_t^{j_t - k_t} \dots s_l^{j_l}) \\ &- r_1(s_1^{j_1} s_2^{j_2} \dots s_t^{j_t - k_t + 1} \dots s_l^{j_l}) \\ &\vdots \\ &- r_{k_t - 1}(s_1^{j_1} s_2^{j_2} \dots s_t^{j_t - 1} \dots s_l^{j_l}) \,. \end{aligned} \tag{50}$$

By the induction assumption, each term on the right hand side of Equation (50) is contained in M_C, so that indeed $s_1^{j_1} s_2^{j_2} \dots s_l^{j_l} \in M_C$. This shows that $R[s_1, \dots, s_l] = M_C$, so that $R[s_1, \dots, s_l]$ is indeed a finitely generated module over R. □

Proposition 2.10. *Let R be a subring of S. An element $s \in S$ is integral over R if and only if $R[s]$ is a finitely generated module over R.*

Proof. If s is integral over R then it follows from Lemma 2.9 that $R[s]$ is finitely generated. Conversely, suppose $R[s]$ is a finitely generated module over R, and write $\{x_1, \dots, x_k\}$ for a set of generators. By definition of $R[s]$, polynomials $p_1, \dots, p_k \in R[X]$ exist such that $p_i(s) = x_i$ for all $i \in \{1, \dots, k\}$. Denote by d_i the degree of p_i, and let d be some positive integer satisfying $d > \max(d_1, \dots, d_k)$. As we have $s^d \in R[s]$, we see that elements $r_1, \dots, r_k \in R$ exist such that

$$s^d = r_1 x_1 + r_2 x_2 + \dots + r_k x_k = r_1 p_1(s) + r_2 p_2(s) + \dots + r_k p_k(s) \,. \tag{51}$$

In other words, we may define the polynomial

$$p(X) = X^d - r_1 p_1(X) - r_2 p_2(X) - \dots - r_k p_k(X) \,, \tag{52}$$

which has coefficients in R, degree $d \geq 1$ and leading coefficient 1. We then see from Equation (51) that $p(s) = 0$, which shows that s is indeed integral over R. □

A useful consequence of Lemma 2.9 and Proposition 2.10 is:

Proposition 2.11. *Let R be a Noetherian subring of S. The set of all elements that are integral over R forms a subring of S. In other words, given two elements $x, y \in S$ that are both integral over R, the elements $x + y$, xy and rx for any $r \in R$ are also integral over R.*

Proof. Let $x, y \in S$ be integral over R and consider the R-module $R[x, y] \subseteq S$. By Lemma 2.9 this module is finitely generated over R. By Proposition 2.7 the module $R[x, y]$ is therefore Noetherian. Hence, we conclude from Lemma 2.4 that any submodule of it is finitely generated too. In particular, the submodules $R[x + y], R[xy], R[rx] \subseteq R[x, y]$ for any $r \in R$ are finitely generated, so that Proposition 2.10 tells us that $x + y, xy$ and rx are all integral over R. We have already seen that any element in R is integral over R, from which we see that the set of all elements that are integral over R indeed forms a subring of S. This completes the proof. □

We next focus our attention to the case where R is a field. Note that any field is a Noetherian ring, as it only has two ideals ($\{0\}$ and the whole field).

Lemma 2.12. *Let R be a field that is a subring of S. If $s \in S$ is integral over R and its inverse s^{-1} exists then this latter element is also integral over R.*

Proof. Because s is integral over R, we see that a number $k > 0$ and elements $r_0, \ldots, r_{k-1} \in R$ exist such that

$$r_0 + r_1 s + \cdots + r_{k-1} s^{k-1} + s^k = 0\,. \tag{53}$$

Note that we cannot have that r_0 through r_{k-1} all vanish, as that would imply $s^k = 0$. Multiplying this latter expression by $s^{-k} := (s^{-1})^k$ would then give the contradiction $1 = 0$. Assume therefore that $l < k$ is the smallest number such that $r_l \neq 0$. Expression 53 can then be written as

$$r_l s^l + r_{l+1} s^{l+1} + \cdots + r_{k-1} s^{k-1} + s^k = 0\,. \tag{54}$$

If we now multiply by $(r_l)^{-1} s^{-k}$ we get

$$\begin{aligned} &s^{l-k} + r_l^{-1} r_{l+1} s^{l+1-k} + \cdots + r_l^{-1} r_{k-1} s^{-1} + r_l^{-1} \\ =&(s^{-1})^{k-l} + r_l^{-1} r_{l+1} (s^{-1})^{k-l-1} + \cdots + r_l^{-1} r_{k-1} s^{-1} + r_l^{-1} = 0\,, \end{aligned} \tag{55}$$

which shows that s^{-1} is indeed integral over R. □

As an immediate Corollary of Proposition 2.11 and Lemma 2.12 we obtain:

Corollary 2.13. *Let K be a subfield of L (that is, K is a subring of L and both are fields), then the set of elements of L that are integral over K forms a subfield of L.*

Remark 2.14. Corollary 2.13 deals with integral elements over a subfield, though usually another notion is used in this setting: if K is a subfield of L, we say that an element $x \in L$ is *algebraic* over K if a (not necessarily monic) non-zero polynomial $p \in K[X]$ exists such that $p(x) = 0$. Given such a polynomial p, we may simply divide by its leading coefficient to arrange for this polynomial to be monic. Hence, for subfields the notions of integral and algebraic coincide.

More general, given a subring R of a ring S, we may say that an element $s \in S$ is algebraic if $p(s) = 0$ for some $p \in R[X] \setminus \{0\}$. If R is a field then the algebraic elements over R are again precisely those that are integral over R, by the same argument as before. If R is not a field then some care is in order; an element may be algebraic over R but not integral. Consider for instance the case where $R = \mathbb{Z}$ and $S = \mathbb{Q}$, the rational numbers. The element $s = 1/2 \in \mathbb{Q}$ is algebraic over $\mathbb{Z}$, as it satisfies $2s - 1 = 0$. It is not integral over $\mathbb{Z}$, for if it satisfies

$$z_0 + z_1 s + \cdots + z_{n-1} s^{n-1} + s^n = 0$$

for some $n > 0$ and integers $z_0, \ldots, z_{n-1}$, then multiplying by 2^n gives

$$2(2^{n-1} z_0 + 2^{n-2} z_1 + \cdots + z_{n-1}) + 1 = 2z + 1 = 0\,, \tag{56}$$

where $z := 2^{n-1}z_0 + 2^{n-2}z_1 + \cdots + z_{n-1}$ is an integer. This of course contradicts the fact that 0 is even. In fact, it is not hard to show that all elements of $\mathbb{Q}$ are algebraic over $\mathbb{Z}$, whereas the only elements of $\mathbb{Q}$ that are integral over $\mathbb{Z}$ are those in $\mathbb{Z}$. $\triangle$

Recall that a field K is algebraically closed if for each monic polynomial $p \in K[X]$ of degree $d > 0$ there exist d elements $x_1, \ldots, x_d \in K$ (not necessarily distinct) such that

$$p(X) = (X - x_1)(X - x_2) \ldots (X - x_d)\,.$$

An example of an algebraically closed field is given by $\mathbb{C}$, the complex numbers. For such fields we have:

Lemma 2.15. *Let K be a field that is a subring of the domain D. If K is algebraically closed then the only elements in D that are integral over K are those contained in K.*

Proof. Let $s \in D$ be integral over K. It follows that a non-constant monic polynomial $p \in K[X]$ exists such that $p(s) = 0$. As K is algebraically closed, we see that we may write

$$p(X) = (X - x_1)(X - x_2) \ldots (X - x_d)\,,$$

for some elements $x_1, x_2, \ldots, x_d \in K$. From $p(s) = 0$ we therefore get

$$(s - x_1)(s - x_2) \ldots (s - x_d) = 0\,.$$

As D is a domain, we conclude that $s - x_i = 0$ for some $i \in \{1, \ldots, d\}$. From this we see that $s = x_i \in K$, which completes the proof. $\square$

Proposition 2.17 below tells us that the property of being integral 'transfers' across subrings. To prove this, we first need:

Lemma 2.16. *Suppose A is a subring of B and B is a subring of C. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.*

Proof. Suppose B is generated by the elements $b^1, \ldots, b^k$ as a module over A and C is generated by $c^1, \ldots, c^l$ as a module over B. We claim that C is generated by the set of elements $S := \{b^i c^j \mid 1 \leq i \leq k, 1 \leq j \leq l\}$ as a module over A. Let us denote by M_S^A the module generated by S over A, so that we need to show that $M_S^A = C$. On the one hand, we have $M_S^A \subseteq C$ by definition. For the other inclusion, let $c \in C$ be given. As C is generated by $c^1, \ldots, c^l$ as a module over B, we see that we may write

$$c = \sum_{i=1}^{l} b_i c^i\,, \tag{57}$$

for some $b_i \in B$. As B is generated by $b^1, \ldots, b^k$ as a module over A, we may furthermore write

$$b_i = \sum_{j=1}^{k} a_{i,j} b^j \,, \tag{58}$$

for some $a_{i,j} \in A$, for all $i \in \{1, \ldots, l\}$. Combining equations (57) and (58) gives us

$$c = \sum_{i=1}^{l} \sum_{j=1}^{k} a_{i,j} b^j c^i \,, \tag{59}$$

showing that $c \in M_S^A$ and so $C \subseteq M_S^A$. We conclude that $M_S^A = C$, so that C is indeed finitely generated over A. □

Proposition 2.17. *Let R be a Noetherian subring of L and L a subring of S. Suppose L is integral over R and let $s \in S$ be integral over L. Then s is also integral over R.*

Proof. Let $l_0, l_1, \ldots l_{k-1}$ be elements of L such that

$$l_0 + l_1 s + \cdots + l_{k-1} s^{k-1} + s^k = 0 \,. \tag{60}$$

It follows that s is also integral over the ring $R[l_0, l_1, \ldots, l_{k-1}]$. After all, all coefficients in Expression (60) lie in $R[l_0, l_1, \ldots, l_{k-1}]$. We conclude by Proposition 2.10 that the ring $R[l_0, l_1, \ldots, l_{k-1}][s]$ is finitely generated over $R[l_0, l_1, \ldots, l_{k-1}]$. Next, as every element of L is integral over R we conclude from Lemma 2.9 that $R[l_0, l_1, \ldots, l_{k-1}]$ is finitely generated over R. By Lemma 2.16 we therefore see that $R[l_0, l_1, \ldots, l_{k-1}][s]$ is finitely generated over R. As R is Noetherian, we conclude from Proposition 2.7 that $R[l_0, l_1, \ldots, l_{k-1}][s]$ is a Noetherian module over R. Next, Lemma 2.4 tells us that the submodule $R[s] \subseteq R[l_0, l_1, \ldots, l_{k-1}][s]$ is finitely generated over R, and we finally conclude from Proposition 2.10 that s is indeed integral over R. This completes the proof. □

2.3 Transcendence degree for fields

Next, we focus more on field extensions (i.e. subfields of fields) and develop a way of quantifying their relative size. To this end, we first introduce the notion of algebraic independence. Especially helpful for writing this subsection were the excellent notes on transcendence degree by Prof. A. Wright [3].

Definition 2.18. Let L be a field and $K \subseteq L$ a subfield of L. The finite set $\{x_1, \ldots, x_n\} \subseteq L$ is called *algebraically independent* over K if the only polynomial $p \in K[X_1, \ldots, X_n]$ satisfying $p(x_1, \ldots, x_n) = 0$ is the zero-polynomial $p = 0$. We will simply write 'algebraically independent' if the subfield K is clear from context. An infinite set $S \subseteq L$ is called algebraically independent over K if each finite subset of S is algebraically independent.
If a set is not algebraically independent then we call it algebraically dependent. △

Remark 2.19. Note that we do not necessarily need each of the variables X_1 through X_n to appear in a polynomial in $K[X_1, \ldots, X_n]$. In fact, for any $k < n$ we have a natural inclusion of $K[X_1, \ldots, X_k]$ into $K[X_1, \ldots, X_n]$. This shows that any subset of a finite algebraically independent set is algebraically independent as well. Hence, we may combine the two parts of Definition 2.18 and simply state that a (finite or infinite) subset $S \subseteq L$ is algebraically independent if and only if for any finite subset $\{x_1, \ldots, x_n\} \subseteq S$ we have $p(x_1, \ldots, x_n) \neq 0$ for all $p \in K[X_1, \ldots, X_n] \setminus \{0\}$. As an immediate consequence of this characterization, we also find that a (finite or infinite) subset $S \subseteq L$ is algebraically independent if and only if each subset of S is algebraically independent. $\triangle$

Remark 2.20. A set of one element $\{x\} \subseteq L$ is algebraically dependent over K if and only if a non-zero polynomial $p \in K[X]$ exists such that $p(x) = 0$, Hence, the set $\{x\}$ is algebraically dependent precisely when x is algebraic over K (equivalently integral, see Remark 2.14). It follows that an algebraically independent set cannot contain elements that are algebraic over K, and so in particular elements of K.
It is sometimes useful to extend the definition of algebraic independence to finite tuples instead of sets. That is, to allow for two or more elements to be the same. This makes no essential difference, as any finite tuple $(x_1, \ldots, x_n)$ satisfying $x_i = x_j$ for some $i \neq j$ gives $p(x_1, \ldots, x_n) = 0$ for $p(X_1, \ldots, X_n) = X_i - X_j$. In other words, algebraically independent tuples can always be seen as algebraically independent sets. We will avoid this subtlety in this text though, by simply focussing on sets alone. $\triangle$

Suppose L is a field, K is a subfield of L and x_1 through x_n are elements of L. Just as with ideals, submodules and subrings, we may define the smallest field $K(x_1, \ldots, x_n) \subseteq L$ containing both K and the elements x_1 through x_n. Similar to the previous constructions, this is done by setting $K(x_1, \ldots, x_n)$ equal to the intersection of all subfields of L containing K and these n elements. The only thing to verify is that the intersection of any collection of subfields of L is again a subfield of L, which is straightforward.
Alternatively, denote by $\mathcal{P}_K(x_1, \ldots, x_n)$ the set of all elements $x \in L$ that may be written as

$$x = p(x_1, \ldots, x_n)(q(x_1, \ldots, x_n))^{-1} \tag{61}$$

for certain $p, q \in K[X_1, \ldots, X_n]$ satisfying $q(x_1, \ldots, x_n) \neq 0$. Note that $\mathcal{P}_K(x_1, \ldots, x_n)$ contains K by setting $p = c$ for $c \in K$ and $q = 1$ (so with both p and q constant polynomials). Likewise, $\mathcal{P}_K(x_1, \ldots, x_n)$ contains x_s for any $s \in \{1, \ldots, n\}$ by setting $p(X_1, \ldots, X_n) = X_s$ and $q = 1$. What is more, given

$$\begin{aligned} x &= p(x_1, \ldots, x_n)(q(x_1, \ldots, x_n))^{-1} \text{ and} \\ y &= p'(x_1, \ldots, x_n)(q'(x_1, \ldots, x_n))^{-1} \end{aligned} \tag{62}$$

for some $p, p', q, q' \in K[X_1, \ldots, X_n]$ satisfying $q(x_1, \ldots, x_n), q'(x_1, \ldots, x_n) \neq 0$,

we have

$$x + y = pq^{-1} + p'q'^{-1} = pq^{-1}q'q'^{-1} + p'q'^{-1}qq^{-1} = (pq' + p'q)(qq')^{-1} . \quad (63)$$

Here we have used p as a shorthand for $p(x_1, \ldots, x_n)$, and so forth. Likewise, we see that

$$xy = pq^{-1}p'q'^{-1} = (pp')(qq')^{-1} . \quad (64)$$

As clearly $qq'(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)q'(x_1, \ldots, x_n) \neq 0$, we conclude that $\mathcal{P}_K(x_1, \ldots, x_n)$ is closed under addition and multiplication. Lastly, if $x \neq 0$ then necessarily $p(x_1, \ldots, x_n) \neq 0$. It follows that

$$x^{-1} = qp^{-1} \in \mathcal{P}_K(x_1, \ldots, x_n) ,$$

so that $\mathcal{P}_K(x_1, \ldots, x_n)$ is in fact a field containing K and x_1 through x_n. From this we conclude that $K(x_1, \ldots, x_n) \subseteq \mathcal{P}_K(x_1, \ldots, x_n)$.
Conversely, any subfield of L containing K and x_1 through x_n necessarily contains all elements of the form (61). We conclude that $\mathcal{P}_K(x_1, \ldots, x_n) \subseteq K(x_1, \ldots, x_n)$ and so $K(x_1, \ldots, x_n) = \mathcal{P}_K(x_1, \ldots, x_n)$. In other words, $K(x_1, \ldots, x_n)$ may also be described as the set of all elements of the form (61).

We will often use the notation

$$\frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} := p(x_1, \ldots, x_n)(q(x_1, \ldots, x_n))^{-1} \quad (65)$$

with $q(x_1, \ldots, x_n) \neq 0$ to denote an element in $K(x_1, \ldots, x_n)$. Lemma 2.22 below motivates this, even though we may also use this notation in case the elements x_1 through x_n are algebraically dependent, contrary to what is required in Lemma 2.22.

We may relate algebraic dependence to the subfield $K(x_1, \ldots, x_n) \subseteq L$ in the following way:

Proposition 2.21. *Suppose K is a subfield of L and let $\{x_1, \ldots, x_n\}$ be a finite subset of L. For any $y \in L \setminus \{x_1, \ldots, x_n\}$, the following are equivalent*

1) The element y is integral over the field $K(x_1, \ldots, x_n)$;

2) The field $K(x_1, \ldots, x_n, y)$ is integral over $K(x_1, \ldots, x_n)$.

If the set $\{x_1, \ldots, x_n\}$ is algebraically independent over K, then 1) and 2) are furthermore equivalent to

3) The set $\{x_1, \ldots, x_n, y\}$ is algebraically dependent over K.

Proof. We start with equivalence between statements 1) and 2). As $y \in K(x_1, \ldots, x_n, y)$, we clearly see that 2) implies 1). Suppose therefore that 1) holds, so that y is integral over the field $K(x_1, \ldots, x_n)$. Let $M \subseteq L$ be the

set of all elements that are integral over $K(x_1, \ldots, x_n)$. We see from Corollary 2.13 that M is a field itself. As M contains both $K(x_1, \ldots, x_n)$ and y, it follows in particular that M contains K and the set $\{x_1, \ldots, x_n, y\}$. Hence, we see that $K(x_1, \ldots, x_n, y) \subseteq M$, so that 2) follows.

Next, suppose the set $\{x_1, \ldots, x_n\}$ is algebraically independent over K, and assume 3) to hold. It follows that a non-zero polynomial $p \in K[X_0, X_1, \ldots, X_n]$ exists such that $p(y, x_1, \ldots, x_n) = 0$. Gathering terms in X_0, we may write

$$\begin{aligned} p(X_0, X_1, \ldots, X_n) = p_0(X_1, \ldots, X_n) + p_1(X_1, \ldots, X_n)X_0 + \ldots \\ + p_k(X_1, \ldots, X_n)X_0^k \,, \end{aligned} \tag{66}$$

for some $k \geq 0$, with $p_0, \ldots, p_k \in K[X_1, \ldots, X_n]$ and where $p_k \neq 0$. We first note that $k > 0$, as otherwise we would have $p_0(x_1, \ldots, x_n) = p(y, x_1, \ldots, x_n) = 0$, with $p_0 \in K[X_1, \ldots, X_n]$ non-zero, contradicting algebraic independence of $\{x_1, \ldots, x_n\}$. Similarly, because $p_k \neq 0$ (as an element of $K[X_1, \ldots, X_n]$), and because the elements x_1 through x_n are algebraically independent, we conclude that $p_k(x_1, \ldots, x_n) \neq 0$. Equation (66) tells us that

$$p_0(x_1, \ldots, x_n) + p_1(x_1, \ldots, x_n)y + \cdots + p_k(x_1, \ldots, x_n)y^k = 0 \,, \tag{67}$$

and so

$$\frac{p_0(x_1, \ldots, x_n)}{p_k(x_1, \ldots, x_n)} + \frac{p_1(x_1, \ldots, x_n)}{p_k(x_1, \ldots, x_n)}y + \cdots + y^k = 0 \,. \tag{68}$$

In other words, we may define the polynomial $q \in K(x_1, \ldots, x_n)[X]$ by

$$q(X) = \frac{p_0(x_1, \ldots, x_n)}{p_k(x_1, \ldots, x_n)} + \frac{p_1(x_1, \ldots, x_n)}{p_k(x_1, \ldots, x_n)}X + \cdots + X^k \,, \tag{69}$$

so that Equation (68) tells us that $q(y) = 0$. This shows that y is integral over $K(x_1, \ldots, x_n)$, so that 1) holds.

Finally, assume 1), so that y is integral over $K(x_1, \ldots, x_n)$. We see that

$$a_0 + a_1 y + \cdots + a_{k-1}y^{k-1} + y^k = 0 \,, \tag{70}$$

for some $k > 0$ and with $a_0, \ldots, a_{k-1} \in K(x_1, \ldots, x_n)$. Note that we may write

$$a_i = \frac{p_i(x_1, \ldots, x_n)}{q_i(x_1, \ldots, x_n)} \text{ for all } i \in \{0, \ldots, k-1\} \,,$$

for some $p_i, q_i \in K[X_1, \ldots, X_n]$ satisfying $q_i(x_1, \ldots, x_n) \neq 0$. Equation (70) then becomes

$$\frac{p_0(x_1, \ldots, x_n)}{q_0(x_1, \ldots, x_n)} + \cdots + \frac{p_{k-1}(x_1, \ldots, x_n)}{q_{k-1}(x_1, \ldots, x_n)}y^{k-1} + y^k = 0 \,. \tag{71}$$

Multiplying by $q_0(x_1,\dots,x_n)\dots q_{k-1}(x_1,\dots,x_n)$ gives

$$\begin{aligned} &p_0(x_1,\dots,x_n)q_1(x_1,\dots,x_n)\dots q_{k-1}(x_1,\dots,x_n) \\ &+q_0(x_1,\dots,x_n)p_1(x_1,\dots,x_n)\dots q_{k-1}(x_1,\dots,x_n)y \\ &\vdots \\ &+q_0(x_1,\dots,x_n)q_1(x_1,\dots,x_n)\dots p_{k-1}(x_1,\dots,x_n)y^{k-1} \\ &+q_0(x_1,\dots,x_n)q_1(x_1,\dots,x_n)\dots q_{k-1}(x_1,\dots,x_n)y^k = 0\,. \end{aligned} \tag{72}$$

Hence, if we define $p \in K[X_0, X_1, \dots, X_n]$ by

$$\begin{aligned} p(X_0,X_1,\dots,X_n) =& p_0(X_1,\dots,X_n)q_1(X_1,\dots,X_n)\dots q_{k-1}(X_1,\dots,X_n) \\ &+q_0(X_1,\dots,X_n)p_1(X_1,\dots,X_n)\dots q_{k-1}(X_1,\dots,X_n)X_0 \\ &\vdots \\ &+q_0(X_1,\dots,X_n)q_1(X_1,\dots,X_n)\dots p_{k-1}(X_1,\dots,X_n)X_0^{k-1} \\ &+q_0(X_1,\dots,X_n)q_1(X_1,\dots,X_n)\dots q_{k-1}(X_1,\dots,X_n)X_0^k\,, \end{aligned} \tag{73}$$

then by Equation (72) we have $p(y, x_1, \dots, x_n) = 0$. We also note that p is not the zero polynomial, as its terms involving X_0^k are given by

$$q_0(X_1,\dots,X_n)q_1(X_1,\dots,X_n)\dots q_{k-1}(X_1,\dots,X_n)X_0^k\,.$$

From $q_i(x_1,\dots,x_n) \neq 0$ we in particular get $q_i(X_1,\dots,X_n) \neq 0$ for all $i \in \{0,\dots,k-1\}$ (i.e., $q_i \neq 0$ as an element of $K[X_1,\dots,X_n]$), and so

$$q_0(X_1,\dots,X_n)q_1(X_1,\dots,X_n)\dots q_{k-1}(X_1,\dots,X_n)X_0^k \neq 0\,.$$

This shows that $\{x_1,\dots,x_n,y\}$ is indeed algebraically dependent, so that 3) holds. This completes the proof. □

Recall that in a domain D we have $xy = 0$ for $x, y \in D$ only when $x = 0$ or $y = 0$. In other words, the product of two non-zero elements is again non-zero, which is equivalent to saying that the set $C := D \setminus \{0\}$ is closed under multiplication. As we also have $1 \in C$ and $0 \notin C$, we conclude that we may form the localization D_C of D by its non-zero elements C. Elements of D_C are of the form $\frac{d}{c}$ for $c, d \in D$ with $c \neq 0$. It is relatively straightforward to determine when two elements of D_C are the same: we have $\frac{d}{c} = \frac{d'}{c'}$ if and only if $e(dc' - d'c) = 0$ for some $e \in C$, but because D is a domain this is equivalent to $dc' - d'c = 0$, or $dc' = d'c$.

Note also that $\frac{d}{c} = 0 := \frac{0}{1}$ if and only if $d = 0$. Hence, in case $\frac{d}{c} \neq 0$ we have $d \in C$, so that $\frac{d}{c}$ has the inverse $\frac{c}{d}$. As clearly $\frac{1}{1} \neq \frac{0}{1}$ (in a domain we always have $1 \neq 0$), we conclude that D_C is in fact a field.

It can furthermore be seen that D_C contains D as a subring. More precisely, there is an injective ring-homomorphism from D into D_C, given by $d \mapsto \frac{d}{1}$. One easily verifies that this is indeed an injective homomorphism.

An important example of this construction is given when D equals $K[X_1, \ldots, X_n]$, the polynomial ring in n variables over a field K. In that case we denote the corresponding localization by the non-zero elements by $K(X_1, \ldots, X_n)$. Note that elements of $K(X_1, \ldots, X_n)$ are given by

$$\frac{p}{q} \text{ with } p, q \in K[X_1, \ldots, X_n], \text{ where } q \neq 0\,.$$

The following lemma justifies the notation $K(X_1, \ldots, X_n)$, in light of the previously defined $K(x_1, \ldots, x_n)$.

Lemma 2.22. *Let K be a subfield of L and let $\{x_1, \ldots, x_n\} \subseteq L$ be a set of algebraically independent elements over K. The subfield $K(x_1, \ldots, x_n) \subseteq L$ is isomorphic to $K(X_1, \ldots, X_n)$. Note that the latter field is defined independently of L.*

Proof. We define the map $\psi : K(X_1, \ldots, X_n) \to K(x_1, \ldots, x_n)$ by

$$\psi\left(\frac{p(X_1, \ldots, X_n)}{q(X_1, \ldots, X_n)}\right) = \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} := p(x_1, \ldots, x_n)(q(x_1, \ldots, x_n))^{-1}\,, \quad (74)$$

where $q \in K[X_1, \ldots, X_n]$ is non-zero. Some work is needed to verify that this is well-defined. First of all, as the elements x_1 through x_n are algebraically independent, we see that $q(x_1, \ldots, x_n) \neq 0$, so that $(q(x_1, \ldots, x_n))^{-1}$ exists. Secondly, if we have

$$\frac{p(X_1, \ldots, X_n)}{q(X_1, \ldots, X_n)} = \frac{p'(X_1, \ldots, X_n)}{q'(X_1, \ldots, X_n)}\,, \quad (75)$$

for some $p, p', q, q' \in K[X_1, \ldots, X_n]$, then $pq' = p'q$ as polynomials. It follows that

$$\begin{aligned} p(x_1, \ldots, x_n)q'(x_1, \ldots, x_n) &= (pq')(x_1, \ldots, x_n) \quad (76)\\ &= (p'q)(x_1, \ldots, x_n) = p'(x_1, \ldots, x_n)q(x_1, \ldots, x_n)\,. \end{aligned}$$

Multiplying both sides by $(q(x_1, \ldots, x_n))^{-1}(q'(x_1, \ldots, x_n))^{-1}$ yields

$$p(x_1, \ldots, x_n)(q(x_1, \ldots, x_n))^{-1} = p'(x_1, \ldots, x_n)(q'(x_1, \ldots, x_n))^{-1}\,,$$

so that ψ is indeed well-defined.
The claim that ψ is a ring-homomorphism follows from some straightforward calculations, and we note that ψ is surjective by construction. It remains to show injectivity. To this end, note that any element of $K(X_1, \ldots, X_n)$ may be written as pq^{-1} for some $p, q \in K[X_1, \ldots, X_n] \subseteq K(X_1, \ldots, X_n)$. The equality $\psi(pq^{-1}) = 0$ gives $\psi(p)\psi(q)^{-1} = 0$ and so $\psi(p) = 0$. As the elements of $\{x_1, \ldots, x_n\}$ are algebraically independent, we conclude that $p = 0$ and therefore $pq^{-1} = 0$. This completes the proof. □

Next, we need the notion of a maximal algebraically independent set.

Definition 2.23. Let K be a subfield of L and let S be an algebraically independent subset of L. We say that S is *maximal* if for any set $T \subseteq L$ satisfying $S \subsetneq T$ we have that T is algebraically dependent over K. $\triangle$

The following easy lemma tells us that maximality does not have to be checked for all supersets.

Lemma 2.24. *The algebraically independent set $S \subseteq L$ is maximal if and only if for any element $x \in L \setminus S$ the set $S \cup \{x\}$ is algebraically dependent.*

Proof. If S is maximal then for any element $x \in L \setminus S$ the set $S \cup \{x\}$ is algebraically dependent, by definition. Suppose therefore that none of the sets $S \cup \{x\}$ with $x \notin S$ is algebraically independent, and let $T \subseteq L$ be a given set strictly containing S. We pick an element $y \in T \setminus S$, so that $S \cup \{y\} \subseteq T$ is algebraically dependent. By Remark 2.19 the set T is algebraically dependent as well, showing that S is indeed maximal. $\square$

The following result will be very useful for determining whether or not a finite algebraically independent set is maximal.

