Computing primary decompositions of ideals

Odina, Anton

Computing primary decompositions of ideals

Anton Odina

odinaanton0@gmail.com

Bachelor thesis

July 16, 2024

Thesis supervisor: prof. dr. R.M. van Luijk

Leiden University
Mathematical Institute

Contents

Acknowledgement

I want to sincerely thank my supervisor for pointing out various different proofs of some results in this thesis, for encouraging me to think about geometrical aspects of some results and for showing me that examples are indispensable for a mathematician.

1 Introduction

This thesis consists of two main parts. In the first part we delve into the theory of primary decompositions of submodules of a given module over a commutative ring. In the second part we explore how we can explicitly calculate primary decompositions of ideals in polynomial rings over a field that satisfies some conditions.

The first part can be found in Section 2. We will briefly elaborate on the content of this section. Let R be a commutative ring and M an R-module. For an ideal $J \subset R$, we call the set

$$\sqrt{J} := \{r \in R : r^n \in J \text{ for some integer } n \geq 1\}$$

the *radical* of J. The radical of J is an ideal in R by the commutativity of R.

For any $m \in M$ we define $\text{ann}_R(m) := \{r \in R : r \cdot m = 0\}$. We also define $\text{ann}_R(M) := \bigcap_{m \in M} \text{ann}_R(m)$. If the base ring of the module is clear, we also write $\text{ann}(M)$ or $\text{ann}(m)$ instead of $\text{ann}_R(M)$ or $\text{ann}_R(m)$. Note that $\text{ann}(m)$ is an ideal in R by the commutativity of R, and therefore so is $\text{ann}(M)$.

Furthermore, a prime ideal $P \subset R$ is called an *associated prime ideal* of M if there exists an element $m \in M$ such that $P = \text{ann}(m)$. We denote the set of associated prime ideals of M by $\text{Ass}_R(M)$ or $\text{Ass}(M)$ if the base ring R is clear from the context. This set is called the *assassinator* of M.

A submodule $N \subset M$ is called *primary* if $N \neq M$ and for all $r \in R$ and $m \in M$ it holds that: if $r \cdot m \in N$ and $m \notin N$, then $r^k \cdot M \subset N$ for some integer $k \geq 1$. If in addition R is a Noetherian ring, i.e., every ideal in R is finitely generated, and M is a finitely generated R-module, then we can reformulate this definition. This is the content of Theorem 1.1.

Theorem 1.1. *Let R be a Noetherian ring, M a finitely generated R-module and let $N \subsetneq M$ be a submodule. Then N is a primary submodule of M if and only if M/N has exactly one associated prime ideal. In this case, $P_N := \sqrt{\text{ann}(M/N)}$ is the associated prime ideal of M/N, and we say that N is a P_N-primary submodule of M.*

To be more precise, the assumption that M is finitely generated can be left out for the implication from left to right. The main difficulty is proving the converse. In the first three Subsections 2.1, 2.2 and 2.3 we collect the necessary tools for a proof of Theorem 1.1. In Subsection 2.4 we will prove this theorem.

Now, suppose that R is a Noetherian ring. Then a *minimal primary decomposition* of a submodule $N \subset M$ is a finite expression $N = \bigcap_{i=1}^{l} N_i$ such that for each $1 \leq i \leq l$ we have that $N_i \subset M$ is a primary submodule, where say we have that $\text{Ass}(M/N_i) = \{P_i\}$ for some prime ideal $P_i \subset R$ using Theorem 1.1, and such that for any $1 \leq j \leq l$ we have that $N \neq \bigcap_{i \neq j} N_i$ and for all $t \neq r$ it holds that $P_t \neq P_r$.

In Section 2, we will exhibit several results on minimal primary decompositions of submodules. To be more precise, we will first concern ourselves with the existence of minimal primary decompositions of submodules. In fact, Theorem 1.2 tells us under which conditions the existence of minimal primary decompositions is guaranteed. In the last subsection of Section 2 we will prove Theorem 1.2 using Theorem 1.1.

Theorem 1.2. *Let R be a Noetherian ring and let M be a finitely generated R-module. Then any submodule $N \subset M$ has a minimal primary decomposition.*

Additionally, we will exhibit two results on the uniqueness of minimal primary decompositions. These results are often referred to in the literature as the first and second uniqueness theorem on primary decompositions. The first uniqueness theorem is Theorem 1.3.

Theorem 1.3. *Let R be a Noetherian ring and let M be an R-module. Suppose that $N \subset M$ is a submodule that has a minimal primary decomposition $N = \bigcap_{i=1}^{l} N_i$, where say for each $1 \leq i \leq l$ we have that $\text{Ass}(M/N_i) = \{P_i\}$ for some prime ideal $P_i \subset R$. Then we have that $\text{Ass}(M/N) = \{P_1, ..., P_l\}$.*

In fact, in Subsection 2.5 we will see that the assumption that the submodules $N_1, ..., N_l$ are primary can be omitted, see also Theorem 2.62. The second uniqueness theorem is Theorem 1.4.

Theorem 1.4. *Let R be a Noetherian ring, M an R-module and let $N \subset M$ be a submodule that has a minimal primary decomposition $N = \bigcap_{i=1}^{l} N_i$, where say for each $1 \leq i \leq l$ we have that $\text{Ass}(M/N_i) = \{P_i\}$ for some prime ideal $P_i \subset R$. Suppose that $P_t \in \text{Ass}(M/N)$ is a minimal element. Then the P_t-primary component N_t of N is uniquely determined by N.*

We refer for a more precise version of the latter theorem to Theorem 2.64. Throughout Section 2, we will make use of localisation of rings and modules. In Appendix A we summarise some constructions and results on this subject.

The second part of this thesis can be found in Section 3. We will exhibit a special case of the algorithm for computing primary decompositions presented in the paper [GTZ88].

To be more precise, let k be a field and let n be a positive integer. Moreover, let us define $\mathbf{x} := \{x_1, ..., x_n\}$ and $k[\mathbf{x}] := k[x_1, ..., x_n]$. The polynomial ring $k[\mathbf{x}]$ is a Noetherian ring, as we will see in Subsection 2.1, see also Theorem 2.6. Therefore, if we consider $k[\mathbf{x}]$ as a module over itself, then it follows from Theorem 1.2 that any submodule of $k[\mathbf{x}]$ has a minimal primary decomposition. Notice that the $k[\mathbf{x}]$-submodules of $k[\mathbf{x}]$ are precisely the ideals of $k[\mathbf{x}]$. Therefore, we conclude that any ideal of $k[\mathbf{x}]$ has a minimal primary decomposition.

In Section 3, we will demonstrate how the algorithm presented in the paper [GTZ88] for ideals in $k[\mathbf{x}]$ works, under some additional conditions on the field k, see the algorithm `PrimaryDecomp` for the exact conditions. For example, any algebraic number field, i.e., any finite extension of $\mathbf{Q}$, will satisfy these conditions, as we will explain in Subsection 3.6, see also Remark 3.50. Moreover, we will explain in Subsection 3.6 how we can computationally make a primary decomposition of an ideal in $k[\mathbf{x}]$ minimal, see also Remark 3.49.

We will now briefly elaborate on the approach of the algorithm. For this purpose, we will define the dimension of an ideal in $k[\mathbf{x}]$. Let $J \subset k[\mathbf{x}]$ be an ideal. We define the *dimension* of the ideal J, which we will denote by $\dim(J)$, to be

$$\dim(J) := \max\Big\{\#\mathbf{u} : \mathbf{u} \subset \mathbf{x} \text{ such that } J \cap k[\mathbf{u}] = (0)\Big\},$$

where we additionally define $\dim(k[\mathbf{x}]) := -1$. The main idea of the procedure is to reduce the problem to that of computing primary decompositions of zero-dimensional ideals. In Subsection 3.6 we will elaborate on this reduction. In fact, we will in turn reduce the problem even further. We will see in Subsection 3.5 that, in order to calculate a primary decomposition of a zero-dimensional ideal $J \subset k[\mathbf{x}]$, it suffices to compute a primary decomposition of $\sqrt{J}$. The book [BW98] introduces the algorithm for computing minimal primary decompositions of zero-dimensional ideals right along the algorithm for the case of zero-dimensional radical ideals. We have split up these two cases.

In Subsection 3.4, we will show how we can compute a primary decomposition of $\sqrt{J}$, which in essence breaks down to the factorisation of squarefree univariate polynomials with coefficients in k. Moreover, we also need a computational way of finding generators of $\sqrt{J}$, which we will explain in Subsection 3.3.

Furthermore, in Subsection 3.1 we will introduce some terminology and recall a result in the theory of Gröbner bases, and in Subsection 3.2 we will give a useful characterisation of zero-dimensional ideals.

2 Existence and uniqueness of primary decompositions

In this section, we will only consider commutative rings and modules over commutative rings. We will follow Section 6 of Chapter 2 in [Mat89] throughout this section. We will state any alterations of the results and their proofs in this book.

We now introduce some convenient notation, which we will use throughout this thesis. Let R and S be commutative rings and let $f\colon R \to S$ be a ring homomorphism. For an ideal $J \subset S$ we call the ideal $f^{-1}(J)$ *the contraction of* J with respect to f, and we denote this ideal by J^{c}. Also, for an ideal $I \subset R$ we call the ideal $(f(I)) \subset S$ *the extension of* I with respect to f, and we denote this ideal by I^{e}.

Moreover, we denote the contraction of the ideal I^{e} with respect to f and the extension of the ideal J^{c} with respect to f by I^{ec} and J^{ce} respectively.

2.1 Noetherian modules and rings

An important notion in the theory of primary decompositions of submodules is that of a *Noetherian* module. We will define this notion and state some fundamental results about Noetherian modules.

Definition 2.1. An R-module M over a commutative ring R is called *Noetherian* if any non-empty set of submodules of M has a maximal element with respect to inclusion.

There are also other equivalent formulations of a Noetherian module which are often useful.

Proposition 2.2. *Let M be an R-module. Then following are equivalent:*

(1) M is Noetherian.

(2) Any ascending chain $N_1 \subset N_2 \subset N_3 \subset ...$ of submodules of M stabilises after finitely many steps, i.e., there exists an integer $k \geq 1$ such that $N_k = N_l$ for all integers $l \geq k$.

(3) Every submodule of M is finitely generated over R.

Proof. For the proof, see [Con, Theorem 1.7, p. 2]. □

Similarly, we have the notion of a *Noetherian* ring which we define as follows.

Definition 2.3. A commutative ring R is called *Noetherian* if it is a Noetherian R-module with the natural scalar multiplication.

Remark 2.4. Note that if we see R as an R-module with the natural scalar multiplication, then the submodules of R are exactly the ideals in R. Therefore, in this case the equivalent statements in Proposition 2.2 are for ideals in R.

Example 2.5. Any principal ideal domain R is a Noetherian ring as any ideal in R is finitely generated.

For a given Noetherian ring R we can also make new Noetherian rings, namely polynomial rings over R.

Theorem 2.6 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then $R[x]$ is also a Noetherian ring.*

Proof. For the proof of the statement, see [Lan02, Theorem 4.1, p. 186]. □

As a consequence of Theorem 2.6 we now also know, by means of induction on n, that in fact $R[x_1, ..., x_n]$ is a Noetherian ring if R is a Noetherian ring.

Corollary 2.7. *Let R be a Noetherian ring and $n \geq 1$ an integer. Then $R[x_1, ..., x_n]$ is a Noetherian ring.*

Nonexamples 2.8. For a non-zero commutative ring R the polynomial ring with infinitely many variables $R[x_1, x_2, x_3, ...]$, where for all $i \neq j$ we have that $x_i \neq x_j$, is not a Noetherian ring, because we have the ascending chain $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset ...$ which does not stabilise.

Furthermore, $\mathbf{Q}$ seen as a $\mathbf{Z}$-module is not a Noetherian module, because, for instance, we have the ascending chain $(7^{-1}) \subset (7^{-2}) \subset (7^{-3}) \subset ...$ which also does not stabilise.

There are fundamental results about Noetherian modules which will be of great importance to us. We state these results now.

Lemma 2.9. *If M is a Noetherian R-module, then for any submodule $N \subset M$ the quotient R-module M/N is also Noetherian.*

Proof. By Proposition 2.2 it suffices to check whether every submodule of M/N is finitely generated over R. Every submodule of M/N is of the form L/N for some submodule $L \subset M$ containing N. As M is Noetherian, L is finitely generated over R. Hence, L/N is also finitely generated over R. □

Lemma 2.10. *Let $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ be a short exact sequence of R-modules. If L and N are Noetherian, then M is also Noetherian.*

Proof. For the proof, see [Mat89, Theorem 3.1 (ii), p. 15]. □

Corollary 2.11. *Let $l \geq 1$ be an integer. If $M_1, ..., M_l$ are Noetherian R-modules, then $\bigoplus_{i=1}^{l} M_i$ is also a Noetherian R-module.*

Proof. It suffices to prove this statement for $l = 2$, as we can then proceed to prove the statement by induction on l. In order to deduce that $M_1 \oplus M_2$ is Noetherian if M_1 and M_2 are Noetherian, we apply Lemma 2.10 to the short exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$. □

The following result establishes a relation between a Noetherian R-module M and a Noetherian ring R.

Theorem 2.12. *If M is a finitely generated R-module over a Noetherian ring R, then M is a Noetherian R-module.*

Proof. Say M is generated over R by $m_1, ..., m_k \in M$ where $k \geq 1$ is an integer. Consider then the surjective R-linear map $\varphi\colon R^k \to M$ defined by $\varphi((r_1, ..., r_k)) := \sum_{i=1}^{k} r_i \cdot m_i$. We know by the first isomorphism theorem for R-modules that $R^k/\ker(\varphi) \cong_R M$. Furthermore, R^k is a Noetherian R-module by Corollary 2.11, as R is a Noetherian ring by assumption. Thus, it follows from Lemma 2.9 that the quotient $R^k/\ker(\varphi)$ is a Noetherian R-module. We conclude that M is Noetherian. □

2.2 Noetherian topological spaces and Zariski topology on spectrum of rings

To be able to formulate what we will show in this subsection we will first define and recall some terminology from commutative algebra and algebraic geometry.

Let R be a commutative ring. The *spectrum* of R is the set of prime ideals in R, which we will denote by $\mathrm{Spec}(R)$. In fact, we can endow the set $\mathrm{Spec}(R)$ with a topology. In order to do this, we define for any ideal $J \subset R$ the subset $V(J) := \{P \in \mathrm{Spec}(R) : J \subset P\}$. Lemma 2.13 tells us that we can define the closed subsets of $\mathrm{Spec}(R)$ to be the subsets of the form $V(J)$ for an ideal $J \subset R$. This topology on $\mathrm{Spec}(R)$ is called the *Zariski topology*. We now state and prove this lemma.

Lemma 2.13. *Let R be a commutative ring. Then the following hold:*

(1) For any two ideals $J_1, J_2 \subset R$ we have that $V(J_1) \cup V(J_2) = V(J_1 \cap J_2)$.

(2) For any set of ideals $\{I_\alpha\}_\alpha$ of R it holds that $\bigcap_\alpha V(J_\alpha) = V\left(\sum_\alpha J_\alpha\right)$.

Proof. We only show (1), because (2) is clear. The inclusion $V(J_1) \cup V(J_2) \subset V(J_1 \cap J_2)$ is clear. As for the other inclusion, if P is a prime ideal of R such that $J_1 \cap J_2 \subset P$, then either J_1 or J_2 is contained in P, because if there is an element $r \in J_1$ such that $r \notin P$, then for any element $s \in J_2$ we have that $r \cdot s \in J_1 \cdot J_2 \subset J_1 \cap J_2 \subset P$. By the primality of P we know then that $s \in P$. □

Next, we will define the notion of an *irreducible* topological space and *irreducible component* of a topological space.

Definition 2.14. A topological space X is called *irreducible* if $X \neq \varnothing$ and X cannot be written as an union of two proper closed subspaces. Otherwise, we say that X is *reducible*. A subspace $Y \subset X$ is called irreducible if it is irreducible in the subspace topology.

Definition 2.15. Let X be a topological space and $Y \subset X$ a subspace. Then Y is called an *irreducible component* of X if it is maximal with respect to inclusion among irreducible subspaces of X.

The main result in this subsection is Theorem 2.16, and we now state this result. This theorem is crucial for the proof of Theorem 2.35 in Subsection 2.3. Theorem 2.16 is implicitly used in the proof of Theorem 6.5 (ii) & (iii) in [Mat89, p. 39], of which the content is the same as that of Theorem 2.35. We fill this gap in the proof of Theorem 6.5 (ii) & (iii) by proving Theorem 2.16.

Theorem 2.16. *Let R be a Noetherian ring and $C \subset \mathrm{Spec}(R)$ a non-empty closed subspace. Then there exists a finite and unique set of prime ideals $\{P_1, ..., P_m\}$ such that $C = \bigcup_{i=1}^{m} V(P_i)$. In fact, the closed subspaces $V(P_1), ..., V(P_m)$ are the irreducible components of C, and the prime ideals $P_1, ..., P_m$ are exactly the minimal prime ideals in C with respect to inclusion.*

Now, in the remainder of this subsection we will proceed to prove Theorem 2.16. We will prove this theorem using Proposition 2.18 and Proposition 2.25. The first proposition that we will formulate is Proposition 2.18, and this result states that in a topological space which satisfies a condition that will be apparent in this proposition any non-empty closed subspace can be written as a finite union of irreducible closed subspaces.

Furthermore, in Proposition 2.25 we will establish, for an arbitrary commutative ring R, a natural bijection between $\mathrm{Spec}(R)$ and the set of irreducible closed subspaces of $\mathrm{Spec}(R)$.

Definition 2.17. A topological space X is called *Noetherian* if the closed subspaces in X satisfy the descending chain condition, i.e., for any descending chain $C_1 \supset C_2 \supset C_3 \supset ...$ of closed sets in X there exists an integer $n \geq 1$ such that for all $m \geq n$ we have that $C_n = C_m$.

We now state Proposition 2.18 without proof.

Proposition 2.18. *Let X be a Noetherian topological space and $Y \subset X$ a non-empty closed subspace. Then Y can be written uniquely as a union $Y = \bigcup_{i=1}^{m} Y_i$ of irreducible closed subspaces $Y_i \subset Y$, where for $i \neq j$ we have that $Y_i \not\subset Y_j$.*

Proof. For the proof, see [Har77, Proposition 1.5, p. 5]. □

Remark 2.19. Let X and Y be as in Proposition 2.18 and write $Y = \bigcup_{i=1}^{m} Y_i$ as in Proposition 2.18. Then the irreducible closed subspaces $Y_i \subset Y$ are irreducible components of Y. On the other hand, any irreducible component of Y is equal to one of the subspaces Y_i. Therefore, the set of irreducible closed subspaces $\{Y_1, ..., Y_m\}$ is equal to the set of irreducible components of Y.

Next, we will state and prove Proposition 2.25. We will prove this proposition using Lemma 2.23, for which we will recall some terminology in commutative algebra. Let R be a commutative ring and let $J \subset R$ be an ideal. If $\sqrt{J} = J$, then we say that J is a *radical ideal*. One easily sees that the radical of any ideal is a radical ideal. Furthermore, an element $r \in R$ is called *nilpotent* if there exists an integer $k \geq 1$ such that $r^k = 0 \in R$. The set of nilpotent elements of a ring R is denoted by $\mathrm{nil}(R)$ and is called the *nilradical* of R.

Remark 2.20. We can also characterise radical ideals as follows. An ideal $J \subset R$ is radical if and only if R/J has no non-zero nilpotent elements, i.e., $\mathrm{nil}(R/J) = (0)$. A ring, not necessarily commutative, that has no non-zero nilpotent elements is called a *reduced ring*.

The nilradical of an ideal is in fact an ideal of R as the following result shows, because an arbitrary intersection of ideals is an ideal in a commutative ring.

Proposition 2.21. *Let R be commutative ring. Then we have that* $\mathrm{nil}(R) = \bigcap_{P \in \mathrm{Spec}(R)} P$.

Proof. For the proof, see [AM69, Proposition 1.8, p. 5]. □

Remark 2.22. Let R be a commutative ring and let $J \subset R$ be an ideal. Recall the notation for contracting and extending ideals with respect to a ring homomorphism defined in the introductory text at the beginning of Section 2. Then the reader readily verifies that $\mathrm{nil}(R/J)^{\mathrm{c}} = \sqrt{J}$, where we take the contraction with respect to the quotient map $\pi \colon R \to R/J$.

Lemma 2.23. *Let R be a commutative ring and let $J \subset R$ be an ideal. Then we have that $\sqrt{J} = \bigcap_{P \in V(J)} P$.*

Proof. By Remark 2.22 it holds that $\sqrt{J} = \mathrm{nil}(R/J)^{\mathrm{c}}$, where we take the contraction with respect to the quotient map $\pi \colon R \to R/J$. Furthermore, by Proposition 2.21 it follows that

$$\mathrm{nil}(R/J)^{\mathrm{c}} = \bigcap_{P \in \mathrm{Spec}(R/J)} P^{\mathrm{c}}.$$

On the other hand, we have a natural bijection between $\mathrm{Spec}(R/J)$ and $V(J)$, given by mapping a prime ideal P in $\mathrm{Spec}(R/J)$ to the prime ideal P^{c} in $V(J)$, where we contract the ideal P with respect to π. The statement follows. □

Remark 2.24. Let R be a commutative ring and set $\mathscr{J} := \{J : J \subset R \text{ ideal}\}$. We define for any subset $A \subset \operatorname{Spec}(R)$ the ideal $I(A) := \bigcap_{P \in A} P$. We have the following well-defined mappings

$$\begin{aligned} \mathscr{J} &\longleftrightarrow \{A \subset \operatorname{Spec}(R)\} \\ J &\longmapsto V(J) \\ I(A) &\longleftarrow\!\shortmid A, \end{aligned}$$

which are both inclusion reversing.

Next, we will state and prove Proposition 2.25. This is Exercise 4.10 in [Mat89, Paragraph 4, p. 29].

Proposition 2.25. *Let R be a commutative ring. Then the mappings in Remark 2.24 restrict to the maps*

$$\{J : J \subset R \textit{ radical ideal }\} \overset{1-1}{\longleftrightarrow} \{V(I) : I \subset R \textit{ ideal}\} \tag{1}$$

$$\operatorname{Spec}(R) \overset{1-1}{\longleftrightarrow} \{V(J) : V(J) \textit{ irreducible}\}, \tag{2}$$

which are both bijections.

Proof. To prove that (1) is indeed a bijection, we need to check the well-definedness of the map from right to left. This follows from Lemma 2.23 and the fact that the radical of an ideal is a radical ideal. It is then easily verified that the mappings are each other's inverse using Lemma 2.23 and the fact that for any ideal $I \subset R$ we have that $V(I) = V(\sqrt{I})$.

In order to prove that (2) is indeed a bijection, it suffices to check the well-definedness and the surjectivity of the map from left to right, because we are restricting bijection (1).

We first check the well-definedness of the map from left to right. Let $P \in \operatorname{Spec}(R)$, then we want to show that $V(P)$ is irreducible. Note that $P \in V(P)$, hence $V(P) \neq \varnothing$. If $V(P) = V_1 \cup V_2$ for two closed sets $V_1, V_2 \subset V(P)$, then $I(V_1) \cap I(V_2) = P$ by bijection (1) as both ideals are radical and they correspond to $V(P)$. Hence, $I(V_1) \cdot I(V_2) \subset P$ and therefore either $I(V_1) \subset P$ or $I(V_2) \subset P$ as P is a prime ideal. Thus, either $V_1 \supset V(P)$ or $V_2 \supset V(P)$ by bijection (1). We conclude that $V(P)$ is irreducible.

Next, we prove the surjectivity of the map from left to right. Let $V(J) \subset \operatorname{Spec}(R)$ be an irreducible subspace. By bijection (1) we may assume without loss of generality that J is radical. Then we will now show that J is in fact a prime ideal. For any $t \in R$ we write the subspace $V(\ (t)\ )$ as $V(t)$ for our convenience.

Let $r, s \in R$ such that $rs \in J$. Then we see that $V(J) \subset V(rs)$, whereas it holds that $V(rs) = V(r) \cup V(s)$. The reader then easily verifies that $(V(J) \cap V(r)) \cup (V(J) \cap V(s)) = V(J)$. Note that both subspaces $V(J) \cap V(r)$ and $V(J) \cap V(s)$ are closed in $\operatorname{Spec}(R)$. It follows that $V(J)$ is equal to either $V(J) \cap V(r)$ or $V(J) \cap V(s)$, because $V(J)$ is by assumption an irreducible subspace. Let us assume without loss of generality that $V(J)$ is equal to $V(J) \cap V(r)$. Then, we see that $V(J)$ is contained in $V(r)$. Thus, we see that $I(V(r)) \subset I(V(J))$, because the map $I(-)$ is inclusion reversing.