Lemma 2.25. *Suppose the elements $x_1, \ldots, x_n \in L$ are algebraically independent over the subfield $K \subseteq L$. Then $\{x_1, \ldots, x_n\}$ is maximal if and only if L is integral over the subfield $K(x_1, \ldots, x_n)$.*

Proof. From Lemma 2.24 we see that $\{x_1, \ldots, x_n\}$ is maximal if and only if $\{x_1, \ldots, x_n, y\}$ is algebraically dependent for all $y \in L \setminus \{x_1, \ldots, x_n\}$. By Proposition 2.21 this holds if and only if every element $y \in L \setminus \{x_1, \ldots, x_n\}$ is integral over $K(x_1, \ldots, x_n)$. As clearly the elements x_1 through x_n are integral over $K(x_1, \ldots, x_n)$, the result follows. $\square$

The following proposition will be essential for showing that the so-called transcendence degree is well-defined.

Proposition 2.26. *Let K be a subfield of L and let $\{x_1, \ldots, x_n\} \subseteq L$ be a finite, maximal, algebraically independent set over K. Suppose the set $\{y_1, \ldots, y_k\} \subseteq L$ is likewise algebraically independent over K, and assume $k \leq n$. Then for some $n - k$ indices $\{i_{k+1}, \ldots, i_n\} \subseteq \{1, \ldots, n\}$, the set $\{y_1, \ldots, y_k, x_{i_{k+1}}, \ldots, x_{i_n}\}$ is maximal algebraically independent as well.*

In the following proof, we will often use the notation $\{x_1, \ldots, \widehat{x_i}, \ldots, x_n\}$ to denote $\{x_1, \ldots, x_n\} \setminus \{x_i\}$. That is, $\{x_1, \ldots, x_n\}$ with x_i left out. Likewise, if $(x_1, \ldots, x_n)$ is an ordered sequence of n elements, then $(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$ denotes the ordered sequence of $n-1$ elements given by $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. If for instance we have a polynomial $p \in K[X_1, \ldots, X_{n-1}]$, then the expression $p(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$ denotes p with this sequence of $n-1$ elements plugged in.

Proof of Proposition 2.26. We will prove the statement by replacing elements of $\{x_1, \ldots, x_n\}$ by those in $\{y_1, \ldots, y_k\}$, one at a time, starting with y_1. If $y_1 = x_i$ for some $i \in \{1, \ldots, n\}$, then trivially the set $\{y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n\} =$

$\{x_1, \ldots, x_n\}$ is maximal algebraically independent. Note that this set has n (distinct) elements, something we will use later on. Suppose therefore that $y_1 \notin \{x_1, \ldots, x_n\}$, so that the set $\{y_1, x_1, \ldots, x_n\}$ is algebraically dependent by maximality of $\{x_1, \ldots, x_n\}$. It follows that a non-zero polynomial $p \in K[X_0, X_1, \ldots, X_n]$ exists such that $p(y_1, x_1, \ldots, x_n) = 0$. We gather all such polynomials in the set

$$\mathcal{P}_1 := \{p \in K[X_0, X_1, \ldots, X_n] \setminus \{0\} \mid p(y_1, x_1, \ldots, x_n) = 0\},$$

which is therefore non-empty.

Given any polynomial $p \in K[X_0, X_1, \ldots, X_n]$, we furthermore denote by $I_p \subseteq \{0, 1, \ldots, n\}$ the set of indices i for which the variable X_i appears in p. More precisely, any polynomial may be written as a unique linear combination of monomials $X_0^{i_0} X_1^{i_1} \ldots X_n^{i_n}$ where $i_0, i_1, \ldots, i_n \geq 0$, with coefficients in K. We set $j \in I_p$ if and only if p has a term $X_0^{i_0} X_1^{i_1} \ldots X_n^{i_n}$ with $i_j > 0$ appear in this way with a non-zero coefficient. For instance, we have $I_{X_0^2 X_1 - X_4} = \{0, 1, 4\}$, $I_{X_0^2 X_1 - X_4 + X_4} = I_{X_0^2 X_1} = \{0, 1\}$ and $I_0 = I_1 = \emptyset$. We then use

$$\Omega_1 := \{I_p \mid p \in \mathcal{P}_1\},$$

to denote all index sets of polynomials in $\mathcal{P}_1$.

We next make some observations about Ω_1. First of all, it is clear that $\mathcal{P}_1$ does not contain any constant polynomials, as the zero-polynomial is excluded by definition. As a result, Ω_1 does not contain the empty set. Next, we note that $\{0\} \notin \Omega_1$. Otherwise a non-zero polynomial $p \in K[X_0] \subseteq K[X_0, X_1, \ldots, X_n]$ would exist such that $p(y_1) = 0$, contradicting algebraic independence of $\{y_1, \ldots, y_k\}$ (by contradicting algebraic independence of its subset $\{y_1\}$). Finally, we see that any set $I_p \in \Omega_1$ necessarily contains 0. Otherwise a non-zero polynomial $p \in K[X_1, \ldots, X_n] \subseteq K[X_0, X_1, \ldots, X_n]$ would exist such that $p(x_1, \ldots, x_n) = 0$, contradicting algebraic independence of $\{x_1, \ldots, x_n\}$.

As $\mathcal{P}_1 \neq \emptyset$, we may choose a polynomial $q \in \mathcal{P}_1$ such that I_q is minimal. In other words, for any strict subset $J \subsetneq I_q$ there does not exist a polynomial $r \in \mathcal{P}_1$ such that $J = I_r$. This can for instance be done by choosing q such that the number of elements in I_q is minimal. In what follows, we fix such a polynomial $q \in \mathcal{P}_1$ satisfying this minimality condition. By the above observations on Ω_1, there exists an index $i \in I_q \setminus \{0\}$, so that X_i appears in $q(X_0, X_1, \ldots, X_n)$. Fixing such a value of i, we gather terms in X_i and write

$$\begin{aligned} q(X_0, X_1, \ldots, X_n) = {} & q_0(X_0, X_1, \ldots, \widehat{X_i}, \ldots, X_n) \\ & + q_1(X_0, X_1, \ldots, \widehat{X_i}, \ldots, X_n) X_i \\ & \vdots \\ & + q_l(X_0, X_1, \ldots, \widehat{X_i}, \ldots, X_n) X_i^l, \end{aligned} \tag{77}$$

for some $l > 0$ and where $q_l \neq 0$. It follows that

$$\begin{aligned} 0 = \; & q_0(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n) \\ & + \; q_1(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n)x_i \\ & \vdots \\ & + q_l(y_1, x_1, \ldots, \widehat{x_i}, , \ldots, x_n)x_i^l \,. \end{aligned} \tag{78}$$

We claim that $q_l(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n) \neq 0$. To see why, note that $I_{q_l} \subseteq I_q \setminus \{i\}$, as q_l is formed by collecting terms in X_i. It follows from minimality of I_q that $q_l \notin \mathcal{P}_1$. As we also have $q_l \neq 0$, we conclude that indeed $q_l(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n) \neq 0$. We may thus write

$$0 = \frac{q_0(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n)}{q_l(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n)} + \frac{q_1(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n)}{q_l(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n)}x_i + \cdots + x_i^l \,, \tag{79}$$

which shows that x_i is integral over the field $K(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n)$. From Proposition 2.21 we conclude that

$$K(y_1, x_1, \ldots, x_n) \text{ is integral over } K(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n). \tag{A1}$$

As $\{x_1, \ldots, x_n\}$ is a maximal algebraically independent set over K, it follows from Lemma 2.25 that L is integral over $K(x_1, \ldots, x_n)$. Hence, L is also integral over the larger field $K(y_1, x_1, \ldots, x_n)$. Combined with Observation (A1), we conclude from Proposition 2.17 that

$$L \text{ is integral over } K(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n). \tag{B1}$$

We next wish to show that $\{y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n\}$ is an algebraically independent set over K. If this is not the case, then it follows from Lemma 2.21 –applied to the algebraically independent set $\{x_1, \ldots, \widehat{x_i}, \ldots, x_n\}$– that $K(y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n)$ is algebraic over $K(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$. Proposition 2.17 combined with Observation (B1) now tells us that L is algebraic over $K(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$. We conclude by Lemma 2.25 that the algebraically independent set $\{x_1, \ldots, \widehat{x_i}, \ldots, x_n\}$ is maximal, contradicting our assumption that the set $\{x_1, \ldots, x_n\}$ is algebraically independent. Hence, we see that $\{y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n\}$ is indeed algebraically independent. We may therefore apply Lemma 2.25 to this set, so that Observation (B1) tells us that $\{y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n\}$ is a maximal algebraically independent set. As we assumed that $y_1 \notin \{x_1, \ldots, x_n\}$, we also see that $\{y_1, x_1, \ldots, \widehat{x_i}, \ldots, x_n\}$ consists of n (distinct) elements.

Suppose next that we have shown that $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$ is a maximal algebraically independent set of n elements, for some $m > 1$ and numbers $j_m, \ldots, j_n \in \{1, \ldots, n\}$. If we have $y_m = x_{j_i}$ for some $i \in \{m, \ldots, n\}$, then clearly $\{y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\} = \{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$ is a maximal algebraically independent set over K, consisting of n distinct elements. Suppose therefore that $y_m \notin \{x_{j_m}, \ldots, x_{j_n}\}$, so that in fact $y_m \notin$

$\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$. As this latter set is maximal algebraically independent, we conclude that the set

$$\mathcal{P}_m := \{p \in K[X_0, X_1, \ldots, X_n] \setminus \{0\} \mid p(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}) = 0\},$$

is non-empty. As before, we use

$$\Omega_m := \{I_p \mid p \in \mathcal{P}_m\},$$

to denote all index sets of polynomials in $\mathcal{P}_m$.

Similar to Ω_1, we see that Ω_m does not contain the empty set, as $\mathcal{P}_m$ does not contain any constant polynomials. Likewise, a polynomial in $\mathcal{P}_m$ cannot only involve the variables $X_0, \ldots, X_{m-1}$, as this would contradict algebraic independence of $\{y_1, \ldots, y_m\} \subseteq \{y_1, \ldots, y_k\}$. We conclude that $I \not\subseteq \{0, \ldots, m-1\}$ for all $I \in \Omega_m$. As before, we choose a polynomial $q \in \mathcal{P}_m$ such that I_q is minimal among Ω_m.

Let $i \in \{m, \ldots, n\}$ be an index such that $i \in I_q$, so that X_i appears in q. By the foregoing such an i indeed exists. We rewrite q as in Equation (77) for certain polynomials $q_0, \ldots, q_l$, with $l > 0$, and where q_l is non-zero. From $q \in \mathcal{P}_m$ we get

$$\begin{aligned} 0 = {} & q_0(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}) \\ & + q_1(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}) x_{j_i} \\ & \vdots \\ & + q_l(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}) x_{j_i}^l \,. \end{aligned} \tag{80}$$

Recall that $q_l \neq 0$, so that $q_l(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})$ vanishing implies $q_l \in \mathcal{P}_m$. This contradicts minimality of I_q, and so we conclude that

$$q_l(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}) \neq 0\,. \tag{81}$$

We may therefore write

$$\begin{aligned} 0 = {} & \frac{q_0(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})}{q_l(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})} \\ & + \frac{q_1(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})}{q_l(y_m, y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})} x_{j_i} + \cdots + x_{j_i}^l \,. \end{aligned} \tag{82}$$

From this we conclude that x_{j_i} is integral over the field $K(y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})$, so that Proposition 2.21 gives

$$\begin{aligned} & K(y_1, \ldots, y_m, x_{j_m}, \ldots, x_{j_n}) \text{ is integral over} \\ & \qquad K(y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}). \end{aligned} \tag{Am}$$

Since $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$ is maximal, we conclude by Lemma 2.25 that L is integral over $K(y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n})$. Hence, L is integral over the larger field $K(y_1, \ldots, y_m, x_{j_m}, \ldots, x_{j_n})$ as well. Together with Observation (Am), and using Proposition 2.17, we conclude that

$$L \text{ is integral over } K(y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}). \tag{Bm}$$

If we can show that $\{y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$ is algebraically independent, then Observation (Bm) and Lemma 2.25 tell us that this set is maximal. Suppose therefore that it is algebraically dependent. As $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$ is algebraically independent, so is its subset $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$. This latter set is equal to $\{y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$ with the element y_m removed, so that by Proposition 2.21 we see that $K(y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})$ is integral over $K(y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})$. We conclude from Proposition 2.17 and Observation (Bm) that L is integral over $K(y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n})$. Hence, by Lemma 2.25 we conclude that $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$ is a maximal algebraically independent set. This contradicts the assumption that its superset $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$ is algebraically independent. More precisely, here we use that $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$ has n elements, so that $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$ is really a strict subset. We obtained this contradiction by assuming that $\{y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$ is algebraically dependent. Hence, it is independent and therefore maximal by Observation (Bm).

Finally, we claim that $\{y_1, \ldots, y_m, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$ contains n elements, so that we are not showing an element twice. This follows from the fact that $\{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, \widehat{x_{j_i}}, \ldots, x_{j_n}\}$ has precisely $n-1$ elements, together with the assumption that $y_m \notin \{y_1, \ldots, y_{m-1}, x_{j_m}, \ldots, x_{j_n}\}$.

Repeating this procedure gives us $n-k$ (distinct) indices $i_{k+1}, \ldots, i_n \in \{1, \ldots, n\}$ such that $\{y_1, \ldots, y_k, x_{i_{k+1}}, \ldots, x_{i_n}\}$ is a maximal algebraically independent set over K. This completes the proof. □

Remark 2.27. Suppose L is integral over the subfield K. By definition, this means that any singleton set $\{x\}$ for $x \in L$ is algebraically dependent, see also Remark 2.20. It follows that the empty set is maximal algebraically independent over K. Conversely, if the empty set is maximal then any singleton set is necessarily dependent. Hence, any element of L is integral over K. Summarizing, we find that L is integral over K, if and only if the empty set is maximal. △

Proposition 2.28. *Let K be a subfield of L and suppose L contains a finite maximal algebraically independent set over K with $n \geq 0$ elements. It then holds that:*

1. *Any subset of L that is algebraically independent over K is finite, with at most n elements.*

2. *Of the algebraically independent subsets of L, the maximal ones are precisely those with n elements.*

3. *Any algebraically independent set can be extended to a maximal one. More precisely, given any maximal algebraically independent set X, we can extend any algebraically independent set to a maximal one by adding only elements of X.*

Proof. Suppose first that $n = 0$, so that the empty set is maximal. It follows that the empty set is the only algebraically independent set, so that points 1, 2 and 3 follow trivially.
Now suppose $\{x_1, \ldots, x_n\}$ is a given maximal algebraically independent set, consisting of $n > 0$ elements. If $\{y_1, \ldots, y_n\} \subseteq L$ is algebraically independent –likewise with n elements– then Proposition 2.26 tells us $\{y_1, \ldots, y_n\}$ is in fact maximal. We have thus shown that any algebraically independent set of n elements is maximal, which is part of point 2. It follows that any set containing a strict subset of n elements cannot be algebraically independent, which shows point 1.
Next, if $\{y_1, \ldots, y_k\} \subseteq L$ is maximal algebraically independent, then necessarily $k \leq n$. We may therefore apply Proposition 2.26 to the maximal set $\{y_1, \ldots, y_k\}$ and the algebraically independent set $\{x_1, \ldots, x_k\} \subseteq \{x_1, \ldots, x_n\}$. We conclude that $\{x_1, \ldots, x_k\}$ is maximal, which is only possible if $k = n$. This proves the second point.
Finally, point 3 now follows directly from Proposition 2.26, which concludes the proof. □

Proposition 2.28 motivates the following definition.

Definition 2.29. Let K be a subfield of L. We say that the *transcendence degree* of L over K is n for some $n \in \mathbb{N}_{\geq 0}$ if L contains a maximal algebraically independent set over K with n elements. If L does not contain a finite maximal algebraically independent set, then its transcendence degree is infinite. We denote the transcendence degree of L over K by $\mathrm{trdeg}_K(L)$. △

Remark 2.30. Proposition 2.28 guarantees that the transcendence degree is well-defined. In other words, it takes on one unique value. It is not hard to see, using Zorn's lemma, that there always exists a maximal algebraically independent subset of L over K. We will not make use of this, however, nor will we need transcendence degree when it is infinite. △

2.4 Transcendence degree for domains

Note that the definition of algebraic (in)dependence does not require the rings in question to be fields. In other words, given a ring S with subring R, we may say that a finite subset $\{x_1, \ldots, x_n\} \subseteq S$ is algebraically independent over R if the only polynomial $p \in R[X_1, \ldots, X_n]$ satisfying $p(x_1, \ldots, x_n) = 0$ is the zero polynomial. It follows that a finite set is algebraically independent if and only if all of its subsets are. Hence, we may extend this definition to any subset of

S by stating that it is algebraically independent if all of its finite subsets are. Likewise, we say that an algebraically independent set is maximal if it is not strictly contained in any algebraically independent set.

We will not need the notion of algebraic independence is this generality though. Rather, we will investigate a mild generalization of what we looked at in the previous subsection, by considering a domain D that contains a field K as a subring. One important example is given by $D = K[X_1, \ldots, X_n]$, or more generally by $D = K[X_1, \ldots, X_n]/P$ for P a prime ideal. Note that in the latter case we have an injective ring-homomorphism from K to D given by $k \mapsto [k]$. This homomorphism is indeed injective as we have $1 \notin P$.

Recall that we may localize a domain D by the set of its non-zero elements C, which gives rise to a field D_C. We then have an inclusion of D into D_C given by $D \ni d \mapsto \frac{d}{1}$. Hence, if a domain D contains a field K, then we have an inclusion of fields $K \subseteq D_C$. Motivated by this, we define:

Definition 2.31. Let D be a domain containing a field K. The *transcendence degree* of D over K (denoted by $\mathrm{trdeg}_K(D)$) is defined as the transcendence degree of D_C over K. △

The following results relate the definition above back to D. Throughout this subsection we assume that D is a domain containing a field K.

Lemma 2.32. *Given a subset S of D, it holds that S is algebraically independent over K in D, if and only if it is algebraically independent over K in D_C.*

Proof. This follows directly from the definition of algebraic dependence, as for any polynomial $p \in K[X_1, \ldots, X_n]$ the value of $p(s_1, \ldots, s_n)$ for $s_1, \ldots, s_n \in S$ is understood in $D \subseteq D_C$. □

In light of Lemma 2.32, we will henceforth simply state that a subset S of D is algebraically (in)dependent if it is as a subset of D or equivalently D_C.

Lemma 2.33. *Let S be an algebraically independent subset of D and let $x \in D_C \setminus S$ be an element such that $S \cup \{x\}$ is algebraically independent as well. Writing*

$$x = \frac{d}{c} \text{ for some } c, d \in D \text{ with } c \neq 0\,, \tag{83}$$

at least one of the sets $S \cup \{c\}$ and $S \cup \{d\}$ is an algebraically independent subset of D that strictly contains S.

Proof. We prove the lemma by contradiction, and so we start by assuming its conclusion not to hold. In that case, either we have $S = S \cup \{c\}$ and so $c \in S$, or the set $S \cup \{c\}$ is algebraically dependent (and so necessarily $c \notin S$). Likewise, we either have $d \in S$ or the set $S \cup \{d\}$ is algebraically dependent.
As a warm-up we first consider the case where $S = \emptyset$. It follows that the sets

$\{c\}$ and $\{d\}$ are both algebraically dependent over K, which is equivalent to saying that c and d are both integral over K. By Corollary 2.13, applied to the fields $K \subseteq D_C$, we conclude that $x = dc^{-1}$ is integral over K as well. However, this contradicts our assumption that $S \cup \{x\} = \{x\}$ is algebraically independent. We conclude that either $\{c\}$ or $\{d\}$ is algebraically independent.
Now assume the general case, so that S is not necessarily empty. We wish to show that c is integral over the smallest field $K(T_c) \subseteq D_C$ containing K and some finite subset $T_c \subseteq S$. In case we have $c \in S$ we may put $T_c = \{c\}$, as the element c is clearly integral over $K(c)$. If on the other hand $S \cup \{c\}$ is algebraically dependent, then a finite subset of $S \cup \{c\}$ is as well. This subset cannot be contained in S, as this latter set is algebraically independent. Hence, we see that a finite set $T_c \subseteq S$ exists such that $T_c \cup \{c\}$ is algebraically dependent. Note that T_c itself is necessarily algebraically independent, as it is contained in S. We may thus apply Proposition 2.21 to conclude that c is integral over the field $K(T_c)$. In conclusion, we see that in both cases a finite set $T_c \subseteq S$ indeed exists such that c is integral over $K(T_c)$. In exactly the same way, we conclude that d is integral over $K(T_d)$ for some finite subset $T_d \subseteq S$.
Setting $T := T_c \cup T_d \subseteq S$, we conclude that both c and d are integral over $K(T)$. From Corollary 2.13 we see that the set of all elements in D_C that are integral over $K(T)$ forms a field containing both c and d. In particular, the element $x = dc^{-1}$ is integral over $K(T)$.
Applying Proposition 2.21 to x and the finite algebraically independent set T, we conclude that $T \cup \{x\}$ is algebraically dependent. This contradicts our assumption that $S \cup \{x\}$ is algebraically independent, and we conclude that either $S \cup \{c\}$ or $S \cup \{d\}$ has to be an algebraically independent set strictly containing S. This completes the proof. □

Corollary 2.34. *Let S be an algebraically independent subset of D. It holds that S is maximal in D if and only if it is maximal in D_C.*

Proof. If S is not maximal in D, then there exists an algebraically independent set $S' \subseteq D$ that strictly contains S. By Lemma 2.32, S' is also an algebraically independent superset of S in D_C, so that S is not maximal in this field.
Conversely, suppose S is not maximal in D_C. It follows that there exists an element $x \in D_C \setminus S$ such that $S \cup \{x\}$ is algebraically independent. We now see from Lemma 2.33 that S is not maximal in D, which completes the proof. □

Theorem 2.35. *Let D be a domain containing a field K. Given $n \in \mathbb{N}_{\geq 0}$, there exists a maximal algebraically independent set of n elements in D, if and only if one exists in D_C. In particular, the transcendence degree of D over K is n, if and only if there exists a maximal algebraically independent set of n elements in D.*

Proof. It follows directly from Corollary 2.34 that a maximal algebraically independent set of n elements in D implies such a set in D_C (in fact, we may use the same one). Now suppose there is a maximal algebraically independent set of n elements in D_C. If we have $n = 0$ then the empty set is maximal

in both D and D_C by Corollary 2.34. In case $n > 0$ we conclude that there exists an element $x_1 \in D_C$ such that $\{x_1\}$ is algebraically independent. Applying Lemma 2.33 with $S = \emptyset$ and $x = x_1$, we find an algebraically independent set $\{a_1\} \subseteq D$. In case $n = 1$ we conclude from Proposition 2.28 that $\{a_1\}$ is maximal in D_C. Hence by Corollary 2.34 we see that $\{a_1\}$ is also maximal in D. In general, suppose we have found k elements $a_1, \ldots, a_k \in D$ such that $\{a_1, \ldots, a_k\}$ is algebraically independent, with $k \leq n$. If $k = n$ then $\{a_1, \ldots, a_k\}$ is maximal in D_C by Proposition 2.28. Hence, it is maximal in D as well. In case we have $k < n$, it follows from Proposition 2.28 that a set $\{a_1, \ldots, a_k\} \cup \{x_{k+1}\}$ is algebraically independent for some $x_{k+1} \in D_C \setminus \{a_1, \ldots, a_k\}$. By Lemma 2.33 we get an element $a_{k+1} \in D \setminus \{a_1, \ldots, a_k\}$ such that $\{a_1, \ldots, a_k, a_{k+1}\} \subseteq D$ is algebraically independent. Repeating this argument, we end up with an algebraically independent set of n elements $\{a_1, \ldots, a_n\} \subseteq D$, which is maximal by the argument for $k = n$. This completes the proof. □

Remark 2.36. As we have $D \subseteq D_C$, all the conclusions of Proposition 2.28 hold for D as well. More precisely, suppose D has a maximal algebraically independent subset of $n \geq 0$ elements. As algebraically independent subsets of D are algebraically independent in D_C as well, we see that any such subset can have at most n elements. Moreover, by Corollary 2.34 the maximal ones are precisely those with n elements. Finally, given two algebraically independent sets $S, T \subseteq D$ with S maximal, we see that T can be completed to a maximal one by adding only elements of S. △

We end this subsection with a concrete example.

Proposition 2.37. *Let K be a field. The transcendence degree over K of the polynomial ring $K[X_1, \ldots, X_n]$ is equal to n.*

Proof. The elements $X_1, \ldots, X_n$ are algebraically independent in $K[X_1, \ldots, X_n]$, as $p(X_1, \ldots, X_n) = 0$ for $p \in K[X_1, \ldots, X_n]$ means $p = 0$ (tautologically). To see that $\{X_1, \ldots, X_n\}$ is maximal, consider any set $\{X_1, \ldots, X_n, q\}$ for some polynomial $q = q(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n] \setminus \{X_1, \ldots, X_n\}$. We define a new polynomial $\tilde{q} \in K[Y_0, Y_1, \ldots, Y_n]$ given by

$$\tilde{q}(Y_0, Y_1, \ldots, Y_n) = Y_0 - q(Y_1, \ldots, Y_n)\,. \tag{84}$$

Clearly $\tilde{q} \neq 0$, and we furthermore see that $\tilde{q}(q, X_1, \ldots, X_n) = 0$ by construction. Hence, $\{X_1, \ldots, X_n, q\}$ is algebraically dependent, from which we see that $\{X_1, \ldots, X_n\}$ is indeed maximal. The result now follows from Theorem 2.35. □

Corollary 2.38. *For any field K, the transcendence degree of $K(X_1, \ldots, X_n)$ is equal to n.*

Proof. This follows immediately from Proposition 2.37 and the definition of transcendence degree for domains. □

2.5 Noether's normalization lemma

We next need a powerful result known as Noether's normalization lemma. Among other things, it will tell us more about the transcendence degree of domains of the form $K[X_1, \ldots, X_n]/P$, where P is a prime ideal.

Noether's normalization lemma involves the notion of 'finitely generated' in two different settings. One of these we have encountered before: a module M over a ring R is called finitely generated if M is the smallest submodule of itself containing some finite set $\{x_1, \ldots, x_k\}$. Equivalently, if every element $m \in M$ may be written as

$$m = r_1 x_1 + \cdots + r_k x_k \,, \tag{85}$$

for some $r_1, \ldots, r_k \in R$, see Subsection 2.1. Recall that if R is a subring of a ring S, then S may also be viewed as a module over R. The statement of Noether's normalization lemma will be that for a ring S (of a certain kind), there exists a subring R (of a special form) such that S is finitely generated as a module over R.

The other notion pertains to a ring R that contains a field K as a subring. Such a ring is sometimes called an *algebra* over K. We say that the algebra R is *finitely generated* if finitely many elements $x_1, \ldots, x_k \in R$ exist such that every element $r \in R$ may be written as

$$r = p(x_1, \ldots, x_k) \,, \tag{86}$$

for some polynomial $p \in K[X_1, \ldots, X_k]$. Note that this does not imply that every element in R may be written as a linear combination of the x_i with coefficients in K, i.e., as $c_1 x_1 + \cdots + c_k x_k$ for some $c_1, \ldots, c_k \in K$. The set of all elements in R that may be written this way does not in general form a ring.

Examples of finitely generated algebras over K are given by $K[X_1, \ldots, X_n]$ and more generally by $K[X_1, \ldots, X_n]/I$ for some ideal $I \subsetneq K[X_1, \ldots, X_n]$. The generators are given by X_1 through X_n and their quotient classes, respectively. In fact, the following result shows that these are essentially all examples.

Lemma 2.39. *Every finitely generated algebra over a field K is isomorphic (as a ring) to an algebra of the form $K[X_1, \ldots, X_n]/I$ for some ideal $I \subsetneq K[X_1, \ldots, X_n]$.*

Proof. Let R be an algebra over K generated by the elements $x_1, \ldots, x_n$. We define a map ψ from $K[X_1, \ldots, X_n]$ to R by setting $\psi(p) = p(x_1, \ldots, x_n)$ for $p \in K[X_1, \ldots, X_n]$. One easily verifies that ψ is a ring-homomorphism. Moreover, it follows from the definition of a finitely generated algebra that ψ is surjective. Let I denote the kernel of ψ, so that by the first isomorphism theorem for rings we have

$$K[X_1, \ldots, X_n]/I \cong R \,. \tag{87}$$

It remains to show that I is not equal to $K[X_1, \ldots, X_n]$. However, if it were then we would have $1 = 0$ in R, contradicting the fact that R contains the field K as a subring. □

Note that the identification between $K[X_1, \ldots, X_n]/I$ and R in the proof of Lemma 2.39 also respects the inclusion of K into both rings.

Corollary 2.40. *Every finitely generated algebra is a Noetherian ring.*

Proof. By Hilbert's basis theorem (Lemma 1.3) together with Lemma 1.5, the ring $K[X_1, \ldots, X_n]$ is Noetherian. Now consider an ideal $I \subseteq K[X_1, \ldots, X_n]$, together with the quotient ring and projection $\pi : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]/I$. If J is an ideal of $K[X_1, \ldots, X_n]/I$, then $\pi^{-1}(J)$ is an ideal of $K[X_1, \ldots, X_n]$. Hence, by Lemma 1.5 we see that $\pi^{-1}(J)$ is finitely generated, say by elements $s_1, \ldots, s_t$. It follows that J is generated by the elements $\pi(s_1), \ldots, \pi(s_t)$. This shows that every ideal of $K[X_1, \ldots, X_n]/I$ is finitely generated, so that it is likewise a Noetherian ring. The result now follows from Lemma 2.39. □

If R is an algebra over the field K, and if $\{y_1, \ldots, y_k\}$ is some finite subset of R, then we define $K[y_1, \ldots, y_k] \subseteq R$ as the set of all elements in R that may be written as $p(y_1, \ldots y_k)$ for some $p \in K[X_1, \ldots, X_k]$. Note that we have already encountered this construction in Subsection 2.2. It follows that $K[y_1, \ldots, y_k]$ is a subring of R and a finitely generated algebra over K in its own right. The following easy lemma justifies the notation for $K[y_1, \ldots, y_k]$.

Lemma 2.41. *If $\{y_1, \ldots, y_k\} \subseteq R$ is algebraically independent over K, then $K[y_1, \ldots, y_k]$ is isomorphic to the polynomial ring $K[X_1, \ldots, X_k]$.*

Proof. The proof is essentially contained in that of Lemma 2.22. We define a map $\psi : K[X_1, \ldots, X_k] \to K[y_1, \ldots, y_k]$ by $\psi(p) = p(y_1, \ldots, y_k)$. This map is surjective by definition of $K[y_1, \ldots, y_k]$ and injective by the algebraic independence of $\{y_1, \ldots, y_k\}$, which proves the two rings are isomorphic. □

The main result of this subsection is:

Theorem 2.42 (Noether's normalization lemma)**.** *Let R be a finitely generated algebra over the field K. There exists a finite subset $\{y_1, \ldots, y_k\} \subseteq R$ which is algebraically independent over K, such that R is a finitely generated module over the subring $K[y_1, \ldots, y_k]$.*

If R is given by $K[X_1, \ldots, X_n]/I$ for some ideal $I \subsetneq K[X_1, \ldots, X_n]$, then we may assume $k \leq n$. More precisely, we may assume $k = n$ if $I = \{0\}$ and $k < n$ otherwise.

The proof of Theorem 2.42 relies on the following result. In essence, it shows that the base-d numeral system is well-defined for any integer $d \geq 2$.

Lemma 2.43. *Let d be a natural number larger than 1. Given a non-negative integer M, if we have*

$$\sum_{m=0}^{M} a_m d^m = \sum_{m=0}^{M} b_m d^m \tag{88}$$

for some numbers $a_0, \ldots, a_M, b_0, \ldots, b_M \in \{0, 1, \ldots, d-1\}$, then necessarily $a_0 = b_0, \ldots, a_M = b_M$.

Proof. The result follows by induction on M. For $M = 0$, Equation (88) simply states $a_0 = b_0$. Now suppose the result holds for $M-1$, where $M > 0$. It follows from Equation (88) that $a_0 - b_0$ is divisible by d, so that $a_0 = b_0 + kd$ for some $k \in \mathbb{Z}$. This is clearly only possible for $k = 0$, and we conclude that $a_0 = b_0$. Subtracting a_0 from both sides and dividing by d, Equation (88) becomes

$$\sum_{m=0}^{M-1} a_{m+1} d^m = \sum_{m=0}^{M-1} b_{m+1} d^m \,. \tag{89}$$

By induction, we also find $a_1 = b_1, \ldots, a_M = b_M$, which completes the proof. □

Proof of Theorem 2.42. By Lemma 2.39 we may assume that R is given by $K[X_1, \ldots, X_n]/I$ for some ideal $I \subsetneq K[X_1, \ldots, X_n]$. If $I = \{0\}$ then we may choose $\{y_1, \ldots, y_k\} = \{X_1, \ldots, X_n\}$, which is an algebraically independent set by the proof of Proposition 2.37. Note that in the case of $I = \{0\}$ we therefore find $k = n$.

Our proof will proceed by induction on n. More precisely, we will prove that for the ring $R = K[X_1, \ldots, X_n]/I$ with $I \subsetneq K[X_1, \ldots, X_n]$ there exist k algebraically independent elements $\{y_1, \ldots, y_k\} \subseteq R$ such that R is finitely generated over $K[y_1, \ldots, y_k]$, where $k \leq n$ in general and with $k < n$ if $I \neq \{0\}$.

Note that for $n = 0$ we have $R = K$ and so $I = \{0\}$. Hence, this case is already covered and we found $k = n = 0$, so that indeed $k \leq n$.

As a warm-up, we also present the case $n = 1$ separately. We are thus interested in algebras of the form $K[X]/I$. Again we may assume that $I \neq \{0\}$, as we have already covered $I = \{0\}$. We may therefore pick a non-zero polynomial $p \in I$. Note that p is not constant, as $I \subsetneq K[X]$. After dividing by the leading coefficient, we may furthermore assume that p is monic. We denote by $\bar{X}$ the class of X in $K[X]/I$, so that we have $p(\bar{X}) = 0$ in $K[X]/I$. It follows that the element $\bar{X} \in K[X]/I$ is integral over K, so that by Lemma 2.9 we find that $K[\bar{X}]$ is a finitely generated module over K. Of course any element in $K[X]/I$ may be written as $q(\bar{X})$ for some $q \in K[X]$, so that $K[\bar{X}] = K[X]/I$. Hence, we find that $K[X]/I$ is a finitely generated module over K, which means we have shown the result with $0 = k < n = 1$.

Now suppose we have $n > 1$. Again the case $K[X_1, \ldots, X_n]/I$ with $I = \{0\}$ is taken care of, and we found $k = n$. We therefore assume that $I \neq \{0\}$ and pick a non-constant polynomial $p \in I$. We may write

$$p(X_1, \ldots, X_n) = \sum_{J \in \mathcal{J}} a_J X_1^{J_1} \ldots X_n^{J_n} \,, \tag{90}$$

where $\mathcal{J}$ is some non-empty set of multi-indices $J = (J_1, \ldots, J_n) \in (\mathbb{Z}_{\geq 0})^n$, with each $a_J \in K$ non-zero. Note that by assumption $\mathcal{J}$ contains at least one multi-index $J \neq (0, \ldots, 0)$. If we denote by $\bar{X}_i$ the class of X_i in $K[X_1, \ldots, X_n]/I$ for

all $i \in \{1, \ldots, n\}$, then it follows from $p \in I$ that

$$\sum_{J \in \mathcal{J}} a_J \bar{X}_1^{J_1} \ldots \bar{X}_n^{J_n} = 0 \text{ in } K[X_1, \ldots, X_n]/I\,. \tag{91}$$

We now let $d > 1$ be an integer satisfying

$$d > \max(J_i \mid i \in \{1, \ldots, n\}, J = (J_1, \ldots, J_n) \in \mathcal{J})\,. \tag{92}$$

Moreover, we set

$$\begin{array}{rclcl} z_2 & := & \bar{X}_2 & - & \bar{X}_1^d \\ z_3 & := & \bar{X}_3 & - & \bar{X}_1^{d^2} \\ & \vdots & & & \\ z_n & := & \bar{X}_n & - & \bar{X}_1^{d^{n-1}} \end{array} \quad \text{so that} \quad \begin{array}{rclcl} \bar{X}_2 & = & z_2 & + & \bar{X}_1^d \\ \bar{X}_3 & = & z_3 & + & \bar{X}_1^{d^2} \\ \vdots & & & & \\ \bar{X}_n & = & z_n & + & \bar{X}_1^{d^{n-1}}\,. \end{array}$$

This transforms a term $a_J \bar{X}_1^{J_1} \ldots \bar{X}_n^{J_n}$ into

$$a_J \bar{X}_1^{L_J} + \sum_{i < L_J} p_{i,J}(z_2, \ldots, z_n) \bar{X}_1^i\,,$$

where $L_J := J_1 + J_2 d + \cdots + J_n d^{n-1}$ and with each $p_{i,J}$ a polynomial with coefficients in K. Now by Lemma 2.43, there is a unique $\tilde{J} \in \mathcal{J}$ for which $L_{\tilde{J}}$ is largest. That is, $L_{\tilde{J}} > L_J$ for all $J \in \mathcal{J} \setminus \{\tilde{J}\}$. It follows from Equation (91) that

$$\begin{aligned} 0 &= \sum_{J \in \mathcal{J}} a_J \bar{X}_1^{J_1} \ldots \bar{X}_n^{J_n} = \sum_{J \in \mathcal{J}} \left(a_J \bar{X}_1^{L_J} + \sum_{i < L_J} p_{i,J}(z_2, \ldots, z_n) \bar{X}_1^i \right) \\ &= a_{\tilde{J}} \bar{X}_1^{L_{\tilde{J}}} + \sum_{i < L_{\tilde{J}}} q_i(z_2, \ldots, z_n) \bar{X}_1^i\,, \end{aligned} \tag{93}$$

for certain polynomials q_i with coefficients in K. Note that $L_{\tilde{J}} > 0$ as $J \neq (0, \ldots, 0)$ for at least one $J \in \mathcal{J}$. Multiplying both sides of Equation (93) with $a_{\tilde{J}}^{-1}$, we finally arrive at

$$0 = \bar{X}_1^{L_{\tilde{J}}} + \sum_{i < L_{\tilde{J}}} a_{\tilde{J}}^{-1} q_i(z_2, \ldots, z_n) \bar{X}_1^i\,. \tag{94}$$

This proves that $\bar{X}_1$ is integral over the ring $K[z_2, \ldots, z_n]$. By Lemma 2.9 we find that $K[z_2, \ldots, z_n][\bar{X}_1]$ is a finitely generated module over $K[z_2, \ldots, z_n]$. Of course, $K[z_2, \ldots, z_n][\bar{X}_1]$ is a ring containing K, z_2 through z_n and $\bar{X}_1$, and so containing K and $\bar{X}_1$ through $\bar{X}_n$. We therefore have $K[z_2, \ldots, z_n][\bar{X}_1] = K[\bar{X}_1, \ldots, \bar{X}_n] = K[X_1, \ldots, X_n]/I$ and we conclude that $K[X_1, \ldots, X_n]/I$ is a finitely generated module over $K[z_2, \ldots, z_n]$.

Next, we note that $K[z_2, \ldots, z_n]$ is a finitely generated algebra over K. By the proof of Lemma (2.39) we have $K[z_2, \ldots, z_n] \cong K[X_1, \ldots, X_{n-1}]/\hat{I}$ for

some ideal $\hat{I} \subsetneq K[X_1, \ldots, X_{n-1}]$. By the induction hypothesis there exist elements $y_1, \ldots, y_k \in K[z_2, \ldots, z_n]$, algebraically independent over K, such that $K[z_2, \ldots, z_n]$ is finitely generated over $K[y_1, \ldots, y_k]$. Moreover, we have $k \leq n-1$. In conclusion, $K[X_1, \ldots, X_n]/I$ is a finitely generated module over $K[z_2, \ldots, z_n]$ and $K[z_2, \ldots, z_n]$ is a finitely generated module over $K[y_1, \ldots, y_k]$, where $k < n$. It now follows by Lemma (2.16) that $K[X_1, \ldots, X_n]/I$ is a finitely generated module over $K[y_1, \ldots, y_k]$, which completes the proof. □

The following lemma is very useful in combination with Theorem 2.42.

Lemma 2.44. *Let R be a ring with a Noetherian subring T and suppose R is finitely generated as a module over T. Then, each element of R is integral over T.*

Proof. As R is a finitely generated module over a Noetherian ring, it follows from Proposition 2.7 that R is a Noetherian module. We now fix an element $x \in R$ and note that by Lemma 2.4 the submodule $T[x] \subseteq R$ is finitely generated over T. By Proposition 2.10, this implies that x is integral over T, which completes the proof. □

In the context of Theorem 2.42, it follows from Corollary 2.40 (or from Lemma 2.41 combined with Hilbert's basis theorem, Lemma 1.3) that $K[y_1, \ldots, y_k]$ is Noetherian. Hence, by Lemma 2.44 we see that the algebra R is also integral over $K[y_1, \ldots, y_k]$ in Theorem 2.42.

Proposition 2.45. *Let R be an algebra over a field K and suppose $\{y_1, \ldots, y_k\} \subseteq R$ is a finite set of elements that is algebraically independent over K, and such that R is integral over $K[y_1, \ldots, y_k]$. If R is a domain then the number k is necessarily equal to the transcendence degree of R over K.*

Proof. As $\{y_1, \ldots, y_k\}$ is algebraically independent, by Theorem 2.35 it suffices to show that for any $x \in R \setminus \{y_1, \ldots, y_k\}$ the set $\{x, y_1, \ldots, y_k\}$ is algebraically dependent. However, as x is integral over $K[y_1, \ldots, y_k]$, it follows that $m \in \mathbb{N}$ and polynomials $p_0, \ldots, p_{m-1} \in K[X_1, \ldots, X_k]$ exist such that

$$x^m + \sum_{i=0}^{m-1} p_i(y_1, \ldots, y_k) x^i = 0\,. \tag{95}$$

If we now define the polynomial $p \in K[X_0, \ldots, X_k]$ by

$$p(X_0, \ldots, X_k) = X_0^m + \sum_{i=0}^{m-1} p_i(X_1, \ldots, X_k) X_0^i\,, \tag{96}$$

then clearly $p(x, y_1, \ldots, y_k) = 0$. Moreover, p is not the zero-polynomial as it contains a term X_0^m. Hence, the set $\{x, y_1, \ldots, y_k\}$ is indeed algebraically dependent, which completes the proof. □

In the context of Theorem 2.42, we see that for R a domain the number k is uniquely determined as the transcendence degree.

2.6 Proof of Hilbert's Nullstellensatz

Let Λ be a subset of the polynomial ring $K[X^1, \ldots, X^n]$, where K is any field. Recall that $V(\Lambda) \subseteq K^n$ denotes the set of points in K^n on which all polynomials in Λ vanish. A subset of K^n that may be written this way –that is, as $V(\Lambda)$ for some $\Lambda \subseteq K[X^1, \ldots, X^n]$– is called an algebraic set. In Subsection 1.1 we have seen that for any algebraic set $W \subseteq K^n$ there exists an ideal $J \subseteq K[X^1, \ldots, X^n]$ such that $W = V(J)$. Moreover, J may be assumed radical –i.e. $\sqrt{J} = J$– as we have seen in Subsection 1.3. We thus have a surjective map V from the set

$$\{ \text{ radical ideals of } K[X^1, \ldots, X^n] \}$$

to

$$\{ \text{ algebraic sets in } K^n \},$$

which takes the ideal J and outputs the algebraic set $V(J)$. Given an algebraic set W, we may moreover write down explicitly an element in the pre-image of this map V. To this end, we defined $I(W) \subseteq K[X^1, \ldots, X^n]$ as the set of polynomials that vanish on all points in W. In Subsection 1.5 we saw that $I(W)$ is indeed a radical ideal satisfying $W = V(I(W))$. The map V is therefore a bijection if we can show that $I(V(J)) = J$ for any radical ideal J. This result only holds when K is algebraically closed though, and it follows from Hilbert's Nullstellensatz below.

Theorem 2.46 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field. For any ideal $J \subseteq K[X_1, \ldots, X_n]$ we have $I(V(J)) = \sqrt{J}$.*

Note that if $\sqrt{J} = J$ then indeed $I(V(J)) = \sqrt{J} = J$. The proof of Hilbert's Nullstellensatz will use Zariski's lemma given below, which in turn uses Noether's normalization lemma.

Theorem 2.47 (Zariski's lemma)**.** *Let L be a field and $K \subseteq L$ a subfield of L. If L is a finitely generated algebra over K, then L is in fact a finitely generated module over K.*

Note that modules over fields are simply vector spaces, with the finitely generated ones being precisely those that are finite dimensional.

Proof of Zariski's lemma. As L is a finitely generated algebra over K, it follows from Noether's normalization lemma (Theorem 2.42) that finitely many elements $y_1, \ldots, y_k \in L$ exist such that L is finitely generated over $K[y_1, \ldots, y_k]$ as a module. The elements y_1 through y_k may furthermore be assumed algebraically independent over K. We are therefore done if we can show that $k = 0$, as this means L is a finitely generated module over K. Suppose otherwise, so that we may consider the element $y_1 \in L$. As $\{y_1, \ldots, y_k\}$ is algebraically independent, we have $y_1 \neq 0$ so that the element y_1^{-1} exists. By Lemma 2.44 we have that y_1^{-1} is integral over $K[y_1, \ldots, y_k]$. This implies that a number $m > 0$ and polynomials $p_0, \ldots, p_{m-1} \in K[X_1, \ldots, X_k]$ exist such that

$$y_1^{-m} + \sum_{\ell=0}^{m-1} p_\ell(y_1, \ldots, y_k) y_1^{-\ell} = 0\,. \tag{97}$$

Multiplying by y_1^m, we obtain

$$1 + \sum_{\ell=0}^{m-1} p_\ell(y_1, \dots, y_k) y_1^{m-\ell} = 0\,. \tag{98}$$

Hence we see that $q(y_1, \dots, y_k) = 0$, where $q \in K[X_1, \dots, X_k]$ is given by

$$q(X_1, \dots, X_k) = 1 + \sum_{\ell=0}^{m-1} p_\ell(X_1, \dots, X_k) X_1^{m-\ell}\,. \tag{99}$$

By algebraic independence of $\{y_1, \dots, y_k\}$ this means that $q = 0$. However, from Expression (99) we clearly see that $q(0, X_2, \dots, X_k) = 1$. This contradiction shows that indeed $k = 0$, which completes the proof. □

Proof of Hilbert's Nullstellensatz. By Lemma 1.27 we have $J \subseteq I(V(J))$. Taking the radical of both ideals, we get $\sqrt{J} \subseteq \sqrt{I(V(J))} = I(V(J))$ by lemmas 1.15 and 1.25.

For the reverse inclusion, let $f \in I(V(J))$ be given and suppose that $f \notin \sqrt{J}$. This implies in particular that $J \neq K[X_1, \dots, X_n]$. From Proposition 1.24 we know that $\sqrt{J}$ is equal to the intersection of all prime ideals containing J. Hence, there exists at least one prime ideal P containing J such that $f \notin P$. We fix such an ideal P and use it to construct a ring that will play an important role throughout the proof. First, consider the domain

$$D = K[X_1, \dots, X_n]/P\,. \tag{100}$$

We denote by $\bar{f}$ the class of f in D, so that $\bar{f} \neq 0$ by assumption. As D is a domain, we see that 0 is not contained in the set

$$C = \{1, \bar{f}, \bar{f}^2, \dots\}\,. \tag{101}$$

Hence, C is multiplicative and we may form the localization D_C. Note that there is an inclusion ι of D into D_C given by $x \mapsto \frac{x}{1}$. Finally, we pick a maximal ideal $\mathcal{M}$ of D_C and form the quotient field

$$L = D_C/\mathcal{M}\,. \tag{102}$$

We thus have the following rings with morphisms among them:

$$K[X_1, \dots, X_n] \xrightarrow{\pi_P} D \xrightarrow{\iota} D_C \xrightarrow{\pi_\mathcal{M}} L\,, \tag{103}$$

where π_P is the projection along P and $\pi_\mathcal{M}$ is the projection along $\mathcal{M}$.

We will write $\bar{g} := \pi_P(g) \in D$ for the image of an element $g \in K[X_1, \dots, X_n]$ and $\left[\frac{d}{c}\right] := \pi_\mathcal{M}\left(\frac{d}{c}\right) \in L$ for the image of an element $\frac{d}{c} \in D_C$. Next, we collect

some properties of L.
First of all, we have an inclusion of K into L given by

$$r \mapsto \left[\frac{\bar{r}}{\bar{1}}\right] \qquad \text{for } r \in K\,. \tag{104}$$

This map is indeed injective, as $\left[\frac{\bar{r}}{\bar{1}}\right] = 0$ implies that $\frac{\bar{r}}{\bar{1}} \in \mathcal{M}$. This is only possible for $r = 0$, as otherwise $\frac{\bar{r}}{\bar{1}}$ is a unit with inverse $\frac{\overline{r-1}}{\bar{1}}$, contradicting that $\mathcal{M}$ is maximal.
Secondly, we claim that L is a finitely generated algebra over K. To see why, note that any element in L may be written as $\left[\frac{\bar{p}}{\bar{f}^s}\right]$ for some $p \in K[X_1, \ldots, X_n]$ and a non-negative integer s. Now, we may write

$$p(X_1, \ldots, X_n) = \sum_{J \in \mathcal{J}} a_J X_1^{J_1} \ldots X_n^{J_n}\,, \tag{105}$$

where $\mathcal{J}$ is some finite set of multi-indices $J = (J_1, \ldots, J_n) \in (\mathbb{Z}_{\geq 0})^n$ and with $a_J \in K$. It follows that

$$\begin{aligned}\left[\frac{\bar{p}}{\bar{f}^s}\right] &= \left[\frac{\sum_{J \in \mathcal{J}} \bar{a}_J \overline{X}_1^{J_1} \ldots \overline{X}_n^{J_n}}{1}\right] \left[\frac{1}{\bar{f}^s}\right] \\ &= \sum_{J \in \mathcal{J}} \left[\frac{\bar{a}_J}{\bar{1}}\right] \left[\frac{\overline{X}_1}{\bar{1}}\right]^{J_1} \cdots \left[\frac{\overline{X}_n}{\bar{1}}\right]^{J_n} \left[\frac{\bar{1}}{\bar{f}}\right]^{s}\,.\end{aligned} \tag{106}$$

Hence, if we set $x_i := \left[\frac{\overline{X}_i}{\bar{1}}\right]$ for $i \in \{1, \ldots, n\}$ and $y := \left[\frac{\bar{1}}{\bar{f}}\right]$, then Equation (106) reads

$$\left[\frac{\bar{p}}{\bar{f}^s}\right] = q(x_1, \ldots, x_n, y)\,, \tag{107}$$

with $q \in K[X_1, \ldots, X_{n+1}]$ given by

$$q(X_1, \ldots, X_{n+1}) = p(X_1, \ldots, X_n) X_{n+1}^s \tag{108}$$

and where we identify K with its image in L under the inclusion (104). This shows that L is generated as an algebra over K by the elements x_1 to x_n and y. In particular, L is indeed a finitely generated algebra over K.
Next, it follows from Zariski's lemma (Theorem 2.47) that L is in fact a finitely generated module over K. Lemma 2.44 moreover tells us that each element of L is integral over K.
Finally, as K is assumed algebraically closed, it follows from Lemma 2.15 that the only elements of L that are integral over K are those contained in K. We conclude that L has to be equal to K. In other words, the map (104) is surjective, and therefore a bijection. We will denote its inverse by $\psi\colon L \to K$.

We conclude that we may extend the series of maps in Expression (103) to

$$K[X_1, \ldots, X_n] \xrightarrow{\pi_P} D \xrightarrow{\iota} D_C \xrightarrow{\pi_{\mathcal{M}}} L \xrightarrow{\psi} K\,. \tag{109}$$

We will denote the resulting map by $\theta := \psi \circ \pi_{\mathcal{M}} \circ \iota \circ \pi_P \colon K[X_1, \ldots, X_n] \to K$. Note that by construction, θ is the identity on the constant polynomials. Hence, we may describe θ fully by specifying $\theta(X_i) =: c_i \in K$, for all $i \in \{1, \ldots, n\}$. After that, the map θ is simply given by evaluation at the point $c = (c_1, \ldots, c_n) \in K^n$. That is, we have

$$\theta(p) = p(c_1, \ldots, c_n) \quad \text{ for all } p \in K[X_1, \ldots, X_n]\,. \tag{110}$$

We claim that θ vanishes on all elements in the ideal P. Indeed, we have $\theta = \psi \circ \pi_{\mathcal{M}} \circ \iota \circ \pi_P$ and $\pi_P(p) = 0$ for all $p \in P$, by definition of the latter map. We therefore have $p(c_1, \ldots, c_n) = 0$ for all $p \in P$ and, because $J \subseteq P$, we also find $p(c_1, \ldots, c_n) = 0$ for all $p \in J$. In other words, we conclude that $c \in V(J)$. As $f \in I(V(J))$ by assumption, we also have $f(c_1, \ldots, c_n) = 0$ and so $\theta(f) = 0$. However, as ψ is a bijection, this implies that

$$\pi_{\mathcal{M}} \circ \iota \circ \pi_P(f) = \left[\frac{\bar{f}}{1}\right] = 0\,. \tag{111}$$

Hence, we have $\frac{\bar{f}}{1} \in \mathcal{M}$. This is a contradiction, as $\frac{\bar{f}}{1}$ is a unit in D_C with inverse $\frac{1}{\bar{f}}$, and because $\mathcal{M}$ was assumed maximal. We arrived at this contradiction by assuming that $f \notin \sqrt{J}$. Hence, we see that $I(V(J)) \subseteq \sqrt{J}$ and so $I(V(J)) = \sqrt{J}$, which completes the proof. □

2.7 Consequences of Hilbert's Nullstellensatz

Now that we have developed quite some algebraic machinery, we can return to the setting of algebraic sets and see what the consequences are of these previous results. Throughout this subsection we will often use Hilbert's Nullstellensatz (Theorem 2.46). Recall that this theorem gives us a one-to-one correspondence between algebraic sets and radical ideals when the field K is algebraically closed. We begin by exploring some straightforward instances of this correspondence. The first of these in fact do not require K to be algebraically closed.

Lemma 2.48. *Let K be a field and n a natural number. We have*

1. *$V(K[X_1, \ldots, X_n]) = \emptyset$ and $I(\emptyset) = K[X_1, \ldots, X_n]$;*
2. *$V(0) = K^n$.*

Proof. The set $V(K[X_1, \ldots, X_n])$ consists of all points in K^n on which all polynomials vanish. As $K[X_1, \ldots, X_n]$ includes the polynomial that is constant equal to 1, we see that this set is necessarily empty.
Next, the ideal $I(\emptyset)$ consists of all polynomials without restrictions (they are required to vanish on the empty set). Hence, we indeed have $I(\emptyset) = K[X_1, \ldots, X_n]$.
Finally, we have $V(0) = K^n$ as the zero polynomial vanishes everywhere. □

Remark 2.49. It is not hard to see that 0 and $K[X_1, \ldots, X_n]$ are both radical ideals of $K[X_1, \ldots, X_n]$. For the former this can be seen using the fact that for any element x in a domain we have $x = 0$ if and only if $x^m = 0$ for some $m \in \mathbb{N}$. For the latter it follows because $I \subseteq \sqrt{I}$ for any ideal I, and so $K[X_1, \ldots, X_n] \subseteq \sqrt{K[X_1, \ldots, X_n]}$ which implies $\sqrt{K[X_1, \ldots, X_n]} = K[X_1, \ldots, X_n]$. △

Remark 2.50. Note that we do not in general have $I(K^n) = 0$. For instance, if K denotes the field with two elements, $K = \mathbb{Z}/2\mathbb{Z}$, and if we choose $n = 1$, then $I(K^n) = I(\mathbb{Z}/2\mathbb{Z})$ contains the polynomial $(X - 0)(X - 1) = X^2 - X = X^2 + X \neq 0$. After all, $(X - 0)(X - 1)$ vanishes on both points of $\mathbb{Z}/2\mathbb{Z}$, 0 and 1. This shows that in this case $I(K^n) \neq 0$.
More generally, let K be a finite field consisting of the elements $\{x_1, \ldots, x_m\}$, and define the polynomial

$$p(X) = (X - x_1)(X - x_2) \ldots (X - x_m) = X^m + \text{ 'lower order terms'}. \quad (112)$$

We see that $p \neq 0$, yet by construction $p \in I(K)$. This shows that for finite fields K we always have $I(K) \neq 0$. △

If we restrict to algebraically closed fields, then we get the missing case of Lemma 2.48:

Lemma 2.51. *For K an algebraically closed field and n a natural number we have $I(K^n) = 0$.*

Proof. From Lemma 2.48 we know that $V(0) = K^n$. Using Hilbert's Nullstellensatz (Theorem 2.46) we obtain $I(K^n) = I(V(0)) = \sqrt{0} = 0$. □

Remark 2.52. Remark 2.50 and Lemma 2.51 tell us that, apparently, finite fields are never algebraically closed. In other words, algebraically closed fields always have infinitely many elements. △

A very surprising consequence of Hilbert's Nullstellensatz is the following result, sometimes referred to as the *weak Nullstellensatz*:

Lemma 2.53. *Let K be an algebraically closed field and n a natural number. Given a proper ideal $J \subsetneq K[X_1, \ldots X_n]$, there always exists a point $c \in K^n$ that is a common zero of all polynomials in J.*
In fact, given any set of polynomials $\Lambda \subseteq K[X_1, \ldots X_n]$, there exists a common zero of all polynomials in Λ if and only if the ideal I_Λ generated by Λ is not the full ring $K[X_1, \ldots X_n]$.

Proof. Assume the ideal J is not the whole ring $K[X_1, \ldots X_n]$. If $V(J) = \emptyset$, then by Hilbert's Nullstellensatz we find $\sqrt{J} = I(V(J)) = I(\emptyset) = K[X_1, \ldots, X_n]$, where the last step uses Lemma 2.48. It follows in particular that $1 \in \sqrt{J}$, so that $1 = 1^m \in J$ for some $m \in \mathbb{N}$. This contradicts that J is proper, and we conclude that $V(J)$ contains at least one point.
Given a set $\Lambda \subseteq K[X_1, \ldots X_n]$, we have $V(\Lambda) = V(I_\Lambda)$ by Lemma 1.2. By the first part of this lemma and Lemma 2.48, we have $V(I_\Lambda) = \emptyset$ if and only if $I_\Lambda = K[X_1, \ldots X_n]$. This completes the proof. □

Remark 2.54. Lemma 2.53 really requires the field K to be algebraically closed. For instance, when $K = \mathbb{R}$ and $n = 1$ we can take J to be the ideal generated by $X^2 + 1$. Clearly $J \neq K[X]$, but nevertheless $V(J) = V(\{X^2 + 1\}) = \emptyset$. $\triangle$

The next obvious candidates to explore regarding Hilbert's Nullstellensatz are the maximal ideals. Recall that maximal ideals are prime, whereas we know from Lemma 1.19 that prime ideals are radical. To investigate maximal ideals, we first recap some results on the functions V and I that relate radical ideals of $K[X_1, \ldots, X_n]$ to algebraic sets of K^n.

From lemmas 1.6 and 1.26 we see that V and I are order-reversing. That is,

$$J_1 \subseteq J_2 \implies V(J_2) \subseteq V(J_1) \text{ and} \tag{113}$$

$$W_1 \subseteq W_2 \implies I(W_2) \subseteq I(W_1)\,, \tag{114}$$

for radical ideals J_1, J_2 and algebraic sets W_1, W_2. From Proposition 1.11 we see that

$$V\left(I_1 \cap I_2 \cap \cdots \cap I_k\right) = V(I_1) \cup V(I_2) \cup \cdots \cup V(I_k) \tag{115}$$

for ideals $I_1, \ldots, I_k$. Moreover, from Lemma 1.18 we see that if I_1 to I_k are radical, then

$$\sqrt{I_1 \cap I_2 \cap \cdots \cap I_k} = \sqrt{I_1} \cap \sqrt{I_2} \cdots \cap \sqrt{I_k} = I_1 \cap I_2 \cap \cdots \cap I_k\,, \tag{116}$$

so that $I_1 \cap I_2 \cap \cdots \cap I_k$ is radical too. From Lemma 1.29 we see that conversely

$$I(W_1 \cup W_2 \cup \cdots \cup W_k) = I(W_1) \cap I(W_2) \cap \cdots \cap I(W_k) \tag{117}$$

for algebraic sets $W_1, \ldots, W_k$.