Moreover, it follows from bijection (1) and the assumption that J is radical that $J = I(V(J))$. On the other hand, $(r) \subset I(V(r))$, because we know by Lemma 2.23 that $I(V(r)) = \sqrt{(r)}$. Putting the results together, we see that $r \in J$. We conclude that J is a prime ideal. This concludes the proof. □

The last observation, which is crucial for the proof of Theorem 2.16, is that if R is a Noetherian ring, then $\operatorname{Spec}(R)$ with the Zariski topology is a Noetherian topological space; this is the content of the following lemma, which is in fact Exercise 4.9 in [Mat89, Paragraph 4, p. 29].

Lemma 2.26. *If R is a Noetherian ring, then* $\operatorname{Spec}(R)$ *equipped with the Zariski topology is a Noetherian topological space.*

Proof. Let $(V(J_n))_{n \geq 1}$ be a descending chain of closed sets in $\operatorname{Spec}(R)$ and without loss of generality, we may assume that J_n are radical ideals for all $n \geq 1$ by bijection (1) in Proposition 2.25. It follows from Remark 2.24 that we get an ascending chain of ideals $(\ I(V(J_n))\ )_{n \geq 1}$, where $I(V(J_n)) = J_n$ for all $n \geq 1$ by bijection (1) in Proposition 2.25. Because R is Noetherian, the chain $(J_n)_{n \geq 1}$ stabilises after finitely many steps by Theorem 2.2. Hence, so does $(V(J_n))_{n \geq 1}$ and this concludes the proof. □

Finally, we will prove Theorem 2.16.

Proof of Theorem 2.16. The first statement follows from Proposition 2.18 applied to $\mathrm{Spec}(R)$.

We now turn to the second statement. We know that the subspaces $V(P_i)$ are maximal among irreducible subspaces of C, hence by the inclusion reversing bijection (2) in Proposition 2.25 it follows that the prime ideals P_i are minimal among prime ideals in C.

On the other hand, a minimal prime ideal P in C corresponds, by the same inclusion reversing bijection as in the previous paragraph, to an irreducible component $V(P_k)$ of C. Therefore, P is equal to P_k. □

2.3 Assassinator and support of modules

The main objective of this subsection is to prove Theorem 2.35. We will now explain the essence of this theorem.

Let R be a commutative ring and let M be an R-module. The set $\mathrm{Supp}(M) := \{P \in \mathrm{Spec}(R) : M_P \neq 0\}$ is called the *support* of M. Recall the definition of $\mathrm{Ass}(M)$ given in Section 1. Now, if in addition R is a Noetherian ring and M is a finitely generated R-module, then Theorem 2.35 asserts that the set of minimal elements with respect to inclusion of $\mathrm{Supp}(M)$ and $\mathrm{Ass}(M)$ are in fact equal.

The main ingredients for the proof of this theorem are Proposition 2.28, 2.29 and 2.32. We first prove Proposition 2.28 using the following lemma.

Lemma 2.27. *Let M be an R-module. Then any maximal element with respect to inclusion in the set $\mathscr{A} := \{\mathrm{ann}(m) : m \in M \backslash \{0\}\}$ is an associated prime of M.*

Proof. Let $J := \mathrm{ann}(m_0) \in \mathscr{A}$ be a maximal element. To prove that J is in fact a prime ideal, let $r, s \in R$ such that $r \cdot s \in J$ and assume that $s \notin J$. It follows that $\mathrm{ann}(s \cdot m_0) \in \mathscr{A}$, where $J \subset \mathrm{ann}(s \cdot m_0)$. Hence, by the maximality of J, we know that $J = \mathrm{ann}(s \cdot m_0)$. We conclude that $r \in J$. We conclude that J is a prime ideal and the statement follows. □

Before we can state Proposition 2.28, we need to define one more notion. We call an element $r \in R$ a *zero-divisor* of M if there exists a non-zero element $m \in M$ such that $r \cdot m = 0 \in M$.

Proposition 2.28. *Let R be a Noetherian ring and M a non-zero R-module. Then*

(1) $\mathrm{Ass}(M) \neq \varnothing$;

(2) $\{$ *zero-divisors of* $M\} = \bigcup_{P \in \mathrm{Ass}(M)} P$.

Proof. To prove (1), we want to first note that the set of ideals $\mathscr{A} := \{\mathrm{ann}(m) : 0 \neq m \in M\}$ is non-empty as $M \neq 0$. As R is a Noetherian ring, we know that there exists a maximal element $J := \mathrm{ann}(m_0) \in \mathscr{A}$ for some $m_0 \in M$, which is an associated prime ideal of M by Lemma 2.27.

We now show that (2) holds. The inclusion $\supset$ is clear. As for the other inclusion, let $r \in R$ be a zero-divisor of M, then $r \in \mathrm{ann}(m)$ for some non-zero $m \in M$. Now, the set

$$\mathscr{B} := \{\mathrm{ann}(n) : \mathrm{ann}(m) \subset \mathrm{ann}(n) \text{ and } 0 \neq n \in M\}$$

is not empty and due to the fact that R is Noetherian there exists a maximal element $I \in \mathscr{B}$. In fact, I is a prime ideal and the proof of this is similar to the proof of Lemma 2.27. The assertion follows. □

We shall now state and prove Proposition 2.29 using Proposition A.4, Lemma A.1 and Lemma A.3. The second statement in Theorem 6.2 in [Mat89, Paragraph 6, p. 38], is in essence the content of Proposition 2.29. However, we give a more precise version of this theorem.

Proposition 2.29. *Let R be a Noetherian ring, $S \subset R$ a multiplicative set and let M be an R-module. Moreover, set $\mathscr{P}_S := \{P : P \in \mathrm{Spec}(R)$ such that $P \cap S = \varnothing\}$ and let $\varphi \colon \mathscr{P}_S \to \mathrm{Spec}(R_S)$ be the bijection found in Proposition A.4. Then restricting the map φ to $\mathscr{P}_S \cap \mathrm{Ass}_R(M)$ gives rise to a well-defined map $\mathscr{P}_S \cap \mathrm{Ass}_R(M) \to \mathrm{Ass}_{R_S}(M_S)$, which is again a bijection.*

Proof. Let us denote the restriction of φ to $\mathscr{P}_S \cap \mathrm{Ass}_R(M)$ by σ. Moreover, let $\iota\colon R \to R_S$ be the canonical ring homomorphism.

We first show that σ maps into $\mathrm{Ass}_{R_S}(M_S)$, so let $P \in \mathscr{P}_S \cap \mathrm{Ass}_R(M)$. Then we know that there exists an element $m_0 \in M$ such that $P = \mathrm{ann}_R(m_0)$. With the aid of Lemma A.3 it is easily verified that $\varphi(P) := P^{\mathrm{e}} = \mathrm{ann}_{R_S}(m_0/1)$, where we take the extension of P with respect to ι. We conclude that $\sigma\colon \mathscr{P}_S \cap \mathrm{Ass}_R(M) \to \mathrm{Ass}_{R_S}(M_S)$ is a well-defined map.

To prove that σ is a bijection it suffices to show that σ is surjective, because the injectivity of σ follows from the fact that σ is a restriction of φ, where the map φ is injective. Thus, let $J \in \mathrm{Ass}_{R_S}(M_S)$. Then by assumption there exists an element $m_0/s_0 \in M_S$ such that $J = \mathrm{ann}_{R_S}(m_0/s_0)$.

Moreover, it follows from Proposition A.4 that $\varphi^{-1}(J) := J^{\mathrm{c}} \in \mathscr{P}_S$, where we take the contraction of J with respect to ι, because J is in particular a prime ideal of R_S. To finish the proof, it suffices to show that J^{c} is contained in $\mathrm{Ass}_R(M)$, because we know by Proposition A.4 that $\varphi(J^{\mathrm{c}}) := J^{\mathrm{ce}} = J$, where we take the extension of J^{c} with respect to ι.

Notice that in fact $\mathrm{ann}_{R_S}(m_0/s_0) = \mathrm{ann}_{R_S}(m_0/1)$. Now, we claim that there exists and element $t \in S$ such that $J^{\mathrm{c}} = \mathrm{ann}_R(t \cdot m_0)$. As we already know that J^{c} is a prime ideal, this claim would finish the proof. We proceed to prove this claim.

Because R is a Noetherian ring, we know by Proposition 2.2 that J^{c} is generated by finitely many elements $b_1, ..., b_n \in R$. We now show that $J = (b_1/1, ..., b_n/1)$. We know that $J^{\mathrm{ce}} = J$ by Proposition A.4. Therefore, for all $1 \leq k \leq n$ it holds that $\iota(b_k) = b_k/1$ is contained in J. On the other hand, for any element $b = \sum_{k=1}^n r_k b_k \in J^{\mathrm{c}}$ we have that $\iota(b) \in (b_1/1, ..., b_n/1)$.

By the previous paragraph, $\mathrm{ann}_{R_S}(m_0/1) = (b_1/1, ..., b_n/1)$. Therefore, for every $1 \leq k \leq n$ there exists an element $s_k \in S$ such that $s_k b_k m_0 = 0$. Consider $t := \prod_{k=1}^n s_k \in S$. By construction of t, we know that $J^{\mathrm{c}} = (b_1, ..., b_n) \subset \mathrm{ann}_R(t \cdot m_0)$. For the other inclusion, notice that for an element $a \in \mathrm{ann}_R(t \cdot m_0)$ we have that $\iota(a) = a/1 \in \mathrm{ann}_{R_S}(m_0/1) = J$, hence $a \in J^{\mathrm{c}}$. This proves the claim and concludes the proof. □

An immediate consequence of the previous proposition is the following result.

Corollary 2.30. *Let R be a Noetherian ring, M an R-module and let $P \in \mathrm{Spec}(R)$. Moreover, let $\iota\colon R \to R_P$ be the canonical ring homomorphism. Then $P \in \mathrm{Ass}_R(M)$ if and only if $P^{\mathrm{e}} \in \mathrm{Ass}_{R_P}(M_P)$ where we take the extension of P with respect to ι.*

Proof. Apply Proposition 2.29 to the multiplicatively closed set $S := R \backslash P$. □

Lastly, we prove Proposition 2.32.

Lemma 2.31. *Let M be an R-module. Then* $\mathrm{Supp}(M) \subset V(\mathrm{ann}(M))$.

Proof. For a prime ideal $P \in \mathrm{Supp}(M)$, there exists an element $m/s \in M_P$ with $m/s \neq 0/1$. Furthermore, we have that $\mathrm{ann}(m) \cap R \backslash P = \varnothing$ by the assumption that $m/s \neq 0/1$. We conclude that $\mathrm{ann}(M) \subset P$. □

Proposition 2.32. *Let M be a finitely generated R-module. Then* $\mathrm{Supp}(M) = V(\mathrm{ann}(M))$.

Proof. By Lemma 2.31 it suffices to show that $V(\mathrm{ann}(M)) \subset \mathrm{Supp}(M)$. Say M is generated by $m_1, ..., m_k$ for some integer $k \geq 1$.

Notice that if P is a prime ideal in R such that there exists an element $m \in M$ with $\mathrm{ann}(m) \subset P$, then we know that $m/1 \neq 0/1$ in M_P, i.e., then we know that P is contained in the support of M. In fact, we will show that if P is a prime ideal in R with the property that $\mathrm{ann}(M) \subset P$, then for some $1 \leq j \leq k$ it holds that $\mathrm{ann}(m_j) \subset P$.

We will show the contrapositive of the latter statement. Let P be a prime ideal in R and assume that for all $1 \leq i \leq k$ there exists an element $t_i \in R \backslash P$ such that $t_i \in \mathrm{ann}(m_i)$. Then the element $t := \prod_{i=1}^k t_i \in R \backslash P$ is contained in $\mathrm{ann}(M)$, because it annihilates every m_i. Thus we see that $\mathrm{ann}(M) \not\subset P$. □

Remark 2.33. We wish to point out that the assumption that M is finitely generated cannot be omitted in the assumption of Proposition 2.32. Consider for Example the ring $R := \mathbf{Z}$ and $M := \bigoplus_{n \geq 1} \mathbf{Z}/(p^n)$ for a prime $p \in \mathbf{Z}$. We have that $\mathrm{ann}(M) = (0)$ and therefore $V(\mathrm{ann}(M)) = \mathrm{Spec}(R)$. On the other hand, $\mathrm{Supp}(M) = \{(p)\}$ which we leave to the reader to verify.

We need one more small observation to prove Theorem 2.35. We will state this in the following remark.

Remark 2.34. A useful way of thinking about associated prime ideals is given by the following equivalence. Let $P \subset R$ be a prime ideal and let M be an R-module. Then P is an associated prime ideal of M if and only if there exists an injective R-linear map $R/P \to M$.

The following theorem is Theorem 6.5 (ii) & (iii) in [Mat89, Paragraph 6.5, p. 39]. We give a more detailed proof of this theorem.

Theorem 2.35. *Let R be a Noetherian ring and let M be an R-module. Then the following hold:*

(1) $\mathrm{Ass}(M) \subset \mathrm{Supp}(M)$.

(2) If in addition M is a finitely generated R-module, then the set of minimal elements with respect to inclusion of $\mathrm{Supp}(M)$ *and* $\mathrm{Ass}(M)$ *are equal.*

Proof. We first show that (1) holds. Let $P \in \mathrm{Ass}_R(M)$, then it follows from Corollary 2.30 that we have $P^{\mathrm{e}} \in \mathrm{Ass}_{R_P}(M_P)$, where we take the extension of P with respect to the canonical ring homomorphism $\iota\colon R \to R_P$. Hence, by Remark 2.34 there exists an injective R_P-linear map $R_P/P^{\mathrm{e}} \to M_P$, where $R_P/P^{\mathrm{e}} \neq 0$ because P^{e} is a prime ideal. We conclude that $P \in \mathrm{Supp}(M)$.

We proceed to prove (2). To prove that any minimal element $P \in \mathrm{Supp}(M)$ is also a minimal element of $\mathrm{Ass}_R(M)$, it is enough to prove that any minimal element $P \in \mathrm{Supp}(M)$ is contained in $\mathrm{Ass}_R(M)$ by (1).

Let $P \in \mathrm{Supp}(M)$ be a minimal element, then by the minimality of P we have that

$$\mathrm{Supp}(M) \cap \{Q \in \mathrm{Spec}(R) : Q \subset P\} = \{P\}.$$

Note that $\{Q \in \mathrm{Spec}(R) : Q \subset P\} = \{Q \in \mathrm{Spec}(R) : Q \cap R\backslash P = \varnothing\} := \mathscr{P}_P$ using the notation of Proposition A.4. Therefore, by (1) we know that $\mathrm{Ass}_R(M) \cap \mathscr{P}_P \subset \{P\}$. Furthermore, $\mathrm{Ass}_{R_P}(M_P)$ is in bijection with $\mathrm{Ass}_R(M) \cap \mathscr{P}_P$ by Proposition 2.29. On the other hand, as R_P is a Noetherian ring by Proposition A.2 and $M_P \neq 0$ by assumption, it follows that $\mathrm{Ass}_{R_P}(M_P) \neq \varnothing$ by Proposition 2.28. We conclude that $P \in \mathrm{Ass}_R(M)$.

We now show that also any minimal element $P \in \mathrm{Ass}_R(M)$ is also minimal in $\mathrm{Supp}(M)$. To see this, let $P \in \mathrm{Ass}_R(M)$ be a minimal element. Note that $\mathrm{Supp}(M) = V(\mathrm{ann}(M))$ by Proposition 2.32. It follows from Theorem 2.16 that we can write $\mathrm{Supp}(M) = \bigcup_{i=1}^{k} V(P_i)$, where the prime ideals $P_1, ..., P_k$ are the minimal elements of $\mathrm{Supp}(M)$.

To prove that P is also minimal in $\mathrm{Supp}(M)$, we let $P' \in \mathrm{Supp}(M)$ such that $P' \subset P$ and show that $P' = P$. We have that $P_j \subset P'$ for some $1 \leq j \leq k$, and P_j is a minimal element of $\mathrm{Supp}(M)$. Therefore, by the third paragraph in this, we know that $P_j \in \mathrm{Ass}_R(M)$, with the property that $P_j \subset P$. However, P is minimal in $\mathrm{Ass}_R(M)$, thus $P_j = P' = P$. □

Remark 2.36. Let R be a Noetherian ring and M a finitely generated R-module. Because the subspace $\mathrm{Supp}(M) \subset \mathrm{Spec}(R)$ is closed by Proposition 2.32, we can write $\mathrm{Supp}(M) = \bigcup_{i=1}^{k} V(P_i)$ by Theorem 2.16, where the prime ideals $P_1, ..., P_k$ are the minimal elements of $\mathrm{Supp}(M)$.

We call the prime ideals $P_1, ..., P_k$ the *isolated associated prime ideals* of M, i.e., the minimal elements of $\mathrm{Ass}(M)$ are the isolated associated prime ideals. The remaining prime ideals in $\mathrm{Ass}(M)$ are called *embedded associated prime ideals* of M. In fact, there are also only finitely many embedded associated prime ideals in this case. This follows from the fact that $\mathrm{Ass}(M)$ is a finite set, if R is Noetherian and if M is a finitely generated R-module, see [Mat89, Theorem 6.5 (i), p. 39].

2.4 Primary and irreducible submodules

In this subsection, we shall prove Theorem 2.47; this is Theorem 1.1 in Section 1. We then deduce Corollary 2.50 from this which states that irreducible submodules are primary submodules under the same assumptions as in Theorem 2.47. We will first define what irreducible submodules of an R-module are.

Definition 2.37. Let M be an R-module. A submodule $N \subset M$ is called *irreducible* if $N \neq M$ and N cannot be written as an intersection of two strictly larger submodules of M. Otherwise, N is called *reducible*.

If we consider R as an R-module with the natural scalar multiplication, then an ideal satisfying the conditions of Definition 2.37 will be called an *irreducible ideal*. We now give an example of an irreducible ideal and a reducible ideal.

Example 2.38. Let R be a principal ideal domain and let $p \in R$ be an irreducible element. Then for any positive integer l the ideal $(p^l) \subset R$ is irreducible. Indeed, suppose that there exist elements $r, s \in R$ such that $(p^l) = (r) \cap (s)$. We know that $(r) \cap (s) = (\mathrm{lcm}(r, s))$. Thus, we see that p^l divides r or s, i.e., either (r) or (s) is contained in (p^l). Therefore, as $(p^l) \subset R$ is a proper ideal of R, we conclude that (p^l) is an irreducible ideal of R.

Nonexample 2.39. Let R be a unique factorisation domain and consider the ideal $(x^2, xy, y^2) \subset R[x, y]$. Set $J := (x^2, xy, y^2)$. Then J is not irreducible, because we claim that we can write $J = (x, y^2) \cap (y, x^2)$, where it is clear that both the ideals appearing in the intersection strictly contain J. Indeed, the inclusion $J \subset (x, y^2) \cap (y, x^2)$ is clear.

To prove the other inclusion, let $f \in (x, y^2) \cap (y, x^2)$. Then there exist polynomials $f_1, f_2, g_1, g_2 \in R[x, y]$ such that $f = f_1x + f_2y^2 = g_1x^2 + g_2y$. By rearranging the terms, we get that $(f_1 - g_1x)x = (g_2 - f_2y)y$. Thus, we know that there exists a polynomial $h \in R[x, y]$ such that $g_2 - f_2y = hx$, because x and y are coprime and $R[x, y]$ is a unique factorisation domain. Now, note that $f - f_2y^2 = g_1x^2 + (g_2 - f_2y)y = g_1x^2 + hxy$, thus we see that $f \in J$. Therefore, we conclude that $J = (x, y^2) \cap (y, x^2)$.

Now, recall the definition of a primary submodule of an R-module from Section 1. We can restate this definition as follows.

Proposition 2.40. *Let M be an R-module and $N \subset M$ a submodule. Then N is primary if and only if $N \neq M$ and for every zero-divisor $r \in R$ of M/N it holds that $r \in \sqrt{\mathrm{ann}(M/N)}$.*

Proof. If $N \subset M$ is primary and $r \in R$ is a zero-divisor for M/N, then there exists an element $m \in M$ such that $r \cdot m \in N$ with $m \notin N$. Because N is primary, this means that $r^k \cdot M \subset N$ for an integer $k \geq 1$. Hence, $r \in \sqrt{\mathrm{ann}(M/N)}$.

To prove the other direction, let $r \in R$ and $m \in M$ where $m \notin N$ such that $r \cdot m \in N$. So, r is a zero-divisor for M/N and therefore by assumption $r \in \sqrt{\mathrm{ann}(M/N)}$. Hence, there exists a $k \geq 1$ such that $r^k \cdot M \subset N$. □

Remark 2.41. If we consider R as an R-module with the natural scalar multiplication, then an ideal $J \subset R$ is primary by definition if $J \neq R$ and for all $r, s \in R$ it holds that: if $r \cdot s \in J$ and $s \notin J$, then $r^k \in J$ for some integer $k \geq 1$. In this case, we say that J is a *primary ideal* of R. Notice that any prime ideal in R is a primary ideal.

Also, in this case Proposition 2.40 reduces to the equivalence that an ideal $J \subset R$ is primary if and only if $J \neq R$ and all the zero-divisors of R/J are nilpotent.

We will now consider examples and nonexamples of primary submodules in an R-module.

Examples 2.42. (1) Let R be a unique factorisation domain and let $p \in R$ be an irreducible element. Then for any positive integer m the ideal $(p^m) \subset R$ is primary. Indeed, let $r, s \in R$ such that $r \cdot s \in (p^m)$ and $s \notin (p^m)$. Thus, if we factorise $r \cdot s$ into powers of irreducible elements and a unit, we see that p^m will appear in this factorisation. As p^m does not divide s, we see that p divides r by merely comparing the exponents of p appearing in the factorisation of r and s respectively. We conclude that $r^m \in (p^m)$, and thus we see that (p^m) is a primary ideal of R.

(2) Let R be a domain. Then the ideal $J := (x^2, xy, y^2) \subset R[x, y]$ is primary. Indeed, to see this we will use the equivalence stated for primary ideals in Remark 2.41. Set $S := R[x, y]/J$ and notice that for any $f \in S$ there exist constants $c_0, c_1, c_2 \in R$ such that $f = c_0 + c_1x + c_2y$ in S. Let now $a := a_0 + a_1x + a_2y \in S$

be a zero-divisor, i.e., suppose there exists a non-zero element $b := b_0 + b_1x + b_2y \in S$ such that $a \cdot b = 0$ in S. Then, by working out the brackets, we see that $a_0b_0 = 0$, $a_0b_1 + a_1b_0 = 0$ and $a_0b_2 + a_2b_0 = 0$. From the first equality, we see that $a_0 = 0$ or $b_0 = 0$, as R is a domain by assumption. If $a_0 = 0$, then we see that $a^2 = 0$ in S, so in this case a is indeed nilpotent. On the other hand, if $b_0 = 0$, then after a short moment of reflection, using the fact that $b \neq 0$ in S, we see that $a_0 = 0$, and we already know in this case that a is nilpotent. Thus, we see that in either case a is nilpotent, hence we conclude that J is a primary ideal.

(3) Consider the $\mathbf{Z}$-submodule $N := \langle (1,1) \rangle$ of $\mathbf{Z}^2$. The reader then readily verifies, by explicitly checking the definition given in Section 1, that N is a primary submodule of $\mathbf{Z}^2$.

Nonexamples 2.43. (1) Let R be a unique factorisation domain and let $p, q \in R$ be two different irreducible elements. Then the ideal $I := (pq) \subset R$ is not primary. This follows from the fact that $pq \in I$ with $p \notin I$, but no power of q is contained in I.

(2) Let R be a non-zero commutative ring. Then the ideal $J := (xy, y^2) \subset R[x, y]$ is not a primary ideal, because $xy \in J$ and $y \notin J$ but no power of x is contained in J.

(3) Consider the $\mathbf{Z}$-module $M := \mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ and the submodule $N := \langle (1, \overline{1}) \rangle \subset M$. Then N is not a primary submodule of M. Indeed, note that $a := (1, \overline{4})$ is not contained in N, where $2 \cdot a = (2, \overline{2})$ is contained in N. However, for no positive integer l does the inclusion $2^l \cdot M \subset N$ hold, because for any positive integer l the element $2^l \cdot (1, \overline{0}) = (2^l, \overline{0})$ is not contained in N. Therefore, we see that N is by definition not a primary submodule of M.

We will now show that the radical of any primary ideal in a commutative ring is in fact a prime ideal.