To investigate maximal ideals, we will write $\mathcal{M}_c \subseteq K[X_1, \ldots, X_n]$ with $c = (c_1, \ldots, c_n) \in K^n$ for the ideal generated by the elements $X_1 - c_1, \ldots, X_n - c_n$. The reason for introducing these is the following:

Proposition 2.55. *Let K be algebraically closed. The ideals $\mathcal{M}_c$ are precisely all maximal ideals of $K[X_1, \ldots, X_n]$ and we have $V(\mathcal{M}_c) = \{c\}$.*

Proof. We begin by showing that $V(\mathcal{M}_c) = \{c\}$. As $\mathcal{M}_c$ is generated by $X_1 - c_1, \ldots, X_n - c_n$, it follows from Lemma 1.2 that $V(\mathcal{M}_c)$ consists of all points on which each polynomial $X_i - c_i$ vanishes. Of course the condition $X_i - c_i = 0$ is equivalent to $X_i = c_i$, and so we indeed find $V(\mathcal{M}_c) = \{c\}$. It follows in particular that $1 \notin \mathcal{M}_c$, so that each $\mathcal{M}_c$ is a proper ideal.

To show that $\mathcal{M}_c$ is maximal, we consider the ring $K[X_1, \ldots, X_n]/\mathcal{M}_c$. Given a polynomial $p \in K[X_1, \ldots, X_n]$, we denote by $\bar{p}$ its class in this quotient ring. Consider the ring-homomorphism ι from K to $K[X_1, \ldots, X_n]/\mathcal{M}_c$, given by $\iota(c) = \bar{c}$. Here $c \in K$ is seen as a constant polynomial in $K[X_1, \ldots, X_n]$. As $\mathcal{M}_c$ is a proper ideal, it follows that ι is injective. Moreover, for all $i \in$

$\{1, \ldots, n\}$ we have $\overline{X_i} = \overline{(X_i - c_i) + c_i} = \overline{c_i}$. We see that for any polynomial $p \in K[X_1, \ldots, X_n]$ it holds that

$$\overline{p(X_1, \ldots, X_n)} = p(\overline{X_1}, \ldots, \overline{X_n}) = p(\overline{c_1}, \ldots, \overline{c_n}) = \overline{p(c)}\,. \tag{118}$$

This shows that the map ι is in fact surjective, and therefore an isomorphism. As a result $K[X_1, \ldots, X_n]/\mathcal{M}_c$ is a field, and we conclude that $\mathcal{M}_c$ is indeed maximal. Note that we therefore have $\sqrt{\mathcal{M}_c} = \mathcal{M}_c$, so that $\mathcal{M}_c = \sqrt{\mathcal{M}_c} = I(V(\mathcal{M}_c)) = I(\{c\})$.

It remains to show that every maximal ideal is of the form $\mathcal{M}_c$ for some $c \in K^n$. To this end, let $\mathcal{M}$ be a given maximal ideal. From Lemma 2.53 we conclude that there is at least one point contained in $V(\mathcal{M})$. We pick such a point c, so that $\{c\} \subseteq V(\mathcal{M})$. Applying I to both sides of this equation, and using the order-reversing properties of this map, we obtain

$$\mathcal{M} = I(V(\mathcal{M})) \subseteq I(\{c\}) = \mathcal{M}_c\,. \tag{119}$$

As $\mathcal{M}$ and $\mathcal{M}_c$ are both maximal, we conclude that $\mathcal{M} = \mathcal{M}_c$. □

Next, we want to explore the correspondence given by Hilbert's Nullstellensatz when it comes to prime ideals. To this end, we define:

Definition 2.56. An algebraic set $W \subseteq K^n$ is called *irreducible* if $W \neq \emptyset$ and if in addition the following holds: if we can write $W = U_1 \cup U_2$ for some algebraic sets $U_1, U_2 \subseteq K^n$, then either $W = U_1$ or $W = U_2$. △

Note that if $W = U_1 \cup U_2$ and $W = U_1$, then since $U_2 \subseteq U_1 \cup U_2$ we have $U_2 \subseteq U_1$. The reverse inclusion of course holds when $W = U_2$ instead. The following useful result gives a somewhat easier characterization of irreducible algebraic sets.

Lemma 2.57. *Let $W \subseteq K^n$ be a non-empty algebraic set. The set W is irreducible if and only if it satisfies the following: if we can write $W \subseteq U_1 \cup U_2$ for some algebraic sets $U_1, U_2 \subseteq K^n$, then either $W \subseteq U_1$ or $W \subseteq U_2$.*

Proof. Suppose W has the property that $W \subseteq U_1 \cup U_2$ for algebraic sets U_1 and U_2 implies $W \subseteq U_1$ or $W \subseteq U_2$. If in particular we have $W = U_1 \cup U_2$, then without loss of generality $W \subseteq U_1$. It follows that $W \subseteq U_1 \subseteq U_1 \cup U_2 = W$, so that $W = U_1$. This shows that W is irreducible.

Conversely, suppose W is irreducible and assume we have $W \subseteq U_1 \cup U_2$ for some algebraic sets U_1 and U_2. It follows that $W \subseteq W \cap (U_1 \cup U_2) = (W \cap U_1) \cup (W \cap U_2) \subseteq W$, so that $W = (W \cap U_1) \cup (W \cap U_2)$. Recall that $W \cap U_1$ and $W \cap U_2$ are both again algebraic sets, so that without loss of generality we have $W = W \cap U_1 \subseteq U_1$. This completes the proof. □

The reason for introducing irreducible algebraic sets is of course:

Proposition 2.58. *Let K be an algebraically closed field. Given a prime ideal $P \subseteq K[X_1, \ldots, X_n]$, the corresponding algebraic set $V(P)$ is irreducible. Conversely, if an algebraic set $W \subseteq K^n$ is irreducible then $I(W)$ is a prime ideal.*

To prove Proposition 2.58 we need the following lemma.

Lemma 2.59. *Let P be a prime ideal in some ring R. If we may write $P = I \cap J$ for some ideals I and J, then $P = I$ or $P = J$.*

Proof. Clearly $P \subseteq I$ and $P \subseteq J$. Hence, if the result of the lemma does not hold then we may pick elements $x \in I \setminus P$ and $y \in J \setminus P$. It follows that $xy \in I \cap J = P$. However, as P is prime this implies $x \in P$ or $y \in P$. From this contradiction we see that indeed $P = I$ or $P = J$. □

Proof of Proposition 2.58. Let P be a prime ideal and suppose we may write $V(P) = U_1 \cup U_2$. Using Hilbert's Nullstellensatz we get $P = I(V(P)) = I(U_1 \cup U_2) = I(U_1) \cap I(U_2)$. Lemma 2.59 now tells us that (without loss of generality) we have $P = I(U_1)$. It follows that $V(P) = V(I(U_1)) = U_1$, so that $V(P)$ is indeed irreducible. Note that $V(P) \neq \emptyset$ as $P \neq K[X_1, \ldots, X_n]$.

Now suppose W is an irreducible algebraic set. As W is non-empty, we see that $I(W)$ is a proper ideal of $K[X_1, \ldots, X_n]$. Let $p, q \in K[X_1, \ldots, X_n]$ be elements such that $pq \in I(W)$. From $\{pq\} \subseteq I(W)$ we get $W = V(I(W)) \subseteq V(\{pq\})$ by Lemma 1.6. Now, if a point $c \in K^n$ is a zero of the polynomial pq, then it is in the zero-set of either p or q. Hence we have $W \subseteq V(\{pq\}) \subseteq V(\{p\}) \cup V(\{q\})$. By Lemma 2.57 we may assume without loss of generality that $W \subseteq V(\{p\}) = V(I_p)$, with I_p the ideal generated by p. We therefore get $\sqrt{I_p} = I(V(I_p)) \subseteq I(W)$. As $p \in I_p \subseteq \sqrt{I_p}$ we see that $p \in I(W)$, showing that $I(W)$ is indeed prime. □

Irreducible sets are furthermore important as they serve as the indivisible "atoms" of algebraic sets, as the following results make clear.

Theorem 2.60. *Let $W \subseteq K^n$ be a non-empty algebraic set, with K algebraically closed. There exist finitely many irreducible algebraic sets $U_1, \ldots, U_k \subseteq K^n$ such that*

$$W = U_1 \cup \cdots \cup U_k \,. \tag{120}$$

Proof. If W is itself irreducible, then we are done; we may simply write

$$W = U_1 \,.$$

In case W is not irreducible we may write

$$W = W_0 \cup W_1 \;\text{ with }\; W \neq W_0, W_1 \,.$$

Note that we therefore have $W_0, W_1 \subsetneq W$ and $W_0, W_1 \neq \emptyset$. If both W_0 and W_1 are irreducible then again we are done. Otherwise, we decompose further. If W_0 is not irreducible we write

$$W_0 = W_{00} \cup W_{01} \;\text{ with }\; W_{00}, W_{01} \subsetneq W_0 \,.$$

If W_1 is not irreducible we write

$$W_1 = W_{10} \cup W_{11} \text{ with } W_{10}, W_{11} \subsetneq W_1 .$$

This yields either two new algebraic sets (either W_{00} and W_{01}, or W_{10} and W_{11}) or four new ones (W_{00}, W_{01}, W_{10} and W_{11}). If each of these are irreducible then we are done, if some are not then we proceed as before. For instance,

$$W_{11} = W_{110} \cup W_{111} \text{ with } W_{110}, W_{111} \subsetneq W_{11} ,$$

and in general

$$W_s = W_{s0} \cup W_{s1} \text{ with } W_{s0}, W_{s1} \subsetneq W_s ,$$

for s a finite sequence of 0's and 1's, and where $s0$ ($s1$) is the sequence obtained by placing a 0 (a 1) to the right of s. This process ends when for some $k \in \mathbb{N}$, for all sequences s of length k that we have constructed the set W_s is irreducible. In that case we find the required decomposition of W into the algebraic sets W_t, for t any sequence for which W_t is defined and irreducible.

We now show that this process indeed has to terminate, by supposing otherwise and arriving at a contradiction. So, Suppose that the aforementioned process does not terminate. In that case we find algebraic sets W_s for sequences s of arbitrary length. We denote by $\mathcal{S}$ the set of all sequences we construct in this way. Note that for any sequence s we have $s0 \in \mathcal{S} \implies s, s1 \in \mathcal{S}$ and likewise $s1 \in \mathcal{S} \implies s, s0 \in \mathcal{S}$. Now, given $s \in \mathcal{S}$ we define

$$T(s) = \sup\{m \in \mathbb{N} \mid si_1i_2 \dots i_m \in \mathcal{S} \text{ for some } i_1, i_2, \dots, i_m \in \{0,1\}\} , \quad (121)$$

where similar to before the sequence $si_1i_2 \dots i_m$ is obtained from s by first placing $i_1 \in \{0,1\}$ to the right of it, then i_2, etc. Now, either $T(0) = \infty$ or $T(1) = \infty$, for if $T(0), T(1) \leq m$ for some $m \in \mathbb{N}$, then $T(s) \leq m$ for any sequence $s \in \mathcal{S}$. Let $j_1 \in \{0,1\}$ be such that $T(j_1) = \infty$. It follows that $j_10, j_11 \in \mathcal{S}$. Moreover, if $T(j_10), T(j_11) \leq m$ for some $m \in \mathbb{N}$, then $T(j_1) \leq m+1$ which is a contradiction. Hence $T(j_1j_2) = \infty$ for some $j_2 \in \{0,1\}$. We proceed to built a sequence like this. If $j_1 \dots j_k \in \mathcal{S}$ satisfies $T(j_1 \dots j_k) = \infty$, then $j_1 \dots j_k0, j_1 \dots j_k1 \in \mathcal{S}$. Moreover, if $T(j_1 \dots j_k0), T(j_1 \dots j_k1) \leq m$ for some $m \in \mathbb{N}$, then we arrive at the contradiction $T(j_1 \dots j_k) \leq m+1$. Hence, we get $j_1 \dots j_kj_{k+1} \in \mathcal{S}$ satisfying $T(j_1 \dots j_kj_{k+1}) = \infty$ for some $j_{k+1} \in \{0,1\}$, and so forth.
This gives us an infinite chain of algebraic sets

$$W_{j_1} \supsetneq W_{j_1j_2} \supsetneq \dots . \quad (122)$$

Applying I to these gives us the chain of radical ideals

$$I(W_{j_1}) \subsetneq I(W_{j_1j_2}) \subsetneq \dots \subseteq K[X_1, \dots, X_n] . \quad (123)$$

However, this directly contradicts the fact that $K[X_1, \dots, X_n]$ is Noetherian. We see that the aforementioned process has to terminate, giving the required decomposition. □

Note that from Expression (120) we may always obtain a decomposition with the property that none of the U_i are contained in any other, i.e. $U_i \subseteq U_j \implies i = j$ (which in particular excludes doubles among the U_i). This can be done by simply discarding algebraic sets that are contained in others. For these decompositions we in fact have uniqueness, as the following result shows.

Theorem 2.61. *Suppose $U_1, \dots, U_k, V_1, \dots, V_l \subseteq K^n$ are irreducible algebraic sets such that*

$$U_1 \cup \cdots \cup U_k = V_1 \cup \cdots \cup V_l \,, \tag{124}$$

and suppose in addition that $U_i \subseteq U_j \implies i = j$ and $V_i \subseteq V_j \implies i = j$. Then, $k = l$ and after reordering we have $U_i = V_i$ for all $i \in \{1, \dots, k\}$.

Proof. Assume without loss of generality that $k \geq l$. Given $i \in \{1, \dots, k\}$ we see from Equation (124) that

$$U_i \subseteq V_1 \cup \cdots \cup V_l \,. \tag{125}$$

As U_i is irreducible, we may use Lemma 2.57 to conclude that either $U_i \subseteq V_1$ or $U_i \subseteq V_2 \cup \cdots \cup V_l$. Using this argument repeatedly gives us

$$U_i \subseteq V_{\sigma(i)} \tag{126}$$

for some $\sigma(i) \in \{1, \dots, l\}$. If we then use the exact same argument on $V_{\sigma(i)}$ we obtain

$$V_{\sigma(i)} \subseteq U_j \tag{127}$$

for some $j \in \{1, \dots, k\}$. However, equations (126) and (127) together give $U_i \subseteq V_{\sigma(i)} \subseteq U_j$, which by assumption means $i = j$. As a consequence, we find $U_i = V_{\sigma(i)}$. To summarize, we have found a function $\sigma \colon \{1, \dots, k\} \to \{1, \dots, l\}$ satisfying $U_i = V_{\sigma(i)}$ and we furthermore assumed $k \geq l$. Hence, the proof is done if we can show that σ is injective. However, if $\sigma(i) = \sigma(j)$ for some $i, j \in \{1, \dots, k\}$ then $U_i = V_{\sigma(i)} = V_{\sigma(j)} = U_j$, from which it follows that $i = j$ due to the fact that our decompositions do not contain doubles. This completes the proof. □

We conclude this subsection by using the correspondence between algebraic sets and radical ideals in a different direction from what we have mostly done so far.

Corollary 2.62. *Let K be an algebraically closed field and $J \subsetneq K[X_1, \dots, X_n]$ a proper radical ideal. There exists a unique decomposition*

$$J = P_1 \cap \cdots \cap P_k \,, \tag{128}$$

with $P_1, \dots, P_k$ prime ideals satisfying $P_i \subseteq P_j \implies i = j$.

Proof. As J is proper, we see that the algebraic set $V(J)$ is not empty. By Theorem 2.60 we may write

$$V(J) = U_1 \cup \cdots \cup U_k \tag{129}$$

for certain irreducible algebraic sets $U_1, \ldots, U_k$. We may furthermore assume there are no inclusions between the different U_i. Applying I gives

$$J = I(V(J)) = I(U_1) \cap \cdots \cap I(U_k)\,, \tag{130}$$

where by Proposition 2.58 each $I(U_i)$ is prime. If we have $I(U_i) \subseteq I(U_j)$ for some $i, j \in \{1, \ldots, k\}$, then $U_i = V(I(U_i)) \supseteq V(I(U_j)) = U_j$ and hence $i = j$. We thus find the required decomposition by setting $P_i = I(U_i)$.
As for uniqueness, suppose

$$J = Q_1 \cap \cdots \cap Q_l\,, \tag{131}$$

for some prime ideals $Q_1, \ldots, Q_l$, with no inclusions among them. Applying V we obtain the decomposition into irreducible algebraic sets

$$V(J) = V(Q_1) \cup \cdots \cup V(Q_l)\,, \tag{132}$$

again with no inclusions, as can be seen by applying I and using the order-reversing properties of this map. By Theorem 2.61 we see that $k = l$ and $V(Q_i) = U_i$ for all $i \in \{1, \ldots, k\}$, after reordering. Hence, we get $Q_i = I(V(Q_i)) = I(U_i)$ for all i, which proves uniqueness. □

3 The dimension theorem

3.1 Local rings

We next want to prove the so-called dimension theorem. It will allow us to associate to a finitely generated module over a ring a number –that naturally plays the role of a dimension– in multiple equivalent ways. The ring in question will have to be Noetherian and *local*, a property we define and investigate in this subsection. In the next we motivate local rings from a geometric point of view.

Definition 3.1. A commutative ring with 1 is called *local* if it has precisely one maximum ideal. △

As the name suggests, local rings show up naturally when localizing, see Lemma 3.2 below. Recall that for a prime ideal P in a ring R, we have that the complement P^c contains 1 but not 0. Moreover, if we are given $x, y \in P^c$ then likewise $xy \in P^c$, as $xy \in P$ would imply either $x \in P$ or $y \in P$ by definition of a prime ideal. Hence, localization by the complement of a prime ideal always makes sense.

Lemma 3.2. *Let P be a prime ideal in a ring R and denote by $C = P^c$ its complement. The corresponding localization R_C is a local ring with unique maximal ideal given by*

$$P_C = \left\{ \frac{x}{d} \;\middle|\; x \in P, d \in P^c = C \right\}. \tag{133}$$

Proof. We know from Subsection 1.4 that P_C is indeed an ideal. If $1 \in P_C$ then

$$\frac{1}{1} = \frac{x}{c} \quad \text{for some } x \in P,\, c \in P^c \tag{134}$$

and so $dx = dc$ for some $d \in P^c$. As $x \in P$, we see that $dx = dc \in P$. Hence, either $d \in P$ or $c \in P$. Both are contradictions, and we see that instead $1 \notin P_C$. In other words, P_C is a proper ideal of R_C.
Note that the proof is therefore done if we can show for any proper ideal $I \subsetneq R_C$ that $I \subseteq P_C$. This establishes both that P_C is maximal, as any ideal J satisfying $P_C \subseteq J \subseteq R_C$ either satisfies $J = R_C$ or $J = P_C$, and that P_C is the only maximal ideal, as any maximal ideal $\mathcal{M}$ has to satisfy $\mathcal{M} \subseteq P_C \subsetneq R_C$ and so $\mathcal{M} = P_C$. However, any element in a proper ideal I is of the form $\frac{x}{c}$ with $x \in P$ and $c \in C$, as otherwise it would have the inverse $\frac{c}{x}$ and so I wouldn't be proper. Hence, we necessarily have $I \subseteq P_C$, which completes the proof. □

A useful property of local rings is the following:

Lemma 3.3. *The unique maximal ideal of a local ring consists of precisely all non-invertible elements.*

Proof. Let R be a local ring with unique maximal ideal $\mathcal{M}$. As $\mathcal{M}$ is proper, we see that it is contained in the set of all non-invertible elements. Conversely,

suppose $x \in R$ is non-invertible and consider the ideal Rx consisting of all elements of the form rx with $r \in R$. This is a proper ideal, and so it is contained in a maximal ideal. As $\mathcal{M}$ is the only maximal ideal around, we necessarily have $x \in Rx \subseteq \mathcal{M}$. Hence, $\mathcal{M}$ contains all non-invertible elements, which completes the proof. □

To further motivate the name local ring, we next show that any such ring may be obtained by localizing some ring by the complement of a prime ideal.

Lemma 3.4. *Let R be a local ring with unique maximal ideal $\mathcal{M}$ and write $C = \mathcal{M}^c$ for its complement. The rings R and R_C are isomorphic.*

Proof. Define the map $\psi : R \to R_C$ by

$$\psi(x) = \frac{x}{1}\,. \tag{135}$$

It is easy to see that ψ is a ring-homomorphism, and we claim it is in fact an isomorphism. To show injectivity, suppose $\psi(x) = \psi(y)$ for some $x, y \in R$. It follows that $cx = cy$ for some $c \in C$. However, by Lemma 3.3 we know that C consists of precisely all invertible elements in R. Hence we obtain $x = y$, from which it follows that ψ is indeed injective.
For surjectivity, let $\frac{x}{c} \in R_C$ be given. As $c \in C$ is invertible, we see that

$$\frac{x}{c} = \frac{cc^{-1}x}{c} = \frac{c}{c}\frac{c^{-1}x}{1} = \frac{c^{-1}x}{1} = \psi(c^{-1}x)\,, \tag{136}$$

so that $\frac{x}{c}$ is reached by ψ. Hence this map is bijective, which proves the claim of the lemma. □

3.2 Local rings motivated

We next show how local rings appear when dealing with algebraic sets. Let K be a field and $J \subsetneq K[X_1, \ldots, X_n]$ a proper ideal of its polynomial ring in n variables. Assume that the corresponding algebraic set $V(J) \subseteq K^n$ is non-empty. We may define a function from $V(J)$ to K by simply restricting any polynomial $f \in K[X_1, \ldots, X_n]$ to $V(J)$. However, this has some redundancy in it, as any map $h \in J$ will vanish on $V(J)$ by definition of this algebraic set. This means we may instead view the elements of the quotient ring $K[X_1, \ldots, X_n]/J$ as functions on $V(J)$, by associating to $[f] \in K[X_1, \ldots, X_n]/J$ the restriction $f|_{V(J)}$ of $f \in K[X_1, \ldots, X_n]$ to $V(J)$. This is well-defined, precisely because for $h \in J$ we have $h|_{V(J)} = 0$ and so $(f+h)|_{V(J)} = f|_{V(J)} + h|_{V(J)} = f|_{V(J)}$ for any polynomial f. The map $[f] \mapsto f|_{V(J)}$ is also a morphism of K-algebras between $K[X_1, \ldots, X_n]/J$ and the algebra of functions on $V(J)$, in the sense that

$$\begin{aligned} (rf)|_{V(J)} &= r(f|_{V(J)}) \\ (f+g)|_{V(J)} &= f|_{V(J)} + g|_{V(J)} \\ (fg)|_{V(J)} &= f|_{V(J)} g|_{V(J)} \end{aligned} \tag{137}$$

for all $f, g \in K[X_1, \ldots, X_n]$ and $r \in K$.
Let us assume from here on out that K is algebraically closed and J is radical. If $f \in K[X_1, \ldots, X_n]$ satisfies $f|_{V(J)} = 0$, then $f \in I(V(J)) = \sqrt{J} = J$. Hence, in this case the map $[f] \mapsto f|_{V(J)}$ is injective, meaning that the elements of $K[X_1, \ldots, X_n]/J$ may be viewed as (distinct) functions on $V(J)$.

We will continue this idea of associating some ring of functions on $V(J)$ (or rather, objects very similar to functions) to an algebraic construction involving J. To this end, we pick a prime ideal $P \subseteq K[X_1, \ldots, X_n]$ such that $J \subseteq P$. It follows in particular that $V(P) \subseteq V(J)$. Let us denote by $[P]$ the corresponding ideal in $K[X_1, \ldots, X_n]/J$. In other words,

$$[P] = \pi_J(P) = \{[f] \mid f \in P\} \subseteq K[X_1, \ldots, X_n]/J\,, \tag{138}$$

with $\pi_J : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]/J$ the canonical projection. Note that, as $J \subseteq P$, it holds that $[f] \in [P]$ for $f \in K[X_1, \ldots, X_n]$ if and only if $f \in P$. Moreover, there is a well-defined surjective ring-homomorphism

$$\kappa : K[X_1, \ldots, X_n]/J \to K[X_1, \ldots, X_n]/P \tag{139}$$

which sends the class in $K[X_1, \ldots, X_n]/J$ of an elements in $K[X_1, \ldots, X_n]$ to its class in $K[X_1, \ldots, X_n]/P$. We see that the kernel of κ is given by $[P]$. Hence, by the first isomorphism theorem we get

$$\left(K[X_1, \ldots, X_n]/J\right)/[P] \cong K[X_1, \ldots, X_n]/P\,. \tag{140}$$

As P is prime, $K[X_1, \ldots, X_n]/P$ is a domain, from which it follows that $[P]$ is prime in $K[X_1, \ldots, X_n]/J$ as well. We may therefore localize $K[X_1, \ldots, X_n]/J$ by the complement of $[P]$, which gives us the local ring

$$R_P^J := \left(K[X_1, \ldots, X_n]/J\right)_{[P]^c}\,. \tag{141}$$

We will relate this ring to the rational functions defined "around" the algebraic set $V(P)$, in a way that we will now make clear.

Recall that there is a topology on K^n where the closed sets are precisely all algebraic sets, called the Zariski topology.

Definition 3.5. Given a radical ideal J and a prime ideal P such that $J \subseteq P$, we call a set $A \subseteq V(J)$ a *pseudo-neighborhood* of $V(P)$ in $V(J)$ if it satisfies:

1. A is a Zariski open subset of $V(J)$ with the induced topology. In other words, there exists an algebraic set $W \subseteq K^n$ such that $A = W^c \cap V(J)$;
2. A has non-empty intersection with $V(P)$, i.e. $A \cap V(P) \neq \emptyset$. △

Next, we denote by $\mathcal{S}_P^J$ the set of all pairs (h, A) such that:

1. A is a pseudo-neighborhood of $V(P)$ in $V(J)$;

2. h is a function from A to K;

3. There exist polynomials $f, g \in K[X_1, \ldots, X_n]$ with $g(x) \neq 0$ for all $x \in A$, such that
$$h = \frac{f|_A}{g|_A} \text{ on } A\,. \tag{142}$$

We next put an equivalence relation $\sim$ on $\mathcal{S}_P^J$, by stating that $(h, A) \sim (j, B)$ if and only if there exists a pseudo-neighborhood C of $V(P)$ in $V(J)$, such that

1. $C \subseteq A \cap B$;

2. h and j agree on C. That is, $h|_C = j|_C$.

In order to verify that $\sim$ is indeed an equivalence relation, we first need the following useful lemma. In what follows, we will often write "pseudo-neighborhood of $V(P)$" or simply "pseudo-neighborhood" when we mean "pseudo-neighborhood of $V(P)$ in $V(J)$", and when $V(J)$ and $V(P)$ are clear from context. Recall that we assume throughout this subsection that K is algebraically closed and J is a proper radical ideal.

Lemma 3.6. *The intersection of finitely many pseudo-neighborhoods of $V(P)$ in $V(J)$ is a pseudo-neighborhood of $V(P)$ in $V(J)$.*

Proof. Let $A_i \subseteq V(J)$ for $i \in \{1, \ldots, m\}$ be pseudo-neighborhoods of $V(P)$. It follows that there are algebraic sets W_i such that $A_i = W_i^c \cap V(J)$ for all i. Correspondingly, we have

$$A_1 \cap \cdots \cap A_m = W_1^c \cap \cdots \cap W_m^c \cap V(J) = (W_1 \cup \cdots \cup W_m)^c \cap V(J)\,, \tag{143}$$

so that $A_1 \cap \cdots \cap A_m$ is a Zariski open subset of $V(J)$ as well.
Now suppose $A_1 \cap \cdots \cap A_m \cap V(P) = \emptyset$. As $V(P) \subseteq V(J)$, it follows that

$$\begin{aligned}(W_1 \cup \cdots \cup W_m)^c \cap V(P) &= W_1^c \cap \cdots \cap W_m^c \cap V(P) \\ = W_1^c \cap \cdots \cap W_m^c \cap V(J) \cap V(P) &= A_1 \cap \cdots \cap A_m \cap V(P) = \emptyset\,.\end{aligned} \tag{144}$$

Hence, we find $V(P) \subseteq W_1 \cup \cdots \cup W_m$. By Proposition 2.58 $V(P)$ is irreducible, and so by repeated use of Lemma 2.57 we find $V(P) \subseteq W_i$ for some $i \in \{1, \ldots, m\}$. This implies $V(P) \cap W_i^c = \emptyset$. We therefore find

$$A_i \cap V(P) = (W_i^c \cap V(J)) \cap V(P) = W_i^c \cap V(P) = \emptyset\,, \tag{145}$$

contradicting that A_i is a pseudo-neighborhood of $V(P)$. This contradiction arose from assuming $A_1 \cap \cdots \cap A_m \cap V(P) = \emptyset$. Hence, we see that $A_1 \cap \cdots \cap A_m$ is indeed a pseudo-neighborhood of $V(P)$ as well, which completes the proof. □

Proposition 3.7. *The relation $\sim$ defined on $\mathcal{S}_P^J$ above is an equivalence relation.*

Proof. It is clear that $(h, A) \sim (h, A)$, as A is a pseudo-neighborhood of $V(P)$ satisfying $A \subseteq A \cap A$ and h tautologically agrees with itself on A.
Likewise $(h, A) \sim (j, B)$ clearly implies $(j, B) \sim (h, A)$, by choosing the same pseudo-neighborhood contained in $A \cap B$ on which h and j agree.
Now suppose $(h, A) \sim (j, B)$ and $(j, B) \sim (\ell, C)$. Assume $D \subseteq A \cap B$ is a pseudo-neighborhood of $V(P)$ on which h and j agree, and $E \subseteq B \cap C$ is a pseudo-neighborhood of $V(P)$ on which j and ℓ agree. By Lemma 3.6, $D \cap E$ is a pseudo-neighborhood of $V(P)$, and we have $D \cap E \subseteq A \cap B \cap C \subseteq A \cap C$. Finally, we see that

$$h|_{D\cap E} = j|_{D\cap E} = \ell|_{D\cap E}\,, \tag{146}$$

showing that $(h, A) \sim (\ell, C)$. This proves that $\sim$ is indeed an equivalence relation. □

We denote by $\mathcal{O}_P^J$ the set of equivalence classes of $\mathcal{S}_P^J$ under $\sim$.
Next, we want to put a ring structure on $\mathcal{O}_P^J$. The following easy observation will be very useful, as it allows us to pick convenient representatives of classes in $\mathcal{O}_P^J$.