Proposition 2.44. *If $J \subset R$ is a primary ideal, then $\sqrt{J} \subset R$ is a prime ideal.*

Proof. Let $r, s \in R$ be given such that $r \cdot s \in \sqrt{J}$ and assume that $s \notin \sqrt{J}$. Then there exists an integer $l \geq 1$ such that $r^l \cdot s^l \in J$ with $s^l \notin J$ as $s \notin \sqrt{J}$. Because J is primary, there exists and integer $k \geq 1$ s.t. $r^k \in J$. We conclude that $r \in \sqrt{J}$. □

Remark 2.45. The converse of Proposition 2.44 is false. To see this, consider the ideal $J := (xy, y^2)$ in Nonexamples 2.43 (2), under the additional assumption that R is a unique factorisation domain. Then we claim that $\sqrt{J} = (y)$. The inclusion $(y) \subset \sqrt{J}$ is clear. Moreover, note that $(y) \subset R[x, y]$ is a prime ideal, as $y \in R[x, y]$ is an irreducible polynomial. Thus, (y) is in particular a radical ideal. Notice that $J \subset (y)$, as both generators of J are divisible by y. Hence, we see that $\sqrt{J} \subset \sqrt{(y)} = (y)$. We conclude that $\sqrt{J} = (y)$.

Before we prove Theorem 2.47, we wish to point out that the content of this theorem is the same as that of Theorem 6.6 in [Mat89, Paragraph 6, p. 40]. However, we have noticed that one direction of the equivalence in Theorem 6.6 also holds for non-finitely generated modules over Noetherian rings. We state this in the following lemma.

Lemma 2.46. *Let R be a Noetherian ring, M an R-module and let $N \subset M$ be a primary submodule. Then $\mathrm{Ass}(M/N) = \{P_N\}$ with $P_N = \sqrt{\mathrm{ann}(M/N)}$. Furthermore, $\mathrm{ann}(M/N)$ is a primary ideal of R.*

Proof. Note that by Proposition 2.28 we have that $\mathrm{Ass}(M/N) \neq \varnothing$. Let $P \in \mathrm{Ass}(M/N)$ and let us define $J := \mathrm{ann}(M/N)$. We will show that $P = \sqrt{J}$. There exists an element $m_0 \in M/N$ such that $P = \mathrm{ann}(m_0)$ by assumption. We see in particular that any $r \in P$ is a zero-divisor for M/N. Because N is primary, we know that $r \in \sqrt{J}$ by Proposition 2.40. Hence, $P \subset \sqrt{J}$.

On the other hand, $J \subset P$ and therefore $\sqrt{J} \subset \sqrt{P} = P$. The last equality holds, because prime ideals are radical. The fact that $\mathrm{ann}(M/N)$ is primary follows from Proposition 2.40. □

We shall now state and prove Theorem 2.47.

Theorem 2.47. *Let R be a Noetherian ring, M a finitely generated R-module and let $N \subsetneq M$ be a submodule. Then N is a primary submodule of M if and only if M/N has exactly one associated prime ideal. In this case, $P_N := \sqrt{\operatorname{ann}(M/N)}$ is the associated prime ideal of M/N, and we say that N is a P_N-primary submodule of M.*

Proof. We prove that if $\operatorname{Ass}(M/N)$ consists of one prime ideal, then N is primary. The other direction follows from Lemma 2.46.

Let $N \subset M$ be a submodule such that $\operatorname{Ass}(M/N) = \{P\}$ for some prime ideal $P \subset R$. Because $\operatorname{Ass}(M/N)$ consists of one prime ideal P, we know that P is a minimal element of $\operatorname{Ass}(M/N)$. It follows from Theorem 2.35 and Remark 2.36 that $\operatorname{Supp}(M/N) = V(P)$ as M/N is a finitely generated R-module. On the other hand, by Proposition 2.32 it also holds that $\operatorname{Supp}(M/N) = V(\operatorname{ann}(M/N))$. It follows from bijection (1) in Proposition 2.25 that $\sqrt{\operatorname{ann}(M/N)} = P$.

We now check that N is primary by making use of Proposition 2.40. Let $r \in R$ be a zero-divisor for M/N. It follows from Proposition 2.28 (2) that $r \in P = \sqrt{\operatorname{ann}(M/N)}$, where we use the fact that $N \neq M$. We conclude that N is primary. □

Remark 2.48. Let R be a Noetherian ring and consider R as an R-module with the natural scalar multiplication. The statement of Theorem 2.47 in this case reduces to the following. An ideal $J \subsetneq R$ is primary if and only if R/J has exactly one associated prime ideal. In this case, $P_J := \sqrt{\operatorname{ann}(R/J)}$ is the associated prime ideal of R/J, where in turn the reader easily verifies that $P_J = \sqrt{J}$, and we say that J is a P_J-primary ideal of R.

To deduce Corollary 2.50 we need one more observation. This is stated in the following lemma which holds in general, i.e., the assumptions of Theorem 2.47 do not need to be satisfied for the lemma to hold. The content of Lemma 2.49 is the same as that Theorem 6.8 (i). However, we give more details of the proof this result.

Lemma 2.49. *Let R be a Noetherian ring, M be an R-module and let $N \subsetneq M$ be a submodule. If $N \subset M$ is an irreducible submodule, then M/N has exactly one associated prime ideal.*

Proof. As by assumption R is a Noetherian ring and $N \subset M$ is a proper submodule, it follows from Proposition 2.28 that $\operatorname{Ass}(M/N) \neq \varnothing$.

Now, we prove the contrapositive of the statement. Assume there exist $P, Q \in \operatorname{Ass}(M/N)$ with $P \neq Q$, where $P = \operatorname{ann}(m_P)$ and $Q = \operatorname{ann}(m_Q)$ for non-zero elements $m_P, m_Q \in M/N$. To prove that N is reducible, it suffices to show that $Rm_P \cap Rm_Q = (0) \subset M/N$, because under the quotient map $\pi\colon M \to M/N$ we would then get that $N = \pi^{-1}(Rm_P) \cap \pi^{-1}(Rm_Q)$, where the submodules of M appearing in the intersection are strictly larger than N as $m_P, m_Q \neq 0$.

In order to show that $Rm_P \cap Rm_Q = (0)$, we assume the contrary and deduce a contradiction. Assume there exists a non-zero $m \in Rm_P \cap Rm_Q$, then we have that $m = r \cdot m_P = s \cdot m_Q$ for some $r, s \in R$. The reader easily verifies that $\operatorname{ann}(r \cdot m_P) = \operatorname{ann}(m_P)$ and $\operatorname{ann}(s \cdot m_Q) = \operatorname{ann}(m_Q)$, by using the fact that P and Q are prime ideals and the assumption that $m \neq 0$. Thus, we see that

$$P = \operatorname{ann}(m_P) = \operatorname{ann}(r \cdot m_P) = \operatorname{ann}(s \cdot m_Q) = \operatorname{ann}(m_Q) = Q,$$

which contradicts the assumption that $P \neq Q$. We conclude that $Rm_P \cap Rm_Q = (0)$, and this finishes the proof. □

Corollary 2.50. *Let R be a Noetherian ring and let M be a finitely generated R-module. If $N \subset M$ is an irreducible submodule, then N is a primary submodule.*

Proof. Immediate consequence of Lemma 2.49 and Theorem 2.47. □

Remark 2.51. The converse of Corollary 2.50 is false in general. Let k be a field. Then the ideal $(x^2, xy, y^2) \subset k[x, y]$ defined in Nonexample 2.39 is reducible, but we have seen in Examples 2.42 (2) that this ideal is in fact primary.

2.5 Existence and uniqueness of primary decompositions

In this subsection, we will prove Theorem 2.61; this is Theorem 1.2 in Section 1. Furthermore, we will prove the first and second uniqueness theorems on primary decompositions, Theorem 2.62 and Theorem 2.64 respectively; this is Theorem 1.3 and Theorem 1.4. We also state the well-known Lasker-Noether theorem on primary decompositions in Noetherian rings as Corollary 2.66, which is a special case of the three aforementioned theorems.

We first introduce some convenient terminology on decompositions of submodules.

Definition 2.52. Let R be a commutative ring, M an R-module, $N \subset M$ a submodule and let $l \geq 0$ be an integer. An expression $N = \bigcap_{i=1}^{l} N_i$ for submodules $N_i \subset M$ is called a *decomposition* of N. A decomposition of N is called *irredundant* if for all $1 \leq j \leq l$ it holds that $\bigcap_{i \neq j} N_i \not\subset N_j$, i.e., for each j we have that $N \neq \bigcap_{i \neq j} N_i$.

We define the intersection over an empty index set of submodules of M to be equal to M.

Definition 2.53. Let R be a commutative ring, M an R-module and let $N \subset M$ be a submodule. Furthermore, let $N = \bigcap_{i=1}^{l} N_i$ be a decomposition of N. If in addition the submodules N_i are irreducible or primary, then this expression is called an *irreducible decomposition* or *primary decomposition* of N respectively.

Remark 2.54. Let R be a Noetherian ring, M an R-module and let $N \subsetneq M$ be a submodule. If N has a primary decomposition $N = \bigcap_{i=1}^{l} N_i$, then for each $1 \leq i \leq l$ we know by Lemma 2.46 that M/N_i has exactly one associated prime ideal.

We will recall the definition of a minimal primary decomposition of a submodule stated in Section 1. In the book [Mat89], such a decomposition is called a *shortest primary decomposition*. We give a slightly more precise version of the latter definition.

Definition 2.55. Let R be a Noetherian ring, M an R-module and let $N \subset M$ be a submodule. A *minimal primary decomposition* of N is an irredundant primary decomposition $N = \bigcap_{i=1}^{l} N_i$ of N, where say for each $1 \leq i \leq l$ we have that $\operatorname{Ass}(M/N_i) = \{P_i\}$ for some prime ideal $P_i \subset R$, such that for each $i \neq j$ we have that $P_i \neq P_j$. In this case, for each $1 \leq t \leq l$ the submodule N_t is called the *P_t-primary component* of N.

Note that the primary components as in Definition 2.55 may depend on the given decomposition, see also Examples 2.69. We will now proceed to prove Theorem 2.61, which we will prove using Proposition 2.56 and Proposition 2.60. We first state and prove Proposition 2.56.

Proposition 2.56. *Let R be a commutative ring and let M be a Noetherian R-module. Then any submodule $N \subset M$ has an irreducible decomposition.*

Proof. If $N = M$, then we can take the empty decomposition of M which is an irreducible decomposition. We now prove the assertion for proper submodules of M.

Let $\mathscr{A}$ be the set of proper submodules of M that do not have an irreducible decomposition. We will show that $\mathscr{A}$ is empty by assuming the contrary. Suppose $\mathscr{A} \neq \varnothing$. Because M is a Noetherian R-module, there exists a maximal element $M_0 \in \mathscr{A}$ which has to be reducible. Hence, we can write $M_0 = N_1 \cap N_2$ for submodules $N_1, N_2 \subset M$ such that $N_1 \neq M \neq N_2$. Furthermore, by the maximality of M_0 we know that $N_1, N_2 \notin \mathscr{A}$. Therefore, both submodules N_1 and N_2 have an irreducible decomposition. By combining these irreducible decompositions, we get an irreducible decomposition of M_0. This is a contradiction.

We conclude that $\mathscr{A} = \varnothing$ and the statement follows. □

We shall now prove Proposition 2.60, which tells us how we can make a primary decomposition minimal.

Remark 2.57. Let R be a commutative ring, M, N be R-modules and let $f\colon M \to N$ be an injective R-linear map. Then it follows by the injectivity of f that for any $m \in M$ we have that $\operatorname{ann}(m) = \operatorname{ann}(f(m))$. Therefore, we see that $\operatorname{Ass}(M) \subset \operatorname{Ass}(N)$.

Proposition 2.58. *Let R be a commutative ring and let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of R-modules. Then we have that $\mathrm{Ass}(M_2) \subset \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M_3)$.*

Proof. For the proof, see [Mat89, Theorem 6.3, p. 38]. □

Corollary 2.59. *Let $M_1, ..., M_k$ be R-modules. Then we have that $\mathrm{Ass}\left(\bigoplus_{i=1}^k M_i\right) = \bigcup_{i=1}^k \mathrm{Ass}(M_i)$.*

Proof. It suffices to prove the statement for $k = 2$, because we can then proceed to prove the assertion with induction on k. For the case of $k = 2$, we apply Proposition 2.58 to the exact sequence given by $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ and deduce that $\mathrm{Ass}(M_1 \oplus M_2) \subset \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M_2)$. On the other hand, we also know that $\mathrm{Ass}(M_1), \mathrm{Ass}(M_2) \subset \mathrm{Ass}(M_1 \oplus M_2)$ by Remark 2.57, because we have the natural imbeddings $M_1 \hookrightarrow M_1 \oplus M_2$ and $M_2 \hookrightarrow M_1 \oplus M_2$. □

Proposition 2.60. *Let R be a Noetherian ring and let M be an R-module. Suppose that $N, L \subsetneq M$ are submodules such that $\mathrm{Ass}(M/N) = \mathrm{Ass}(M/L) = \{P\}$ for some prime ideal $P \subset R$. Then it holds that $\mathrm{Ass}\,(M/(N \cap L)) = \{P\}$.*

Proof. Consider the R-linear map $\varphi\colon M \to M/N \oplus M/L$ defined for $m \in M$ by $\varphi(m) := (\overline{m}, \overline{m})$. Notice that $\ker(\varphi) = N \cap L$ and thus we get an induced injective R-linear map $\overline{\varphi}\colon M/(N \cap L) \to M/N \oplus M/L$. Hence, $\mathrm{Ass}\,(M/(N \cap L)) \subset \mathrm{Ass}(M/N \oplus M/L)$ by Remark 2.57. It follows from Proposition 2.58 that we have $\mathrm{Ass}(M/N \cap L) \subset \mathrm{Ass}(M/N) \cup \mathrm{Ass}(M/L) = \{P\}$. On the other hand, by Proposition 2.28 we know that $\mathrm{Ass}\,(M/(N \cap L)) \neq \varnothing$, because R is a Noetherian ring and $M/(N \cap L) \neq 0$. We conclude that we have $\mathrm{Ass}\,(M/(N \cap L)) = \{P\}$. □

We shall now state and prove Theorem 2.61.

Theorem 2.61. *Let R be a Noetherian ring and let M be a finitely generated R-module. Then any submodule $N \subset M$ has a minimal primary decomposition.*

Proof. If $N = M$, then we can take the empty decomposition which is a minimal primary decomposition of M. Let $N \subsetneq M$ be a submodule. We know by Theorem 2.12 that M is a Noetherian R-module. Hence, it follows from Proposition 2.56 that N has an irreducible decomposition $N = \bigcap_{i=1}^l N_i$, where we know by Lemma 2.49 that for each $1 \leq i \leq l$ we have that $\mathrm{Ass}(M/N_i) = \{P_i\}$ for some prime ideal $P_i \subset R$.

This irreducible decomposition is a primary decomposition by Corollary 2.50. We can make this decomposition irredundant, if necessary, by removing finitely submodules in the decomposition. In order to make it a minimal primary decomposition, we can group submodules N_i, N_j with $P_i = P_j$ together to one submodule $N_i \cap N_j$ which is by Proposition 2.60 and Theorem 2.47 still a P_i-primary submodule. This concludes the proof. □

We will now state and prove the first uniqueness theorem, Theorem 2.62. The content of this theorem is the same as that of Theorem 6.8 (ii) in [Mat89, Paragraph 6, p. 41]. However, we have noticed that Theorem 6.8 (ii) also holds for non-finitely generated modules M over Noetherian rings, and for arbitrary irredundant decompositions of a submodule $N \subset M$ with the property that for each $1 \leq i \leq l$ the module M/N_i has exactly one associated prime ideal.

Theorem 2.62. *Let R be a Noetherian ring and let M be an R-module. Suppose that $N \subset M$ is a submodule that has an irredundant decomposition $N = \bigcap_{i=1}^l N_i$ with the property that for each $1 \leq i \leq l$ we have that $\mathrm{Ass}(M/N_i) = \{P_i\}$ for some prime ideal $P_i \subset R$, and with the property that for $i \neq j$ we have that $P_i \neq P_j$. Then it holds that $\mathrm{Ass}(M/N) = \{P_1, ..., P_l\}$.*

Proof. Set $A := \bigcup_{i=1}^l \mathrm{Ass}(M/N_i)$ and $L := \bigoplus_{i=1}^l M/N_i$. Note that that the cardinality of A is equal to l, because the prime ideals P_i are all different by assumption.

Consider the R-linear map $f\colon M \to L$ defined by $f(m) := (\overline{m}, ..., \overline{m})$. Because $\ker(f) = \bigcap_{i=1}^l N_i = N$, we get an induced injective R-linear map $\overline{f}\colon M/N \to L$. Hence, by Remark 2.57 and Corollary 2.59 we know that $\mathrm{Ass}(M/N) \subset A$. Therefore, $\mathrm{Ass}(M/N) \subset \{P_1, ..., P_l\}$.

We now prove the other inclusion. Because the decomposition is irredundant, for all j there exists an element $n_j \in \bigcap_{i\neq j} N_i$ such that $n_j \notin \bigcap_{i=1}^{l} N_i$, i.e., $n_j \notin N_j$. Let $1 \leq j \leq l$. Then we will now show that $P_j \in \mathrm{Ass}(M/N)$.

We restrict the injective R-linear map $\overline{f}$ in the second paragraph to the R-linear map $f_j \colon (\overline{n_j}) \to L$, where $(\overline{n_j})$ is a submodule of M/N with $0 \neq \overline{n_j} \in M/N$. In fact, the map f_j is injective and $\mathrm{im}(f_j) \subset M/N_j$ where we consider M/N_j as a submodule of L. It follows from Remark 2.57 that we have an inclusion $\mathrm{Ass}(\,(\overline{n_j})\,) \subset \mathrm{Ass}(M/N_j) = \{P_j\}$. On the other hand, we know by Proposition 2.28 that $\mathrm{Ass}(\,(\overline{n_j})\,) \neq \varnothing$, because $\overline{n_j} \neq 0$ and R is a Noetherian ring by assumption.

We conclude that for each j it holds that $\{P_j\} = \mathrm{Ass}(\,(\overline{n_j})\,) \subset \mathrm{Ass}(M/N)$. This concludes the proof. □

Remark 2.63. Let R be a Noetherian ring, M an R-module and let $N \subset M$ be a submodule. Suppose that $N = \bigcap_{i=1}^{k} N_i$ and $N = \bigcap_{j=1}^{l} L_i$ are two different decompositions of N satisfying the conditions of Theorem 2.62 with $\mathrm{Ass}(M/N_i) = \{P_i\}$ and $\mathrm{Ass}(M/L_j) = \{Q_j\}$, then the first uniqueness theorem asserts that we have $\{P_1, ..., P_k\} = \{Q_1, ..., Q_l\}$. In particular, we have that $k = l$.

The first uniqueness theorem also states that for any prime ideal $P \in \mathrm{Ass}(M/N)$, we can find in a given decomposition $N = \bigcap_{i=1}^{k} N_i$, satisfying the conditions of the theorem, exactly one submodule N_r such that $\mathrm{Ass}(M/N_r) = \{P\}$.

By Remark 2.54 we know that any minimal primary decomposition of N satisfies the conditions of the first uniqueness theorem.

We now state and prove the second uniqueness theorem, Theorem 2.64. The content of this theorem is the same as that of Theorem 6.8 (iii) in [Mat89, Paragraph 6, p.41]. However, we have noticed that Theorem 6.8 (iii) also holds for non-finitely generated modules over Noetherian rings. The proof of the second uniqueness theorem makes use of Lemma A.5 and A.6, both of which can be found in Appendix A.

Theorem 2.64. *Let R be a Noetherian ring, M an R-module and let $N \subset M$ be a submodule that has a minimal primary decomposition $N = \bigcap_{i=1}^{l} N_i$, where say for each $1 \leq i \leq l$ we have that $\mathrm{Ass}(M/N_i) = \{P_i\}$ for some prime ideal $P_i \subset R$. Suppose that $P_t \in \mathrm{Ass}(M/N)$ is a minimal element and let $\iota \colon M \to M_{P_t}$ be the canonical map. Then the P_t-primary component N_t of N is equal to $\iota^{-1}(N_{P_t})$.*

Proof. Set $P := P_t$ and note that by Lemma 2.46 for each $1 \leq i \leq l$ we have that $P_i = \sqrt{\mathrm{ann}(M/N_i)}$. By the minimality of P in $\mathrm{Ass}(M/N)$ we know that for $j \neq t$ we have that $P_j \not\subset P$. Therefore, it follows from Lemma 2.31 that for $j \neq t$ it holds that $P \notin \mathrm{Supp}(M/N_j)$ because we have that $V(P_j) = V(\mathrm{ann}(M/N_j))$. In other words, for each $j \neq t$ we have that $(M/N_j)_P = 0$.

Now, it follows from Lemma A.5 that for each $1 \leq j \leq l$ the exact sequence $0 \to N_j \to M \to M/N_j \to 0$ is mapped into the exact sequence $0 \to (N_j)_P \to M_P \to (M/N_j)_P \to 0$. Therefore, for $j \neq t$ we deduce that $(N_j)_P = M_P$.

On the other hand, it follows from Lemma A.6 that $N_P = \bigcap_{i=1}^{l} (N_i)_P$. Hence, $N_P = (N_t)_P$ and therefore $\iota^{-1}(N_P) = \iota^{-1}(\,(N_t)_P\,)$. It is easily verified that $\iota^{-1}(\,(N_t)_P\,) = N_t$, which concludes the proof. □

Remark 2.65. Let R be a Noetherian ring, M an R-module and let $N \subset M$ be a submodule. If $N = \bigcap_{i=1}^{l} N_i$ and $N = \bigcap_{j=1}^{l} L_j$ are two different minimal primary decompositions, where $P_t \in \mathrm{Ass}(M/N)$ is a minimal element, then the P_t-primary components in both decompositions are equal, i.e., $L_t = N_t$.

Note that we implicitly make use of the first uniqueness theorem in the formulation and proof of Theorem 2.64, because we use the fact that every associated prime ideal in $\mathrm{Ass}(M/N)$ corresponds to precisely one primary component.

We summarise the contents of Theorem 2.61, 2.62 and 2.64 in the special case when we consider a Noetherian ring as a module over itself with the natural scalar multiplication.

Corollary 2.66 (Lasker-Noether)**.** *Let R be a Noetherian ring and let $J \subset R$ be an ideal. Then there exist primary ideals $Q_1, ..., Q_l \subset R$ such that*

(1) $J = \bigcap_{i=1}^{l} Q_i$ is a minimal primary decomposition of J;

(2) the associated prime ideals $\sqrt{Q_1}, ..., \sqrt{Q_l}$ of R/J are unique up to reordering;

(3) for any minimal element P among the associated prime ideals of R/J the primary component Q corresponding to P is uniquely determined by J.

Proof. Consider R as an R-module with the natural scalar multiplication. By Remark 2.48 we see that (1) follows from Theorem 2.61, (2) follows from Theorem 2.62 and (3) follows from 2.64. □

Remark 2.67. Let R be a Noetherian ring and let $J \subset R$ be an ideal. Moreover, let $J = \bigcap_{i=1}^{l} Q_i$ be a minimal primary decomposition of J. Then primary components of J appearing in the decomposition corresponding to isolated or embedded associated prime ideals of R/J will be called *isolated* or *embedded primary components* of J respectively.

It is easily verified that $\sqrt{J} = \bigcap_{i=1}^{l} \sqrt{Q_i}$. Note that this is a primary decomposition of $\sqrt{J}$, which we can turn into a minimal primary decomposition by leaving out the embedded associated prime ideals of R/J.

It follows from Theorem 2.62 that $R/\sqrt{J}$ has no embedded associated prime ideals. Therefore, we know in particular by Corollary 2.66 (3) that minimal primary decompositions of $\sqrt{J}$ are unique up to reordering.

We would also like to note the following. If an ideal $J \subset R$ in a Noetherian ring has an embedded primary component, then J will have multiple possible minimal primary decompositions.

Theorem 2.68. *Let R be a Noetherian ring and $J \subset R$ an ideal. Suppose that R/J has an embedded associated prime ideal P. Then J will have infinitely many different minimal primary decompositions which differ in the primary component belonging to P.*

Proof. For the proof, see [SZ65, Theorem 22, p. 231]. □

Examples 2.69. Let k be a field and let n be a positive integer. It follows from Theorem 2.6 that the polynomial ring $k[x_1, ..., x_n]$ is a Noetherian ring. Hence, any ideal $I \subset k[x_1, ..., x_n]$ has a minimal primary decomposition by Corollary 2.66. We will now exhibit some examples of minimal primary decompositions of ideals in $\mathbf{Q}[x, y, z]$.

(1) For the ideal $I_1 := (yz^2, z(x^2 - y^2), zy(x + y), z^4) \subset \mathbf{Q}[x, y, z]$ we have that

$$I_1 = (z) \cap (x + y, z^2) \cap (x^2, xyz, y^2z, yz^2, y^3, z^4) = (z) \cap (x + y, z^2) \cap (x^2, y, z^4)$$

are both minimal primary decompositions of I_1. The primary component $(x + y, z^2)$ appearing in both decompositions is in fact embedded. Moreover, the primary component $(x^2, xyz, y^2z, yz^2, y^3, z^4)$ in the first decomposition of I_1 is also embedded, whereas in the second decomposition (x^2, y, z^4) is also an embedded primary component of I_1. The ideal (z) is an isolated primary component of I. We will see in Example 3.52 in Subsection 3.6 how we can computationally find these primary decompositions of I_1 along with the associated prime ideals of I_1.