Lemma 3.8. *Given $(h, A) \in \mathcal{S}_P^J$ and B a pseudo-neighborhood of $V(P)$ in $V(J)$, we have the well-defined element $(h|_{A\cap B}, A \cap B) \in \mathcal{S}_P^J$. Moreover, it holds that $(h, A) \sim (h|_{A\cap B}, A \cap B)$.*

Proof. It follows from Lemma 3.6 that $A \cap B$ is again a pseudo-neighborhood of $V(P)$. Now suppose f and g are polynomials with g nowhere vanishing on A, such that we may write

$$h = \frac{f|_A}{g|_A} \text{ on } A\,. \tag{147}$$

Then clearly

$$h|_{A\cap B} = \frac{f|_{A\cap B}}{g|_{A\cap B}} \text{ on } A \cap B\,, \tag{148}$$

with g nowhere vanishing on $A \cap B$. This shows that $(h|_{A\cap B}, A \cap B)$ is an element of $\mathcal{S}_P^J$ as well.
Of course the functions h and $h|_{A\cap B}$ agree on the pseudo-neighborhood $A \cap B$, and trivially $A \cap B \subseteq A \cap (A \cap B)$, which shows that indeed $(h, A) \sim (h|_{A\cap B}, A \cap B)$. □

Let us denote by $[h, A] \in \mathcal{O}_P^J$ the class of $(h, A) \in \mathcal{S}_P^J$ under $\sim$. We define addition in $\mathcal{O}_P^J$ by setting

$$[h, A] + [j, B] = [(h + j)|_{A\cap B}, A \cap B]\,. \tag{149}$$

To see that this is well-defined, note that $A \cap B$ is a pseudo-neighborhood of $V(P)$ on which $h + j$ is defined. Moreover, we may write

$$h = \frac{f|_A}{g|_A} \text{ on } A \text{ and } j = \frac{\tilde{f}|_B}{\tilde{g}|_B} \text{ on } B \tag{150}$$

for some $f, g, \tilde{f}, \tilde{g} \in K[X_1, \ldots, X_n]$ with g nowhere vanishing on A and $\tilde{g}$ nowhere vanishing on B. It follows that

$$(h+j)|_{A\cap B} = \frac{(f\tilde{g}+\tilde{f}g)|_{A\cap B}}{(g\tilde{g})|_{A\cap B}} \tag{151}$$

with $g\tilde{g}$ nowhere vanishing on $A \cap B$. This shows that $((h+j)|_{A\cap B}, A\cap B)$ is a well-defined element of $\mathcal{S}_P^J$, so that the class $[(h+j)|_{A\cap B}, A\cap B] \in \mathcal{O}_P^J$ likewise makes sense.
If we have $[h, A] = [\ell, C]$, then h and ℓ agree on some pseudo-neighborhood $D \subseteq A \cap C$. We have

$$[\ell, C] + [j, B] = [(\ell + j)|_{C\cap B}, C \cap B]\,, \tag{152}$$

and so we have to show that $((h+j)|_{A\cap B}, A\cap B) \sim ((\ell+j)|_{C\cap B}, C\cap B)$. To this end, we consider the pseudo-neighborhood $D\cap B \subseteq A\cap B\cap C$. As h, j and ℓ are all defined on $D\cap B$, and because $h|_D = \ell|_D$, we see that $(h+j)|_{D\cap B} = (\ell+j)|_{D\cap B}$. Hence, we indeed have $[(h+j)|_{A\cap B}, A\cap B] = [(\ell+j)|_{C\cap B}, C\cap B]$. One verifies in exactly the same way that choosing another representative for the class $[j, B]$ likewise does not change the outcome.

We can now make $\mathcal{O}_P^J$ into a group by choosing the zero-element to be $[0|_{V(J)}, V(J)]$. Note that $V(J) = \emptyset^c \cap V(J)$ and

$$0|_{V(J)} = \frac{0|_{V(J)}}{1|_{V(J)}}\,. \tag{153}$$

We moreover see that

$$[0|_{V(J)}, V(J)] + [h, A] = [(0+h)|_{V(J)\cap A}, V(J)\cap A] = [h, A]\,, \tag{154}$$

for all $[h, A] \in \mathcal{O}_P^J$, and likewise $[h, A] + [0|_{V(J)}, V(J)] = [h, A]$. In fact, it is clear from Equation (149) that addition is commutative. The additive inverse of $[h, A]$ is $[-h, A]$, which is well-defined and indeed gives

$$[h, A] + [-h, A] = [(h-h)|_{A\cap A}, A\cap A] = [0|_A, A] = [0|_{V(J)}, V(J)]\,. \tag{155}$$

Here the last step follows from Lemma 3.8.
Associativity follows likewise from applying Lemma 3.8, as we have

$$\begin{aligned}
&\big([h, A] + [j, B]\big) + [\ell, C] \qquad (156)\\
=&\big([h|_{A\cap B\cap C}, A\cap B\cap C] + [j|_{A\cap B\cap C}, A\cap B\cap C]\big) + [\ell|_{A\cap B\cap C}, A\cap B\cap C]\\
=&[(h+j)|_{A\cap B\cap C}, A\cap B\cap C] + [\ell|_{A\cap B\cap C}, A\cap B\cap C]\\
=&[(h+j+\ell)|_{A\cap B\cap C}, A\cap B\cap C]\\
=&[h|_{A\cap B\cap C}, A\cap B\cap C] + [(j+\ell)|_{A\cap B\cap C}, A\cap B\cap C]\\
=&[h|_{A\cap B\cap C}, A\cap B\cap C] + \big([j|_{A\cap B\cap C}, A\cap B\cap C] + [\ell|_{A\cap B\cap C}, A\cap B\cap C]\big)\\
=&[h, A] + \big([j, B] + [\ell, C]\big)\,,
\end{aligned}$$

for all $[h, A], [j, B], [\ell, C] \in \mathcal{O}_P^J$. To finish putting a ring structure on $\mathcal{O}_P^J$, we define multiplication by

$$[h, A][j, B] = [(hj)|_{A\cap B}, A \cap B]\,. \tag{157}$$

Verifying that this is well-defined is almost the same as for addition. For instance, we may write

$$h = \frac{f|_A}{g|_A} \text{ on } A \text{ and } j = \frac{\tilde{f}|_B}{\tilde{g}|_B} \text{ on } B \tag{158}$$

for some $f, g, \tilde{f}, \tilde{g} \in K[X_1, \ldots, X_n]$, with g nowhere vanishing on A and $\tilde{g}$ nowhere vanishing on B. It follows that

$$(hj)|_{A\cap B} = \frac{(f\tilde{f})|_{A\cap B}}{(g\tilde{g})|_{A\cap B}}\,, \tag{159}$$

and as before we note that $g\tilde{g}$ is nowhere vanishing on $A\cap B$. The multiplicative identity is given by $[1|_{V(J)}, V(J)]$, which by Lemma 3.8 is also given by $[1|_A, A]$ for any pseudo-neighborhood A. One easily verifies that $[1|_{V(J)}, V(J)]$ is indeed the multiplicative identity element. Commutativity of multiplication follows immediately from Equation (157), and one verifies the other properties of a commutative ring just as we did for associativity of addition, using Lemma 3.8. For instance,

$$\begin{aligned}
&\big([h, A] + [j, B]\big)[\ell, C] \qquad (160)\\
=&\big([h|_{A\cap B\cap C}, A \cap B \cap C] + [j|_{A\cap B\cap C}, A \cap B \cap C]\big)[\ell|_{A\cap B\cap C}, A \cap B \cap C]\\
=&[(h + j)|_{A\cap B\cap C}, A \cap B \cap C][\ell|_{A\cap B\cap C}, A \cap B \cap C]\\
=&[(h + j)\ell|_{A\cap B\cap C}, A \cap B \cap C]\\
=&[(h\ell + j\ell)|_{A\cap B\cap C}, A \cap B \cap C]\\
=&[(h\ell)|_{A\cap B\cap C}, A \cap B \cap C] + [(j\ell)|_{A\cap B\cap C}, A \cap B \cap C]\\
=&[h|_{A\cap B\cap C}, A \cap B \cap C][\ell|_{A\cap B\cap C}, A \cap B \cap C]\\
+&[j|_{A\cap B\cap C}, A \cap B \cap C][\ell|_{A\cap B\cap C}, A \cap B \cap C]\\
=&[h, A][\ell, C] + [j, B][\ell, C]
\end{aligned}$$

for all $[h, A], [j, B], [\ell, C] \in \mathcal{O}_P^J$, which shows distributivity.

Remark 3.9. If P is maximal, then by Proposition 2.55 we may write $P = \mathcal{M}_p$ for some $p \in K^n$, and we have $V(\mathcal{M}_p) = \{p\}$. In that case the identity $A \cap V(P) \neq \emptyset$ for a set $A \subseteq K^n$ is of course equivalent to $p \in A$. Hence, we see that a pseudo-neighborhood of $V(P)$ is then simply an open neighborhood of the point p in $V(J)$ with the induced Zariski topology. It follows that $\mathcal{O}_{\mathcal{M}_p}^J$ consists of rational functions defined on a neighborhood of p in $V(J)$, identified when they agree on some (smaller) neighborhood of this point. Note that we have $J \subseteq \mathcal{M}_p$ for the radical ideal J if and only if $p \in V(J)$. △

The following theorem ties the two topics discussed in this subsection together. In particular, it shows that each $\mathcal{O}_P^J$ is a local ring.

Theorem 3.10. *Let K be an algebraically closed field with $J \subsetneq K[X_1, \ldots, X_n]$ a proper radical ideal, and suppose P is a prime ideal satisfying $J \subseteq P$. The rings $R_P^J = (K[X_1, \ldots, X_n]/J)_{[P]^c}$ and $\mathcal{O}_P^J$ are isomorphic.*

In order to prove Theorem 3.10 we first need some notation. Given a polynomial $g \in K[X_1, \ldots, X_n]$, we set

$$A_g = (g^{-1}(0))^c \cap V(J)\,, \tag{161}$$

where we suppress the dependency on J in A_g to keep the notation light. Note that A_g is a Zariski open subset of $V(J)$ with the induced topology, as $g^{-1}(0) = V(\{g\})$ is an algebraic set. The following lemma tells us when A_g is a pseudo-neighborhood of $V(P)$.

Lemma 3.11. *The set A_g is a pseudo-neighborhood of $V(P)$ if and only if $g \notin P$. Moreover, A_g depends only on the class of g in $K[X_1, \ldots, X_n]/J$. That is, given $h \in J$ we have $A_g = A_{g+h}$.*

Proof. As $P = \sqrt{P} = I(V(P))$ by Hilbert's Nullstellensatz, we see that $g \in P$ if and only if g vanishes identically on $V(P)$. Since,

$$A_g \cap V(P) = (g^{-1}(0))^c \cap V(J) \cap V(P) = (g^{-1}(0))^c \cap V(P)\,, \tag{162}$$

we see that $A_g \cap V(P) = \emptyset$ if and only if g vanishes identically on $V(P)$. Together this implies that $A_g \cap V(P) \neq \emptyset$ –i.e. A_g is a pseudo-neighborhood of $V(P)$– if and only if $g \notin P$.
To show that $A_g = A_{g+h}$ for all $g \in K[X_1, \ldots, X_n]$ and $h \in J$, it suffices to show that $A_g \subseteq A_{g+h}$. After all, we then get $A_{g+h} \subseteq A_{(g+h)+(-h)} = A_g$ from which $A_g = A_{g+h}$. To show the former inclusion, let $x \in A_g$ be given. It follows that $x \in V(J)$ and $g(x) \neq 0$. Now as $J = \sqrt{J} = I(V(J))$, we have $h(x) = 0$ and so $(g+h)(x) = g(x) \neq 0$. Hence $x \in A_{g+h}$ and so indeed $A_g \subseteq A_{g+h}$. This completes the proof. □

The last part of Lemma 3.11 serves as a warm-up for some of the things we have to verify in the proof Theorem 3.10. We will however not explicitly use it.

Proof of Theorem 3.10. We will show that the two rings are isomorphic by defining the map

$$\psi\colon R_P^J \to \mathcal{O}_P^J\,, \quad \frac{[f]}{[g]} \mapsto \left[\frac{f|_{A_g}}{g|_{A_g}}, A_g\right]\,. \tag{163}$$

We first need to verify that this is well-defined.

Firstly, as $[g] \in [P]^c$ we see that $g \notin P$, so that by Lemma 3.11 the set A_g is a pseudo-neighborhood of $V(P)$. As $A_g \subseteq (g^{-1}(0))^c$ we see that $\frac{f|_{A_g}}{g|_{A_g}}$ is a well-defined function on A_g. Moreover, this function is the restriction of a

rational function, showing that the right hand side of Equation (163) in indeed a class in $\mathcal{S}_P^J$.

Secondly, suppose

$$\frac{[f]}{[g]} = \frac{[h]}{[j]} \in R_P^J \,, \tag{164}$$

for some $f, g, h, j \in K[X_1, \ldots, X_n]$ with $[g], [j] \in [P]^c$. To conclude that the map ψ is well-defined, we need to show that

$$\left(\frac{f|_{A_g}}{g|_{A_g}}, A_g\right) \sim \left(\frac{h|_{A_j}}{j|_{A_j}}, A_j\right) . \tag{165}$$

It follows from Equation (164) that there exists an element $\ell \in K[X_1, \ldots, X_n]$ such that $[\ell] \in [P]^c$, and for which

$$[\ell][f][j] = [\ell][h][g] \tag{166}$$

as elements in $K[X_1, \ldots, X_n]/J$. This is equivalent to

$$\ell f j - \ell h g \in J \,. \tag{167}$$

As we have $[g], [j], [\ell] \in [P]^c$, we see that $g, j, \ell \notin P$. Therefore, the sets A_g, A_j and A_ℓ are all pseudo-neighborhoods of $V(P)$, and by Lemma 3.6 so is $A := A_g \cap A_j \cap A_\ell$.

Now choose $x \in A$. As $J = I(V(J))$, it follows from (167) that

$$\ell(x) f(x) j(x) - \ell(x) h(x) g(x) = 0 \,. \tag{168}$$

Moreover, as g, j and ℓ are non-vanishing on A, we may divide by $\ell(x)g(x)j(x)$ to arrive at

$$\frac{f(x)}{g(x)} - \frac{h(x)}{j(x)} = 0 \,. \tag{169}$$

We conclude that $\frac{f}{g}$ and $\frac{h}{j}$ agree on A, from which the equivalence (165) follows. Hence, ψ is indeed a well-defined map.

Next up is showing that ψ is a ring-homomorphism. On the one hand, we have

$$\psi\left(\frac{[f]}{[g]} + \frac{[h]}{[j]}\right) = \psi\left(\frac{[f][j] + [h][g]}{[g][j]}\right) = \left[\frac{(fj + hg)|_{A_{gj}}}{(gj)|_{A_{gj}}}, A_{gj}\right] . \tag{170}$$

On the other, we see that

$$\begin{aligned} &\psi\left(\frac{[f]}{[g]}\right) + \psi\left(\frac{[h]}{[j]}\right) = \psi\left(\frac{[f][j]}{[g][j]}\right) + \psi\left(\frac{[g][h]}{[g][j]}\right) \\ &= \left[\frac{(fj)|_{A_{gj}}}{(gj)|_{A_{gj}}}, A_{gj}\right] + \left[\frac{(hg)|_{A_{gj}}}{(gj)|_{A_{gj}}}, A_{gj}\right] = \left[\frac{(fj + hg)|_{A_{gj}}}{(gj)|_{A_{gj}}}, A_{gj}\right] , \end{aligned} \tag{171}$$

so that ψ respects addition. One shows in a similar way that ψ respects multiplication. Next, we note that $A_1 = V(J)$, so that

$$\psi\left(\frac{[f]}{[1]}\right) = \left[\frac{f|_{V(J)}}{1|_{V(J)}}, V(J)\right] = [f|_{V(J)}, V(J)]\,, \tag{172}$$

for any polynomial $f \in K[X_1, \ldots, X_n]$. In particular, this holds for the constants $f = c \in K$.

To show that ψ is surjective, let $(h, A) \in \mathcal{S}_P^J$ be given. By definition, there exist polynomials $f, g \in K[X_1, \ldots, X_n]$ with g nowhere vanishing on A, such that h agrees with $\frac{f}{g}$ on A. We fix such f and g. As A is a pseudo-neighborhood of $V(P)$, we see that $A \cap V(P) \neq \emptyset$. This means there are points in $V(P)$ on which g does not vanish, and so $g \notin I(V(P)) = P$. Note also that by assumption, $A \subseteq A_g$. It follows from Lemma 3.8 that

$$\psi\left(\frac{[f]}{[g]}\right) = \left[\frac{f|_{A_g}}{g|_{A_g}}, A_g\right] = \left[\frac{f|_{A_g \cap A}}{g|_{A_g \cap A}}, A_g \cap A\right] = \left[\frac{f|_A}{g|_A}, A\right] = [h, A]\,. \tag{173}$$

Hence, ψ reaches every element in $\mathcal{O}_P^J$.

It remains to show injectivity. To this end, suppose that

$$\psi\left(\frac{[f]}{[g]}\right) = \left[\frac{f|_{A_g}}{g|_{A_g}}, A_g\right] = [0, V(J)]\,. \tag{174}$$

It follows that $\frac{f}{g}$ vanishes on some pseudo-neighborhood $A \subseteq A_g$, from which we see that $f|_A = 0$. We now have a closer look at the set A. By assumption we may write $A = W^c \cap V(J)$ for some algebraic set W. Let us write $W = V(L)$ for some radical ideal L. From $A \cap V(P) \neq \emptyset$ we see that $W^c \cap V(P) = W^c \cap V(J) \cap V(P) = A \cap V(P) \neq \emptyset$, and hence $V(P) \nsubseteq W = V(L)$. We may thus conclude that $L \nsubseteq P$. It follows that we may pick an element $\ell \in L \setminus P$. In particular, we see that $[\ell] \in [P]^c$.

Now, from $\ell \in L = I(V(L)) = I(W)$ we see that ℓ vanishes identically on W. Hence, the product $f\ell$ vanishes identically on $V(J) \subseteq (W^c \cap V(J)) \cup W$. We conclude that $f\ell \in I(V(J)) = J$, and so $[f\ell] = 0$ in $K[X_1, \ldots, X_n]/J$. As $[\ell] \in [P]^c$ we finally see that

$$\frac{[f]}{[g]} = \frac{[f]}{[g]}\frac{[\ell]}{[\ell]} = \frac{[f\ell]}{[g\ell]} = 0\,. \tag{175}$$

This shows that ψ is indeed injective, and so a ring-isomorphism. This completes the proof. □

Remark 3.12. Note that for constants $c, d \in K$ we have

$$\frac{[c]}{[1]} = \frac{[d]}{[1]} \text{ in } R_P^J\,, \tag{176}$$

if and only if $[c][\ell] = [d][\ell]$ for some $\ell \in P^c$, which is equivalent to $(c-d)\ell \in J \subseteq P$. From $\ell \notin P$ we see that $c - d \in P$, which is only possible when $c = d$. Hence, R_P^J contains K, and can thus be seen as an algebra over this field. From Equation (172) in the proof of Theorem 3.10 we see that $\mathcal{O}_P^J$ contains K as the classes of constant functions:

$$K \cong \{[c|_{V(J)}, V(J)] \mid c \in K\}\,. \tag{177}$$

As we have $[c|_{V(J)}, V(J)][h, A] = [ch, A]$ for all $c \in K$ and $[h, A] \in \mathcal{O}_P^J$, we see that K acts on $\mathcal{O}_P^J$ simply by scalar multiplication of the locally defined function h. △

We may think of Theorem 3.10 as giving us a geometric interpretation of the rings R_P^J, especially when $V(P)$ is just a single point in $V(J)$, see Remark 3.9. To emphasize this geometric character, we will sometimes write $\mathcal{O}_W^V := \mathcal{O}_P^J$ if $V = V(J)$ and $W = V(P)$. If the irreducible algebraic set W is a single point $p \in K^n$, we will write $\mathcal{O}_p^V := \mathcal{O}_W^V$.

Alternatively, we may think of Theorem 3.10 as providing us with algebraic information on the rings $\mathcal{O}_P^J$. For instance, it follows immediately that the rings $\mathcal{O}_P^J$ are all local. We next gather some more straightforward properties of R_P^J, which therefore also hold for $\mathcal{O}_P^J$. First we need:

Lemma 3.13. *Let R be a ring, $I \subseteq R$ an ideal and $C \subseteq R$ a multiplicative subset. If R is a Noetherian ring, then so are the quotient R/I and the localization R_C.*

Proof. We begin with R/I. Suppose we have ideals $J_i \subseteq R/I$ for $i \in \mathbb{N}$ satisfying

$$J_1 \subseteq J_2 \subseteq \cdots \subseteq R/I\,. \tag{178}$$

It follows that we have the sequence of ideals

$$\pi^{-1}(J_1) \subseteq \pi^{-1}(J_2) \subseteq \cdots \subseteq R\,, \tag{179}$$

where $\pi\colon R \to R/I$ denotes the canonical projection. As R is Noetherian, we see that some $n \in \mathbb{N}$ exists such that $\pi^{-1}(J_i) = \pi^{-1}(J_j)$ for all $i, j > n$. Applying π and using the fact that this map is surjective, we get

$$J_i = \pi(\pi^{-1}(J_i)) = \pi(\pi^{-1}(J_j)) = J_j \text{ for all } i, j > n\,. \tag{180}$$

This shows that R/I is indeed Noetherian as well.

Next, suppose we have ideals $L_i \subseteq R_C$ for $i \in \mathbb{N}$ satisfying

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq R_C\,. \tag{181}$$

In Subsection 1.4 we constructed the ideal $N(L) \subseteq R$ out of an ideal $L \subseteq R_C$, and it follows from Lemma 1.21 that we have

$$N(L_1) \subseteq N(L_2) \subseteq \cdots \subseteq R\,. \tag{182}$$

Again some $m \in \mathbb{N}$ exists such that $N(J_i) = N(J_j)$ for all $i, j > m$. Using Lemma 1.21 we see that

$$L_i = (N(L_i))_C = (N(L_j))_C = L_j \text{ for all } i, j > m\,, \tag{183}$$

which shows that R_C is Noetherian as well. □

Corollary 3.14. *The rings R_P^J and $\mathcal{O}_P^J$ are Noetherian.*

Proof. As K is a field, it follows from Hilbert's basis theorem (Lemma 1.3) that $K[X_1, \ldots, X_n]$ is Noetherian. Applying Lemma 3.13 shows that $K[X_1, \ldots, X_n]/J$ is Noetherian, and using this lemma again we see that $R_P^J = (K[X_1, \ldots, X_n]/J)_{[P]^c}$ is Noetherian too. Finally the same holds for $\mathcal{O}_P^J$, as by Theorem 3.10 we have $\mathcal{O}_P^J \cong R_P^J$. □

We will next show that the ring $\mathcal{O}_W^V$ does not depend "too strongly" on the algebraic set V.

Theorem 3.15. *Let K be an algebraically closed field with proper radical ideals $J, M \subseteq K[X_1, \ldots, X_n]$. Suppose P is a prime ideal such that $J \subseteq P$, but $M \nsubseteq P$. That is, $V(P) \subseteq V(J)$ but $V(P) \nsubseteq V(M)$. Then the rings $\mathcal{O}_P^{J\cap M} = \mathcal{O}_{V(P)}^{V(J)\cup V(M)}$ and $\mathcal{O}_P^J = \mathcal{O}_{V(P)}^{V(J)}$ are isomorphic.*

In order to prove Theorem 3.15, we first need some lemmas.

Lemma 3.16. *Assume the setting of Theorem 3.15. Given any pseudo-neighborhood A of $V(P)$ in $V(J) \cup V(M) = V(J \cap M)$, the set $A \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J)$.*

Proof. We first claim that $D := V(M)^c \cap V(J \cap M)$ is a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$. To this end, note that D is Zariski open in $V(J \cap M)$ by construction. Moreover, if $D \cap V(P) = V(M)^c \cap V(J \cap M) \cap V(P) = \emptyset$ then, since $V(P) \subseteq V(J) \cup V(M) = V(J \cap M)$, we find $V(M)^c \cap V(P) = \emptyset$. Therefore $V(P) \subseteq V(M)$ and hence $M \subseteq P$. This contradicts our assumptions on M and P though, and we conclude that instead $D \cap V(P) \neq \emptyset$. Hence D is indeed a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$.

From Lemma (3.6) we conclude that $A \cap D$ is a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$ as well. However, as $A \subseteq V(J \cap M)$ we have $A \cap D = A \cap V(M)^c \cap V(J \cap M) = A \cap V(M)^c$. Hence, we have found that $A \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$.
Of course we may not immediately conclude that $A \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J)$. However, we do see that $A \cap V(M)^c \cap V(P) \neq \emptyset$.

If we write $A = W^c \cap V(J \cap M)$ for some algebraic set W, then

$$\begin{aligned} A \cap V(M)^c &= W^c \cap V(J \cap M) \cap V(M)^c \\ &= W^c \cap (V(J) \cup V(M)) \cap V(M)^c \\ &= W^c \cap V(J) \cap V(M)^c = (W \cup V(M))^c \cap V(J)\,. \end{aligned} \tag{184}$$

It follows that $A \cap V(M)^c$ is contained in $V(J)$ and indeed a Zariski open subset thereof. From this we see that $A \cap V(M)^c$ is also a pseudo-neighborhood of $V(P)$ in $V(J)$. □

Lemma 3.17. *Assume the setting of Theorem 3.15. Given any pseudo-neighborhood C of $V(P)$ in $V(J)$, the set $C \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in both $V(J)$ and $V(J \cap M)$.*

Proof. We first note that $V(J \cap M)$ is trivially a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$. Hence, it follows from Lemma 3.16 that $D := V(J \cap M) \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J)$. As $C \subseteq V(J) \subseteq V(J \cap M)$, we see that

$$C \cap V(M)^c = C \cap V(J \cap M) \cap V(M)^c = C \cap D\,. \tag{185}$$

Thus we may conclude from Lemma 3.6 that $C \cap V(M)^c$ is indeed a pseudo-neighborhood of $V(P)$ in $V(J)$, and so in particular $(C \cap V(M)^c) \cap V(P) \neq \emptyset$.

Next, note that we may write $C = W^c \cap V(J)$ for some algebraic set W, as C is Zariski open in $V(J)$. It follows that

$$\begin{aligned} C \cap V(M)^c &= W^c \cap V(J) \cap V(M)^c = W^c \cap (V(J) \cup V(M)) \cap V(M)^c \\ &= (W \cup V(M))^c \cap V(J \cap M)\,, \end{aligned} \tag{186}$$

from which we see that $C \cap V(M)^c$ is Zariski open in $V(J \cap M)$ as well. This shows that $C \cap V(M)^c$ is also a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$, which completes the proof. □

Proof of Theorem 3.15 . We define the map

$$\phi\colon \mathcal{O}_P^{J\cap M} \to \mathcal{O}_P^J\,, \quad [h, A] \mapsto [h|_{A\cap V(M)^c}, A \cap V(M)^c]\,. \tag{187}$$

We start by verifying that this map is well-defined.

First, as A is a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$, it follows from Lemma 3.16 that $A \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J)$.

Next, since $h : A \mapsto K$ can be written as the restriction to A of a rational function, the analogues statement holds for $h|_{A\cap V(M)^c}$. From this we see that $[h|_{A\cap V(M)^c}, A \cap V(M)^c]$ is a well-defined element of $\mathcal{O}_P^J$.

Finally, suppose $[h, A] = [\ell, B] \in \mathcal{O}_P^{J\cap M}$. Let $C \subseteq A \cap B$ be a pseudo-neighborhood of $V(P)$ in $V(J\cap M)$ on which h and ℓ agree. Then these functions also agree on $C \cap V(M)^c \subseteq A \cap B \cap V(M)^c = (A \cap V(M)^c) \cap (B \cap V(M)^c)$. Moreover, as before we see that $C \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J)$ and so we conclude that

$$[h|_{A\cap V(M)^c}, A \cap V(M)^c] = [\ell|_{B\cap V(M)^c}, B \cap V(M)^c]\,. \tag{188}$$

This shows that ϕ is indeed a well-defined map.

It is now straightforward to see that ϕ is a ring-homomorphism. For instance, on the one hand we have

$$\begin{aligned} \phi([h, A] + [\ell, B]) &= \phi([(h + \ell)|_{A\cap B}, A \cap B]) \\ &= [(h + \ell)|_{A\cap B\cap V(M)^c}, A \cap B \cap V(M)^c]\,, \end{aligned} \tag{189}$$

for all $[h, A], [\ell, B] \in \mathcal{O}_P^{J\cap M}$. Using Lemma 3.8 we see on the other hand that

$$\begin{aligned}\phi([h, A]) + \phi([\ell, B]) &= \phi([h|_{A\cap B}, A \cap B]) + \phi([\ell|_{A\cap B}, A \cap B]) \\ &= [h|_{A\cap B\cap V(M)^c}, A \cap B \cap V(M)^c] \\ &+ [\ell|_{A\cap B\cap V(M)^c}, A \cap B \cap V(M)^c] \\ &= [(h + \ell)|_{A\cap B\cap V(M)^c}, A \cap B \cap V(M)^c] \,,\end{aligned} \tag{190}$$

so that $\phi([h, A] + [\ell, B]) = \phi([h, A]) + \phi([\ell, B])$.