(2) For the ideal $I_2 := (x(x - 1), x(z - 1), y + z^2 - 1, z^2(z - 1)) \subset \mathbf{Q}[x, y, z]$ it holds that

$$I_2 = (x, y, z - 1) \cap (x, y - 1, z^2) \cap (x - 1, y, z - 1)$$

is the minimal primary decomposition of I_2. The three primary components appearing this decomposition of I_2 are isolated. We will see in Example 3.37 in Subsection 3.5 how we can calculate this primary decomposition of I_2.

(3) For the ideal $I_3 := (x(x^2 + y), z(x^2 + y), xz^2, yz^2, z^3) \subset \mathbf{Q}[x, y, z]$ we have that

$$I_3 = (x, z) \cap (x^2 + y, z^2) \cap (x, y, z^3) = (x, z) \cap (x^2 + y, z^2) \cap (x^3, x^2z, xz^2, y, z^3)$$

are both minimal primary decompositions of I_3. The primary components (x, z) and (x^2+y, z^2) appearing in both decompositions of I_3 are isolated. On the other hand, the primary components (x, y, z^3) and $(x^3, x^2z, xz^2, y, z^3)$ appearing in the first and second decomposition of I_3 respectively are embedded.

(4) For the ideal $I_4 := (xy, xz, yz) \subset \mathbf{Q}[x, y, z]$ it holds that

$$I_4 = (x, z) \cap (x, y) \cap (y, z)$$

is the minimal primary decomposition of I_4. All three primary components of I_4 are in fact isolated. For calculating primary decompositions of monomial ideals, i.e., ideals generated by monomials, there is a variety of interesting algorithms, see for instance [MS05, Section 5.2, p. 87] or [EGSS13, p. 77].

3 Calculating primary decompositions in polynomial rings

Throughout this section, k will be a field and n will be a positive integer. Recall the definitions of $\mathbf{x}$ and $k[\mathbf{x}]$ given in Section 1. We have mentioned in Section 1 that $k[\mathbf{x}]$ is a Noetherian ring; observe that this follows from Theorem 2.6. Therefore, by Corollary 2.66 any ideal in $k[\mathbf{x}]$ has a minimal primary decomposition, as was mentioned in Section 1.

We have the convention in this section that the field k can be represented on a computer system such that we can add and multiply elements in this field on this computer. Furthermore, we also require that we can compute inverses of non-zero elements in k.

We will exhibit in this section a special case of the algorithm presented in the paper [GTZ88] with which we can calculate a primary decomposition of an arbitrary ideal $J \subset k[\mathbf{x}]$ along with generators for each associated prime ideal of $k[\mathbf{x}]/J$, if the cardinality of the field k is infinite and for any subset of variables $\mathbf{u} \subset \mathbf{x}$ it holds that $k(\mathbf{u})$ is a perfect field with the property that we can compute factorisations of squarefree univariate polynomials with coefficients in $k(\mathbf{u})$ and squarefree parts of univariate polynomials with coefficients in $k(\mathbf{u})$. For example, any algebraic number field will satisfy these conditions, see also Remark 3.50.

In fact, for the case $n = 1$ we already know how to compute primary decompositions of ideals in $k[\mathbf{x}]$. In this case, the problem of finding a primary decomposition of an ideal in $I \subset k[x]$ reduces to factoring a univariate polynomial. Indeed, as $k[x]$ is a principal ideal domain, any ideal $I \subset k[x]$ is generated by a monic univariate polynomial $f \in k[x]$. Factor $f = \prod_{i=1}^{m} p_i^{e_i}$ where for each $i \neq j$ we have that p_i and p_j are pairwise coprime irreducible polynomials in $k[x]$. Then the reader easily verifies that $(f) = \bigcap_{i=1}^{m} (p_i^{e_i})$. Moreover, it follows from Examples 2.42 (1) that each ideal $(p_i^{e_i})$ is primary. Therefore, for the remainder of this section n will be an integer greater than or equal to 2, unless otherwise mentioned.

In this section, we will follow Chapter 8 of the book [BW98]. We will state any adjustments that we have made in the results, and their proofs, and formulations of the algorithms. The algorithm in this book is in turn based on the algorithm presented in the paper [GTZ88]. Currently, there are also two completely different algorithms for computing primary decompositions of ideals in polynomial rings. We refer the interested reader to the papers [EHV92] and [SY96] for these algorithms.

The computer algebra system Macaulay2 has a software package named `PrimaryDecomposition` in which the algorithms, for computing primary decompositions of ideals in polynomial rings over fields, in the papers [GTZ88],[EHV92] and [SY96] are implemented. Also, the computer algebra system Singular has a library called `primdec.lib`, where the algorithms presented in the papers [GTZ88] and [SY96] are implemented for polynomial rings over fields.

We will extensively make use of the theory on Gröbner bases in this section. For an introduction of this subject we refer to [vzGG14, Chapter 21, p. 591] or [CLO18, Chapter 2, p. 49]. Throughout this section, we have the convention that $0 \in k[\mathbf{x}]$ is not contained in any Gröbner basis of an ideal in $k[\mathbf{x}]$, and that the empty set is the only Gröbner basis of the zero ideal in $k[\mathbf{x}]$.

3.1 Notation, inverse block orders and calculating elimination ideals

This subsection is dedicated to introduce notation, to define what inverse block orders are and to recall how we can compute elimination ideals. We start with the notation.

Notation 3.1. Let k be a field. For any subset of variables $\mathbf{u} \subset \mathbf{x}$ we denote by

$$M(\mathbf{u}) := \left\{ \prod_{i=1}^{r} u_i^{e_i} : \text{ for each } 1 \leq i \leq n \text{ we have that } e_i \in \mathbf{Z}_{\geq 0} \text{ and } u_i \in \mathbf{u} \right\}$$

the set of monomials in variables $\mathbf{u}$. We set $M(\varnothing) := \{1\}$. We also denote by $k[\mathbf{u}]$ the polynomial ring over k with variables in the set $\mathbf{u}$. We define $k[\varnothing] := k$ and $k(\varnothing) := k$.

Let $<$ be a monomial order on $M(\mathbf{x})$ and let $\mathbf{u} \subset \mathbf{x}$. We say that $\mathbf{u} < \mathbf{x}\backslash\mathbf{u}$ if and only if for every $m_1 \in M(\mathbf{u})$ and for every $1 \neq m_2 \in M(\mathbf{x}\backslash\mathbf{u})$ we have that $m_1 < m_2$.

We now define what an inverse block order on $M(\mathbf{x})$ with respect to a subset of variables is.

Definition 3.2. Let $\mathbf{u} \subset \mathbf{x}$ be a subset of variables and let $<_1$ and $<_2$ be two monomial orders on $M(\mathbf{u})$ and $M(\mathbf{x}\backslash\mathbf{u})$ respectively. We then define a relation $<$ on $M(\mathbf{x})$ as follows. Let $s, t \in M(\mathbf{x})$ be two monomials, and let $s_1, t_1 \in M(\mathbf{u})$ and $s_2, t_2 \in M(\mathbf{x}\backslash\mathbf{u})$ be such that $s = s_1 \cdot s_2$ and $t = t_1 \cdot t_2$; we define $s < t$ if and only if it holds that $s_2 <_2 t_2$ or we have that $s_2 = t_2$ and $s_1 <_1 t_1$. The relation $<$ is a monomial order on $M(\mathbf{x})$, and we call $<$ an *inverse block order* on $M(\mathbf{x})$ with respect to $\mathbf{u}$.

Example 3.3. Let $\mathbf{u} \subset \mathbf{x}$ be a subset of variables and let $<$ be a lexicographical monomial order on $M(\mathbf{x})$, where the variables in $\mathbf{u}$ are all smaller than the variables in $\mathbf{x}\backslash\mathbf{u}$. Then this monomial order $<$ is an inverse block order on $M(\mathbf{x})$ with respect to $\mathbf{u}$.

Remark 3.4. Let $<$ be an inverse block order on $M(\mathbf{x})$ with respect to a subset of variables $\mathbf{u} \subset \mathbf{x}$ and let $s, t \in M(\mathbf{x})$ and write for $s_1, t_1 \in M(\mathbf{u})$ and $s_2, t_2 \in M(\mathbf{x}\backslash\mathbf{u})$ the monomials s and t as $s = s_1 \cdot s_2$ and $t = t_1 \cdot t_2$. Moreover, let $<'$ be the restriction of the monomial order $<$ to $M(\mathbf{x}\backslash\mathbf{u})$. Observe that if $s < t$, then it holds that $s_2 \leq' t_2$.

We will see in Subsection 3.6 that inverse block orders play an important role in computing primary decompositions of arbitrary ideals in $k[\mathbf{x}]$.

Remark 3.5. Let $\mathbf{u} \subset \mathbf{x}$ be a subset of variables. Note that a lexicographical monomial order on $M(\mathbf{x})$, where each variable in $\mathbf{u}$ is less than every variable in $\mathbf{x}\backslash\mathbf{u}$, satisfies the property that $\mathbf{u} < \mathbf{x}\backslash\mathbf{u}$. Any inverse block order on $M(\mathbf{x})$ with respect to $\mathbf{x}\backslash\mathbf{u}$ will also satisfy this property.

Next, let k be a field, $\mathbf{u} \subset \mathbf{x}$ a subset of variables and let $J \subset k[\mathbf{x}]$ be an ideal. We call the ideal $J \cap k[\mathbf{u}]$ the *elimination ideal* of J with respect to $\mathbf{u}$. The following proposition tells us exactly how we can compute generators for any elimination ideal of J. We will omit the proof.

Proposition 3.6. *Let k be a field, $\mathbf{u} \subset \mathbf{x}$ a subset of variables and let $J \subset k[\mathbf{x}]$ be an ideal. Let also $<$ be a monomial order on $M(\mathbf{x})$ such that $\mathbf{u} < \mathbf{x}\backslash\mathbf{u}$. Suppose that G is a Gröbner basis of J with respect to $<$. Then $G \cap k[\mathbf{u}]$ is a Gröbner basis of $J \cap k[\mathbf{u}]$ with respect to the restriction of $<$ to $M(\mathbf{u})$.*

Proof. For the proof see, [BW98, Proposition 6.15, p. 257] □

We summarise the procedure of computing an elimination ideal of J with respect to $\mathbf{u}$ in the algorithm `Elimination`.

Algorithm `Elimination`

Input: A field k, a subset $\mathbf{u} \subset \mathbf{x}$ of variables and a finite set $F \subset k[\mathbf{x}]$.
Output: A reduced Gröbner basis $G \subset k[\mathbf{u}]$ of the elimination ideal $(F) \cap k[\mathbf{u}]$.

1: pick a monomial order $<$ on $M(\mathbf{x})$ such that $\mathbf{u} < \mathbf{x}\backslash\mathbf{u}$
2: $H \leftarrow$ the reduced Gröbner basis of (F) with respect to $<$
3: $G \leftarrow H \cap k[\mathbf{u}]$
4: **return** G

3.2 Characterisation of zero-dimensional ideals in polynomial rings over fields

For any field extension $k \subset \ell$ and for any set $S \subset k[\mathbf{x}]$, we denote the zero locus of S in $\mathbf{A}^n(\ell)$ by $Z(S, \ell)$, where $Z(S, \ell)$ is contained in $\mathbf{A}^n(\ell)$. Recall the definition of the dimension of an ideal in $k[\mathbf{x}]$ given in Section 1. The main result of this subsection is Theorem 3.15, which states three equivalent statements regarding a zero-dimensional ideal $J \subset k[\mathbf{x}]$, the zero locus $Z(J, \overline{k})$ and the k-dimension of the k-vector space of the quotient ring $k[\mathbf{x}]/J$ which we denote by $\dim_k(k[\mathbf{x}]/J)$.

This result will be a very useful tool in the remainder of this section. For example, we will be able to easily deduce that zero-dimensional prime ideals in $k[\mathbf{x}]$ are maximal.

Definition 3.7. Let $J \subset k[\mathbf{x}]$ be an ideal. We call a subset of variables $\mathbf{u} \subset \mathbf{x}$ with the property that $J \cap k[\mathbf{u}] = (0)$ an *independent set of variables mod J*. If $\mathbf{u} \subset \mathbf{x}$ is an independent set of variables mod J such that it is not contained properly in any other independent set of variables mod J, then we say that $\mathbf{u}$ is a *maximally independent set of variables mod J*.

Remark 3.8. Let $J \subset k[\mathbf{x}]$ be an ideal. The terminology used for a subset of the variables $\mathbf{x}$ in Definition 3.7 originates from a more general term. Recall that in a k-algebra B a finite set of elements $\{b_1, ..., b_m\} \subset B$ is called *algebraically independent over k* if the only polynomial f with coefficients in k satisfying the equality $f(b_1, ..., b_m) = 0$ in B is the zero polynomial.

Let $\mathbf{u} \subset \mathbf{x}$ be a subset of variables. We see that $\mathbf{u}$ is an independent set of variables mod J if and only if $\pi(\mathbf{u}) \subset k[\mathbf{x}]/J$ is an algebraically independent set over k, where $\pi \colon k[\mathbf{x}] \to k[\mathbf{x}]/J$ is the quotient map.

Remark 3.9. Let k be a field and let $F \subset k[\mathbf{x}]$ be a finite subset. We can compute a maximally independent set of variables mod (F) by mere brute force, i.e., we can compute for every subset of variables the ideal $(F) \cap k[\mathbf{u}]$ by a call of the algorithm `Elimination` and check whether this elimination ideal is the zero ideal. However, there is a more efficient way of computing a maximally independent set of variables mod (F). We will not explain this algorithm in this thesis; we refer to [BW98, Proposition 9.29, p. 449] for a complete description of this procedure.

Before we proceed to prove Theorem 3.15, we first make three observations on the dimension of an ideal.

Remark 3.10. For ideals $I, J \subset k[\mathbf{x}]$ such that $I \subset J$, we have that $\dim(J) \leq \dim(I)$. This follows from the observation that for any $\mathbf{u} \subset \mathbf{x}$ with the property that $J \cap k[\mathbf{u}] = (0)$ it also holds that $I \cap k[\mathbf{u}] = (0)$, because of the inclusion.

Remark 3.11. Let $J \subsetneq k[\mathbf{x}]$ be an ideal. Then $\dim(J) = 0$ if and only if for every $1 \leq i \leq n$ there exists a non-constant univariate polynomial $f_i \in J \cap k[x_i]$. This equivalence follows directly from the definition.

Remark 3.12. The definition of an ideal $J \subset k[\mathbf{x}]$ may seem a bit unorthodox if the reader is familiar with the Krull dimension of an ideal J, i.e., the Krull dimension of the quotient ring $k[\mathbf{x}]/J$. These definitions are in fact equivalent, i.e., they yield the same value for a fixed ideal. It requires a bit of work to see this, which we will not do here. Fortunately, we will not need this equivalence in the remainder of this section.

In the proof of Theorem 3.15, we will make use of Lemma 3.13. For any field extension $k \subset \ell$ and for any subset $W \subset \mathbf{A}^n(\ell)$ we denote the set of polynomials in $k[\mathbf{x}]$ which vanish on W by $I(W, k)$. Note that the set $I(W, k)$ is an ideal of $k[\mathbf{x}]$.

Lemma 3.13. *Let k be a field, $\overline{k}$ an algebraic closure of k and $J \subset k[\mathbf{x}]$ be an ideal. Then $I(Z(J, \overline{k}), k) = \sqrt{J}$.*

Proof. For the proof see, [BvLT24, Corollary 3.1.18, p. 19]. □

Remark 3.14. Let $J \subset k[\mathbf{x}]$ be an ideal and let $\overline{k}$ be an algebraic closure of k. Then we have that $J = k[\mathbf{x}]$ if and only if $Z(J, \overline{k})$ is empty.

We now explain why this is true. If $J = k[\mathbf{x}]$, then $Z(J, \overline{k})$ is empty as $1 \in J$. On the other hand, suppose that $Z(J, \overline{k}) = \varnothing$, then by Lemma 3.13 we know that $\sqrt{J} = I(Z(J, \overline{k}), k) = k[\mathbf{x}]$. This means that $J = k[\mathbf{x}]$.

We now state and prove Theorem 3.15. This theorem is a combination of Theorem 6.54 in [BW98, Section 6.3, p. 274] and Proposition 8.27 in [BW98, Section 8.3, p.347]. However, our proof of this theorem does not use Gröbner bases of ideals.

Theorem 3.15. *Let $J \subsetneq k[\mathbf{x}]$ be an ideal and $\overline{k}$ an algebraic closure of k. Then the following are equivalent:*

(1) $\dim(J) = 0$.

(2) $\dim_k(k[\mathbf{x}]/J) < \infty$.

(3) $Z(J, \overline{k})$ *is a finite set.*

Proof. We first show that (1) implies (2). It follows from the assumption that for every $1 \leq i \leq n$ there exists a non-constant polynomial $f_i \in J \cap k[x_i]$. Consider the natural morphism of k-algebra's

$$\varphi \colon k[\mathbf{x}]/(f_1, ..., f_n) \twoheadrightarrow k[\mathbf{x}]/J$$

which is surjective. Now, $k[\mathbf{x}]/(f_1, ..., f_n)$ is a finite-dimensional k-vector space, because the set of monomials $\{\prod_{i=1}^n x_i^{e_i} : \text{ for every } 1 \leq i \leq n \text{ we have } e_i < \deg(f_i)\}$ forms a k-basis for $k[\mathbf{x}]/(f_1, ..., f_n)$. Hence, by the surjectivity of φ, we know that $k[\mathbf{x}]/J$ is a finite-dimensional k-vector space.

Next, we prove that (2) implies (1). To prove that $\dim(J) = 0$, it suffices to show that for every $1 \leq i \leq n$ there exists a non-constant polynomial $f_i \in J \cap k[x_i]$. Let $1 \leq i \leq n$, $\iota_i \colon k[x_i] \hookrightarrow k[\mathbf{x}]$ be the inclusion and let $\pi_i \colon k[\mathbf{x}] \to k[\mathbf{x}]/J$ be the projection map. Consider the composition $\pi_i \circ \iota_i \colon k[x_i] \to k[\mathbf{x}]/J$ and note that $\pi_i \circ \iota_i$ does not map everything to zero, because J is a proper ideal of $k[\mathbf{x}]$.

Moreover, the codomain of $\pi_i \circ \iota_i$ is a finite-dimensional k-vector space by assumption, whereas the domain is an infinite-dimensional k-vector space. Therefore, $\pi_i \circ \iota_i$ is not injective, i.e., there exists a non-zero polynomial $f_i \in J \cap k[x_i]$. Furthermore, as $\pi_i \circ \iota_i$ is not the zero map, we also know that f_i is not a constant. We conclude that J is a zero-dimensional ideal.

We now explain why (1) implies (3). If $\dim(J) = 0$, then for every $1 \leq i \leq n$ there exists a non-constant polynomial $f_i \in J \cap k[x_i]$. For the set $S := \{f_1, ..., f_n\}$ we have $(S) \subset J$. Hence, $Z(J, \overline{k}) \subset Z(S, \overline{k})$ whereas the cardinality of $Z(S, \overline{k})$ is at most equal to $\prod_{i=1}^n \deg(f_i)$. We conclude that $Z(J, \overline{k})$ is a finite set.

Lastly, we show that (3) implies (1). Suppose that $Z(J, \overline{k}) = \{P_1, ..., P_r\}$ for some $r \in \mathbf{Z}_{\geq 1}$. Note that $Z(J, \overline{k})$ is not empty by Remark 3.14.

Let ℓ be the field generated by all the coordinates of the points $P_1, ..., P_r$ over k. This is a finite field extension of k, i.e., $\dim_k(\ell) < \infty$. We will consider ℓ^r as a k-algebra with pointwise addition and multiplication. Next, consider the following morphism of k-algebra's $\psi \colon k[\mathbf{x}] \to \ell^r$ defined by $f \mapsto (f(P_i))_{i=1}^r$. By definition of ψ we see that $\ker(\psi) = I(Z(J, \overline{k}), k)$. By Lemma 3.13 we now know that $\ker(\psi) = \sqrt{J}$. Thus, we have an induced injective morphism of k-algebra's $\overline{\psi} \colon k[\mathbf{x}]/\sqrt{J} \hookrightarrow \ell^r$. Therefore,

$$\dim_k \left(k[\mathbf{x}]/\sqrt{J} \right) = \dim_k \left(\operatorname{im} \left(\overline{\psi} \right) \right) \leq \dim_k(\ell^r) = r \cdot \dim_k(\ell) < \infty.$$

We have already shown that (2) implies (1) and we may use this implication for $\sqrt{J}$ as this is still a proper ideal. Hence, $\dim(\sqrt{J}) = 0$. This means that for every $1 \leq i \leq n$ there exists a non-constant polynomial $g_i \in \sqrt{J} \cap k[x_i]$. Thus, for every $1 \leq i \leq n$ there exists an integer $N_i \geq 1$ such that $g_i^{N_i} \in J \cap k[x_i]$, where $g_i^{N_i}$ is not a constant. Therefore, we see that $\dim(J) = 0$. This concludes the proof of the Theorem 3.15. □

We can easily deduce from this theorem that a zero-dimensional prime ideal $J \subset k[\mathbf{x}]$ is maximal. This is the content of the following lemma.

Lemma 3.16. *If $J \subset k[\mathbf{x}]$ is a zero-dimensional prime ideal, then J is maximal.*

Proof. To prove that J is maximal it suffices to show that $k[\mathbf{x}]/J$ is a field. Note that $k[\mathbf{x}]/J$ is a commutative ring, so we only need to show that every non-zero polynomial in $k[\mathbf{x}]/J$ has an inverse. Let f be a non-zero polynomial in $k[\mathbf{x}]/J$. Consider then the k-linear map $\varphi : k[\mathbf{x}]/J \to k[\mathbf{x}]/J$ defined by $\varphi(h) := f \cdot h$. In

fact, φ is injective. Indeed, to show this let $h \in k[\mathbf{x}]/J$ such that $f \cdot h = 0 \in k[\mathbf{x}]/J$. Due to the assumption that J is prime, we know that $k[\mathbf{x}]/J$ is a domain. As f is a non-zero element of $k[\mathbf{x}]/J$, we see that $h = 0$.

By Theorem 3.15 we know that $k[\mathbf{x}]/J$ is a finite dimensional k-vector space. Therefore, φ is also surjective. This means that there exists a polynomial $g \in k[\mathbf{x}]/J$ such that $\varphi(g) = f \cdot g = 1 \in k[\mathbf{x}]/J$. We see that f has an inverse and therefore $k[\mathbf{x}]/J$ is a field. □

Remark 3.17. Let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal. Moreover, let $J = \bigcap_{i=1}^{l} Q_i$ be a minimal primary decomposition of J. For each $1 \leq i \leq l$ we have an inclusion $J \subset \sqrt{Q_i}$, thus it follows from Remark 3.10 that $\dim(\sqrt{Q_i}) = 0$. Therefore, by Lemma 3.16 each associated prime ideal $\sqrt{Q_i}$ is maximal. By the minimality of the primary decomposition, this tells us that J has no embedded primary components. It follows from Corollary 2.66 (3) that each primary component Q_i of J is unique up to reordering. Hence, we can speak of *the* minimal primary decomposition of J.

3.3 Computing radicals of zero-dimensional ideals

In this subsection, we will see how we can compute generators of the radical of a zero-dimensional ideal in $k[\mathbf{x}]$, if k is a perfect field such that squarefree parts of univariate polynomials with coefficients in k can be computed.

Recall that for an element $r \in R$ in a unique factorisation domain R, where $r = u \cdot \prod_{i=1}^{m} p_i^{e_i}$ is the unique factorisation of r with $u \in R^\times$ a unit and for $i \neq j$ we have that p_i and p_j are coprime irreducible elements of R, *a squarefree part* of r is equal to $\prod_{i=1}^{m} p_i$. Moreover, we say that r is *squarefree* if r and a squarefree part of r are associated elements in R. In the case of $R = k[\mathbf{x}]$, we can speak of *the* squarefree part of a polynomial $f \in k[\mathbf{x}]$, by choosing the irreducible elements in the factorisation of f to be monic.

Theorem 3.23 will reduce the problem of computing generators of the radical of a zero-dimensional ideal in $k[\mathbf{x}]$ to that of computing squarefree parts of univariate polynomials with coefficients in k, assuming that k is a perfect field.

We now proceed to prove Theorem 3.23. The theorem will follow from Proposition 3.21. For proving Proposition 3.21, we will make use of the following lemmata.