It remains to show that ϕ is a bijection. For surjectivity, suppose we are given $[h, C] \in \mathcal{O}_P^J$. It follows from Lemma 3.17 that $C \cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J)$. Hence, by Lemma 3.8 we may write $[h, C] = [h|_{C\cap V(M)^c}, C\cap V(M)^c] \in \mathcal{O}_P^J$. Likewise by Lemma 3.17, $C\cap V(M)^c$ is a pseudo-neighborhood of $V(P)$ in $V(J\cap M)$, and so $[h|_{C\cap V(M)^c}, C\cap V(M)^c]$ is also a well-defined element of $\mathcal{O}_P^{J\cap M}$. We clearly have $\phi([h|_{C\cap V(M)^c}, C \cap V(M)^c]) = [h|_{C\cap V(M)^c}, C \cap V(M)^c] = [h, C]$, which proves surjectivity.
For injectivity, suppose $\phi([h, A]) = [h|_{A\cap V(M)^c}, A \cap V(M)^c] = 0$. Then h vanishes on some pseudo-neighborhood C of $V(P)$ in $V(J)$ contained in $A\cap V(M)^c$. In particular, we have $C \subseteq V(M)^c$ and so $C = C \cap V(M)^c$. By Lemma 3.17, C is therefore a pseudo-neighborhood of $V(P)$ in $V(J \cap M)$. As we have $C \subseteq A$, we conclude that $[h, A] = [h|_C, C] = [0|_C, C] = 0$, which shows that ϕ is injective. Hence, ϕ is an isomorphism between the two rings, which concludes the proof. □

Remark 3.18. Recall from Subsection 2.7 that for any non-empty algebraic set $V \subseteq K^n$ we may write

$$V = W_1 \cup \cdots \cup W_k \tag{191}$$

for some irreducible algebraic sets W_i. This expression is unique if it holds that none of the W_i is included in any other, which we now assume. Suppose we have $W \subseteq V$ for some irreducible algebraic set W. We claim that $W \subseteq W_i$ for at least one $i \in \{1, \ldots, k\}$. To see why, note that we may write

$$V = V \cup W = W_1 \cup \cdots \cup W_k \cup W \,. \tag{192}$$

As the decomposition in (191) is unique (under the assumption of no non-trivial inclusions) we see that either $W \subseteq W_i$ or $W_i \subsetneq W$ for some i. In the latter case, we may write

$$V = W_1 \cup \cdots \cup \widehat{W_i} \cup \cdots \cup W_k \cup W \,, \tag{193}$$

where $\widehat{W_i}$ means we do not take the union with W_i. Again by uniqueness of the decomposition (191) we see that this is not possible. We conclude that instead $W \subseteq W_i$ for some i, and so the set

$$\mathcal{I}_W^V := \{i \in \{1, \ldots, k\} \mid W \subseteq W_i\} \tag{194}$$

is non-empty. Repeated use of Theorem 3.15 now tells us that

$$\mathcal{O}_W^V = \mathcal{O}_W^{\bigcup_{i=1}^k W_i} \cong \mathcal{O}_W^{\bigcup_{i\in\mathcal{I}_W^V} W_i} \,. \tag{195}$$

In other words, $\mathcal{O}_W^V$ only depends on those irreducible components of V that contain W. $\triangle$

Remark 3.18 motivates the following result.

Theorem 3.19. *Let $P, Q_1, \ldots, Q_m \subseteq K[X_1, \ldots, X_n]$ with $m \geq 1$ be prime ideals satisfying $Q_i \subseteq Q_j \implies i = j$ and where $Q_i \subseteq P$ for all i. Assume K is algebraically closed. The ring $\mathcal{O}_P^{Q_1 \cap \cdots \cap Q_m}$ is a domain if and only if $m = 1$.*

Proof. Suppose first that $m > 1$. We will construct m non-zero elements in $\mathcal{O}_P^{Q_1 \cap \cdots \cap Q_m}$ whose product is zero. To this end, we start by fixing an index $i \in \{1, \ldots, m\}$. For all $j \neq i$ we have $Q_j \nsubseteq Q_i$, and so we may pick an element $f_{j,i} \in Q_j \setminus Q_i$. It follows that their product

$$f_i := \prod_{\substack{j=1 \\ j \neq i}}^{m} f_{j,i} \tag{196}$$

is contained in $Q_1 \cap \cdots \cap \widehat{Q_i} \cap \cdots \cap Q_m$, where $\widehat{Q_i}$ means we do not take the intersection with Q_i. Moreover, if $f_i \in Q_i$ then $f_{j,i} \in Q_i$ for some $j \neq i$, contradicting that $f_{j,i} \in Q_j \setminus Q_i$. In conclusion, we find

$$f_i \in Q_1 \cap \cdots \cap \widehat{Q_i} \cap \cdots \cap Q_m \setminus Q_i \,. \tag{197}$$

For each $i \in \{1, \ldots, m\}$ we now fix an element f_i satisfying Equation (197).

Consider the elements $[f_i|_{V(Q_1 \cap \cdots \cap Q_m)}, V(Q_1 \cap \cdots \cap Q_m)] \in \mathcal{O}_P^{Q_1 \cap \cdots \cap Q_m}$. It is not hard to see that these are indeed well-defined. We claim that $[f_i|_{V(Q_1 \cap \cdots \cap Q_m)}, V(Q_1 \cap \cdots \cap Q_m)] \neq 0$. To see why, suppose otherwise. It follows that f_i vanishes on some pseudo-neighborhood A of $V(P)$ in $V(Q_1 \cap \cdots \cap Q_m)$. We write $A = W^c \cap V(Q_1 \cap \cdots \cap Q_m)$ for some algebraic set W. From $V(P) \subseteq V(Q_1) \cup \cdots \cup V(Q_1) = V(Q_1 \cap \cdots \cap Q_m)$ we see that

$$W^c \cap V(P) = W^c \cap V(Q_1 \cap \cdots \cap Q_m) \cap V(P) = A \cap V(P) \neq \emptyset \,. \tag{198}$$

Hence, we have $V(P) \nsubseteq W$. We write $W = V(J)$ for some radical ideal J, and it follows that $J \nsubseteq P$. We may therefore pick an element $h \in J \setminus P$, which means in particular that $h \notin Q_i$. As f_i vanishes identically on $A = W^c \cap V(Q_1 \cap \cdots \cap Q_m)$ and $h \in J = I(V(J))$ vanishes identically on $V(J) = W$, we conclude that $f_i h$ vanishes identically on $V(Q_1 \cap \cdots \cap Q_m) = V(Q_1) \cup \cdots \cup V(Q_m)$. In particular, $f_i h$ vanishes identically on $V(Q_i)$. From $Q_i = I(V(Q_i))$ we conclude that $f_i h \in Q_i$ and so $f_i \in Q_i$ or $h \in Q_i$. Both options do not hold though, and so we have to conclude that instead $[f_i|_{V(Q_1 \cap \cdots \cap Q_m)}, V(Q_1 \cap \cdots \cap Q_m)] \neq 0$. Nevertheless, clearly

$$\prod_{i=1}^{m} f_i \in Q_1 \cap \cdots \cap Q_m = I(V(Q_1 \cap \cdots \cap Q_m)) \,, \tag{199}$$

(here we use $m > 1$). It follows that

$$\begin{aligned}
&\prod_{i=1}^{m}[f_i|_{V(Q_1\cap\cdots\cap Q_m)}, V(Q_1\cap\cdots\cap Q_m)] \qquad (200)\\
&= \left[\prod_{i=1}^{m} f_i|_{V(Q_1\cap\cdots\cap Q_m)}, V(Q_1\cap\cdots\cap Q_m)\right]\\
&= \left[0|_{V(Q_1\cap\cdots\cap Q_m)}, V(Q_1\cap\cdots\cap Q_m)\right] = 0\,,
\end{aligned}$$

showing that $\mathcal{O}_P^{Q_1\cap\cdots\cap Q_m}$ is indeed not a domain when $m > 1$.

Finally suppose $m = 1$ and write $Q_1 = Q$. By Theorem 3.10 the ring $\mathcal{O}_P^Q$ is isomorphic to R_P^Q. Suppose therefore that we have

$$\frac{[f]}{[g]}\frac{[h]}{[j]} = \frac{[fh]}{[gj]} = 0 \qquad (201)$$

for elements $\frac{[f]}{[g]}$ and $\frac{[h]}{[j]}$ in $R_P^Q = (K[X_1,\ldots,X_n]/Q)_{[P]^c}$. It follows that

$$[\ell][fh] = 0 \text{ in } K[X_1,\ldots,X_n]/Q \qquad (202)$$

for some $\ell \notin P$, and so

$$\ell f h \in Q\,. \qquad (203)$$

As Q is prime, we see that $f \in Q$, $h \in Q$ or $\ell \in Q$. The last option is not possible though, as $Q \subseteq P$ and $\ell \notin P$. Hence $f \in Q$ or $h \in Q$, from which

$$\frac{[f]}{[g]} = 0 \text{ or } \frac{[h]}{[j]} = 0\,. \qquad (204)$$

This shows that R_P^Q and therefore $\mathcal{O}_P^Q$ is indeed a domain. □

We end this subsection with the following remarkable result. It tells us that the ring $R^J_{\mathcal{M}_p}$ directly gives us information about the position of a point p within the algebraic set $V(J)$.

Corollary 3.20. *Let $V \subseteq K^n$ be a non-empty algebraic set with K algebraically closed, and let $J = I(V)$ be its corresponding radical ideal. Write*

$$V = W_1 \cup \cdots \cup W_k \qquad (205)$$

for the unique decomposition of V into irreducible algebraic sets W_i that have no non-trivial inclusion relations. Given a point $p \in V$, the ring $R^J_{\mathcal{M}_p}$ is a domain if and only if p is contained in exactly one of the W_i.

Proof. Remark 3.18 tells us that

$$\mathcal{O}_p^V \cong \mathcal{O}_p^{\bigcup_{i\in\mathcal{I}_p^V} W_i}\,, \qquad (206)$$

where $\mathcal{I}_p^V$ denotes the set of those $i \in \{1, \ldots, k\}$ for which $p \in W_i$. As each W_i is irreducible, we see that $W_i = V(Q_i)$ for some prime ideals Q_i. It follows that we may write

$$\mathcal{O}_p^{\bigcup_{i\in\mathcal{I}_p^V} W_i} = \mathcal{O}_p^{\bigcup_{i\in\mathcal{I}_p^V} V(Q_i)} = \mathcal{O}_p^{V\left(\bigcap_{i\in\mathcal{I}_p^V} Q_i\right)} = \mathcal{O}_{\mathcal{M}_p}^{\bigcap_{i\in\mathcal{I}_p^V} Q_i}. \tag{207}$$

Now, as there are no non-trivial inclusions among the W_i, the same holds for the Q_i. Moreover, by definition we have $p \in W_i$ for all $i \in \mathcal{I}_p^V$, and so $Q_i \subseteq \mathcal{M}_p$ for all $i \in \mathcal{I}_p^V$. It therefore follows from Theorem 3.19 that $\mathcal{O}_p^V$ is a domain, if and only if $\#\mathcal{I}_p^V = 1$. That is, if and only if p is contained in only one of the sets W_i. As $\mathcal{O}_p^V \cong R^J_{\mathcal{M}_p}$ by Theorem 3.10, the result follows. □

3.3 Composition series

Now that we have provided a geometric interpretation of local rings, we return to the study of these algebraic objects. As mentioned before, we wish to associate a notion of dimension to these rings, and more generally to modules over them. We start by investigating those modules that are "smallest" in a way. That is, the ones that will turn out to have dimension 0. Throughout this subsection R is a commutative ring with 1, as always, but not necessarily local or Noetherian yet. Much of the material here comes from the excellent slides by Prof. Easdown in [4].

To keep the notation light, we will denote the zero-module $\{0\}$ simply by 0. We start with the following important definition.

Definition 3.21. Let M be a module over a ring R. A *composition series* for M is a finite chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M\,, \tag{208}$$

such that no more submodules can be inserted. That is, for any $i \in \{1, \ldots, n\}$ and any submodule $\tilde{M}$ satisfying $M_{i-1} \subseteq \tilde{M} \subseteq M_i$, we have $\tilde{M} = M_{i-1}$ or $\tilde{M} = M_i$.

We will call n the length of this composition series. △.

Note that there is no guarantee that a composition series exists for a given module. In fact, we will later classify all modules that have such a series. First we need the following useful notion.

Definition 3.22. A module M is called *simple* if it is non-zero and its only proper submodule is 0. △

Note that a module is simple precisely when it has a composition series of length 1. Our main reason for introducing them, however, is the following.

Lemma 3.23. *Given modules $N \subseteq M$, the quotient M/N is simple if and only if $N \subsetneq M$ and whenever we have a submodule $\tilde{M}$ satisfying $N \subseteq \tilde{M} \subseteq M$, it holds that $\tilde{M} = N$ or $\tilde{M} = M$.*

Proof. Assume first that M/N is simple. As simple modules are non-zero, we see that $N \subsetneq M$. Now let $\tilde{M}$ be given such that $N \subseteq \tilde{M} \subseteq M$. We denote by $\pi : M \to M/N$ the canonical projection, so that we get the chain of submodules $0 \subseteq \pi(\tilde{M}) \subseteq M/N$. By assumption, we therefore have $\pi(\tilde{M}) = 0$ or $\pi(\tilde{M}) = M/N$. In the former case we find $\tilde{M} \subseteq N$ and so $\tilde{M} = N$. In the latter we see that for any $m \in M$ there exists an $\tilde{m} \in \tilde{M}$ such that $\pi(\tilde{m}) = \pi(m)$. In other words, we have $m - \tilde{m} \in N$. However, as $N \subsetneqq \tilde{M}$, we conclude that $m = (m - \tilde{m}) + \tilde{m} \in \tilde{M}$. This shows that in this case $\tilde{M} = M$.

Conversely, suppose we have $N \subsetneq M$ and that no submodule can be strictly inserted. It follows that M/N is non-zero. Moreover, given a submodule $M' \subseteq M/N$, applying π^{-1} we get $N \subseteq \pi^{-1}(M') \subseteq M$. Hence, we either have $\pi^{-1}(M') = N$ or $\pi^{-1}(M') = M$. Applying π we get either $M' = \pi(\pi^{-1}(M')) = \pi(N) = 0$ or $M' = \pi(M) = M/N$, which shows that M/N is indeed simple. □

From Lemma 3.23 we immediately see that a chain of modules

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M\,, \tag{209}$$

is a composition series for M if and only if each quotient M_i/M_{i-1} is simple. We next look at modules with a composition series more closely. An important result concerning such modules is the following.

Theorem 3.24. *Let M be a module over a ring R and suppose it has a composition series of length $n \geq 0$. Then, any composition series for M has length n. Moreover, whenever we have a chain of submodules*

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_k = M\,, \tag{210}$$

it necessarily holds that $k \leq n$. In case $k = n$ it is a composition series, and if $k < n$ we can insert $n - k$ submodules to make it a composition series. That is, there is a composition series

$$0 = M'_0 \subsetneqq M'_1 \subsetneqq \cdots \subsetneqq M'_n = M\,, \tag{211}$$

where the M_0 to M_k are among the M'_0 to M'_n (necessarily in the same order).

To prove Theorem 3.24, we first need the following lemma.

Lemma 3.25. *Suppose we have a module M together with submodules $N, M', M'' \subseteq M$. Assume M' is contained in M'' and that their quotient M''/M' is simple. Then, precisely one of the following two options holds.*

1. *The quotient module $(M'' \cap N)/(M' \cap N)$ is simple;*
2. *We have $(M'' \cap N)/(M' \cap N) = 0$. That is, $M'' \cap N = M' \cap N$.*

If in addition we have $M' \subseteq N$ and option 1 holds, then also $M'' \subseteq N$.

Proof. Note that the two points in the lemma cannot both hold at the same time, as a simple module is always non-zero by definition. We define the homomorphism

$$\begin{aligned} &\psi : M'' \cap N \to M''/M' \\ &\psi(m) = m + M' \,, \end{aligned} \tag{212}$$

which is simply obtained by composing the inclusion of $M'' \cap N$ into M'' with the canonical projection of M'' onto M''/M'. The expression $m + M'$ denotes the class of the element m in M''/M'. We see that $\psi(m) = 0$ if and only if $m \in M'$, and so $\mathrm{Ker}(\psi) = M' \cap M'' \cap N = M' \cap N$. Thus, by the first isomorphism theorem for modules, we get

$$\frac{M'' \cap N}{M' \cap N} \cong \mathrm{Im}(\psi) \subseteq M''/M' \,. \tag{213}$$

As $\mathrm{Im}(\psi)$ is a submodule of the simple module M''/M', there are two possibilities. Either we have $\mathrm{Im}(\psi) = M''/M'$, in which case $(M'' \cap N)/(M' \cap N) \cong M''/M'$ and so $(M'' \cap N)/(M' \cap N)$ is simple, or $\mathrm{Im}(\psi) = 0$, which means we get $(M'' \cap N)/(M' \cap N) = 0$ and so $(M'' \cap N) = (M' \cap N)$.

Now suppose we have $M' \subseteq N$ and that the module $(M'' \cap N)/(M' \cap N)$ is simple. Going through the same steps as before, we cannot arrive at $\mathrm{Im}(\psi) = 0$, as this would give $(M'' \cap N)/(M' \cap N) = 0$. Therefore, we find $\mathrm{Im}(\psi) = M''/M'$ instead. That is, ψ as defined above is surjective. This means that for any $m'' \in M''$, there exists an $n \in M'' \cap N \subseteq N$ such that $m'' + M' = n + M'$. But then $m'' = n + m'$ for some $m' \in M' \subseteq N$ and so $m'' \in N$. That is, we find $M'' \subseteq N$, which completes the proof. □

Proof of Theorem 3.24. Given any R-module N, we denote by $\ell(N)$ the minimum of all lengths of composition series for N if at least one exists, and we set $\ell(N) = \infty$ otherwise. By assumption we have $\ell(M) \neq \infty$, and we set $\tilde{n} := \ell(M)$ for brevity. It follows that a composition series exists for M of length $\tilde{n}$, which we denote by

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{\tilde{n}} = M \,. \tag{214}$$

To start, given a proper submodule N of M, we claim that $\ell(N) < \ell(M)$ (and so in particular $\ell(N) \neq \infty$). To this end, note that we have the chain of submodules

$$0 = M_0 \cap N \subseteq M_1 \cap N \subseteq \cdots \subseteq M_{\tilde{n}} \cap N = M \cap N = N \,. \tag{215}$$

By Lemma 3.23 we see that each factor M_i/M_{i-1} for $i \in \{1, \ldots, \tilde{n}\}$ is simple. Hence, by Lemma 3.25 we conclude that for each i we either have that $(M_i \cap N)/(M_{i-1} \cap N)$ is simple, or that $M_i \cap N = M_{i-1} \cap N$. By discarding doubles in (215), we therefore get a composition series for N of length $\tilde{n}$ or less. This shows that $\ell(N) \neq \infty$ and in fact $\ell(N) \leq \ell(M)$.

To see that $\ell(N) < \ell(M)$, assume that we do not have $M_i \cap N = M_{i-1} \cap N$ for any i in (215), so that this chain is a composition series without us having

to discard doubles. As we have $M_0 = 0 \subseteq N$ and because $(M_1 \cap N)/(M_0 \cap N)$ is simple, we conclude by the second part of Lemma 3.25 that $M_1 \subseteq N$. As $(M_2 \cap N)/(M_1 \cap N)$ is simple, we likewise see that $M_2 \subseteq N$ and so forth. Proceeding in this way, we eventually find $M = M_{\tilde{n}} \subseteq N$ and so $M = N$. This contradicts our assumption on N, and we see that instead $M_i \cap N = M_{i-1} \cap N$ for at least one $i \in \{1, \ldots, \tilde{n}\}$. As we discarded doubles to make (215) into a composition series, we conclude that there is a composition series for N of length strictly less than $\tilde{n} = \ell(M)$. By definition of $\ell(N)$ as the minimum over these lengths, we see that indeed $\ell(N) < \ell(M)$.

Now suppose we have any chain of submodules

$$0 = M'_0 \subsetneq M'_1 \subsetneq \cdots \subsetneq M'_k = M\,. \tag{216}$$

As clearly $\ell(M'_0) = \ell(0) = 0$, we see that $\ell(M'_1) \geq 1$ by the foregoing. Likewise, we get $\ell(M'_2) \geq \ell(M'_1) + 1 \geq 2$, and so forth, leading to $\ell(M'_k) = \ell(M) \geq k$. This shows that the chain (216) can only exist when $k \leq \ell(M)$. In particular, if (216) is a composition series, then $k \leq \ell(M)$ but also $\ell(M) \leq k$ by definition of $\ell(M)$, and so $k = \ell(M)$. In other words, every composition series has the same length.

Returning to a general chain of the form (216), if $k = \ell(M)$ and it is not a composition series, then we can insert a submodule at some place. This gives a chain as in (216) of length $\ell(M) + 1$, contradicting our earlier finding. Hence, if $k = \ell(M)$ then a chain of the form (216) has to be a composition series. If $k < \ell(M)$ then by our previous result it is not a composition series, and so we can insert a submodule somewhere. We can keep doing this until we hit $k = \ell(M)$, by which point it becomes a composition series. Hence, any such chain can be made into a composition series by inserting submodules, which completes the proof. □

To see what modules have a composition series, we need the following definition. Compare to the notion of a Noetherian module, Definition 2.3.

Definition 3.26. A module M is called Artinian if the following holds. Whenever we have a chain of submodules

$$M \supseteq M_0 \supseteq M_1 \supseteq \ldots\,, \tag{217}$$

there exists an $N \geq 0$ such that $M_i = M_j$ for all $i, j \geq N$. In other words, submodules cannot keep decreasing forever. △

We may now state our promised characterization of those modules that admit a composition series.

Theorem 3.27. *A module M has a composition series, if and only if it is both Noetherian and Artinian.*

Proof. Suppose M has a composition series of length $n \geq 0$. If we are given a chain of submodules

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M\,, \tag{218}$$

then at most n of these inclusions are strict. Otherwise, we may form a chain

$$0 = M_0 \subseteq M_{i_1} \subsetneq M_{i_2} \cdots \subsetneq M_{i_{n+2}} \subseteq M\,, \tag{219}$$

for some $i_1 < \cdots < i_{n+2} \in \mathbb{N}$. Hence, after discarding doubles at the ends if needed, we get a chain

$$0 = M'_0 \subsetneq M'_1 \cdots \subsetneq M'_k = M\,, \tag{220}$$

for some $k > n$. This contradicts the result of Theorem 3.24, and so the chain (218) can only have at most n strict inclusions. Hence from some point on, all inclusions are equalities, which proves that M is indeed Noetherian.

In exactly the same way, a chain

$$M \supseteq M_1 \supseteq M_2 \supseteq \ldots \tag{221}$$

with more than n strict inclusions leads to a contradiction, and so the module M is Artinian too.

Now suppose M is both Noetherian and Artinian. Given any proper submodule $N_0 \subsetneq M$, we claim that a submodule N_1 exists such that $N_0 \subsetneq N_1$ and whenever $N_0 \subseteq \tilde{N} \subseteq N_1$ for some submodule $\tilde{N}$, we have $N_0 = \tilde{N}$ or $N_1 = \tilde{N}$. To see why, we set $M_1 = M$. If it holds that no submodule sits between N_0 and M then we may set $N_1 = M$ and we are done. If on the other hand there is a submodule $\tilde{N}$ such that $N_0 \subsetneq \tilde{N} \subsetneq M_1$, then we set $M_2 = \tilde{N} \subsetneq M_1$. Again, since $N_0 \subsetneq M_2$, either we are done or we find a submodule M_3 satisfying $N_0 \subsetneq M_3 \subsetneq M_2$, and so forth. If this process never ends, then we get an infinite chain of submodules

$$M_1 \supsetneq M_2 \supsetneq \ldots\,. \tag{222}$$

This contradicts the assumption that M is Artinian though, and so we conclude that indeed a submodule N_1 exists satisfying $N_0 \subsetneq N_1$ with no submodules in between.

We now set $N_0 = 0$. If $M = 0$ then clearly M has a composition series. If on the other hand $M \neq 0$, then by the claim above we get a submodule N_1 satisfying $0 = N_0 \subsetneq N_1$ with no submodules in between. If $N_1 = M$ then we have found a composition series for M. If not, we may construct a submodule N_2 satisfying $0 = N_0 \subsetneq N_1 \subsetneq N_2$, with no submodules in between. We continue building submodules N_i in this manner, stopping only when we find $N_i = M$. If this process never stops then we get an infinite chain

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subseteq M\,, \tag{223}$$

which contradicts the fact that M is Noetherian. Hence, we eventually find a composition series

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n = M\,, \tag{224}$$

for M, which completes the proof. □

3.4 A brief foray into homological algebra

We now take a small break from composition series to talk about exact sequences of modules. For our purposes, this is simply some new notation that captures certain relations between modules in a convenient way. However, the study of these objects, homological algebra, is very important throughout mathematics and has applications ranging from differential geometry to data analysis.

To introduce exact sequences, suppose we have a module M together with a submodule $N \subseteq M$. We denote by $\iota : N \to M$ the inclusion of N into M and by $\pi : M \to M/N$ the canonical projection onto the quotient. We may now write down the following sequence of modules and homomorphisms:

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0\,, \tag{225}$$

where the maps to and from the zero-module are zero-homomorphisms. This sequence has some interesting properties. For instance, if we look at the map ι going into the module M, then by definition $\mathrm{Im}(\iota) = N$. On the other hand, the map π going out of the module M satisfies $\mathrm{Ker}(\pi) = N$. Hence, if we look at the two maps involving M, we find the relation

$$\mathrm{Im}(\iota) = \mathrm{Ker}(\pi)\,. \tag{226}$$

This is not exclusive to M though. If we focus on the maps involving N, then we see that

$$\mathrm{Im}(0) = \mathrm{Ker}(\iota)\,, \tag{227}$$

both being equal to 0 as ι is injective. Similarly, for M/N we have

$$\mathrm{Im}(\pi) = \mathrm{Ker}(0) = M/N\,, \tag{228}$$

as π is surjective. Motivated by this, we may forget about the actual submodule N and its quotient, and focus only on these relations between the various images and kernels. That is, we consider a sequence

$$0 \longrightarrow M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \longrightarrow 0\,, \tag{229}$$

for some modules M_0, M_1 and M_2 and homomorphisms f and g. The first and last maps are again zero-homomorphisms. In addition, we require that

$$\begin{aligned} 0 = \mathrm{Im}(0) &= \mathrm{Ker}(f)\,; \\ \mathrm{Im}(f) &= \mathrm{Ker}(g)\,; \\ \mathrm{Im}(g) &= \mathrm{Ker}(0) = M_2\,. \end{aligned} \tag{230}$$

A sequence (229) satisfying the conditions (230) is called a *short exact sequence* of modules. Note that the condition $\mathrm{Ker}(f) = 0$ is just saying that f is injective, whereas the condition $\mathrm{Im}(g) = M_2$ means that g is surjective.

As f is injective, we may view $M_0 \cong \mathrm{Im}(f)$ as a submodule of M_1. Moreover, because g is surjective, it follows by the first isomorphism theorem that

$M_1/\operatorname{Im}(f) = M_1/\ker(g) \cong \operatorname{Im}(g) = M_2$. We see that we are essentially back at the situation (225) that motivated the generalization (229). That is, we have

$$0 \longrightarrow \operatorname{Im}(f) \xrightarrow{\iota} M_1 \xrightarrow{\pi} M_1/\operatorname{Im}(f) \longrightarrow 0\,, \tag{231}$$

with ι and π again denoting the inclusion and canonical projection, respectively.

We may formalize this equivalence between the sequences (229) and (231) by noting that we have a *commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_0 & \xrightarrow{f} & M_1 & \xrightarrow{g} & M_2 & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{Id}_{M_1}} & & \downarrow{\scriptstyle [g]^{-1}} & & \downarrow \\ 0 & \longrightarrow & \operatorname{Im}(f) & \xrightarrow{\iota} & M_1 & \xrightarrow{\pi} & M_1/\operatorname{Im}(f) & \longrightarrow & 0 \end{array}\,, \tag{232}$$

where all maps to and from the zero-module are zero-homomorphisms, and where with slight abuse of notation we use f to denote the homomorphism $x \mapsto f(x)$ both from M_0 to M_1 and from M_0 to $\operatorname{Im}(f)$. The map $[g]^{-1}\colon M_2 \to M_1/\operatorname{Im}(f) = M_1/\ker(g)$ is the inverse of the isomorphism $[g]\colon M_1/\ker(g) \to M_2$ which we found by the first isomorphism theorem. Explicitly we have $[g]([x]) = g(x)$ with $[x]$ the class of $x \in M_1$. Note that all five maps at the vertical arrows are isomorphisms.

The term "commutative diagram" pertains to the fact that for each of the four squares in the diagram, we may follow the arrows first down and then to the right, or first to the right and then down, and get the same result. That is, whenever we see a square

$$\begin{array}{ccc} N_1 & \xrightarrow{h_1} & N_2 \\ \downarrow{\scriptstyle j_1} & & \downarrow{\scriptstyle j_2} \\ N_3 & \xrightarrow{h_2} & N_4 \end{array} \tag{233}$$

with modules $N_1, \ldots, N_4$ and homomorphisms h_1, h_2, j_1, j_2, we have

$$h_2 \circ j_1 = j_2 \circ h_1\,. \tag{234}$$

One easily verifies this to be the case for the four squares in the diagram (232). It for instance holds for

$$\begin{array}{ccc} M_1 & \xrightarrow{g} & M_2 \\ \downarrow{\scriptstyle \mathrm{Id}_{M_1}} & & \downarrow{\scriptstyle [g]^{-1}} \\ M_1 & \xrightarrow{\pi} & M_1/\operatorname{Im}(f) \end{array}\,, \tag{235}$$

because $([g] \circ \pi \circ \mathrm{Id}_{M_1})(x) = [g]([x]) = g(x)$ for all $x \in M_1$, and so $\pi \circ \mathrm{Id}_{M_1} = [g]^{-1} \circ g$.

More generally, we may consider any sequence of modules and homomorphisms:

$$\ldots \xrightarrow{f_{-2}} M_{-1} \xrightarrow{f_{-1}} M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} \ldots\,, \tag{236}$$

which may be infinite on either side, start at a module which may or may not be the zero-module, and end at any module. We say it is exact precisely when

$$\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}) \subseteq M_{i+1} \tag{237}$$

for all i for which f_i and f_{i+1} exist.

If we have the sequence

$$0 \xrightarrow{0_{0\to M}} M \xrightarrow{0_{M\to 0}} 0\,, \tag{238}$$

then it is exact if and only if $0 = \mathrm{Im}(0_{0\to M}) = \mathrm{Ker}(0_{M\to 0}) = M$. That is, precisely when $M = 0$. This is useful in the situation where we have a short exact sequence

$$0 \longrightarrow M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \longrightarrow 0\,, \tag{239}$$

and we are given the additional information that $M_1 = 0$. We then get the short exact sequence

$$0 \longrightarrow M_0 \xrightarrow{f} 0 \xrightarrow{g} M_2 \longrightarrow 0\,, \tag{240}$$

and we conclude from the foregoing that $M_0 = M_2 = 0$, as we see two instances of the sequence (238). (The maps f and g in (240) can only be zero-homomorphisms.)

Likewise, we may consider the sequence

$$0 \xrightarrow{0} M_1 \xrightarrow{f} M_2 \xrightarrow{0} 0\,. \tag{241}$$

This is exact if and only if we have both $\mathrm{Ker}(f) = \mathrm{Im}(0) = 0$ and $M_2 = \mathrm{Ker}(0) = \mathrm{Im}(f)$. In other words, precisely when $f\colon M_1 \to M_2$ is an isomorphism. Again, we can imagine a situation where we are given the short exact sequence (239), but this time we know that $M_2 = 0$. It follows that we get the short exact sequence

$$0 \longrightarrow M_0 \xrightarrow{f} M_1 \xrightarrow{0} 0 \longrightarrow 0\,, \tag{242}$$

and we conclude that $M_0 \cong M_1$ with f an isomorphism between the two.

Next, we point out that exact sequences can be broken down into short ones, in the following way. Suppose we are given the exact sequence

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{k-1}} M_k \longrightarrow 0\,, \tag{243}$$

for some $k > 3$. It follows that we have the short exact sequences

$$\begin{aligned}
&0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \mathrm{Im}(f_2) \longrightarrow 0 \ , \qquad (244)\\
&0 \longrightarrow \mathrm{Im}(f_2) \xrightarrow{\iota_{\mathrm{Im}(f_2)}} M_3 \xrightarrow{f_3} \mathrm{Im}(f_3) \longrightarrow 0\\
&\qquad\qquad\qquad\vdots\\
&0 \longrightarrow \mathrm{Im}(f_i) \xrightarrow{\iota_{\mathrm{Im}(f_i)}} M_{i+1} \xrightarrow{f_{i+1}} \mathrm{Im}(f_{i+1}) \longrightarrow 0\\
&\qquad\qquad\qquad\vdots\\
&0 \longrightarrow \mathrm{Im}(f_{k-3}) \xrightarrow{\iota_{\mathrm{Im}(f_{k-3})}} M_{k-2} \xrightarrow{f_{k-2}} \mathrm{Im}(f_{k-2}) \longrightarrow 0\\
&0 \longrightarrow \mathrm{Im}(f_{k-2}) \xrightarrow{\iota_{\mathrm{Im}(f_{k-2})}} M_{k-1} \xrightarrow{f_{k-1}} M_k \longrightarrow 0
\end{aligned}$$

where $\iota_{\mathrm{Im}(f_i)}$ denotes the inclusion of $\mathrm{Im}(f_i)$ into M_{i+1}, and where as before, we change the codomain of f_j from M_{j+1} to $\mathrm{Im}(f_j) \subseteq M_{j+1}$. One easily verifies that these sequences are indeed exact: the map f_1 is injective by assumption, and inclusions are always injective. Likewise, f_{k-1} is surjective by assumption, and each map $f_j \colon M_j \to \mathrm{Im}(f_j)$ is of course surjective too. For the modules in the middle we see that $\mathrm{Im}(\iota_{\mathrm{Im}(f_i)}) = \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$ for all $i \in \{1, \ldots, k-2\}$, because the sequence (243) is exact. Breaking an exact sequence up into small ones can be useful, as it sometimes allows one to lift a result about small exact sequences to one about more general ones, see the proof of Theorem (3.31) below.

Motivated by this useful notation of exact sequences, it can be insightful to know if a given transformation preserves such sequences. We end this subsection with a result that states this to be the case for localization. First, we need some preliminaries.

Recall from Subsection 1.4 that we may localize a ring R with respect to any set $C \subseteq R$ satisfying $1 \in C$, $0 \notin C$ and $x, y \in C \implies xy \in C$. Given such a set $C \subseteq R$ and an R-module M, we may define the R_C-module M_C as follows.

We start with the set of all pairs (m, c), where $m \in M$ and $c \in C$. On this set we define the equivalence relation:

$$(m, c) \sim (n, d) \text{ if and only if there exists an } e \in C \text{ such that } edm = ecn\,.$$

One verifies easily that this is indeed an equivalence relation, and we denote the class of (m, c) by $\frac{m}{c}$. The set of all such classes is denoted by M_C, which we make into an R_C module by defining

$$\begin{aligned}
\frac{m}{c} + \frac{n}{d} &= \frac{dm + cn}{dc}\\
\frac{r}{e} \cdot \frac{m}{c} &= \frac{rm}{ec}\,,
\end{aligned} \qquad (245)$$

for all $\frac{m}{c}, \frac{n}{d} \in M_C$ and $\frac{r}{e} \in R_C$. The zero-element of M_C is given by $\frac{0}{1} = \frac{0}{c}$ for any $c \in C$, and the additive inverse of $\frac{m}{c}$ is given by $\frac{-m}{c}$. Verification that all of this is well-defined, and indeed gives an R_C-module goes in almost exactly the same way as verifying that R_C is a well-defined ring, see Subsection 1.4.

Now, given an R-homomorphism f between two R-modules M and N, we may likewise define an R_C-homomorphism f_C between M_C and N_C, by setting

$$f_C\left(\frac{m}{c}\right) = \frac{f(m)}{c} \in N_C\,. \tag{246}$$

To see that this is well-defined, suppose $\frac{m}{c} = \frac{n}{d} \in M_C$. It follows that $edm = ecn$ for some $e \in C$, and so

$$edf(m) = f(edm) = f(ecn) = ecf(n)\,. \tag{247}$$

This shows that likewise $\frac{f(m)}{c} = \frac{f(n)}{d} \in N_C$. Moreover, given $\frac{m}{c}, \frac{m'}{c'} \in M_C$ and $\frac{r}{d} \in R_C$, we have

$$\begin{aligned} f_C\left(\frac{m}{c} + \frac{m'}{c'}\right) = f_C\left(\frac{c'm + cm'}{cc'}\right) = \frac{f(c'm + cm')}{cc'} \\ = \frac{c'f(m) + cf(m')}{cc'} = \frac{f(m)}{c} + \frac{f(m')}{c'} = f_C\left(\frac{m}{c}\right) + f_C\left(\frac{m'}{c'}\right) \end{aligned} \tag{248}$$

and

$$\begin{aligned} f_C\left(\frac{r}{d} \cdot \frac{m}{c}\right) = f_C\left(\frac{rm}{dc}\right) = \frac{f(rm)}{dc} = \frac{rf(m)}{dc} = \frac{r}{d} \cdot \frac{f(m)}{c} \\ = \frac{r}{d} \cdot f_C\left(\frac{m}{c}\right)\,, \end{aligned} \tag{249}$$

which shows that f_C is indeed an R_C-homomorphism. Following our usual convention, we will now drop the symbol "$\cdot$" from our notation for the action of R_C on M_C.

The following lemma tells us that going from R-modules and homomorphisms to the corresponding R_C-modules and homomorphisms preserves exact sequences.

Lemma 3.28. *Let $C \subseteq R$ be a multiplicative set. Given an exact sequence*

$$N \xrightarrow{f} M \xrightarrow{g} P \tag{250}$$

of R-modules, the corresponding sequence

$$N_C \xrightarrow{f_C} M_C \xrightarrow{g_C} P_C\,, \tag{251}$$

is exact too.

Proof. We are given that $\mathrm{Im}(f) = \mathrm{Ker}(g)$, and we need to show that $\mathrm{Im}(f_C) = \mathrm{Ker}(g_C)$. To this end, suppose we have $f_C\left(\frac{n}{c}\right) = \frac{f(n)}{c} \in \mathrm{Im}(f_C)$, for some $\frac{n}{c} \in N_C$. It follows that $g_C\left(\frac{f(n)}{c}\right) = \frac{g(f(n))}{c} = \frac{0}{c} = 0$, as $g \circ f = 0$ (i.e. we have $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$). We conclude that $\mathrm{Im}(f_C) \subseteq \mathrm{Ker}(g_C)$.

Conversely, suppose we have $\frac{m}{d} \in \mathrm{Ker}(g_C)$. It follows that $g_C\left(\frac{m}{d}\right) = \frac{g(m)}{d} = \frac{0}{1}$. Hence, there exists an $e \in C$ such that $eg(m) = g(em) = 0$. We see that $em \in \mathrm{Ker}(g) = \mathrm{Im}(f)$, and so $em = f(n)$ for some $n \in N$. Now consider the element $\frac{n}{ed} \in N_C$. We see that

$$f_C\left(\frac{n}{ed}\right) = \frac{f(n)}{ed} = \frac{em}{ed} = \frac{m}{d}\,, \tag{252}$$

where the last step holds because $1(d)(em) = 1(ed)(m) = dem$. Hence we find $\mathrm{Ker}(g_C) \subseteq \mathrm{Im}(f_C)$, and so indeed $\mathrm{Ker}(g_C) = \mathrm{Im}(f_C)$. □

Note that 0_C is the zero-module, as we have $\frac{0}{c} = \frac{0}{1}$ for any $c \in C$. Hence, given a short exact sequence

$$0 \longrightarrow M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \longrightarrow 0 \tag{253}$$

of R-modules, the corresponding sequence

$$0 \longrightarrow (M_0)_C \xrightarrow{f_C} (M_1)_C \xrightarrow{g_C} (M_2)_C \longrightarrow 0 \tag{254}$$

is exact too.

3.5 More on composition series

We continue our investigation of composition series. In light of Theorem 3.27, which tells us that a module has a composition series if and only if it is both Noetherian and Artinian, it makes sense to investigate Artinian modules in some more detail first. Recall from Lemma 2.5 that for a module M with submodule N, it holds that M is Noetherian if and only if both N and M/N are Noetherian. Due to the similar definitions of Noetherian and Artinian modules, it comes as no surprise that the same holds in the Artinian setting. That is, we have:

Lemma 3.29. *Given a module M with submodule $N \subseteq M$, we have that M is Artinian if and only if both N and M/N are Artinian.*

Proof. Suppose first that M is Artinian. If we have any descending chain of submodules in N, then that is also a descending chain of submodules in M. Hence, from some point on this chain only lists the same submodule, which shows that N is Artinian. Now suppose we have a chain of submodules in M/N

$$M/N \supseteq M_1' \supseteq M_2' \supseteq \dots\,. \tag{255}$$

We denote by $\pi : M \to M/N$ the canonical projection. It follows that we get a chain of submodules

$$M \supseteq \pi^{-1}(M_1') \supseteq \pi^{-1}(M_2') \supseteq \dots . \tag{256}$$

As M is assumed Artinian, we see that for some $n \geq 1$ we have $\pi^{-1}(M_i') = \pi^{-1}(M_j')$ whenever $i, j \geq n$. Applying π and using that this map is surjective, we obtain $M_i' = \pi(\pi^{-1}(M_i')) = \pi(\pi^{-1}(M_j')) = M_j'$ for all $i, j \geq n$. This shows that M/N is Artinian too.

Conversely, assume both N and M/N are Artinian, and suppose we have a chain of submodules

$$M \supseteq M_1 \supseteq M_2 \supseteq \dots . \tag{257}$$

We obtain the chains of submodules

$$N \supseteq M_1 \cap N \supseteq M_2 \cap N \supseteq \dots \tag{258}$$

and

$$M/N \supseteq \pi(M_1) \supseteq \pi(M_2) \supseteq \dots . \tag{259}$$

By assumption, there exist $n, n' \geq 1$ such that $M_i \cap N = M_j \cap N$ whenever $i, j \geq n$ and $\pi(M_i) = \pi(M_j)$ whenever $i, j \geq n'$. By picking a larger value of n or n' if necessary, we may of course assume $n = n'$. Let i, j be given such that $i \geq j \geq n$, so that $M_i \subseteq M_j$. Given $x \in M_j$ we have $\pi(x) \in \pi(M_j) = \pi(M_i)$, and so $\pi(x) = \pi(y)$ for some $y \in M_i$. It follows that $x - y \in N$, and as we also have $M_i \subseteq M_j$, we in fact find $x - y \in N \cap M_j$. Using that $N \cap M_j = N \cap M_i$ we therefore find $x - y \in M_i$. As $y \in M_i$, we conclude that $x \in M_i$ and so $M_j \subseteq M_i$. This shows that $M_j = M_i$ for all $i, j \geq n$, from which we see that M is indeed Artinian. □

The following definition is directly motivated by Theorem 3.24 in Subsection 3.3.

Definition 3.30. Given a module M with a composition series, we define the *length* of M (denoted by $\ell(M)$) to be the length of any composition series for M. If M has no composition series then we set $\ell(M) = \infty$. △

The next result tells us that the length of a module plays well with exact sequences.

Theorem 3.31. *Let*

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \dots \xrightarrow{f_{k-1}} M_k \longrightarrow 0\,, \tag{260}$$

be an exact sequence of R-modules where $\ell(M_j) < \infty$ for all $j \in \{1, \dots, k\}$. We have

$$\sum_{j=1}^{k} (-1)^j \ell(M_j) = 0\,. \tag{261}$$

Proof. Note that if $k = 1$ in (260), we have $M_1 = 0$ and so $\ell(M_1) = 0$. This is of course in agreement with Equation (261). Likewise, for $k = 2$ we find $M_1 \cong M_2$ and so $\ell(M_1) = \ell(M_2)$, which is equivalent to Equation (261) in this case.

We next assume $k = 3$. By the discussion in the previous subsection, we may assume that M_1 is a submodule of M_2 with M_3 given by the quotient M_2/M_1. For simplicity we write $\ell_j = \ell(M_j)$ for all j, and we start by giving a composition series

$$0 = N_0 \subsetneq \cdots \subsetneq N_{\ell_1} = M_1 \tag{262}$$

for M_1, as well as a composition series

$$0 = N'_0 \subsetneq \cdots \subsetneq N'_{\ell_3} = M_2/M_1 \tag{263}$$

for M_3. Let $\pi\colon M_2 \to M_2/M_1$ denote the canonical projection of M_2 onto M_2/M_1. It follows that we get the chain of submodules

$$\begin{aligned} 0 &= N_0 \subsetneq \cdots \subsetneq N_{\ell_1} = M_1 \\ &= \pi^{-1}(N'_0) \subseteq \pi^{-1}(N'_1) \subseteq \cdots \subseteq \pi^{-1}(N'_{\ell_3}) = M_2\,. \end{aligned} \tag{264}$$

By assumption, each quotient N_j/N_{j-1} for $j \in \{1, \dots, \ell_1\}$ is simple. Hence, if we show that $\pi^{-1}(N'_i)/\pi^{-1}(N'_{i-1})$ is simple for each $i \in \{1, \dots, \ell_3\}$ then Equation (264) gives a composition series for M_2. To this end, we consider the homomorphism

$$\begin{aligned} \psi\colon \pi^{-1}(N'_i) &\to N'_i/N'_{i-1} \\ n &\mapsto [n] + N'_{i-1}\,, \end{aligned} \tag{265}$$

which is simply the composition of π with the canonical projection of N'_i onto N'_i/N'_{i-1}. Here we have set $[n] = \pi(n)$ for the class of n in M_2/M_1, and $[n]+N'_{i-1}$ for the corresponding class in N'_i/N'_{i-1} whenever $[n] \in N'_i$. It is clear that ψ is surjective, as the restriction of π to $\pi^{-1}(N'_i)$ of course reaches all of N'_i. Moreover, for $n \in \pi^{-1}(N'_{i-1})$ we have $[n] \in N'_{i-1}$ and so $\psi(n) = [n] + N'_{i-1} = 0$. Hence, we find $\pi^{-1}(N'_{i-1}) \subseteq \mathrm{Ker}(\psi)$.

Conversely, if $\psi(n) = 0$ then $\pi(n) = [n] \in N'_{i-1}$, from which $n \in \pi^{-1}(N'_{i-1})$. We conclude that $\pi^{-1}(N'_{i-1}) = \mathrm{Ker}(\psi)$ and so by the first isomorphism theorem

$$\pi^{-1}(N'_i)/\pi^{-1}(N'_{i-1}) \cong N'_i/N'_{i-1}\,. \tag{266}$$

From the fact that the chain (263) is a composition series, we see that N'_i/N'_{i-1} is simple. Hence, so is $\pi^{-1}(N'_i)/\pi^{-1}(N'_{i-1})$ and we conclude that Equation (264) indeed gives a composition series for M_2. It follows that $\ell_2 = \ell_1 + \ell_3$, and so indeed

$$\sum_{j=1}^{3} (-1)^j \ell(M_j) = -\ell_1 + (\ell_1 + \ell_3) - \ell_3 = 0\,. \tag{267}$$

Finally, for $k > 3$ it follows from the previous subsection that we have the short exact sequences

$$\begin{array}{c} 0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \mathrm{Im}(f_2) \longrightarrow 0 \ , \\ \vdots \\ 0 \longrightarrow \mathrm{Im}(f_i) \xrightarrow{\iota_{\mathrm{Im}(f_i)}} M_{i+1} \xrightarrow{f_{i+1}} \mathrm{Im}(f_{i+1}) \longrightarrow 0 \\ \vdots \\ 0 \longrightarrow \mathrm{Im}(f_{k-2}) \xrightarrow{\iota_{\mathrm{Im}(f_{k-2})}} M_{k-1} \xrightarrow{f_{k-1}} M_k \longrightarrow 0 \end{array} \tag{268}$$

where $i \in \{2, \ldots, k-3\}$ (which is considered the empty set for $k = 4$). As $\mathrm{Im}(f_j) \subseteq M_{j+1}$ for all $j \in \{2, \ldots, k-2\}$, we conclude from lemmas 2.5 and 3.29, together with Theorem 3.27, that all the modules in the short exact sequences of (268) have finite length. We may therefore use our previous find for $k = 3$, to conclude that the alternating sum of the lengths of the modules in each short exact sequence vanishes. This gives us

$$\begin{aligned} 0 &= \ell(M_1) - \ell(M_2) + \ell(\mathrm{Im}(f_2)) \\ &+ \sum_{i=2}^{k-3} (-1)^{i+1} [\ell(\mathrm{Im}(f_i)) - \ell(M_{i+1}) + \ell(\mathrm{Im}(f_{i+1}))] \\ &+ (-1)^{k-1} [\ell(\mathrm{Im}(f_{k-2})) - \ell(M_{k-1}) + \ell(M_k)] \\ &= \ell(M_1) - \ell(M_2) + \ell(\mathrm{Im}(f_2)) \\ &+ \sum_{i=2}^{k-3} (-1)^{i+1} \ell(\mathrm{Im}(f_i)) - \sum_{i=2}^{k-3} (-1)^{i+1} \ell(M_{i+1}) + \sum_{i=2}^{k-3} (-1)^{i+1} \ell(\mathrm{Im}(f_{i+1}))] \\ &+ (-1)^{k-1} [\ell(\mathrm{Im}(f_{k-2})) - \ell(M_{k-1}) + \ell(M_k)] \\ &= \ell(M_1) - \ell(M_2) - \sum_{i=2}^{k-3} (-1)^{i+1} \ell(M_{i+1}) - (-1)^{k-1} \ell(M_{k-1}) + (-1)^{k-1} \ell(M_k) \\ &+ \sum_{i=2}^{k-3} (-1)^{i+1} \ell(\mathrm{Im}(f_i)) + \sum_{i=2}^{k-3} (-1)^{i+1} \ell(\mathrm{Im}(f_{i+1}))] \\ &+ (-1)^{k-1} \ell(\mathrm{Im}(f_{k-2})) + \ell(\mathrm{Im}(f_2)) \, . \end{aligned} \tag{269}$$

We now change the summation index in the last sum of Equation (269), by

setting $j = i + 1$. This gives us

$$
\begin{aligned}
0 &= \ell(M_1) - \ell(M_2) - \sum_{i=2}^{k-3} (-1)^{i+1} \ell(M_{i+1}) \\
&\quad - (-1)^{k-1} \ell(M_{k-1}) + (-1)^{k-1} \ell(M_k) \\
&\quad + \sum_{i=2}^{k-3} (-1)^{i+1} \ell(\mathrm{Im}(f_i)) + \sum_{j=3}^{k-2} (-1)^{j} \ell(\mathrm{Im}(f_j)) \\
&\quad + (-1)^{k-1} \ell(\mathrm{Im}(f_{k-2})) + \ell(\mathrm{Im}(f_2)) \\
&= \ell(M_1) - \ell(M_2) + \sum_{i=2}^{k-3} (-1)^{i+2} \ell(M_{i+1}) + (-1)^{k} \ell(M_{k-1}) + (-1)^{k+1} \ell(M_k) \\
&\quad + \sum_{i=2}^{k-2} (-1)^{i+1} \ell(\mathrm{Im}(f_i)) + \sum_{j=2}^{k-2} (-1)^{j} \ell(\mathrm{Im}(f_j)) \\
&= \sum_{i=0}^{k-1} (-1)^{i+2} \ell(M_{i+1}) = \sum_{j=1}^{k} (-1)^{j+1} \ell(M_j) \,,
\end{aligned}
\tag{270}
$$

where in the last step we have again set $j = i+1$. This completes the proof. □

For completeness, we end this subsection with what can be seen as the main result on composition series.

Theorem 3.32 (The Jordan-Hölder theorem)**.** *Suppose we have two composition series for the module M:*

$$
\begin{aligned}
0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M \,; \\
0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_\ell = M \,.
\end{aligned}
\tag{271}
$$

Then the corresponding simple quotient modules are isomorphic, after reordering indices if necessary. That is, there exists a permutation σ of $\{1, \ldots, \ell\}$ such that

$$
M_i / M_{i-1} \cong N_{\sigma(i)} / N_{\sigma(i)-1} \ \textit{for all } i \,. \tag{272}
$$

In what follows we will make frequent use of the fact that for any proper submodule P of a module M of finite length, we have $\ell(P) < \ell(M)$. The fact that P has finite length follows from lemmas 2.5 and 3.29, combined with Theorem 3.27. Moreover, any composition series for P can be made into a larger chain of submodules by adding $P \subsetneq M$ at the end. By Theorem 3.24, this chain can be made into a composition series for M by inserting submodules if needed, which shows that indeed $\ell(P) < \ell(M)$. Alternatively, this observation was a step in the proof of Theorem 3.24.

Proof of Theorem 3.32. We prove the theorem by induction on ℓ. Note that for $\ell = 0$ we have $M = 0$ and there is nothing to prove. In case of $\ell = 1$ we clearly have

$$
M_1 / M_0 = M = N_1 / N_0 \,, \tag{273}
$$

and so the result holds true.

Now suppose we have $\ell > 1$, and assume the result holds for all lower values of ℓ. If we are in the lucky case where $M_{\ell-1} = N_{\ell-1}$, then because $\ell(M_{\ell-1}) < \ell(M)$ the inductive assumption gives us a permutation σ' of $\{1, \ldots, \ell-1\}$ such that

$$M_i/M_{i-1} \cong N_{\sigma'(i)}/N_{\sigma'(i)-1} \text{ for all } i \in \{1, \ldots, \ell-1\}\,. \tag{274}$$

Here we have used that removing M from the chains in (271) gives two composition series for $M_{\ell-1} = N_{\ell-1}$. Since $M_\ell/M_{\ell-1} = M/M_{\ell-1} = N_\ell/N_{\ell-1}$, we get the required permutation σ of $\{1, \ldots, \ell\}$ by setting $\sigma(i) = \sigma'(i)$ for all $i < \ell$ and $\sigma(\ell) = \ell$.

We therefore assume from here on out that $M_{\ell-1} \neq N_{\ell-1}$. Note that we cannot have $M_{\ell-1} \subseteq N_{\ell-1}$, as this would imply $M_{\ell-1} \subsetneq N_{\ell-1} \subsetneq M$, contradicting that the first chain in (271) is a composition series. Similarly, we cannot have $N_{\ell-1} \subseteq M_{\ell-1}$. It follows that $N_{\ell-1} \cap M_{\ell-1} \subsetneq M_{\ell-1}$, so that the quotient module $M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})$ is non-zero. Now consider the homomorphism

$$\psi : M_{\ell-1} \to M/N_{\ell-1}\,, \tag{275}$$

given by the composition of the inclusion of $M_{\ell-1}$ into M, followed by the canonical projection onto $M/N_{\ell-1}$. It is not hard to see that the kernel of ψ is exactly given by $M_{\ell-1} \cap N_{\ell-1}$. Hence by the first isomorphism theorem, we find that $M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})$ is isomorphic to a submodule of the simple module $M/N_{\ell-1}$. Because we excluded the possibility that $M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})$ is the zero-module, we conclude that instead

$$M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1}) \cong M/N_{\ell-1}\,. \tag{276}$$

In exactly the same way, we find that

$$N_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1}) \cong M/M_{\ell-1}\,. \tag{277}$$

As $N_{\ell-1} \cap M_{\ell-1}$ is a submodule of M, we may write down a composition series for it:

$$0 = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d = N_{\ell-1} \cap M_{\ell-1}\,. \tag{278}$$

In turn, we may extend this to a composition series for $M_{\ell-1}$, by setting

$$0 = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d = N_{\ell-1} \cap M_{\ell-1} \subsetneq M_{\ell-1}\,, \tag{279}$$

and likewise to one for $N_{\ell-1}$:

$$0 = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d = N_{\ell-1} \cap M_{\ell-1} \subsetneq N_{\ell-1}\,. \tag{280}$$

Note that these are indeed composition series, as $M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})$ and $N_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})$ are simple by equations (276) and (277), respectively.

As before, Equation (271) gives us composition series for $M_{\ell-1}$ and $N_{\ell-1}$ as well, by removing the M at the end. That is, we have the composition series

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{\ell-1}\,, \tag{281}$$

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{\ell-1}\,. \tag{282}$$

Hence, any composition series for $M_{\ell-1}$ or $N_{\ell-1}$ has length $\ell-1$, so that the value of d in the series (278) is equal to $\ell-2$ (for instance due to the fact that (279) is a composition series for $M_{\ell-1}$ of length $d+1$). More importantly, we may use the inductive assumption on the composition series (279) and (281) to conclude that there is a bijection between the modules in

$$\{P_1/P_0, \ldots, P_{\ell-2}/P_{\ell-3}, M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})\} \tag{283}$$

and those in

$$\{M_1/M_0, \ldots, M_{\ell-1}/M_{\ell-2}\}\,, \tag{284}$$

which sends a module to an isomorphic one. By Equation (277) this can be extended to a bijection between

$$\{P_1/P_0, \ldots, P_{\ell-2}/P_{\ell-3}, M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1}), N_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})\} \tag{285}$$

and

$$\{M_1/M_0, \ldots, M_{\ell-1}/M_{\ell-2}, M_\ell/M_{\ell-1}\}\,, \tag{286}$$

again matching modules with isomorphic ones.

In precisely the same way, using the induction hypothesis on the series (280) and (282), we conclude that such a matching exists between

$$\{P_1/P_0, \ldots, P_{\ell-2}/P_{\ell-3}, N_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})\} \tag{287}$$

and

$$\{N_1/N_0, \ldots, N_{\ell-1}/N_{\ell-2}\}\,. \tag{288}$$

Combining this observation with Equation (276), we get such a correspondence between

$$\{P_1/P_0, \ldots, P_{\ell-2}/P_{\ell-3}, N_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1}), M_{\ell-1}/(N_{\ell-1} \cap M_{\ell-1})\} \tag{289}$$

and

$$\{N_1/N_0, \ldots, N_{\ell-1}/N_{\ell-2}, N_\ell/N_{\ell-1}\}\,. \tag{290}$$

As the sets (285) and (289) agree, we see that a bijection exists between the sets (286) and (290), which sends modules to isomorphic ones. Hence, the statement of the theorem holds for ℓ as well, so that the proof follows by induction. □

3.6 Support and associated primes

We next introduce two ways of associating prime ideals to a module. The first one is:

Definition 3.33. Let M be a module over the ring R. A prime ideal $P \subseteq R$ is said to be in the *support* of M if the corresponding localization M_{P^c} is not the zero-module. We denote the set of all such primes for M by $\mathrm{Supp}(M)$. $\triangle$

The following result relates the support of a module to that of a submodule and its corresponding quotient.

Proposition 3.34. *Let N be a submodule of M. We have*

$$\mathrm{Supp}(M) = \mathrm{Supp}(N) \cup \mathrm{Supp}(M/N)\,. \tag{291}$$

Proof. Recall that we have the short exact sequence

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0\,, \tag{292}$$

where ι is the inclusion of N into M and π denotes the canonical projection onto M/N. Given a prime ideal P of R, it follows from Lemma (3.28) that we get the corresponding short exact sequence of R_{P^c} modules

$$0 \longrightarrow N_{P^c} \xrightarrow{\iota_{P^c}} M_{P^c} \xrightarrow{\pi_{P^c}} (M/N)_{P^c} \longrightarrow 0\,. \tag{293}$$

Now suppose we have $P \in \mathrm{Supp}(M)$, so that $M_{P^c} \neq 0$. As the sequence (293) is exact, we have either $N_{P^c} \neq 0$ or $(M/N)_{P^c} \neq 0$, as otherwise $M_{P^c} = 0$. See the discussion in Subsection 3.4. Hence we find $P \in \mathrm{Supp}(N) \cup \mathrm{Supp}(M/N)$.