Lemma 3.18. *Let k be a field, $J \subset k[\mathbf{x}]$ an ideal and let $f \in k[x_1]$ be a polynomial. Moreover, let also $g_1, ..., g_m \in k[x_1]$ be pairwise coprime polynomials such that $f = \prod_{i=1}^{m} g_i$. Then, $(J, f) = \bigcap_{i=1}^{m} (J, g_i) \subset k[\mathbf{x}]$.*

Proof. We may assume without loss of generality that f is monic. The statement is clear for $m = 1$. Assume that $m \geq 2$. It is clear that $(J, f) \subset \bigcap_{i=1}^{m} (J, g_i)$. We will show the other inclusion. Let $h \in \bigcap_{i=1}^{m} (J, g_i)$. Then for each $1 \leq i \leq m$ there exist polynomials $q_i \in k[\mathbf{x}]$ and $t_i \in J$ such that $h = t_i + q_i \cdot g_i$.

Now, for each $1 \leq j \leq m$ define $f_j := \prod_{i \neq j} g_i \in k[x_1]$. It follows that for each $1 \leq j \leq m$ we have that

$$h \cdot f_j = t_j \cdot f_j + q_j \cdot \prod_{i=1}^{m} g_i \in (J, f).$$

We will now show that $\gcd(f_1, ..., f_m) = 1$, i.e., the polynomials $f_1, ..., f_m$ are pairwise coprime. Suppose that $p \in k[x_1]$ is an irreducible polynomial such that for each $1 \leq i \leq m$ we have that $p | f_i$. This means in particular that p appears in the factorisation of $f_1 = \prod_{i=2}^{m} g_i$. Moreover, the polynomials $g_2, ..., g_m$ are pairwise coprime, hence there exists exactly one index $2 \leq r \leq m$ such that $p | g_r$. On the other hand, p also divides f_r, but this means that p has to divide g_1. This contradicts the fact that g_1 and g_r are coprime. We conclude that $\gcd(f_1, ..., f_m) = 1$.

Therefore, there exist polynomials $s_1, ..., s_m \in k[x_1]$ such that $\sum_{i=1}^{m} s_i \cdot f_i = 1$. By multiplying the latter equation on both sides with h yields that $h = \sum_{i=1}^{m} s_i \cdot h \cdot f_i \in (J, f)$. This conclude the proof. □

Lemma 3.19. *Let k be a field and $f \in k[x]$ such that $\gcd(f, f') = 1$. Then f is squarefree.*

Proof. We will prove the contrapositive of the statement. Let $f \in k[x]$ be a non-squarefree polynomial. Then there exists a non-constant polynomial $h \in k[x]$ and a polynomial $g \in k[x]$ such that $f = h^2 \cdot g$. Note that $f' = 2 \cdot h \cdot h' \cdot g + h^2 \cdot g'$. Thus, we see that h divides $\gcd(f, f')$. Hence, we conclude that $\gcd(f, f') \neq 1$. □

Lemma 3.20. *Let k be a perfect field and let $f \in k[x]$ be a squarefree polynomial. Then* $\gcd(f, f') = 1$.

Proof. For the proof, see [BW98, Theorem 7.36, p. 311]. □

We are now able to prove Proposition 3.21. This proposition is in fact Lemma 8.13 in [BW98, Section 8.2, p. 341]. We give a more detailed proof this result.

Proposition 3.21 (Seidenberg)**.** *Let k be a field and let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal. If for every $1 \leq i \leq n$ there exists a univariate polynomial $f_i \in J \cap k[x_i]$ such that* $\gcd(f_i, f_i') = 1$*, then J is a finite intersection of maximal ideals.*

Proof. We will prove the theorem with induction on n.

We first consider the case $n = 1$. In this case, $J = (f)$ for some monic polynomial $f \in k[x_1]$, because $k[x_1]$ is a principal ideal domain. By Lemma 3.20 we know that f_1 is squarefree. Furthermore, as $f_1 \in J = (f)$, we see that f also must be squarefree. Say $f = \prod_{j=1}^{t} g_j$ with $g_j \in k[x_1]$ pairwise coprime irreducible factors of f. The reader easily verifies that $(f) = \bigcap_{j=1}^{t}(g_j)$. Furthermore, for every $1 \leq j \leq t$ the ideal (g_i) is a maximal ideal, because non-zero prime ideals in a principal ideal domain are maximal.

Let now $n \geq 2$ and assume now that the theorem holds for all $1 \leq m < n$. We will show that the theorem also holds for the case n. Let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal with $f_1, ..., f_n$ as in the hypothesis of the theorem. Again, by Lemma 3.19 the polynomials $f_1, ..., f_n$ are all squarefree. Factor $f_n = \prod_{j=1}^{s} h_j$ with $h_j \in k[x_n]$ pairwise coprime irreducible factors of f_n. By applying Lemma 3.18 to f_n and $h_1, ..., h_s$ we get that $J = (J, f_n) = \bigcap_{j=1}^{s}(J, h_j)$. In order to prove that I is a finite intersection of maximal ideals, it suffices to show that for every $1 \leq j \leq s$ the ideal (J, h_j) is a finite intersection of maximal ideals.

Let $1 \leq j \leq n$ and define $\ell_j := k[x_n]/(h_j)$. Consider the surjective morphism of k-algebra's

$$\varphi_j \colon k[x_n][x_1, ..., x_{n-1}] \twoheadrightarrow \ell_j[x_1, ..., x_{n-1}]$$

defined by mapping $\varphi_j(g(x_1, x_2..., x_n)) := g(x_1, x_2, ..., \overline{x_n})$. Set $I := \varphi_j(J)$ and note that by the surjectivity of φ_j, I is an ideal of $\ell_j[x_1, ..., x_{n-1}]$. Furthermore, for every $1 \leq i < n$ the polynomial $f_i \in I$ still has the property that $\gcd(f_i, f_i') = 1$ as ℓ_j is a field extension of k.

We now briefly explain why $\ker(\varphi_j) = (h_j) \subset k[\mathbf{x}]$. The inclusion $(h_j) \subset \ker(\varphi_j)$ is clear. To show why the other inclusion also holds, let $g \in \ker(\varphi_j)$. The set of all monomials in variables $x_1, ..., x_{n-1}$ including $1 \in \ell_j$ forms a ℓ_j-basis of $\ell_j[x_1, ..., x_{n-1}]$. Let us call this set of monomials B. Hence, if $\varphi_j(g) = g(x_1, ..., \overline{x_n}) = 0 \in \ell_j[x_1, ..., x_{n-1}]$, then every coefficient of $g \in k[x_n][x_1, ..., x_{n-1}]$ must be divisible by h_j. Indeed, this follows by looking at every coefficient of $\varphi_j(g)$ with respect to B. Therefore, g itself will indeed be divisible by h_j.

Thus, we conclude that $\ker(\varphi_j) = (h_j)$. Furthermore, the reader easily verifies that $\varphi_j^{-1}(I) = (J, h_j)$. Hence, we get an induced isomorphism of k-algebra's

$$\overline{\varphi_j} \colon k[x_n][x_1, ..., x_{n-1}]/(J, h_j) \xrightarrow{\cong} \ell_j[x_1, ..., x_{n-1}]/I.$$

As J is zero-dimensional, we know that (J, h_j) is also zero-dimensional by Remark 3.10. Therefore, by Theorem 3.15 we see that $\dim_k(k[x_n][x_1, ..., x_{n-1}]/(J, h_j)) < \infty$, and by the isomorphism $\overline{\varphi_j}$ we know that $\dim_k(\ell_j[x_1, ..., x_{n-1}]/I) < \infty$. It follows that $\dim_{\ell_j}(\ell_j[x_1, ..., x_{n-1}]/I) < \infty$, because ℓ_j is a field extension of k. Therefore, again by Theorem 3.15 we see that $\dim(I) = 0$.

Thus, the induction hypothesis applies to I and the polynomial ring $\ell_j[x_1, ..., x_{n-1}]$. Hence, there exist finitely many maximal ideals $M_1, ..., M_r \subset \ell_j[x_1, ..., x_{n-1}]$ such that $I = \bigcap_{m=1}^{r} M_m$. Note that for every $1 \leq m \leq r$ the ideal $\varphi_j^{-1}(M_m) \subset k[\mathbf{x}]$ is still maximal. We see that

$$(J, h_j) = \varphi_j^{-1}(I) = \bigcap_{m=1}^{r} \varphi_j^{-1}(M_m),$$

i.e., (J, h_j) is a finite intersection of maximal ideals. Thus the the theorem also holds for the case n. This concludes the proof. □

Remark 3.22. Let k be a field and let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal satisfying the conditions of Proposition 3.21. Then we see that J is a radical ideal, as it follows from Proposition 3.21 that it is an intersection of prime ideals.

We now state and prove Theorem 3.23. The content of this theorem is the same as that of Lemma 8.19 in [BW98, Section 8.2, p.343]. However, we fill in some details in the proof of this result that were left to the reader.

Theorem 3.23. *Let k be a perfect field and $J \subset k[\mathbf{x}]$ a zero-dimensional ideal. Let us denote for each $1 \leq i \leq n$ the monic generator of $J \cap k[x_i]$ by $f_i \in k[x_i]$ and let $g_i \in k[x_i]$ be the squarefree part of f_i. Then $\sqrt{J} = (J, g_1, ..., g_n) \subset k[\mathbf{x}]$.*

Proof. Set $I := (J, g_1, ..., g_n)$. Note that we have $\sqrt{J} \subset \sqrt{I}$, due to the inclusion $J \subset I$. The proof consists of two arguments. We first argue that $I \subset \sqrt{J}$ and we then proceed to explain that I is in fact radical. From these observations, we see that $\sqrt{J} \subset \sqrt{I} = I \subset \sqrt{J}$, i.e., $I = \sqrt{J}$.

To show that $I \subset \sqrt{J}$, it suffices to elaborate why for every $1 \leq i \leq n$ we have that $g_i \in \sqrt{J}$. Let $1 \leq i \leq n$ and let m_i be the largest multiplicity among the irreducible factors in the unique factorisation of f_i into irreducible polynomials. It then follows that $g_i^{m_i} \in (f_i) = J \cap k[x_i] \subset J$, as g_i is the squarefree part of f_i. Hence, we see that for every $1 \leq i \leq n$ we have that $g_i \in \sqrt{J}$.

We now explain why I is radical. Note that I contains for every $1 \leq i \leq n$ a squarefree univariate polynomial $g_i \in k[x_i]$. Because k is perfect, we know by Lemma 3.20 that for all $1 \leq i \leq n$ we have that $\gcd(g_i, g_i') = 1$. It follows from Remark 3.22 that I is radical. This concludes the proof. □

We now explain how we can compute generators of the radical of a zero-dimensional ideal $(F) \subset k[\mathbf{x}]$, where $F \subset k[\mathbf{x}]$ is a finite set, if k is a perfect field such that squarefree parts of univariate polynomials with coefficients in k can be computed. For each $1 \leq i \leq n$ we can compute the monic generator f_i of $(F) \cap k[x_i]$ by applying the algorithm `Elimination` with input the field k, the subset $\mathbf{u} := \{x_i\}$ and the set F. In order to compute generators of the radical of (F), it suffices to compute for each $1 \leq i \leq n$ the squarefree part of f_i, say g_i, because the set $F \cup \{g_1, ..., g_n\}$ generates the radical of (F) by Theorem 3.23. We summarise the described procedure for calculating the radical of a zero-dimensional ideal in the algorithm `ZeroRadical`.

If the characteristic of the base field k is equal to 0, then computing squarefree parts of univariate polynomials with coefficients in this field is a very simple task. In this case, we have that for a non-constant polynomial $h \in k[x]$, the squarefree part of h is given by h/u with $u := \gcd(h, h')$. If instead the field k is finite, then we can still compute the squarefree part of $h \in k[x]$. However, in this case the problem is a bit more delicate, see for instance [vzGG14, Exercise 14.27, p. 426] or [BW98, Proposition 2.86, p. 104].

Algorithm `ZeroRadical`

Input: A perfect field k, such that squarefree parts of univariate polynomials with coefficients in k can be computed, and a finite set $F \subset k[\mathbf{x}]$ such that $(F) \subset k[\mathbf{x}]$ is a zero-dimensional ideal.
Output: A finite set $H \subset k[\mathbf{x}]$ such that $\sqrt{(F)} = (H)$.

1: $H \leftarrow F$
2: **for** $i = 1, ..., n$ **do**
3: $\quad f_i \leftarrow$ `Elimination`$(k, \{x_i\}, F)$
4: $\quad g_i \leftarrow$ the squarefree part of f_i
5: $\quad H \leftarrow H \cup \{g_i\}$
6: **return** H

3.4 Calculating primary decompositions of zero-dimensional radical ideals

In this subsection, we will explain how we can compute the minimal primary decomposition of a zero-dimensional radical ideal in $k[\mathbf{x}]$, if k is a perfect field, of which the cardinality is infinite, such that we can computationally factorise squarefree univariate polynomials with coefficients in k. Recall from Remark 2.67

that the primary components of a radical ideal $J \subset k[\mathbf{x}]$ are exactly the associated prime ideals of $k[\mathbf{x}]/J$, so in this case, once we have calculated the minimal primary decomposition of J, we know generators for each associated prime ideal of $k[\mathbf{x}]/J$.

The essence of the approach for achieving this is given by Theorem 3.29, which reduces the problem to the factorisation of a univariate polynomial. Before we can formulate and prove this theorem, we need a geometric concept for zero-dimensional ideals.

Definition 3.24. Let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal and let $\overline{k}$ be an algebraic closure of k. We say that J is in *normal position with respect to* x_i if the x_i-components of the points in $Z(J, \overline{k})$ are pairwise different.

We will now proceed to prove Theorem 3.29 and we will then elaborate on the remaining steps for computing the minimal primary decomposition of a zero-dimensional radical ideal. Theorem 3.29 is Proposition 8.69 in [BW98, Section 8.6, p. 372]. However, we give a different proof of Theorem 3.29. In the proof of Theorem 3.29, we will make use of Theorem 3.28. The proof of Theorem 3.28 will in turn make use of Proposition 3.25, which we will now state without proof.

Proposition 3.25. *Let k be a perfect field, let $J \subset k[\mathbf{x}]$ be a zero-dimensional radical ideal and let $\overline{k}$ be an algebraic closure of k. Then* $\dim_k(k[\mathbf{x}]/J) = \#Z(J, \overline{k})$.

Proof. For the proof, see either [KR08, Theorem 3.7.19, p. 253] or [BW98, Theorem 8.32, p. 348]. □

The following lemma will be a useful tool for proving Theorem 3.28 and Theorem 3.29.

Lemma 3.26. *Let k be a field and let $f_1, ..., f_n \in k[x_1]$ be polynomials. Moreover, let $\pi_{f_1} : k[x_1] \to k[x_1]/(f_1)$ be the projection and let $\sigma\colon k[\mathbf{x}] \to k[x_1]$ be the morphism of k-algebra's defined for $h = h(x_1, ..., x_n) \in k[\mathbf{x}]$ by $\sigma(h) := h(x_1, f_2, ..., f_n)$. Then for $\psi_{f_1} := \pi_{f_1} \circ \sigma$ it holds that* $\ker(\psi_{f_1}) = (f_1, x_2 - f_2, x_3 - f_3, ..., x_n - f_n)$.

Proof. Firstly, we will show that $\ker(\sigma) = (x_2 - f_2, x_3 - f_3, ..., x_n - f_n)$. Set $I := (x_2 - f_2, x_3 - f_3, ..., x_n - f_n)$. It is clear that $x_2 - f_2, ..., x_n - f_n \in \ker(\sigma)$, which in turn shows that $I \subset \ker(\sigma)$. To prove the other inclusion, let $h \in \ker(\sigma)$. Define $f := h(x_1, f_2, ..., f_n) \in k[x_1]$, where we only substitute the polynomials $f_2, ..., f_n$ for the variables $x_2, ..., x_n$. Consider then the canonical ring morphism $\pi : k[\mathbf{x}] \to k[\mathbf{x}]/I$. We see that $\pi(f) = \pi(h)$, i.e., $h - f \in I$. On the other hand, $f = 0 \in k[x_1]$, because $f = \sigma(h)$ and $h \in \ker(\sigma)$. We see that $h \in I$. Hence, we conclude that $\ker(\sigma) = I$.

Lastly, we will prove that $\ker(\psi_{f_1}) = (f_1, x_2 - f_2, ..., x_n - f_n)$. Let us define $Q_{f_1} := (f_1, x_2 - f_2, ..., x_n - f_n)$. It is clear that $Q_{f_1} \subset \ker(\psi_{f_1})$. Let now $r \in \ker(\psi_{f_1})$ and define the polynomial $f := r(x_1, f_2, ..., f_n) \in k[x_1]$. By the definition of σ we see that $r - f \in \ker(\sigma)$. Therefore, $\pi_{f_1}(\sigma(r)) = \pi_{f_1}(f) = 0$, i.e., $f \in (f_1)$. Hence, we have that $r \in \ker(\sigma) + (f_1)$, where $\ker(\sigma) + (f_1) = Q_{f_1}$. We conclude that $\ker(\psi_{f_1}) = Q_{f_1}$. □

Before we state and prove Theorem 3.28, we need one more small observation regarding principal radical ideals in unique factorisation domains; we state this in Remark 3.27.

Remark 3.27. Let R be a unique factorisation domain and let r be an element of R. We claim that $(r) \subset R$ is a radical ideal if and only if r is a squarefree element of R.

Indeed, we will first show the contrapositive of the implication from left to right. Let $r \in R$ be a non-squarefree element. Then we will now show that (r) is not a radical ideal. Suppose that $r = u \cdot \prod_{i=1}^m p_i^{e_i}$ with $u \in R^\times$ a unit and $p_i \in R$ pairwise different irreducible factors such that at least one e_j is greater or equal to 2. Set $l := \max_i e_i$ and define $s := \prod_{i=1}^m p_i$.

To prove that (r) is not radical it suffices to show that $(s) = \sqrt{(r)}$, because we have a proper inclusion $(r) \subsetneq (s)$. We see that $(s) = \bigcap_{i=1}^m (p_i)$ and for each $1 \leq i \leq m$ the ideal $(p_i) \subset R$ is prime. Thus, (s) is a radical ideal, because it is equal to a finite intersection of prime ideals. Therefore, $\sqrt{(r)} \subset (s)$. On the other hand, we also have that $s^l \in (r)$, thus $s \in \sqrt{(r)}$. We conclude that $(s) = \sqrt{(r)}$ and this proves the statement.

To prove the other implication, notice that if r is a squarefree element of R, say $r = u \cdot \prod_{i=1}^m p_i$ with $u \in R^\times$ and p_i pairwise different irreducible factors, then we have that $(r) = \bigcap_{i=1}^m (p_i)$. Therefore, (r) is a radical ideal, because it is equal to a finite intersection of prime ideals.

We now state and prove Theorem 3.28. This theorem is Proposition 8.77 in [BW98, Section 8.6, p. 378]. However, our proof of this result will be more precise.

Theorem 3.28. *Let k be a perfect field and let $J \subset k[\mathbf{x}]$ be a zero-dimensional radical ideal. Recall for a subset of variables $\mathbf{u} \subset \mathbf{x}$ the Notation 3.1 for $\mathbf{u} < \mathbf{x}\backslash\mathbf{u}$. Moreover, let $<$ be any monomial order on $M(\mathbf{x})$ such that $\{x_1\} < \{x_2, ..., x_n\}$. If J is in normal position with respect to x_1, then there exist univariate polynomials $g_1, ..., g_n \in k[x_1]$ such that $G := \{g_1, x_2 - g_2, x_3 - g_3, ..., x_n - g_n\}$ is the reduced Gröbner basis of J with respect to $<$.*

Proof. There exists a non-constant monic polynomial $g_1 \in k[x_1]$ such that $J \cap k[x_1] = (g_1)$, because J is a zero-dimensional ideal. Let $\overline{k}$ be an algebraic closure of k. Set $d := \dim_k(k[x_1]/(g_1))$, $r := \dim_k(k[\mathbf{x}]/J)$ and set $t := \#\{\text{different zeros of } g_1 \text{ in } \overline{k}\}$.

Let $\iota\colon k[x_1] \hookrightarrow k[\mathbf{x}]$ be the inclusion and let $\pi\colon k[\mathbf{x}] \to k[\mathbf{x}]/J$ be the projection. The composition $\varphi = \pi \circ \iota$ of these morphisms of k-algebra's induces an injective morphism of k-algebra's $\overline{\varphi}\colon k[x_1]/(g_1) \hookrightarrow k[\mathbf{x}]/J$. We will now show that $\overline{\varphi}$ is surjective. In order to prove this, it suffices to show that $r \leq d$, because we know that $d = \dim_k(\mathrm{im}(\overline{\varphi}))$.

We now proceed to prove that $r \leq d$. Note that $\#Z(J, \overline{k}) = \#\{x_1\text{-components of points } b \in Z(J, \overline{k})\}$, because J is in normal position with respect to x_1. On the other hand, any x_1-component of a point $b \in Z(J, \overline{k})$ is a zero of g_1 in $\overline{k}$. Thus, we see that $\#Z(J, \overline{k}) \leq t$.

By Proposition 3.25 we know that $r = \#Z(J, \overline{k})$, thus we see by the previous paragraph that $r \leq t$.

Moreover, by Remark 3.27 we know that g_1 is squarefree, because $J \cap k[x_1]$ is a radical ideal, which in turn follows from the assumption that J is a radical ideal of $k[\mathbf{x}]$. Thus, it follows from Lemma 3.20 that $\gcd(g_1, g_1') = 1$. This means that g_1 is a separable polynomial, i.e., $d = t$. We conclude that $r \leq d$.

Therefore, we now know that $\overline{\varphi}$ is surjective. This means that for each $2 \leq i \leq n$ there exists a class $\overline{g_i} \in k[x_1]/(g_1)$ such that $\overline{\varphi}(\overline{g_i}) = \overline{x_i} \in k[\mathbf{x}]/J$. Hence, for each $2 \leq i \leq n$ there exists a polynomial $g_i \in k[x_1]$ such that $x_i - g_i \in J$. Set $G := \{g_1, x_2 - g_2, x_3 - g_3, ..., x_n - g_n\}$.

Next, we will show that G is a reduced Gröbner basis of J with respect to $<$. Let $f \in J$ be a monic polynomial, then note that f will be non-constant as J is a proper ideal of $k[\mathbf{x}]$. If there exists an index $2 \leq j \leq n$ such that $\mathrm{LT}(f)$ is divisible by a power of x_j, then $\mathrm{LT}(x_j - g_j) = x_j$ will indeed divide $\mathrm{LT}(f)$. If for each $2 \leq j \leq n$ it holds that $\mathrm{LT}(f)$ is not divisible by any power of x_j, then $\mathrm{LT}(f)$ will be a power of x_1. Note that the monomial order $<$ satisfies the property that $\{x_1\} < \{x_2, ..., x_n\}$. Thus the remaining monomials in f cannot be divisible by any of the variables $x_2, ..., x_n$, i.e., $f \in J \cap k[x_1] = (g_1)$. Thus, we see that in this case $\mathrm{LT}(g_1)|\mathrm{LT}(f)$. We conclude that G is a Gröbner basis of J with respect to $<$.

It is clear that this Gröbner basis of J with respect to $<$ is reduced. This conclude the proof. □

Finally, we state and prove Theorem 3.29.

Theorem 3.29. *Let k be a perfect field and let $J \subset k[\mathbf{x}]$ be a zero-dimensional radical ideal, which is in normal position with respect to x_1. Also, let $g \in k[x_1]$ be the non-constant monic generator of $J \cap k[x_1]$. Then g is a squarefree polynomial. Moreover, let $g = \prod_{i=1}^{t} p_i$ be the factorisation of g into pairwise different irreducible factors. Then $J = \bigcap_{i=1}^{t}(J, p_i)$ is a minimal primary decomposition of J.*

Proof. Note that g is a squarefree polynomial by Remark 3.27, because $J \cap k[x_1]$ is a radical ideal. Moreover, it follows from Theorem 3.28 that there exist univariate polynomials $g_1, ..., g_n \in k[x_1]$ with the property that $G := \{g_1, x_2 - g_2, ..., x_n - g_n\}$ is the reduced Gröbner basis of J with respect to a monomial order $<$ on $M(\mathbf{x})$ such that $\{x_1\} < \{x_2, ..., x_n\}$. Recall from Remark 3.5 that such monomial orders exist. It follows from Proposition 3.6 that g_1 is the monic generator of $J \cap k[x_1]$, i.e., $g_1 = g$.

Now, for each $1 \leq i \leq t$, let ψ_{p_i} be as in Lemma 3.26 with $f_1 = p_i$ and $f_j = g_j$ for $2 \leq j \leq n$. Furthermore, let ψ_{g_1} be as in Lemma 3.26, where for $1 \leq j \leq n$ we set $f_j = g_j$.