Conversely, if $P \in \mathrm{Supp}(N) \cup \mathrm{Supp}(M/N)$ then either $N_{P^c} \neq 0$ or $(M/N)_{P^c} \neq 0$. This means the sequence (293) can only be exact if $M_{P^c} \neq 0$ and so $P \in \mathrm{Supp}(M)$, which completes the proof. $\square$

The following useful definition allows for an alternative characterization of the support of a module, in case it is finitely generated.

Definition 3.35. Given an R-module M, its *annihilator* (denoted by $\mathrm{Ann}(M)$) is the ideal of all elements in R that vanish on all of M. That is, we have

$$\mathrm{Ann}(M) = \{r \in R \mid rm = 0 \,\forall\, m \in M\}\,. \tag{294}$$

It is not hard to verify that this is indeed an ideal of R. $\triangle$

Lemma 3.36. *Given a finitely generated R-module M and a prime ideal $P \subseteq R$, we have $P \in \mathrm{Supp}(M)$ if and only if $\mathrm{Ann}(M) \subseteq P$.*

Proof. Suppose first that $P \in \mathrm{Supp}(M)$, so that $M_{P^c} \neq 0$. Let $\frac{m}{c}$ be a non-zero element of M_{P^c}, where $m \in M$ and $c \in P^c$. Suppose that $rm = 0$ for some $r \in P^c$. We note that $\frac{r}{1} \in R_{P^c}$ is a unit with inverse $\frac{1}{r}$, and so it follows that

$$0 \neq \frac{m}{c} = \frac{1}{r}\frac{r}{1}\frac{m}{c} = \frac{rm}{rc} = \frac{0}{rc} = 0\,. \tag{295}$$

This contradiction tells us that no element $r \in P^c$ can satisfy $rm = 0$, and so in particular $r \notin \mathrm{Ann}(M)$ if $r \in P^c$. In other words, we find $P^c \subseteq \mathrm{Ann}(M)^c$ and so $\mathrm{Ann}(M) \subseteq P$.

Now suppose conversely that $\mathrm{Ann}(M) \subseteq P$. It follows that $M \neq 0$, as otherwise we would have $\mathrm{Ann}(M) = R$. Let M be generated by the elements $x_1, \ldots, x_n$ for $n > 0$, and consider the corresponding elements $\frac{x_i}{1} \in M_{P^c}$ for $i \in \{1, \ldots, n\}$. If for all i we have $\frac{x_i}{1} = 0 = \frac{0}{1}$, then there exist $c_i \in P^c$ such that $c_i x_i = 0$. We define the element $c = c_1 c_2 \ldots c_n \in P^c$ and consider the set

$$N = \{x \in M \mid cx = 0\}\,. \tag{296}$$

It is clear that N is a submodule of M containing $x_1, \ldots, x_n$. Hence, we necessarily have $N = M$, and we conclude that $c \in \mathrm{Ann}(M)$. This is a contradiction though, as we have $c \in P^c$ but also $c \in \mathrm{Ann}(M) \subseteq P$. We see that at least one of the elements $\frac{x_i}{1} \in M_{P^c}$ is non-zero, from which it follows that $M_{P^c} \neq 0$. In other words, we find $P \in \mathrm{Supp}(M)$. □

Note that the first part of the proof did not use that M is finitely generated. Hence, for general modules M we have $P \in \mathrm{Supp}(M) \implies \mathrm{Ann}(M) \subseteq P$.

As an immediate consequence of Lemma 3.36, we find

Corollary 3.37. *Let M be a finitely generated module over a ring R, and suppose that $\mathrm{Ann}(M) \neq R$. It holds that*

$$\sqrt{\mathrm{Ann}(M)} = \bigcap_{P \in \mathrm{Supp}(M)} P\,. \tag{297}$$

Proof. Recall from Proposition 1.24 that

$$\sqrt{\mathrm{Ann}(M)} = \bigcap_{\substack{P \text{ prime} \\ \text{ideal,} \\ \mathrm{Ann}(M) \subseteq P}} P\,. \tag{298}$$

By Lemma 3.36, the intersection in Equation (298) is over all prime ideals in $\mathrm{Supp}(M)$, from which the result follows. □

Remark 3.38. Recall from Definition (2.1) that for any module M over a ring R we have $1m = m$ for all $m \in M$. As a consequence, we find that $\mathrm{Ann}(M) = R$ implies $m = 1m = 0$ for all $m \in M$, and so $M = 0$. Conversely, we of course have $\mathrm{Ann}(0) = R$, from which we conclude that $\mathrm{Ann}(M) = R$ if and only if $M = 0$.

Moreover, as any proper ideal is contained in a maximal ideal, we see that for a non-zero module M, there always exists at least one prime ideal P containing $\mathrm{Ann}(M)$. Combined with Lemma 3.36, we conclude that for M finitely generated and non-zero it holds that $\mathrm{Supp}(M)$ is non-empty. We may drop the condition that M is finitely generated though, as any non-zero module contains a non-zero module N that is finitely generated. Take for instance $N = Rx$ for any non-zero $x \in M$. Using Proposition 3.34, we conclude that any non-zero module has a non-empty support. △

From the easy characterization of Lemma 3.36, we see that for a finitely generated module M the following holds: if we have $P \in \mathrm{Supp}(M)$ and if Q is a prime ideal containing P, then also $Q \in \mathrm{Supp}(M)$. It turns out we may drop the condition that M is finitely generated. That is, we have:

Lemma 3.39. *Let M be a module over a ring R and let $P \in \mathrm{Supp}(M)$. If Q is a prime ideal of R satisfying $P \subseteq Q$, then also $Q \in \mathrm{Supp}(M)$.*

Proof. Suppose Q is not contained in $\mathrm{Supp}(M)$. It follows that the module M_{Q^c} is zero. In particular, for any $m \in M$ we have $\frac{m}{1} = \frac{0}{1}$ in M_{Q^c}, from which we see that an element $c_m \in Q^c$ exists such $c_m m = 0$ in M.

Now suppose we are given an element $\frac{m}{d} \in M_{P^c}$, where $d \in P^c$. From $P \subseteq Q$ it follows that $Q^c \subseteq P^c$ and so $c_m \in P^c$. We therefore find

$$\frac{m}{d} = \frac{c_m}{c_m}\frac{m}{d} = \frac{c_m m}{c_m d} = \frac{0}{c_m d} = 0\,, \tag{299}$$

from which we see that $M_{P^c} = 0$. This contradicts the fact that $P \in \mathrm{Supp}(M)$ and we conclude that likewise $Q \in \mathrm{Supp}(M)$. □

The result of Lemma 3.39 suggests we may better understand the support of a module by looking for minimal elements, if these exist. The following definition will be key to understanding such prime ideals.

Definition 3.40. Let M be a module over a ring R. Given an element $x \in M$, we define the *annihilator* of x to be the ideal

$$\mathrm{Ann}(x) := \{r \in R \mid rx = 0\}\,. \tag{300}$$

It is easy to see that $\mathrm{Ann}(x)$ is indeed an ideal of R, for instance by realizing that $\mathrm{Ann}(x) = \mathrm{Ann}(Rx)$.

An *associated prime* of M is a prime ideal $P \subseteq R$ for which it holds that $P = \mathrm{Ann}(x)$ for some $x \in M$. We denote the collection of all associated primes of M by $\mathrm{AP}(M)$. △.

Note that ideals of the form $\mathrm{Ann}(x)$ for $x \in M$ are not necessarily prime. Only those that are go into $\mathrm{AP}(M)$. The following result gives us conditions under which associated primes exist.

Lemma 3.41. *For M a non-zero module over a Noetherian ring R, the set of associated primes $\mathrm{AP}(M)$ is non-empty.*

Proof. We start by picking a non-zero element $x \in M$. As $1x = x \neq 0$, we see that $\mathrm{Ann}(x) \neq R$. Hence, either $\mathrm{Ann}(x)$ is a prime ideal, in which case we have found an element of $\mathrm{AP}(M)$ and we are done, or there exist elements $r_1, s_1 \in \mathrm{Ann}(x)^c$ such that $r_1 s_1 \in \mathrm{Ann}(x)$. In the latter case we have $r_1 s_1 x = 0$, and so $r_1 \in \mathrm{Ann}(s_1 x)$. Moreover, it holds that $r_1 \notin \mathrm{Ann}(x)$ and clearly $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(s_1 x)$. Lastly, we see that $1 s_1 x = s_1 x \neq 0$, and so $\mathrm{Ann}(s_1 x) \neq R$. Summarizing, we find

$$\mathrm{Ann}(x) \subsetneq \mathrm{Ann}(s_1 x) \subsetneq R\,. \tag{301}$$

We can perform the exact same procedure with the element $x' = s_1 x$. Again, we either find $\mathrm{Ann}(s_1 x) \in \mathrm{AP}(M)$, or we find some element $s_2 \in R$ such that

$$\mathrm{Ann}(x) \subsetneq \mathrm{Ann}(s_1 x) \subsetneq \mathrm{Ann}(s_2 x') = \mathrm{Ann}(s_2 s_1 x) \subsetneq R\,. \tag{302}$$

If this process never terminates, then we get an infinite sequence of ideals

$$\mathrm{Ann}(x) \subsetneq \mathrm{Ann}(s_1 x) \subsetneq \mathrm{Ann}(s_2 s_1 x) \subsetneq \mathrm{Ann}(s_3 s_2 s_1 x) \subsetneq \dots\,, \tag{303}$$

which contradicts our assumption that R is Noetherian. Hence, we eventually find a prime ideal in $AP(M)$, which shows that this collection is indeed non-empty. □

We now relate associated primes to the support of a module.

Lemma 3.42. *For any module M we have $\mathrm{AP}(M) \subseteq \mathrm{Supp}(M)$.*

Proof. Let P be a prime ideal in $\mathrm{AP}(M)$. It follows that there exists an $x \in M$ such that $P = \mathrm{Ann}(x)$, and we claim that for such an x the corresponding element $\frac{x}{1} \in M_{P^c}$ is different from zero. Suppose otherwise, so that $\frac{x}{1} = \frac{0}{1} \in M_{P^c}$. It follows that there exists some $c \in P^c$ such that $cx = 0$, which means we have $c \in \mathrm{Ann}(x)$. However, as it also holds that $P = \mathrm{Ann}(x)$, we find $c \in P \cap P^c$. This contradiction shows that indeed $\frac{x}{1} \neq 0$, so that $M_{P^c} \neq 0$. In other words, we find $P \in \mathrm{Supp}(M)$. □

Proposition 3.43. *Let M be a module over a Noetherian ring R. For any ideal $P \in \mathrm{Supp}(M)$, there exists a $Q \in \mathrm{AP}(M)$ such that $Q \subseteq P$.*

Proof. Recall that M_{P^c} is a module over the localized ring R_{P^c}. By assumption, we have $M_{P^c} \neq 0$. Moreover, Lemma 3.13 tells us that R_{P^c} is a Noetherian ring as well. We may therefore use Lemma 3.41 to conclude that there exists a prime ideal $\tilde{Q} \in \mathrm{AP}(M_{P^c})$. Let's say that $\tilde{Q} = \mathrm{Ann}(\frac{x}{c})$ for some $\frac{x}{c} \in M_{P^c}$, and where we have $x \in M$ and $c \in P^c$. We now make some observations about the prime ideal $\tilde{Q} \subseteq R_{P^c}$.

First, we claim that $\mathrm{Ann}(\frac{dx}{c}) = \mathrm{Ann}(\frac{x}{c}) = \tilde{Q}$ for any $d \in P^c$. This follows from the fact that $\frac{d}{1}$ is a unit in R_{P^c} for any $d \in P^c$ (with inverse $\frac{1}{d}$). In general, given a module N over some (commutative) ring S, if we have $y \in N$ and a unit $u \in S$, it follows that $\mathrm{Ann}(y) \subseteq \mathrm{Ann}(uy)$. As we also have $\mathrm{Ann}(uy) \subseteq \mathrm{Ann}(u^{-1}uy) = \mathrm{Ann}(y)$, we find $\mathrm{Ann}(y) = \mathrm{Ann}(uy)$. The claim therefore follows by setting $y = \frac{x}{c} \in M_{P^c}$ and $u = \frac{d}{1} \in R_{P^c}$.

Next, we will show that there exists some $d \in P^c$ with the property that $\mathrm{Ann}(dx) = \mathrm{Ann}(edx) \subseteq R$ for all $e \in P^c$. To this end, note that $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(ex)$ for all $e \in P^c$. If we have $\mathrm{Ann}(x) = \mathrm{Ann}(ex)$ for all $e \in P^c$ then we are done if we set $d = 1$. Otherwise, we may pick a $d_1 \in P^c$ such that $\mathrm{Ann}(x) \subsetneq \mathrm{Ann}(d_1 x)$. In the latter case, we either have $\mathrm{Ann}(d_1 x) = \mathrm{Ann}(e d_1 x)$ for all $e \in P^c$, in which case we are done, or we may pick a $d_2 \in P^c$ such that $\mathrm{Ann}(d_1 x) \subsetneq \mathrm{Ann}(d_2 d_1 x)$. This process has to terminate, as otherwise we find a chain

$$\mathrm{Ann}(x) \subsetneq \mathrm{Ann}(d_1 x) \subsetneq \mathrm{Ann}(d_2 d_1 x) \subsetneq \dots \subseteq R\,, \tag{304}$$

which would contradict the fact that R is Noetherian. We therefore find $d_1, \ldots, d_n$ such that $\mathrm{Ann}(d_n \ldots d_1 x) = \mathrm{Ann}(e d_n \ldots d_1 x)$ for all $e \in P^c$. Setting $d := d_n \ldots d_1$ then gives the required element of P^c.

For the next step, we claim that $N(\tilde{Q}) = \mathrm{Ann}(dx) \subseteq R$, with $d \in P^c$ the element we found in the previous step. To see why, note that $\tilde{Q} = \mathrm{Ann}(\frac{dx}{c})$ by our first observation. Given $r \in N(\tilde{Q})$, it follows that there exists some element $\frac{r}{f} \in \tilde{Q}$ with $f \in P^c$. Hence we have

$$\frac{r}{f}\frac{dx}{c} = \frac{rdx}{fc} = \frac{0}{1}\,. \tag{305}$$

It follows that some $e \in P^c$ exists for which $erdx = r(edx) = 0$. We thus find $r \in \mathrm{Ann}(edx) = \mathrm{Ann}(dx)$, where we have used the property of d from the previous step. This shows that $N(\tilde{Q}) \subseteq \mathrm{Ann}(dx)$.

Conversely, if $s \in \mathrm{Ann}(dx)$ then $sdx = 0$ and so

$$\frac{s}{1}\frac{dx}{c} = \frac{sdx}{c} = \frac{0}{c} = 0\,. \tag{306}$$

Therefore $\frac{s}{1} \in \mathrm{Ann}(\frac{dx}{c}) = \tilde{Q}$ and so $s \in N(\tilde{Q})$. We conclude that $\mathrm{Ann}(dx) \subseteq N(\tilde{Q})$ and so indeed $N(\tilde{Q}) = \mathrm{Ann}(dx)$.

Finally, we will show that $N(\tilde{Q})$ is a prime ideal satisfying $N(\tilde{Q}) \subseteq P$. Note that the ideal $\tilde{Q}$ is prime by assumption, as we have $\tilde{Q} \in AP(M_{P^c})$. It therefore follows from Lemma 1.23 that $N(\tilde{Q})$ is a prime ideal of R that is disjoint from P^c. This last part of course means that $N(\tilde{Q}) \subseteq P$.

To conclude, we find that $Q := N(\tilde{Q})$ is a prime ideal satisfying $Q = \mathrm{Ann}(dx)$. Hence we have $Q \in AP(M)$. As we also found that $Q \subseteq P$, the result follows. □

We next show how associated primes behave with respect to sub- and quotient modules.

Lemma 3.44. *Given a module M with submodule N, we have*

$$\mathrm{AP}(M) \subseteq \mathrm{AP}(N) \cup \mathrm{AP}(M/N)\,. \tag{307}$$

Proof. Let $P \in \mathrm{AP}(M)$ be given, and let $x \in M$ be such that $P = \mathrm{Ann}(x)$. We distinguish two cases: either there exists a $c \in P^c$ such that $cx \in N$, or there is no such element in P^c.

In the first case, we pick such an element c for which $cx \in N$. We claim that $\mathrm{Ann}(cx) = \mathrm{Ann}(x) = P$. To see why, note that $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(cx)$. Conversely, if $r \in \mathrm{Ann}(cx)$ then $rcx = 0$ and so $rc \in \mathrm{Ann}(x) = P$. As P is prime, we either have $r \in P$ or $c \in P$. The last option does not hold by assumption, and so we have $r \in P = \mathrm{Ann}(x)$. We therefore find $\mathrm{Ann}(cx) \subseteq \mathrm{Ann}(x)$ and so $\mathrm{Ann}(cx) = \mathrm{Ann}(x) = P$. Since $cx \in N$, we conclude that $P \in \mathrm{AP}(N)$.

In the second case, we have $cx \notin N$ for all $c \in P^c$. Consider the element $[x] \in M/N$. If $rx = 0$ then clearly $r[x] = [rx] = 0$, and so $\mathrm{Ann}(x) \subseteq \mathrm{Ann}([x])$. On the other hand, if $r \in \mathrm{Ann}([x])$ then $rx \in N$. By assumption, this means we

have $r \notin P^c$ and so $r \in P = \mathrm{Ann}(x)$. We conclude that $\mathrm{Ann}([x]) \subseteq \mathrm{Ann}(x)$ and so $\mathrm{Ann}([x]) = \mathrm{Ann}(x) = P$. This shows that $P \in \mathrm{AP}(M/N)$, which completes the proof. □

We will also make use of the following result.

Lemma 3.45. *Let R be a ring and P a prime ideal of R. If we view R/P as a module over R, then $\mathrm{AP}(R/P) = \{P\}$.*

Proof. Let $r \in R$ and consider the corresponding class $[r] \in R/P$. If we have $r \in P$ then $[r] = 0$ and so $\mathrm{Ann}([r]) = R$. Suppose therefore that $r \notin P$. Given $s \in \mathrm{Ann}([r])$, we see that $s[r] = [sr] = 0$ and so $sr \in P$. As P is prime and since $r \notin P$, we find $s \in P$. This shows that $\mathrm{Ann}([r]) \subseteq P$. Of course for any $p \in P$ we have $p[r] = [pr] = 0$, and so $P = \mathrm{Ann}([r])$. As $P \subsetneq R$ (that is, elements in $R \setminus P$ exist), we indeed find $\mathrm{AP}(R/P) = \{P\}$. □

We next present a very useful result on the structure of finitely generated modules over Noetherian rings. It will also have a surprising consequence for the number of associated primes for such modules.

Proposition 3.46. *Let M be a finitely generated module over a Noetherian ring R. There exist finitely many elements $x_1, \ldots, x_n \in M$ along with prime ideals $P_1, \ldots, P_n \subseteq R$ such that M is generated by $x_1, \ldots, x_n$, and*

$$\langle x_1 \rangle \cong R/P_1\,, \quad \frac{\langle x_1, \ldots, x_i \rangle}{\langle x_1, \ldots, x_{i-1} \rangle} \cong R/P_i \tag{308}$$

for all $i \in \{2, \ldots, n\}$, as modules over R. Here $\langle x_1, \ldots, x_j \rangle$ denotes the submodule of M generated by $x_1, \ldots, x_j$.

In particular, we have a chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M \tag{309}$$

such that

$$M_i/M_{i-1} \cong R/P_i \;\text{ for all }\; i \in \{1, \ldots, n\}\,, \tag{310}$$

for some prime ideals $P_1, \ldots, P_n$. Whenever equations (309) *and* (310) *hold for some (finite number of) submodules M_i and prime ideals P_i, we have*

$$\mathrm{AP}(M) \subseteq \{P_1, \ldots, P_n\} \subseteq \mathrm{Supp}(M)\,. \tag{311}$$

Note that Proposition 3.46 tells us that any finitely generated module over a Noetherian ring has only finitely many associated primes.

Proof of Proposition 3.46. Note that for $M = 0$ we can take $n = 0$. In that case the three sets of prime ideals in Equation (311) are all empty. We therefore assume from here on out that $M \neq 0$.

We start by constructing the elements $x_1, \ldots, x_n$, one at a time. As R is Noetherian, it follows from Lemma 3.41 that M has some associated prime P_1. Let $x_1 \in M$ be such that $P_1 = \mathrm{Ann}(x_1)$, and consider the map $\psi_{x_1} \colon R \to M$

given by $r \mapsto rx_1$. It is not hard to see that ψ_{x_1} is a homomorphism of R-modules, and that its image is $\langle x_1 \rangle$. The kernel of ψ_{x_1} is given by precisely those elements $r \in R$ for which $rx_1 = 0$. That is, we have $\mathrm{Ker}(\psi_{x_1}) = \mathrm{Ann}(x_1) = P_1$. It follows by the first isomorphism theorem for modules that $R/P_1 \cong \langle x_1 \rangle$.

Now suppose we have found elements $x_1, \ldots, x_j \in M$ with $j \geq 1$ such that Equation (308) holds for all $i \in \{2, \ldots, j\}$ and for some prime ideals $P_1, \ldots, P_j$. If M is generated by $x_1, \ldots, x_j$ then we are done with finding the elements $x_1, \ldots, x_n$ of the proposition. Otherwise, the quotient module $M/\langle x_1, \ldots, x_j \rangle$ is non-zero. In this last case, it follows again from Lemma 3.41 that $M/\langle x_1, \ldots, x_j \rangle$ has an associated prime $P_{j+1} \subseteq R$. Let $x_{j+1} \in M$ be such that $P_{j+1} = \mathrm{Ann}([x_{j+1}])$, where $[x_{j+1}]$ denotes the class of x_{j+1} in $M/\langle x_1, \ldots, x_j \rangle$. We claim that

$$R/P_{j+1} \cong \frac{\langle x_1, \ldots, x_{j+1} \rangle}{\langle x_1, \ldots, x_j \rangle} \tag{312}$$

as modules over R. To this end, consider the map $\psi_{x_{j+1}} \colon R \to M/\langle x_1, \ldots, x_j \rangle$ given by $r \mapsto r[x_{j+1}]$. Precisely as before, the kernel of this map is given by $\mathrm{Ann}([x_{j+1}]) = P_{j+1}$, and its image is the submodule of $M/\langle x_1, \ldots, x_j \rangle$ generated by $[x_{j+1}]$, which we denote by $\langle [x_{j+1}] \rangle$. The first isomorphism theorem for modules therefore gives us

$$R/P_{j+1} \cong \langle [x_{j+1}] \rangle \,. \tag{313}$$

On the other hand, we may view $\langle x_1, \ldots, x_{j+1} \rangle / \langle x_1, \ldots, x_j \rangle$ as a submodule of $M/\langle x_1, \ldots, x_j \rangle$. As such, $\langle x_1, \ldots, x_{j+1} \rangle / \langle x_1, \ldots, x_j \rangle$ clearly contains the element $[x_{j+1}]$ and so $\langle [x_{j+1}] \rangle \subseteq \langle x_1, \ldots, x_{j+1} \rangle / \langle x_1, \ldots, x_j \rangle$. Conversely, any element $y \in \langle x_1, \ldots, x_{j+1} \rangle / \langle x_1, \ldots, x_j \rangle$ may be written as

$$y = \left[\sum_{i=1}^{j+1} r_i x_i \right] = [r_{j+1} x_{j+1}] = r_{j+1}[x_{j+1}] \tag{314}$$

for some $r_1, \ldots, r_{j+1} \in R$. We see that $y \in \langle [x_{j+1}] \rangle$ and we conclude that $\langle [x_{j+1}] \rangle = \langle x_1, \ldots, x_{j+1} \rangle / \langle x_1, \ldots, x_j \rangle$. Hence, Equation (312) follows from Equation (313).

If this process never ends, i.e. if at no point M is generated by the x_i we found thus far, then we get an infinite chain of submodules

$$\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \cdots \subseteq M \,. \tag{315}$$

The strict inclusions follow from the fact that the quotient of two subsequent modules is always isomorphic to a module R/P_i, which has more than one element. However, as M is finitely generated over the Noetherian ring R, it follows from Proposition 2.7 that M is a Noetherian module. This contradicts the infinite chain (315) that we found, and we conclude that the aforementioned process has to terminate eventually. In other words, at some point we find $M = \langle x_1, \ldots, x_n \rangle$.

By setting $M_0 = 0$ and $M_i = \langle x_1, \ldots, x_i \rangle$ for all $i \in \{1, \ldots, n\}$, we obtain a chain of submodules as in (309) with the property (310).

Now suppose we have any chain of submodules as in (309) such that (310) holds for some prime ideals $P_1, \ldots, P_n$. We first show that each P_i is contained in $\mathrm{Supp}(M)$. To this end, note that $\mathrm{Ann}(M) \subseteq \mathrm{Ann}(M_i)$ for all $i \in \{1, \ldots, n\}$. After all, given $r \in R$, if $rx = 0$ for all $x \in M$ then in particular $rx = 0$ for all $x \in M_i$. Likewise, if $rx = 0$ for all $x \in M_i$ then in particular $rx \in M_{i-1}$, and so

$$\mathrm{Ann}(M) \subseteq \mathrm{Ann}(M_i) \subseteq \mathrm{Ann}(M_i/M_{i-1})\,. \tag{316}$$

Now, as M_i/M_{i-1} and R/P_i are isomorphic as modules over R, we have $\mathrm{Ann}(M_i/M_{i-1}) = \mathrm{Ann}(R/P_i)$. It clearly holds that $P_i \subseteq \mathrm{Ann}(R/P_i)$. Conversely, if we have $r \in \mathrm{Ann}(R/P_i)$ then $r[1] = [r] = 0$, where $[1]$ denotes the class of 1 in R/P_i. This shows that $r \in P_i$ and so $P_i = \mathrm{Ann}(R/P_i)$. Together with Equation (316) and our observation that $\mathrm{Ann}(M_i/M_{i-1}) = \mathrm{Ann}(R/P_i)$, we conclude that

$$\mathrm{Ann}(M) \subseteq P_i\,. \tag{317}$$

Since M is finitely generated, we may use Lemma 3.36 to conclude that indeed $P_i \in \mathrm{Supp}(M)$.

It remains to show that $\mathrm{AP}(M) \subseteq \{P_1, \ldots, P_n\}$. Using Lemma 3.45, we see that $\mathrm{AP}(M/M_{n-1}) = \mathrm{AP}(R/P_n) = \{P_n\}$. Moreover, it follows from Lemma 3.44 that

$$\mathrm{AP}(M) \subseteq \mathrm{AP}(M_{n-1}) \cup \mathrm{AP}(M/M_{n-1}) = \mathrm{AP}(M_{n-1}) \cup \{P_n\}\,. \tag{318}$$

In exactly the same way, we find for all $i \in \{1, \ldots, n-1\}$ that

$$\mathrm{AP}(M_i) \subseteq \mathrm{AP}(M_{i-1}) \cup \mathrm{AP}(M_i/M_{i-1}) = \mathrm{AP}(M_{i-1}) \cup \{P_i\}\,. \tag{319}$$

Combining these observations, and using that $\mathrm{AP}(M_0) = \mathrm{AP}(0) = \emptyset$, we find

$$\begin{aligned} \mathrm{AP}(M) &\subseteq \mathrm{AP}(M_{n-1}) \cup \{P_n\} \subseteq \mathrm{AP}(M_{n-2}) \cup \{P_{n-1}, P_n\} \subseteq \ldots \\ &\subseteq \mathrm{AP}(M_0) \cup \{P_1, \ldots, P_n\} = \{P_1, \ldots, P_n\}\,. \end{aligned} \tag{320}$$

This completes the proof. □

As a result, we obtain:

Corollary 3.47. *Let M be a non-zero, finitely generated module over a Noetherian ring R, and suppose we have submodules $M_0, \ldots, M_n \subseteq M$ and prime ideals $P_1, \ldots, P_n \subseteq R$ satisfying*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M \tag{321}$$

and

$$M_i/M_{i-1} \cong R/P_i \;\text{ for all }\; i \in \{1, \ldots, n\}\,. \tag{322}$$

It holds that

$$\sqrt{\mathrm{Ann}(M)} = \bigcap_{P \in \mathrm{Supp}(M)} P = \bigcap_{i=1}^{n} P_i = \bigcap_{P \in \mathrm{AP}(M)} P\,. \tag{323}$$

Proof. Recall from Remark 3.38 that $\mathrm{Ann}(M) \neq R$ as $M \neq 0$. Moreover, as M is finitely generated, the first equality in Equation (323) follows directly from Corollary 3.37. Next, using Equation (311) in Proposition 3.46, we conclude that

$$\bigcap_{P \in \mathrm{Supp}(M)} P \subseteq \bigcap_{i=1}^{n} P_i \subseteq \bigcap_{P \in \mathrm{AP}(M)} P \,. \tag{324}$$

Now, from Proposition 3.43 we know that any prime ideal in the support of M contains an associated prime. Hence, we find

$$\bigcap_{P \in \mathrm{AP}(M)} P \quad \subseteq \quad \bigcap_{P \in \mathrm{Supp}(M)} P \,. \tag{325}$$

We conclude that the two inclusions in Equation (324) are in fact equalities, from which the result of the corollary follows. □

Note that Corollary 3.47 still holds for the zero module, if we define the intersection of an empty set of prime ideals to be the full ring R.

4 References

[1] Hartshorne, R. (2013) *Algebraic geometry* (Vol. 52). Springer Science & Business Media

[2] Robert B. Ash (2006) *A Course In Commutative Algebra*, https://faculty.math.illinois.edu/ r-ash/ComAlg.html

[3] Alex Wright, *Transcendence Degree*, http://www-personal.umich.edu/ alexmw/TranscDeg.pdf

[4] David Easdown, *Composition Series*, https://www.maths.usyd.edu.au/u/de/AGR/CommutativeAlgebra/pp768-805.pdf