Then for each $1 \leq i \leq t$ we have that $\ker(\psi_{p_i}) = (J, p_i)$. Now, by the Chinese Remainder Theorem we have a ring isomorphism $\tau\colon k[x_1]/(g_1) \to \prod_{i=1}^{t} k[x_1]/(p_i)$. Moreover, for the ring homomorphism $\rho := \prod_{i=1}^{t} \psi_{p_i}$ we have that $\rho = \tau \circ \psi_{g_1}$. Furthermore, it holds that $\ker(\rho) = \bigcap_{i=1}^{t} \ker(\psi_{p_i}) = \bigcap_{i=1}^{t}(J, p_i)$. On the other

hand, we also have that $\ker(\rho) = \ker(\psi_{g_1}) = J$, where the first equality follows from the injectivity of τ and the second equality holds by Lemma 3.26. We conclude that $J = \bigcap_{i=1}^{t}(J, p_i)$.

We now explain why $J = \bigcap_{i=1}^{t}(J, p_i)$ is a minimal primary decomposition of J. Note that for each $1 \leq i \leq n$ we have an isomorphism $k[\mathbf{x}]/\ker(\psi_{p_i}) \cong k[x_1]/(p_i)$ induced by ψ_{p_i}, where the latter ring is a non-zero domain. Therefore, for each $1 \leq i \leq n$ we know that the ideal $\ker(\psi_{p_i})$ is prime.

To prove the minimality of the primary decomposition, it suffices to check that for all $j \neq m$ we have that $(J, p_j) \not\subset (J, p_m)$. For the sake of contradiction, suppose that for $j \neq m$ we have that $(J, p_j) \subset (J, p_m)$. Then it particular $p_j \in (J, p_m)$, and therefore $1 = \gcd(p_j, p_m) \in (J, p_m)$. However, (J, p_m) is a prime ideal, which is in particular a proper ideal. We conclude that the primary decomposition is minimal, and this concludes the proof. □

Now, let k be a perfect field and let $J \subset k[\mathbf{x}]$ be a zero-dimensional radical ideal. We will now explain how we will compute the minimal primary decomposition of J, if in addition the base field k is not finite. This is explained in a more precise way in [BW98, Section 8.6, p. 372-379], but we explain the remaining steps in the procedure with more intuition backed up by rigorous arguments.

If J is in normal position with respect to one of the variables and we can computationally factorise squarefree univariate polynomials with coefficients in k, then by Theorem 3.29 we know how to compute the minimal primary decomposition of J. However, not all zero-dimensional radical ideals are necessarily in normal position with respect to one of the variables.

The idea is to put an ideal containing J in normal position with respect to a new variable z. We now explain how we will achieve this, if in addition the base field k is not finite.

We know by Theorem 3.16 that $Z(J, \overline{k})$ is a finite set, say $\#Z(J, \overline{k}) := m$. Suppose $c := (c_1, ..., c_n) \in k^n$ and define $g := z - \sum_{i=1}^{n} c_i x_i$. Consider the ideal $I := (J, g) \subset k[x_1, ..., x_n, z]$. Notice that the zero-locus is given by

$$Z(I, \overline{k}) = \left\{ \left(a_1, ..., a_n, \sum_{i=1}^{n} c_i a_i \right) \in \overline{k}^{n+1} : (a_1, ..., a_n) \in Z(J, \overline{k}) \right\}.$$

We see that $Z(I, \overline{k})$ is again a finite set, so by Theorem 3.16 we know that I is a zero-dimensional ideal. Now, in order to put I in normal position with respect to z, we have to pick a vector $c \in k^n$ such that for every $a, b \in Z(J, \overline{k})$ with $a \neq b$ we have that $\sum_{i=1}^{n} c_i a_i \neq \sum_{i=1}^{n} c_i b_i$.

There are exactly $t := \binom{m}{2}$ different pairs $a, b \in Z(J, \overline{k})$ we have to check. Moreover, note that for fixed $a, b \in Z(J, \overline{k})$ with $a \neq b$ the set

$$V_{a,b} := \left\{ (y_1, ..., y_n) \in k^n : \sum_{i=1}^{n} (b_i - a_i) y_i = 0 \right\} \subset k^n$$

is a k-subspace of k^n of dimension at most equal to $n - 1$. Therefore, in order to put I in normal position with respect to z, we want to find a vector $c \in k^n$ which is not contained in any of the k-subspaces $V_{a,b}$.

If the cardinality of the base field k is infinite, then the t subspaces $V_{a,b}$ will not cover the whole of k^n. Thus, in this case there exist vectors $c \in k^n$ which put I in normal position with respect to z. This means that this approach does not work in general for finite fields, because we have no guarantee of finding an appropriate vector $c \in k^n$.

Furthermore, if the cardinality of the base field k is infinite, an arbitrary choice for $c \in k^n$ will most likely put I in normal position with respect to z. In order to put I in normal position with respect to z, we will pick arbitrary n-tuples of k^n and check if I is in normal position with respect to z.

Now, we need a way to check whether I is in normal position with respect to some variable.

We now explain how we can computationally check if an arbitrary zero-dimensional radical ideal Q in $k[\mathbf{x}]$ is in normal position with respect to one of the variables, under the assumption that k is a perfect field. It follows from Theorem 3.28 that we can check for each $1 \leq i \leq n$ if Q is not in normal position with respect to x_i, by simply inspecting the reduced Gröbner basis of Q with respect to a monomial order $<$ on $M(\mathbf{x})$ such that $\{x_i\} < \mathbf{x} \backslash \{x_i\}$.

The following lemma tells us that in order to show that Q is in normal position with respect to one of the variables, say x_1, it is sufficient to check if there exist univariate polynomials $g_1, ..., g_n \in k[x_1]$ such that $(g_1, x_2 - g_2, ..., x_n - g_n) = Q$.

Lemma 3.30. *Let k be a field. Suppose that $Q \subset k[\mathbf{x}]$ is an ideal for which there exist univariate polynomials $g_1, ..., g_n \in k[x_1]$, where g_1 is a non-constant polynomial, such that $(g_1, x_2 - g_2, ..., x_n - g_n) = Q$. Then Q is a zero-dimensional ideal which is in normal position with respect to x_1.*

Proof. Note that $Z(Q, \overline{k}) = \left\{(a, g_2(a), ..., g_n(a)) \in \overline{k}^n : a \in \overline{k} \text{ is a zero of } g_1\right\}$. We see that $Z(Q, \overline{k}) \neq \varnothing$, because g_1 is a non-constant polynomial. It follows from Remark 3.14 that Q is a proper ideal. Furthermore, $\#Z(Q, \overline{k}) \leq \deg(g_1)$ and thus by Theorem 3.15 we know that Q is a zero-dimensional ideal. By the description of $Z(Q, \overline{k})$, it is clear that Q is normal position with respect to x_1. □

Because we know that some vector $c \in k^n$ will put I in normal position with respect to z, it follows from Theorem 3.28 that the ideal I will have a reduced Gröbner basis, with respect to a monomial order $<$ on $M(\mathbf{x} \cup \{z\})$ with $\{z\} < \mathbf{x}$, which satisfies the conditions of Lemma 3.30.

To sum up, in order to check if the vector $c \in k^n$ puts I in normal position with respect to z, it suffices to inspect the reduced Gröbner basis of I with respect to a monomial order $<$ on $M(\mathbf{x} \cup \{z\})$ with $\{z\} < \mathbf{x}$.

We now explain how we can retrieve the minimal primary decomposition of J from a minimal primary decomposition of I. We summarise this in the following lemma. The content of this lemma is the same as that of Lemma 8.73 in [BW98, Section 8.6, p.375]. However, we give for (2)-(4) in Lemma 3.31 a different proof.

Lemma 3.31. *Let $J \subset k[\mathbf{x}]$ be an ideal and let $(c_1, ..., c_n) \in k^n$. Moreover, let z be another independent variable and let $\iota \colon k[\mathbf{x}] \hookrightarrow k[x_1, ..., x_n, z]$ be the inclusion. Define $g := z - \sum_{i=1}^n c_i x_i$ and consider the ideal $I := (J, g) \subset k[x_1, ..., x_n, z]$. Then the following hold:*

(1) If J is a zero-dimensional ideal, then I is also a zero-dimensional ideal.

(2) We have that $I^{\mathrm{c}} = J$, where we take the contraction with respect to the inclusion ι.

(3) If J is radical, then I is also radical.

(4) Suppose that J is a zero-dimensional radical ideal and that $I = \bigcap_{i=1}^r P_i$ is the minimal primary decomposition of I. Then $J = \bigcap_{i=1}^r P_i^{\mathrm{c}}$ is the minimal primary decomposition of J, where we take the contractions with respect to the inclusion ι.

Proof. To show that (1) holds, note that

$$Z(I, \overline{k}) = \left\{ \left(a_1, ..., a_n, \sum_{i=1}^n c_i a_i \right) \in \overline{k}^{n+1} : (a_1, ..., a_n) \in Z(J, \overline{k}) \right\}.$$

Hence, if $\#Z(J, \overline{k}) < \infty$, then also $\#Z(I, \overline{k}) < \infty$. By Theorem 3.15 this is equivalent to statement (1).

Next, we show that (2) holds. Consider the ring homomorphism $\varphi \colon k[x_1, ..., x_n, z] \to k[\mathbf{x}]$ defined for $f \in k[x_1, ..., x_n, z]$ by $\varphi(f) := f(x_1, ..., x_n, \sum_{i=1}^n c_i x_i)$. It is easily verified that $\ker(\varphi) = (g)$. Note that we have that $\mathrm{id}_{k[\mathbf{x}]} = \varphi \circ \iota$. Furthermore, we leave it to the reader to verify that $\varphi^{-1}(J) = I$. From the last two observations we deduce that $J = \varphi^{-1}(J)^{\mathrm{c}} = I^{\mathrm{c}}$, where we take the contraction with respect to the inclusion ι.

We now show that (3) holds. To show that I is radical, it suffices to show that $\sqrt{I} \subset I$. So, let $f \in \sqrt{I}$, then there exists an integer $l \geq 1$ such that $f^l \in I$. Define $h := \varphi(f)$ with φ as in the proof of (2), then under the quotient map $\pi \colon k[x_1, ..., x_n, z] \to k[x_1, ..., x_n, z]/(g)$ we see that $\pi(h) = \pi(f)$ and thus also $\pi(h^l) = \pi(f^l)$. This means that $f - h \in (g)$ and $f^l - h^l \in (g)$. Define $r := f^l - h^l$, then we have that $f^l - r = h^l \in I^{\mathrm{c}}$, and hence by (2) we know that $h^l \in J$. As J is radical, it follows that $h \in J$. We deduce that $f \in (J, g) = I$, as $f - h \in (g)$. We conclude that I is radical.

Lastly, we show that (4) holds. It follows from (2) that $J = \bigcap_{i=1}^r P_i^{\mathrm{c}}$. By (1) and (3) we know that I is a zero-dimensional radical ideal, hence by Remark 3.10 and Lemma 3.16 each primary component P_i of I

is maximal. Furthermore, for every $1 \leq i \leq r$ the ideal $P_i \cap k[\mathbf{x}]$, where $P_i^{\mathrm{c}} := P_i \cap k[\mathbf{x}]$, is indeed a prime ideal, because P_i is a prime ideal. To prove the minimality of the primary decomposition $J = \bigcap_{i=1}^{r} P_i^{\mathrm{c}}$, it suffices to check for every $j \neq i$ we have that $P_j^{\mathrm{c}} \not\subset P_i^{\mathrm{c}}$.

Each component P_m^{c} appearing in this primary decomposition of J is maximal. Indeed, each component P_m^{c} is a zero-dimensional prime ideal, thus using Lemma 3.16 we see that each component P_m^{c} is maximal. Therefore, in order to show the minimality of the primary decomposition $J = \bigcap_{i=1}^{r} P_i^{\mathrm{c}}$, it suffices to show that for each $j \neq i$ the maximal ideals P_i^{c} and P_j^{c} are comaximal, i.e., for each $j \neq i$ there exist polynomials $g_i \in P_i^{\mathrm{c}}$ and $g_j \in P_j^{\mathrm{c}}$ such that $g_i + g_j = 1$.

To show this, let $1 \leq i < j \leq r$ and note that there exist polynomials $f_i \in P_i$ and $f_j \in P_j$ such that $f_i + f_j = 1$, because P_i and P_j are two different maximal ideals as the given primary decomposition of I is minimal. Recall the ring homomorphism $\varphi\colon k[x_1, ..., x_n, z] \to k[\mathbf{x}]$ defined in the proof of (2) with $\ker(\varphi) = (g)$. Notice that $\varphi(f_i) + \varphi(f_j) = 1$. We will now show that $\varphi(f_i) \in P_i^{\mathrm{c}}$ and $\varphi(f_j) \in P_j^{\mathrm{c}}$. In fact, we claim that for each $1 \leq m \leq r$ it holds that $\varphi(P_m) \subset P_m^{\mathrm{c}}$.

To prove the latter inclusion let $1 \leq m \leq r$ and let $f \in P_m$, and note that it holds that $\varphi(f) = \varphi(\iota(\varphi(f)))$, because we have that $\mathrm{id}_{k[\mathbf{x}]} = \varphi \circ \iota$. Therefore, $f - \iota(\varphi(f)) \in \ker(\varphi) = (g)$, where (g) is contained in P_m as I is contained in P_m. Hence, using that $f - \iota(\varphi(f)) \in P_m$ and that $f \in P_m$ by assumption, we see that $\iota(\varphi(f)) \in P_m$, i.e., $\varphi(f) \in P_m^{\mathrm{c}}$. We conclude that $\varphi(P_m) \subset P_m^{\mathrm{c}}$, hence we see that $\varphi(f_i) \in P_i^{\mathrm{c}}$ and $\varphi(f_j) \in P_j^{\mathrm{c}}$. Therefore, P_i^{c} and P_j^{c} are comaximal, and thus we see that the primary decomposition of J is minimal. □

To conclude, assume that k is a perfect field, which is not finite, such that squarefree univariate polynomials with coefficients in k can be computationally factored. It follows from Lemma 3.31, given that the ideal I is in normal position with respect to z, that we can compute the minimal primary decomposition of J by first calculating the minimal primary decomposition of I using Theorem 3.29, and then calculating generators for the elimination ideal $P_i \cap k[\mathbf{x}]$ for each primary component P_i of I with the help of the algorithm `Elimination`. We summarise the described procedure for computing the minimal primary decomposition of a zero-dimensional radical ideal $J \subset k[\mathbf{x}]$ in the algorithm `PrimaryDecompZeroRad`.

Notice that if the characteristic of the base field k is zero, then this procedure will therefore indeed work, assuming that we can computationally factorise squarefree univariate polynomials with coefficients in k. We will exhibit in Example 3.37 and Example 3.52 in Subsection 3.5 and Subsection 3.6 respectively two calculations using the algorithm `PrimaryDecompZeroRad`.

3.5 Computing primary decompositions of zero-dimensional ideals

In this subsection, we will elaborate on how we can compute the minimal primary decomposition of a zero-dimensional ideal $J \subset k[\mathbf{x}]$ along with generators for each associated prime ideal of $k[\mathbf{x}]/J$, if k is a perfect field k, which is not finite, such that squarefree univariate polynomials with coefficients in k can be computationally factored and squarefree parts of univariate polynomials with coefficients in k can be computed.

The main result used for computing the minimal primary decomposition of J is Theorem 3.36, which states that in order to achieve this it suffices to compute the associated prime ideals of $k[\mathbf{x}]/J$; recall from Corollary 2.66(2) that the associated prime ideals of $k[\mathbf{x}]/J$ are unique up to reordering. Before we can formulate and prove this theorem, we have to define what the *univariate exponent* is of a zero-dimensional ideal in $k[\mathbf{x}]$.

Definition 3.32. Let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal. For every $1 \leq i \leq n$ let $f_i \in k[x_i]$ be the monic generator of $J \cap k[x_i]$ and define

$$\mu_i := \max\Big\{ l \in \mathbf{Z}_{\geq 1} : \text{ for some irreducible polynomial } p \in k[x_i] \text{ we have } p^l | f_i \Big\}.$$

Then $\mu := 1 + \sum_{i=1}^{n} (\mu_i - 1) \in \mathbf{Z}_{\geq 1}$ is called the *univariate exponent* of J.

Remark 3.33. Let k be a field and let $F \subset k[\mathbf{x}]$ be a finite set of polynomials such that $(F) \subset k[\mathbf{x}]$ is a zero-dimensional ideal. Assume also that we can factor univariate polynomials with coefficients in k.

Algorithm `PrimaryDecompZeroRad`

Input: A perfect field k, of which the cardinality is infinite, such that squarefree univariate polynomials with coefficients in k can be computationally factored, and a finite set $F \subset k[\mathbf{x}]$ such that $(F) \subset k[\mathbf{x}]$ is a zero-dimensional radical ideal.

Output: A finite list B consisting of finite subsets $G \subset k[\mathbf{x}]$ such that:

(1) for each $G \in B$ we have that (G) is prime and G is a reduced Gröbner basis of this ideal.

(2) $(F) = \bigcap_{G \in B}(G)$ is the minimal primary decomposition of (F).

$H \leftarrow \varnothing, B \leftarrow \varnothing, Q \leftarrow \varnothing$, $T \leftarrow \varnothing$, $h \leftarrow 1$, $p \leftarrow 1$ and $g \leftarrow 1$
pick a monomial order on $M(\mathbf{x} \cup \{z\})$ with $\{z\} < \mathbf{x}$
while H is not of the form as in Theorem 3.28 **do**
    pick $c := (c_1, ..., c_n) \in k^n$
    $g \leftarrow z - \sum_{i=1}^{n} c_i x_i$
    $H \leftarrow$ the reduced Gröbner basis of $(F, g) \subset k[x_1, ..., x_n, z]$ with respect to $<$
$h \leftarrow H \cap k[z]$
$T \leftarrow$ all the different monic irreducible factors of h
while $T \neq \varnothing$ **do**
    pick $p \in T$
    $T \leftarrow T \backslash \{p\}$
    $Q \leftarrow \{H \cup \{p\}\}$
    $G_i \leftarrow$ `Elimination`$(k, \mathbf{x}, Q)$
    $B \leftarrow B \cup \{G_i\}$
return B

We will explain how we can computationally calculate the univariate exponent of (F). Let μ be the univariate exponent of (F) and for $1 \leq i \leq n$ let μ_i be as in Definition 3.32. For each $1 \leq i \leq n$ we can calculate the monic generator of $(F) \cap k[x_i]$ by calling the algorithm `Elimination` with input the field k, the subset $\mathbf{u} := \{x_i\}$ and the set $F \subset k[\mathbf{x}]$.

Then, we factor each of these generators into its irreducible factors. Lastly, we check the exponents of each irreducible factor appearing within the factorisation of one generator. This will give us for each $1 \leq i \leq n$ the value of μ_i and we can then calculate μ.

We now proceed to prove Theorem 3.36. In the proof of this theorem we will make use of Proposition 3.34 and Lemma 3.35. We first state and prove Proposition 3.34.

Proposition 3.34. *Let k be a perfect field and let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal with univariate exponent μ. Then $\left(\sqrt{J}\right)^{\mu} \subset J$.*

Proof. For each $1 \leq i \leq n$ there exists a monic polynomial $f_i \in k[x_i]$ such that $J \cap k[x_i] = (f_i)$. Let g_i be the squarefree part of f_i. It follows from Theorem 3.23 that $\sqrt{J} = (J, g_1, ..., g_n)$.

Furthermore, $\left(\sqrt{J}\right)^{\mu}$ is generated by products of polynomials in $\sqrt{J}$. It suffices to show that these generators are contained in J. Let f be such a generator, then for $1 \leq i \leq \mu$ and $1 \leq j \leq n$ there exist $h_i \in I$ and $t_{i,j} \in k[\mathbf{x}]$ such that

$$f = \prod_{i=1}^{\mu} \left(h_i + \sum_{j=1}^{n} t_{i,j} g_j \right).$$

By expanding the product on the right-hand side, we see that each term in the outer summation will have

at least one h_i except for the last term. Therefore, there exist a polynomial $h \in J$ such that

$$f = h + \underbrace{\prod_{i=1}^{\mu} \left(\sum_{j=1}^{n} t_{i,j} g_j \right)}_{(*)}.$$

Furthermore, by expanding $(*)$, we see that each term q in $(*)$ is of the form $t \cdot \prod_{r=1}^{n} g_r^{e_r}$ for some $t \in k[\mathbf{x}]$ and integers $e_r \geq 0$ such that $\sum_{r=1}^{n} e_r = \mu$. Write $\mu = 1 + \sum_{i=1}^{n} (\mu_i - 1)$ as in Definition 3.32. Thus, we see that for every term there has to be an index j such that $e_j \geq \mu_j$. This means that $f_j | q$, i.e. $q \in (f_j) = J \cap k[x_j] \subset J$. We conclude that $f \in J$. This concludes the proof. □

We now state and prove Lemma 3.35. This lemma will give us a way to check if a zero-dimensional ideal in $k[\mathbf{x}]$ is primary, in the case that k is a perfect field. This lemma is a special case of Lemma 8.48 in [BW98, Section 8.4, p. 357].

Lemma 3.35. *Let k be a perfect field, $J \subset k[\mathbf{x}]$ a zero-dimensional ideal and let $P \subset k[\mathbf{x}]$ be a prime ideal. Then the following are equivalent:*

(1) P is the only prime ideal containing J.

(2) J is a primary ideal with $\sqrt{J} = P$.

(3) P is maximal and there exists an integer $l \geq 1$ such that $P^l \subset J$.

Proof. Firstly, we show that (1) implies (2). By Lemma 2.23 we know that $\sqrt{J} = P$. Next, we show that J is a primary ideal. Let $f, g \in k[\mathbf{x}]$ such that $f \cdot g \in J$ and $f \notin J$. Then note that (J, g) is a proper ideal of $k[\mathbf{x}]$. Indeed, to see this suppose that $(J, g) = k[\mathbf{x}]$ for the sake of a contradiction, then there exist polynomials $h_1 \in J$ and $h_2 \in k[\mathbf{x}]$ such that $1 = h_1 + h_2 \cdot g$. Hence, we get that $f = h_1 \cdot f + h_2 \cdot f \cdot g \in J$, which contradicts the assumption that $f \notin J$.

Furthermore, in a commutative ring R, any proper ideal is contained in some maximal ideal. Therefore, (J, g) is contained in some maximal ideal P', because (J, g) is a proper ideal. This prime ideal P' contains in particular the ideal J. Hence, as P is the only prime ideal containing J, we conclude that $P = P'$. We conclude that $g \in P = \sqrt{J}$, which proves that J is primary.

Next, we explain why (2) implies (3). It follows from Lemma 3.16 that P is maximal. Let us denote the univariate exponent of J by μ. Then we know by Proposition 3.34 that $P^\mu \subset J$, as $P = \sqrt{J}$ by assumption.

Lastly, we show that (3) implies (1). We first explain why there is at most one prime ideal containing J. Let P' be a prime ideal such that $J \subset P'$, then $P^l \subset P'$. It follows that $P \subset P'$, as P' is a prime ideal. Thus, by the maximality of P, we see that $P = P'$. Furthermore, because J is a zero-dimensional ideal, J is in particular a proper ideal. Hence, we know that J is contained in some maximal ideal. We conclude that P is the only prime ideal containing J. □

Finally, we will state and prove Theorem 3.36. The content of this theorem is the same as that of Lemma 8.60 (iii) in [BW98, Section 8.6, p. 367]. However, in the proof of this result we fill in some details that were left to the reader.

Theorem 3.36. *Let k be a perfect field and let $J \subset k[\mathbf{x}]$ be a zero-dimensional ideal with univariate exponent ν. Let $J = \bigcap_{i=1}^{r} Q_i$ be the minimal primary decomposition of J with $\mathrm{Ass}(k[\mathbf{x}]/J) = \{P_1, ..., P_r\}$ where for each $1 \leq j \leq r$ we have $P_j = \sqrt{Q_j}$. Then for each $1 \leq j \leq r$ we have that $Q_j = (J, P_j^\nu) \subset k[\mathbf{x}]$.*

Proof. Let $1 \leq j \leq r$ and set $Q := Q_j$ and $P := P_j$. We will first show that $(J, P^\nu) \subset Q$. Let μ be the univariate exponent of Q.

By Remark 3.10 we know that Q and P are zero-dimensional ideals, because J is by assumption a zero-dimensional ideal. Therefore, for each $1 \leq m \leq n$ there exist non-constant univariate polynomials $f_m, g_m \in k[x_m]$ such that $J \cap k[x_m] = (f_m)$ and $Q \cap k[x_m] = (g_m)$. Now, for each $1 \leq m \leq n$ it holds that

$g_m | f_m$, because we have that $J \subset Q$. Thus, it follows that $\mu \leq \nu$ by comparing for every $1 \leq m \leq n$ the irreducible factors of g_m and f_m. Hence, $P^\nu \subset P^\mu$.

We now apply Proposition 3.34 with $J = Q$ to see that $P^\mu \subset Q$. Thus, we have that $P^\nu \subset Q$. It follows that $(J, P^\nu) \subset Q$.

We proceed to prove that $Q \subset (J, P^\nu)$. We shall first show that (J, P^ν) is P-primary. It follows from the inclusion $(J, P^\nu) \subset Q$ that (J, P^ν) is a proper ideal, because Q is a proper ideal. Furthermore, by the inclusion $J \subset (J, P^\nu)$ we know that (J, P^ν) is a zero-dimensional ideal. Now, by Proposition 3.16 we also know that P is maximal, because by the inclusion $J \subset P$ we know that P is a zero-dimensional ideal. Notice that $P^\nu \subset (J, P^\nu)$. It follows from Lemma 3.35 that (J, P^ν) is P-primary.

The last observation we need is the following. We claim that $\bigcap_{i \neq j} Q_i \not\subset P$. To prove this claim, assume the contrary. Then there exists an integer $l \neq j$ such that $Q_l \subset P$, because P is a prime ideal. Thus, we see that $\sqrt{Q_l} \subset P$. However, this contradicts the minimality of the primary decomposition of J. Hence, there exists a polynomial $h \in \bigcap_{i \neq j} Q_i$ such that $h \notin P$.

We now prove the inclusion $Q \subset (J, P^\nu)$ by hand. Let $g \in Q$, then $h \cdot g \in \bigcap_{i=1}^r Q_i = J \subset (J, P^\nu)$. Furthermore, (J, P^ν) is P-primary, whereas $h \notin P$, i.e., no power of h is contained in (J, P^ν). Thus, we see that $g \in (J, P^\nu)$. This shows the wanted inclusion. We conclude that $Q = (J, P^\nu)$. □

Now, we will explain how we can compute the minimal primary decomposition of a zero-dimensional ideal $J \subset k[\mathbf{x}]$ along with generators for each associated prime ideal of $k[\mathbf{x}]/J$, if k is a perfect field, which is not finite, such that squarefree univariate polynomials with coefficients in k can be computationally factored and squarefree parts of univariate polynomials with coefficients in k can be computed. The reader may rightfully so tend to require that the field k is perfect and not finite, such that *arbitrary* univariate polynomials with coefficients in k can be computationally factored.

In order to compute the primary components of J, it suffices to compute the associated prime ideals of $k[\mathbf{x}]/J$ by Theorem 3.36. In fact, we know by Remark 3.17 that each associated prime ideal of $k[\mathbf{x}]/J$ is isolated. It follows from Remark 2.67 that the associated prime ideals of $k[\mathbf{x}]/J$ are exactly the primary components of $\sqrt{J}$, i.e., the intersection of all the associated prime ideals of $k[\mathbf{x}]/J$ is the minimal primary decomposition of $\sqrt{J}$.

To sum up, in order to compute the minimal primary decomposition of J, it suffices to compute the minimal primary decomposition of $\sqrt{J}$. In Subsection 3.4, we explained how we can compute the minimal primary decomposition of a zero-dimensional radical ideal and we summarised this procedure in the algorithm `PrimaryDecompZeroRad`. Furthermore, in Subsection 3.3 we have seen how we can calculate generators of the radical of a zero-dimensional ideal and we summarised this method in the algorithm `ZeroRadical`.

This now clarifies the correctness and termination of the algorithm `PrimaryDecompZero`. In this algorithm, we will use the following notation. For a finite set $H \subset k[\mathbf{x}]$ and positive integer ν we define the following set

$$H^\nu := \left\{ \prod_{i=1}^{\nu} h_i : \text{ for each } 1 \leq i \leq \nu \text{ we have } h_i \in H \right\}.$$

Recall that we can easily compute squarefree parts of univariate polynomials with coefficients in a field, of which the characteristic is equal to zero, see the last paragraph of Subsection 3.3. Thus, any field with characteristic equal to zero satisfies the conditions of the algorithm `PrimaryDecompZero`, once we can computationally factor squarefree univariate polynomials with coefficients in this field.

Example 3.37. We will illustrate how the algorithm `PrimaryDecompZero` works in practice by exhibiting an example. Let $k := \mathbf{Q}$ and set $\mathbf{x} := \{x, y, z\}$. Define $F := \{x(x-1), x(z-1), y+z^2-1, z^2(z-1)\}$, and consider the proper ideal $I := (F) \subset k[\mathbf{x}]$. The reader easily verifies that $Z(I, \overline{k}) = \{(0,0,1), (1,0,1), (0,1,0)\}$, and thus using Theorem 3.15 we see that I is a zero-dimensional ideal. We will now apply the algorithm `PrimaryDecompZero` to the field k and the set F.

Firstly, we apply the algorithm `ZeroRadical` to the field k and the set F. We leave it to the reader to verify that for the set $E := \{x(x-1), x(z-1), z(z-1), y+z-1\}$ we have that $\sqrt{I} = (E)$.

Algorithm `PrimaryDecompZero`

Input: A perfect field k, of which the cardinality is infinite, such that squarefree univariate polynomials with coefficients in k can be computationally factored and squarefree parts of univariate polynomials with coefficients in k can be computed, and a finite set $F \subset k[\mathbf{x}]$ such that $(F) \subset k[\mathbf{x}]$ is a zero-dimensional ideal.

Output: A finite list P consisting of pairs (G, H) of finite subsets $G, H \subset k[\mathbf{x}]$ such that:

(1) for each $(G, H) \in P$ we have that (G) is primary with $(H) = \sqrt{(G)}$.

(2) $(F) = \bigcap_{(G,H)\in P}(G)$ is the minimal primary decomposition of (F).

1: $E \leftarrow \varnothing$ and $B \leftarrow \varnothing$
2: $E \leftarrow$ `ZeroRadical`(k, F)
3: $B \leftarrow$ `PrimaryDecompZeroRad`(k, E)
4: $\nu \leftarrow$ the univariate exponent of (F); computed as in Remark 3.33
5: **while** $B \neq \varnothing$ **do**
6: pick $H \in B$
7: $B \leftarrow B \backslash \{H\}$
8: $G \leftarrow \{F \cup H^{\nu}\}$
9: $P \leftarrow P \cup \{(G, H)\}$
10: **return** P

Next, we apply the algorithm `PrimaryDecompZeroRad` to the field k and the set E, i.e., we will calculate the minimal primary decomposition of $\sqrt{I}$. We know that $Z(\sqrt{I}, \overline{k}) = Z(I, \overline{k})$, and we see in this case that $\sqrt{I}$ is not in normal position with respect to x, y and z. Thus, we introduce a new variable t, and we want to find $a, b, c \in k$ such that for $g = t-(ax+by+cz) \in k[x, y, z, t]$ we have that $J_g := (E, g) \subset k[x, y, z, t]$ is in normal position with respect to t. In this case, we know the points in $Z(\sqrt{I}, \overline{k})$, so we can explicitly see what points the set $Z(J_g, \overline{k})$ consists of. A small calculation shows that $Z(J_g, \overline{k}) = \{(0, 0, 1, c), (1, 0, 1, a + c), (0, 1, 0, b)\}$.

We see that for instance for $a = -1$, $b = 1$ and $c = 0$ the ideal J is in normal position with respect to t. But notice that if we had $k := \mathbf{F}_2$, then we would not have been able to pick a triple $a, b, c \in k$ for which J_g is in normal position with respect to t.

Next, we pick a monomial order $<$ such that $\{t\} < \mathbf{x}$. For instance, we can take the lexicographical monomial order $<$ on $M(\{x, y, z, t\})$ with $x > y > z > t$. We leave it to the reader to verify that the set defined by $H := \{t^3 - t, x - (1/2)t^2 + (1/2)t, y - (1/2)t^2 - (1/2)t, z + (1/2)t^2 + (1/2)t - 1\}$ is the reduced Gröbner basis of J_g with respect to $<$. We set $h := t^3 - t$ and we factorise $h = t(t - 1)(t + 1)$.

We define the ideals $N_1 := (H, t)$, $N_2 := (H, t-1)$ and $N_3 := (H, t+1)$, which are the primary components of J_g. We now calculate the elimination ideals $P_1 := N_1 \cap k[\mathbf{x}]$, $P_2 := N_2 \cap k[\mathbf{x}]$ and $P_3 := N_3 \cap k[\mathbf{x}]$, which are the primary components of $\sqrt{I}$, by applying the algorithm `Elimination` to the sets $H \cup \{t\}$, $H \cup \{t - 1\}$ and $H \cup \{t + 1\}$ respectively.

Note that the lexicographical monomial order $<$ on $M(\{x, y, z, t\})$ with $t > x > y > z$ is an example of an inverse block order on $M(\{x, y, z, t\})$ with $\mathbf{x} < \{t\}$. In fact, for this monomial order the sets defined by $H_1 := \{t, x, y, z - 1\}$, $H_2 := \{t - 1, x, y - 1, z\}$ and $H_3 := \{t + 1, x - 1, y, z - 1\}$ are the reduced Gröbner bases of N_1, N_2 and N_3 respectively with respect to $<$. Therefore, by inspecting the sets H_1, H_2 and H_3, we see that the sets $S_1 := \{x, y, z - 1\}, S_2 := \{x, y - 1, z\}$ and $S_3 := \{x - 1, y, z - 1\}$ are the reduced Gröbner bases of the ideals P_1, P_2 and P_3 respectively with respect to the restriction of the monomial order of $<$ to $M(\mathbf{x})$.

Thus, we have now calculated the associated prime ideals of $k[\mathbf{x}]/I$, which are given by P_1, P_2 and P_3. Moreover, we leave it to the reader to verify that the univariate exponent of I is equal to 2. Therefore, $Q_1 := (F, S_1^2)$, $Q_2 := (F, S_2^2)$ and $Q_3 := (F, S_3^2)$ are the primary components of I, where we have that $\sqrt{Q_1} = (S_1)$, $\sqrt{Q_2} = (S_2)$ and $\sqrt{Q_3} = (S_3)$. In fact, the reduced Gröbner bases of Q_1, Q_2 and Q_3 with respect to the lexicographical monomial order $<$ with $x > y > z$ are given by the sets $\{x, y, z - 1\}$, $\{x, y - 1, z^2\}$ and

$\{x-1, y, z-1\}$ respectively. We conclude that

$$I = (x, y, z-1) \cap (x, y-1, z^2) \cap (x-1, y, z-1)$$

is the minimal primary decomposition of I.

3.6 Calculating primary decompositions of general ideals

In this subsection, we will at last explain how we can calculate a minimal primary decomposition of an arbitrary ideal $J \subset k[\mathbf{x}]$ along with generators for each associated prime ideal of $k[\mathbf{x}]/J$, if the cardinality of the field k is infinite and for any subset of variables $\mathbf{u} \subset \mathbf{x}$ it holds that $k(\mathbf{u})$ is a perfect field with the property that we can compute factorisations of squarefree univariate polynomials with coefficients in $k(\mathbf{u})$ and squarefree parts of univariate polynomials with coefficients in $k(\mathbf{u})$. The main idea of the procedure, described in this thesis, of finding a primary decomposition of an arbitrary ideal in $k[\mathbf{x}]$ is to reduce the problem to that of calculating a primary decomposition of a zero-dimensional ideal, for which we can apply the algorithm `PrimaryDecompZero` described in Subsection 3.5.

The way we are going to reduce the problem to zero-dimensional ideals is as follows. Let $I \subset k[\mathbf{x}]$ be an ideal and suppose that $\mathbf{u} \subset \mathbf{x}$ is a maximally independent set of variables mod I. We then consider the extension $I^{\mathrm{e}} \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ of I with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. We will now explain why I^{e} is a zero-dimensional ideal. In order to show this, it suffices to check that for any $y \in \mathbf{x}\backslash\mathbf{u}$ there exists a non-zero polynomial $f \in I^{\mathrm{e}} \cap k(\mathbf{u})[y]$. We know by the maximality of the independent set of variables $\mathbf{u}$ that for each $y \in \mathbf{x}\backslash\mathbf{u}$ there exists a non-zero polynomial $f \in I \cap k[\mathbf{u} \cup \{y\}]$, so in particular we have that $f \in I^{\mathrm{e}} \cap k(\mathbf{u})[y]$. We see that I^{e} is indeed a zero-dimensional ideal.

Next, we are left with the problem of retrieving a primary decomposition of the ideal I from a primary decomposition of I^{e}. To fetch some of the primary components of I from a primary decomposition of I^{e}, we can simply contract each of the primary components appearing in the found primary decomposition of I^{e} with respect to ι; this is the content of Lemma 3.38. In general, we will not be able to recover a complete primary decomposition of I from a primary decomposition of I^{e}. This follows from the observation that we do not necessarily have that the ideal I is equal to I^{ec}, where we take the contraction with respect to ι.

Lemma 3.38 is a generalisation of Lemma 8.97 in [BW98, Section 8.7, p. 392].

Lemma 3.38. *Let R and S be commutative rings, $J \subset S$ be an ideal and let $\varphi\colon R \to S$ be a ring morphism. Then the following hold:*

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

(2) If J is a primary ideal, then $\varphi^{-1}(J) \subset R$ is also a primary ideal.

Proof. We first show that (1) holds. Set $I := \varphi^{-1}\left(\sqrt{J}\right)$ and let $r \in I$. Then there exists an integer $l \geq 1$ such that $\varphi(r)^l \in J$. We also know that $\varphi(r)^l = \varphi(r^l)$, thus we see that $r^l \in \varphi^{-1}(J)$, i.e. $r \in \sqrt{\varphi^{-1}(J)}$. To prove the other inclusion, let $r \in \sqrt{\varphi^{-1}(J)}$. Then there exists an integer $m \geq 1$ such that $\varphi(r^m) \in J$, i.e. $\varphi(r)^m \in J$. This means that $\varphi(r) \in \sqrt{J}$, which in turn tells us that $r \in I$. We conclude that (1) holds.

Next, we show that (2) holds. Let $r, s \in R$ such that $r \cdot s \in \varphi^{-1}(J)$ and $r \notin \varphi^{-1}(J)$. This means that $\varphi(r \cdot s) \in J$, whereas $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$. Now, as J is primary and $\varphi(r) \notin J$, it follows that there exists an integer $l \geq 1$ such that $\varphi(s)^l \in J$. Hence, $s^l \in \varphi^{-1}(J)$, as $\varphi(s)^l = \varphi(s^l)$. We conclude that J is primary. □

There are now two problems that remain to be solved to get a complete primary decomposition of I. Firstly, we need a computational way of finding generators of the contraction of an ideal with respect to the inclusion ι. This procedure will be described in the algorithm `Contraction`. Secondly, we need to retrieve the primary components that we lost by extending and contracting the ideal I. We will see that we will be able to computationally find a non-zero polynomial $h \in k[\mathbf{u}]$ such that $I = (I, h) \cap I^{\mathrm{ec}}$, and we can then in principal repeat the whole process with the ideal (I, h). The procedure for finding such a polynomial h will be described in the algorithm `ExtensionContraction`.

A complete description of the approach of finding a primary decomposition of an arbitrary non-zero ideal $I \subset k[\mathbf{x}]$ can be found in the algorithm `PrimaryDecomp`. In Theorem 3.48, we state that this algorithm terminates and correctly outputs a primary decomposition of any ideal in $k[\mathbf{x}]$, under the aforementioned conditions on the polynomial ring $k[\mathbf{x}]$. Moreover, in Remark 3.49 we explain how we can computationally make a primary decomposition of I minimal, and also how we can check what the associated prime ideals of $k[\mathbf{x}]/I$ are.

We will now proceed to formulate and explain the termination and correctness of both algorithms `Contraction` and `ExtensionContraction`. We will start with formulating the algorithm `Contraction`. The main result used by this algorithm is Theorem 3.43. Our main goal for now is to prove this theorem with the help of Lemma 3.41, but first we require a definition.

Definition 3.39. Let R be commutative ring, $I \subset R$ an ideal and let $F \subset R$ be a subset. We call the set given by $\{g \in R : \text{for all } f \in F \text{ we have } g \cdot f \in I\}$ *the quotient of* I *by* F, which we denote by $I : F$.

Remark 3.40. Let R, I and F be as in Definition 3.39. Then it is easily verified that $I : F$ is an ideal of R.

If F consists of one element of R, say $F = \{f\}$, then we write $I : f$ for the quotient of I by F.

Suppose indeed that $F = \{f\}$ and let m be a non-negative integer. Then we have that $I : f^m \subset I : f^{m+1}$, where $f^0 = 1 \in R$. Indeed, to see that this inclusion holds let $g \in I : f^m$. By the definition of the quotient of I by f^m we have that $g \cdot f^m \in I$, and thus $g \cdot f^{m+1} = (g \cdot f^m) \cdot f \in I$ as I is an ideal of R. Moreover, note that $I = I : f^0$. Notice that in the case that $f = 0$ and $m \geq 1$ we have that $I : f^m = R$.

By the previous paragraph we get an ascending chain $I = I : f^0 \subset I : f^1 \subset I : f^2 \subset ...$ in R. If in addition R is a Noetherian ring, then we know by Remark 2.4 and Proposition 2.2 that there exists an integer $l \geq 0$ such that for all $j \geq l$ we have that $I : f^l = I : f^j$. We set $I : f^\infty := \bigcup_{i \geq 0} I : f^i$. In this case, we see that $I : f^l = I : f^\infty$. Moreover, if $f = 0$, then we see that $I : f^\infty = R$.

In the specific case with $R = k[\mathbf{x}]$ for a field k, it follows by the previous paragraph that there exists an integer $l \geq 0$ such that $I : f^l = I : f^\infty$; recall that we know by Theorem 2.6 that $k[\mathbf{x}]$ is a Noetherian ring.

Lemma 3.41 tells us how we can calculate generators for the ideal $I : f^\infty$. This lemma is Proposition 6.37 in [BW98, Section 6.2, p. 267]. However, we fill in some of the details in the proof of this result that were left to the reader.

Lemma 3.41. *Let k be a field, $I \subset k[\mathbf{x}]$ be an ideal and let $f \in k[\mathbf{x}]$ be a polynomial. Moreover, let y be another indeterminate. Set $J := (I, 1 - y \cdot f) \subset k[x_1, ..., x_n, y]$. Then $I : f^\infty = J \cap k[\mathbf{x}]$.*

Proof. If $f = 0$, then by the last paragraph of Remark 3.40 the statement is clear. So, assume that $f \neq 0$. In this case, we will first show the inclusion $J \cap k[\mathbf{x}] \subset I : f^\infty$. Let $g \in J \cap k[\mathbf{x}]$. Then there exist polynomials $h_1, ..., h_m \in I$ and $r_1, ..., r_m, s \in k[x_1, ..., x_n, y]$ such that $g = \sum_{i=1}^m r_i \cdot h_i + s \cdot (1 - y \cdot f)$. Consider the ring morphism $\varphi \colon k[x_1, ..., x_n, y] \to k(x_1, ..., x_n)$ defined for $p = p(x_1, ..., x_n, y) \in k[x_1, ..., x_n, y]$ by $\varphi(p) := p(x_1, ..., x_n, f^{-1})$. Observe that $\varphi(g) = \sum_{i=1}^m r_i(x_1, ..., x_n, f^{-1}) \cdot h_i(x_1, ..., x_n)$. Let d be the maximum of the degrees of the polynomials r_i in the variable y. Then it follows that $f^d \cdot \varphi(g) \in I$.

Moreover, as φ is the identity on $k[\mathbf{x}]$, we know that $f^d \cdot g = \varphi(f^d \cdot g)$. Thus, we see that $f^d \cdot g = f^d \cdot \varphi(g) \in I$, i.e., $g \in I : f^d$. We conclude that $g \in I : f^\infty$.

We move on to prove the other inclusion. Let $g \in I : f^\infty$. Then there exists an integer $l \geq 0$ such that $f^l \cdot g \in I$. Note that $1 \equiv y \cdot f \mod J$, thus in particular we have that $1 \equiv y^l \cdot f^l \mod J$. By multiplying both sides with g, we see that $g \equiv y^l \cdot f^l \cdot g \mod J$. On the other hand, by the assumption that $f^l \cdot g \in I$, we have that $y^l \cdot f^l \cdot g \in J$. We see that $g \equiv 0 \mod J$, i.e. $g \in J$. As we also have that $g \in k[\mathbf{x}]$, we conclude that $g \in J \cap k[\mathbf{x}]$. This concludes the proof. □

Remark 3.42. Let $F \subset k[\mathbf{x}]$ be a finite set and let $f \in k[\mathbf{x}]$ be a polynomial. It follows from Lemma 3.41 that we can calculate a reduced Gröbner basis of $(F) : f^\infty$ by applying the algorithm `Elimination` to the field k, the subset $\mathbf{u} := \mathbf{x}$ of the variables $\mathbf{x} \cup \{y\}$ and the set $F \cup \{1 - y \cdot f\} \subset k[x_1, ..., x_n, y]$.

We can in fact calculate a non-negative integer l such that $(F) : f^l = (F) : f^\infty$ by mere brute force, i.e., we can check for individual non-negative integers whether the property holds. In order to do this, we need to be able to compute for any $g \in k[\mathbf{x}]$ generators of the quotient ideal $(F) : g$. An algorithm for this

computation can be found in [BW98, Corollary 6.34, p. 266]. Note that once we find a non-negative integer l such that $(F) : f^l = (F) : f^\infty$, then for all $m \geq l$ we have that $(F) : f^m = (F) : f^\infty$, because for $m \geq l$ we have that $(F) : f^l \subset (F) : f^m \subset (F) : f^\infty$.

However, this procedure is not efficient. A more efficient way of finding this integer l can be found in [BW98, Proposition 6.37, p. 267].

We now state and prove Theorem 3.43. The content of this theorem is the same as that of Lemma 8.91 in [BW98, Section 8.7, p. 389]. However, we fill in some of the details in the proof of this result that were left to the reader. In this thesis we have the convention $\operatorname{lcm}\{\varnothing\} := 1$.

Theorem 3.43. *Let $\mathbf{u} \subset \mathbf{x}$ be a subset of variables, $J \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ an ideal and let $<$ be a monomial order on $M(\mathbf{x}\backslash\mathbf{u})$. Suppose that G is a Gröbner basis of J with respect to $<$ such that $G \subset k[\mathbf{x}]$. Set $I := (G) \subset k[\mathbf{x}]$ and define $f := \operatorname{lcm}\{\operatorname{Lc}(g) : g \in G\}$, where for each $g \in G$ we take $\operatorname{Lc}(g) \in k[\mathbf{u}]$ with respect to $<$. Then $J^c = I : f^\infty$, where we take the contraction with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$.*

Proof. In the case that $J = (0)$, then $G = \varnothing$ is the only Gröbner basis of J with respect to $<$. Thus, we have that $I = (0)$ and $f = 1$, and hence we see that $I : f^\infty = I = (0)$. On the other hand, we also have that $J^c = (0)$, as ι is injective. We conclude that in this case the statement holds. Assume now that J is a non-zero ideal.

We will first show that $I : f^\infty \subset J^c$. Let $h \in I : f^\infty$. Then there exists an integer $l \geq 0$ such that $f^l \cdot h \in I$. Note that $I \subset J$, thus we see in particular that $f^l \cdot h \in J$. It follows that $h = f^{-l} \cdot f^l \cdot h \in J$, because we have that f is a non-zero polynomial in $k[\mathbf{u}]$ and J is an ideal of $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. Moreover, we also have that $h \in k[\mathbf{x}]$. We see that $h \in J^c$.

We will now prove the other inclusion. Recall that any $h \in J$ reduces via division with remainder in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ by G to 0 in finitely many iterations, because G is a Gröbner basis of J. Let us denote for any $h \in J$ the amount of iterations it takes to reduce h by G to 0 by $DS(h)$. Notice that in each iteration of the division process of $h \in J$ by G we obtain no remainder. We will proceed to prove that for any $h \in J^c$ we have that $h \in I : f^\infty$ with induction on $DS(h)$.

For the case $DS(h) = 0$, we know that $h = 0$ and in this case we have indeed that $h \in I : f^\infty$. Next, let $N \in \mathbf{Z}_{\geq 1}$ and assume that for all $h \in J^c$ with $0 \leq DS(h) < N$, we have that $h \in I : f^\infty$. We will now show that for any $h \in J^c$ with $DS(h) = N$ it holds that $h \in I : f^\infty$.

In the first iteration, we know that there exists a polynomial $g_i \in G$ such that $\operatorname{Lt}(g_i)$ divides $\operatorname{Lt}(h)$ in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. Then for $h' := h - (\operatorname{Lt}(h)/\operatorname{Lt}(g_i)) \cdot g_i \in J$ we have that $DS(h') = N - 1$. Now, write $r := \operatorname{Lc}(h)/\operatorname{Lc}(g_i)$ and $s := \operatorname{Lm}(h)/\operatorname{Lm}(g_i)$. Then note that $r \cdot s = \operatorname{Lt}(h)/\operatorname{Lt}(g_i)$, $r \in k(\mathbf{u})$ and $s \in M(\mathbf{x}\backslash\mathbf{u})$. By definition of f, we know that $\operatorname{Lc}(g_i)$ divides f in $k[\mathbf{u}]$, thus $f \cdot r \in k[\mathbf{u}]$. Write $t := f \cdot (\operatorname{Lt}(h)/\operatorname{Lt}(g_i)) \cdot g_i$, then we see that $t \in J^c$. On the other hand, it holds that $f \cdot h \in J^c$, as $h \in J^c$ by assumption and $f \in k[\mathbf{u}]$. Putting these observations together, we see that $f \cdot h' = f \cdot h - t \in J^c$.

Moreover, $f \in k[\mathbf{u}]$ is a constant in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, thus for $f \cdot h'$ we also have that $DS(f \cdot h') = N - 1$. It follows from the induction hypothesis that $f \cdot h' \in I : f^\infty$.

Now, notice that $t \in I$, because $g_i \in I$ and $f \cdot (\operatorname{Lt}(h)/\operatorname{Lt}(g_i)) \in k[\mathbf{x}]$. This means in particular that $t \in I : f^\infty$. It follows that $f \cdot h = f \cdot h' + t \in I : f^\infty$, which in turn tells us that $h \in I : f^\infty$. This concludes the induction step. We see that for any $h \in J^c$ we have that $h \in I : f^\infty$. This concludes the proof. □

Remark 3.44. Let $\mathbf{u} \subset \mathbf{x}$ be a subset of variables, $J \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ an ideal and let $<$ be a monomial order on $M(\mathbf{x}\backslash\mathbf{u})$. Moreover, suppose that G is a Gröbner basis of J with respect to $<$ such that $G \subset k[\mathbf{x}]$ and set $I := (G) \subset k[\mathbf{x}]$. Also, let $f \in k[\mathbf{u}]$ be as in Theorem 3.43.

We want to remark that any multiple $h \in k[\mathbf{u}]$ of f also has the property that $J^c = I : h^\infty$, where we take the contraction with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. Indeed, the proof of Theorem 3.43 only uses the properties of f that $f \in k[\mathbf{u}]$ and that for each $g \in G$ we have that $\operatorname{Lc}(g)$ divides f in $k[\mathbf{x}]$.

Next, let k be a field, $\mathbf{u} \subset \mathbf{x}$ a subset of variables and let $F \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ be a finite set. We will now explain how we can compute a reduced Gröbner basis of $(F)^c \subset k[\mathbf{x}]$, where we take the contraction with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. In the case that $\mathbf{u} = \varnothing$, the contraction $(F)^c$ is equal to (F), so the problem reduces to calculating a reduced Gröbner basis of (F). Assume now that $\mathbf{u} \neq \varnothing$.

If $F = \{0\}$ or $F = \varnothing$, then the empty set is a reduced Gröbner basis of $(F)^{\mathrm{c}}$. Thus, suppose also that $F \neq \{0\}$ and $F \neq \varnothing$.

Let now $H' \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ be a Gröbner basis of (F) with respect to a monomial order $<$ on $M(\mathbf{x}\backslash\mathbf{u})$. Notice that after multiplying the elements in H' with units in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, we will still have a Gröbner basis of (F) with respect to $<$. Now, we can multiply each element $h \in H'$ by the least common multiple of all denominators of the coefficients in $k[\mathbf{u}]$ appearing in h, to obtain a Gröbner basis H of (F) with respect to $<$ such that $H \subset k[\mathbf{x}]$.

We can now apply Theorem 3.43 to $J = (F)$ and $G = H$. For $f \in k[\mathbf{u}]$ as in this theorem, it follows that $(F)^{\mathrm{c}} = (H) : f^{\infty}$. Furthermore, we know by Remark 3.42 how we can calculate a reduced Gröbner basis of $(H) : f^{\infty}$. We summarise the described procedure in the case that $\mathbf{u} \neq \varnothing$ for calculating a reduced Gröbner basis of $(F)^{\mathrm{c}}$ in the algorithm `Contraction`.

Algorithm `Contraction`

Input: A field k, a non-empty subset $\mathbf{u} \subset \mathbf{x}$ of variables and a finite set $F \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$.
Output: A reduced Gröbner basis $G \subset k[\mathbf{x}]$ of $(F)^{\mathrm{c}} \subset k[\mathbf{x}]$, where the contraction is taken with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$.

1: $H' \leftarrow \varnothing, H \leftarrow \varnothing$ and $G \leftarrow \varnothing$
2: **if** $(F) = (0)$ **then**
3: $\quad G \leftarrow \varnothing$
4: $\quad$ **return** G
5: $H' \leftarrow$ the reduced Gröbner basis of $(F) \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ with respect to a monomial order $<$ on $M(\mathbf{x}\backslash\mathbf{u})$
6: **while** $H' \neq \varnothing$ **do**
7: $\quad$ pick $h \in H'$
8: $\quad H' \leftarrow H'\backslash\{h\}$
9: $\quad q \leftarrow$ least common multiple of all denominators of the coefficients of $h \in k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$
10: $\quad h \leftarrow q \cdot h$
11: $\quad H \leftarrow H \cup \{h\}$
12: $f \leftarrow \operatorname{lcm}\{\mathrm{Lc}(h)\colon h \in H\}$, where for each $h \in H$ we take $\mathrm{Lc}(h)$ with respect to $<$
13: $G \leftarrow$ `Elimination` $(k, \mathbf{x}, H \cup \{1 - y \cdot f\})$, where y is another independent variable
14: **return** G

Now, we will proceed to formulate the algorithm `ExtensionContraction`. For this purpose, we will exhibit and prove three lemmata. The main result used by this algorithm is Lemma 3.46, which states that for any ideal $I \subset k[\mathbf{x}]$ and any subset of variables $\mathbf{u} \subset \mathbf{x}$ we can computationally find a polynomial $f \in k[\mathbf{u}]$ such that $I^{\mathrm{ec}} = I : f^{\infty}$, where we take the extension and contraction with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. We will prove this lemma with the help of Lemma 3.45.

Lemma 3.45. *Let k be a field, $\mathbf{u} \subset \mathbf{x}$ a subset of variables and let $<$ be an inverse block order on $M(\mathbf{x})$ with respect to $\mathbf{u}$. Set $<'$ to be the restriction of $<$ to $M(\mathbf{x}\backslash\mathbf{u})$. Moreover, let $I \subset k[\mathbf{x}]$ be an ideal and suppose that $G \subset k[\mathbf{x}]$ is a Gröbner basis of I with respect to $<$. Then G is a Gröbner basis of $I^{\mathrm{e}} \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ with respect to $<'$, where the extension is taken with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$.*

Proof. In order to prove that G is a Gröbner basis of I^{e} with respect to $<'$, we will show that for any $f \in I^{\mathrm{e}}$ there exists a polynomial $g \in G$ such that $\mathrm{Lt}(g)$ divides $\mathrm{Lt}(f)$ in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, where both leading terms are taken with respect to $<'$. Note that $I^{\mathrm{e}} = (G) \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, as G generates I.

Let $f \in I^{\mathrm{e}}$ and say that $G = \{g_1, ..., g_m\}$. Then there exist polynomials $q_1, ..., q_m \in k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ such that $f = \sum_{i=1}^{m} q_i \cdot g_i$. Now, let r_i be the least common multiple of all the denominators appearing in the coefficients of $q_i \in k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, and set $r := \prod_{i=1}^{m} r_i$. Notice that $r \in k[\mathbf{u}]$ and $r \cdot f \in I$, as G generates I.

We see that there exists a polynomial $g \in G$ such that $\mathrm{Lt}(g)$ divides $\mathrm{Lt}(r \cdot f)$ in $k[\mathbf{x}]$, where both leading terms are taken with respect to $<$, because $r \cdot f \in I$ and G is a Gröbner basis of I. Note that for any $h \in k[\mathbf{x}]$ the leading monomial of h with respect to $<'$ is equal to the part of the leading monomial of h

in the variables $\mathbf{x}\backslash\mathbf{u}$ with respect to $<$. This follows from Remark 3.4. Therefore, we see that $\textsc{Lt}(g)$ still divides $\textsc{Lt}(r \cdot f)$ in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, where both leading terms are taken with respect to $<'$.

Furthermore, as we also know that $r \in k[\mathbf{u}]$ is a constant in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, it follows that $\textsc{Lt}(g)$ divides $\textsc{Lt}(f)$ in $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, where both leading terms are taken with respect to $<'$. We conclude that G is a Gröbner basis of I^{e} with respect to $<'$. □

We now state and prove Lemma 3.46.

Lemma 3.46. *Let k be a field, $\mathbf{u} \subset \mathbf{x}$ a subset of variables and let $<$ be an inverse block order on $M(\mathbf{x})$ with respect to $\mathbf{u}$. Moreover, let $I \subset k[\mathbf{x}]$ be an ideal and assume that $G \subset k[\mathbf{x}]$ is a Gröbner basis of I with respect to $<$. Set $<'$ to be the restriction of $<$ to $M(\mathbf{x}\backslash\mathbf{u})$ and define $f := \operatorname{lcm}\{\textsc{Lc}(g) : g \in G\}$, where for every $g \in G$ we take $\textsc{Lc}(g) \in k[\mathbf{u}]$ with respect to $<'$. Then we have that $I^{\mathrm{ec}} = I : f^{\infty}$, where we take the extension and contraction with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$.*

Proof. It follows from Lemma 3.45 that G is a Gröbner basis of I^{e} with respect to $<'$. Hence, by applying Theorem 3.43 to the monomial order $<'$, to the ideal $J = I^{\mathrm{e}}$ and to the Gröbner basis G of I^{e} we conclude that $I^{\mathrm{ec}} = I : f^{\infty}$. □

Before we can formulate the algorithm `ExtensionContraction`, we need one more observation.

Lemma 3.47. *Let R be a commutative ring, $I \subset R$ be an ideal and let $r \in R$. Moreover let m be a non-negative integer such that $I : r^m = I : r^{\infty}$. Then we have that $I = (I, r^m) \cap (I : r^m)$.*

Proof. The inclusion $I \subset (I, r^m) \cap (I : r^m)$ is clear. We will show the other inclusion. Let $s \in (I, r^m) \cap (I : r^m)$. Then by assumption $r^m \cdot s \in I$ and there exist elements $t \in I$ and $q \in R$ such that $s = t + q \cdot r^m$. By multiplying the last equation on both sides with r^m, we see that $r^m \cdot s = r^m \cdot t + r^{2m} \cdot q$. Thus, it follows that $r^{2m} \cdot q = r^m \cdot s - r^m \cdot t \in I$, i.e. $q \in I : r^{2m}$. On the other hand, note that $I : r^{2m} \subset I : r^{\infty} = I : r^m$. Hence, we see that $r^m \cdot q \in I$. We conclude that $s \in I$ and this proves the wanted equality. □

Now, we will explain how the algorithm `ExtensionContraction` works. Let k be a field, $\mathbf{u} \subset \mathbf{x}$ a subset of variables and let $F \subset k[\mathbf{x}]$ be a finite set. Moreover, let $<$ be an inverse block order on $M(\mathbf{x})$ and let $<'$ be the restriction of the monomial order $<$ to $M(\mathbf{x}\backslash\mathbf{u})$. We will explain how we can compute a non-zero polynomial $f \in k[\mathbf{u}]$ and a non-negative integer l such that $(F) = (F, f^l) \cap (F)^{\mathrm{ec}}$, where we take the extension and contraction with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$.

Notice that in the case that $\mathbf{u} = \varnothing$, we can take $f = 1$ and $l = 1$ for which it trivially holds that $(F) = (F, f^l) \cap (F)^{\mathrm{ec}}$, because in this case ι is the identity on $k[\mathbf{x}]$. Thus, it remains to explain how we can calculate f and l with the required property in the case that $\mathbf{u} \neq \varnothing$.

Let G be a Gröbner basis of (F) with respect to $<$ and let $f \in k[\mathbf{u}]$ be as in Lemma 3.46. It follows from this lemma that $(F)^{\mathrm{ec}} = I : f^{\infty}$. Moreover, we know by Lemma 3.47 that for any integer $l \geq 0$ such that $(F) : f^l = (F) : f^{\infty}$ it holds that $(F) = (F, f^l) \cap (I : f^l)$. Putting these results together we see that $(F) = (F, f^l) \cap (F)^{\mathrm{ec}}$. Furthermore, recall from Remark 3.42 that we can calculate a non-negative integer l with the property that $(F) : f^l = (F) : f^{\infty}$. This now shows that the algorithm `ExtensionContraction` works correctly.

Finally, we will explain how the algorithm `PrimaryDecomp` works. Let k be a field, which is not finite, such that for any subset of variables $\mathbf{u} \subset \mathbf{x}$ it holds that $k(\mathbf{u})$ is a perfect field with the property that we can compute factorisations of squarefree univariate polynomials with coefficients in $k(\mathbf{u})$ and squarefree parts of univariate polynomials with coefficients in $k(\mathbf{u})$. The reader may rightfully so tend to require that k is a field, which is not finite, such that for any subset of variables $\mathbf{u} \subset \mathbf{x}$ it holds that $k(\mathbf{u})$ is a perfect field with the property that *arbitrary* univariate polynomials with coefficients in $k(\mathbf{u})$ can be computationally factored.

In the case that (F) is equal to $k[\mathbf{x}]$, we know that the empty decomposition forms a primary decomposition of (F). Thus, let us assume that (F) is a proper ideal. Moreover, we may also assume that (F) is a non-zero ideal, because the decomposition consisting of only (0) forms a primary decomposition of (0). Indeed, we know that $k[\mathbf{x}]$ is a domain, thus (0) is in fact a prime ideal.

Algorithm `ExtensionContraction`

Input: A field k, a subset $\mathbf{u} \subset \mathbf{x}$ of variables and a finite set $F \subset k[\mathbf{x}]$.

Output: A non-zero polynomial $f \in k[\mathbf{u}]$ and a non-negative integer l such that $(F) = (F, f^l) \cap (F)^{\mathrm{ec}}$, where the extension and contraction are taken with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$.

1: **if** $\mathbf{u} = \varnothing$ **then**
2: $\quad f \leftarrow 1$
3: $\quad l \leftarrow 1$
4: $\quad$ **return** f and l
5: pick an inverse block order on $M(\mathbf{x})$ with respect to $\mathbf{u}$
6: $<' \leftarrow$ the restriction of $<$ to $M(\mathbf{x}\backslash\mathbf{u})$
7: $G \leftarrow$ the reduced Gröbner basis of (F) with respect to $<$
8: $f \leftarrow \operatorname{lcm}\{\mathrm{Lc}(g) : g \in G\}$, where for each $g \in G$ we take $\mathrm{Lc}(g)$ with respect to $<'$
9: $l \leftarrow$ a non-negative integer such that $(F) : f^l = (F) : f^\infty$ using Remark 3.42
10: **return** f and l

First, we calculate a subset of variables $\mathbf{u} \subset \mathbf{x}$ which is a maximally independent set of variables mod (F) using either of the two methods in Remark 3.9.

Next, we consider the extension $(F)^{\mathrm{e}}$ of (F) with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. As we mentioned at the beginning of this subsection, the ideal $(F)^{\mathrm{e}} \subset k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$ is now a zero-dimensional ideal. Moreover, note that $(F)^{\mathrm{e}}$ is generated by the finite set F.

We may and will then apply the algorithm `PrimaryDecompZero` with input the field $k(\mathbf{u})$ and the finite set F. It follows from Lemma 3.38 that we can contract the minimal primary decomposition of $(F)^{\mathrm{e}}$ along with the associated prime ideals of $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]/(F)^{\mathrm{e}}$ with respect to the inclusion ι, i.e., we can contract each individual primary component, appearing in the primary decomposition of $(F)^{\mathrm{e}}$, and each individual associated prime ideal of $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]/(F)^{\mathrm{e}}$ with respect to ι, to obtain a primary decomposition of $(F)^{\mathrm{ec}}$ and generators of the radicals of these primary ideals. In the case that $\mathbf{u} = \varnothing$, these contractions of the primary components of $(F)^{\mathrm{e}}$ will not be necessary, because the extension and contractions now happen with respect to the identity on $k[\mathbf{x}]$.

In the case that $\mathbf{u} \neq \varnothing$, we will accomplish the contraction of the minimal primary decomposition of $(F)^{\mathrm{e}}$ along with the associated prime ideals of $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]/(F)^{\mathrm{e}}$ by calling the algorithm `Contraction` on each primary component of $(F)^{\mathrm{e}}$ and associated prime ideal of $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]/(F)^{\mathrm{e}}$ separately with input the field k, the subset of variables $\mathbf{u}$ and the generators of this component or this associated prime ideal respectively. This primary decomposition of $(F)^{\mathrm{ec}}$ is not yet a complete primary decomposition of (F), as we have mentioned at the beginning of this subsection. See also Example 3.52. Moreover, the calculated radicals of the primary ideals in this decomposition of $(F)^{\mathrm{ec}}$ are not necessarily associated prime ideals of $k[\mathbf{x}]/(F)^{\mathrm{ec}}$. See also Example 3.52. After the algorithm `PrimaryDecomp` is finished, we can check which of these prime ideals are associated prime ideals of $k[\mathbf{x}]/(F)$, which we will explain in Remark 3.49.

With the help of the algorithm `ExtensionContraction`, we can calculate a non-zero polynomial $f \in k[\mathbf{u}]$ and an integer $l \geq 0$ such that $(F) = (F, f^l) \cap (F)^{\mathrm{ec}}$. We then continue recursively by repeating this process with the finite set $F \cup \{f^l\}$.

We will show in Theorem 3.48 that this procedure will eventually end and that the output is correct. We summarise the described procedure for calculating a primary decomposition of an arbitrary non-zero ideal $(F) \subset k[\mathbf{x}]$, under the mentioned assumptions on the field k, in the algorithm `PrimaryDecomp`.

We now prove the termination and correctness of the algorithm `PrimaryDecomp`. The content of Theorem 3.48 is the same as that of Theorem 8.101 in [BW98, Section 8.7, p. 395]. However, we have given an induction proof, instead of a Noetherian induction proof as is given in the proof of Theorem 8.101.

Theorem 3.48. *Let k be a field and let $F \subset k[\mathbf{x}]$ be a finite set, both of which satisfy the conditions in the algorithm* `PrimaryDecomp`*. Then algorithm* `PrimaryDecomp` *terminates after finitely many steps and it correctly outputs a primary decomposition of $(F) \subset k[\mathbf{x}]$.*

Algorithm `PrimaryDecomp`

Input: A field k, of which the cardinality is infinite, such that for any subset of variables $\mathbf{u} \subset \mathbf{x}$ it holds that $k(\mathbf{u})$ is a perfect field with the property that we can compute factorisations of squarefree univariate polynomials with coefficients in $k(\mathbf{u})$ and squarefree parts of univariate polynomials with coefficients in $k(\mathbf{u})$, and a finite set $F \subset k[\mathbf{x}]$ with $F \neq \varnothing$ and $F \neq \{0\}$.

Output: A list L of pairs (G, H) of finite sets $G, H \subset k[\mathbf{x}]$ such that, if $1 \in (F)$ we have that $L = \varnothing$, while otherwise:

(1) for each $(G, H) \in L$ we have that (G) is primary with $(H) = \sqrt{(G)}$ and both sets G and H are a reduced Gröbner basis of the ideals respectively.

(2) $(F) = \bigcap_{(G,H)\in L}(G)$.

(3) for each $(G_1, H_1), (G_2, H_2) \in L$ set of different pairs we have that $(H_1) \neq (H_2)$.

1: $L \leftarrow \varnothing$, $C \leftarrow \varnothing$ and $\mathbf{u} \leftarrow \varnothing$
2: **if** $1 \in (F)$ **then**
3: $\quad L \leftarrow \varnothing$
4: $\quad$ **return** L
5: $\mathbf{u} \leftarrow \{u_1, ..., u_r\}$ a maximally independent set of variables mod (F) using Remark 3.9
6: $Q \leftarrow$ `PrimaryDecompZero`$(k(\mathbf{u}), F)$
7: **if** $\mathbf{u} = \varnothing$ **then**
8: $\quad C \leftarrow Q$
9: $\quad$ skip steps 10-15 and continue at step 16
10: **while** $Q \neq \varnothing$ **do**
11: $\quad$ pick $(A, B) \in Q$
12: $\quad Q \leftarrow Q \backslash \{(A, B)\}$
13: $\quad G \leftarrow$ `Contraction`$(k, \mathbf{u}, A)$
14: $\quad H \leftarrow$ `Contraction`$(k, \mathbf{u}, B)$
15: $\quad C \leftarrow C \cup \{(G, H)\}$
16: $(f, l) \leftarrow$ `ExtensionContraction`$(k, \mathbf{u}, F)$
17: $L \leftarrow C \cup$ `PrimaryDecomp`$(k, F \cup \{f^l\})$
18: **return** L

Proof. Let us assume that $(F) \subset k[\mathbf{x}]$ is a proper ideal, because if $(F) = k[\mathbf{x}]$ the algorithm `PrimaryDecomp` terminates and its output is indeed correct. Before we continue to prove the termination and correctness of `PrimaryDecomp`, we want to note that we correctly apply the three algorithms appearing in the algorithm `PrimaryDecomp` with the stated input. For the calls of `Contraction` and `ExtensionContraction` this is clear.

We also apply the algorithm `PrimaryDecompZero` in step 6 with input $k(\mathbf{u})$ and F correctly; we have explained at the beginning of this subsection that if $\mathbf{u}$ is a maximally independent set of variables mod (F), then $(F)^{\mathrm{e}}$ is a zero-dimensional ideal of $k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$, where we take the extension of (F) with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u})[\mathbf{x}\backslash\mathbf{u}]$. Moreover, the other conditions on the field $k(\mathbf{u})$ in the algorithm `PrimaryDecompZero` are by assumption satisfied.

Now, we will first explain why the algorithm will terminate after finitely many steps.

After the i-th iteration, i.e., after step 15 in the i-th call of the algorithm, we retrieve an integer $l_i \geq 0$ and a polynomial $f_i \in k[\mathbf{x}]$ by the call of `ExtensionContraction` and we recursively call the algorithm `PrimaryDecomp` with input the field k and the set $F \cup \{f_1^{l_1}, ..., f_i^{l_i}\}$. In fact, f_i is not contained in the ideal $(F \cup \{f_1^{l_1}, ..., f_{i-1}^{l_{i-1}}\})$, because f_i is a non-zero polynomial in $k[\mathbf{u}_i]$, where $\mathbf{u}_i$ is a subset of the variables $\mathbf{x}$ picked in step 5 in the i-th call of `PrimaryDecomp` with the property that $(F \cup \{f_1^{l_1}, ..., f_{i-1}^{l_{i-1}}\}) \cap k[\mathbf{u}_i] = (0)$.

If the algorithm were not to terminate, then we would get an ascending chain $(F) \subsetneq (F, f_1^{l_1}) \subsetneq (F, f_1^{l_1}, f_2^{l_2}) \subsetneq ...$ of ideals in $k[\mathbf{x}]$, where this chain would not stabilise after finitely many steps. However, $k[\mathbf{x}]$ is a Noetherian ring and therefore this would contradict Proposition 2.2. We conclude that the

algorithm `PrimaryDecomp` terminates.

We move on to prove the correctness of the algorithm `PrimaryDecomp`. To be more specific, let us denote the amount of recursive calls of `PrimaryDecomp` for the set F by $RC(F)$; we will then verify the properties (1)-(3) of the output of the algorithm with induction on $RC(F)$.

In the case that $RC(F) = 0$, the algorithm terminates at step 4 and the output does indeed satisfy properties (1)-(3).

Now, let $N \in \mathbf{Z}_{\geq 1}$ and assume that the properties (1)-(3) of the output of the algorithm `PrimaryDecomp` hold for all finite sets $F \subset k[\mathbf{x}]$ with the property that $0 \leq RC(F) < N$. Then we will show that for any finite set $F \subset k[\mathbf{x}]$ with $RC(F) = N$ the enlisted properties of the output of `PrimaryDecomp` also hold.

In the first call of the algorithm `PrimaryDecomp`, we compute in step 16 a polynomial $f_1 \in k[\mathbf{u}_1]$ and an integer $l_1 \geq 0$ such that $(F) = (F, f_1^{l_1}) \cap (F)^{\mathrm{ec}}$, where the extension and contraction are taken with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u}_1)[\mathbf{x}\backslash\mathbf{u}_1]$. We then continue recursively with the set $F \cup \{f_1^{l_1}\}$, where the procedure terminates by assumption after $N-1$ steps. By the induction hypothesis, the output L' of `PrimaryDecomp` applied to the field k and to the set $F \cup \{f_1^{l_1}\}$ satisfies properties (1)-(3).

Next, we will show that the list C obtained in the first call of the algorithm `PrimaryDecomp` applied to the field k and to the set F satisfies properties (1) and (3).

We will first verify property (1) for the list C. In the case that $\mathbf{u}_1 = \varnothing$, it is clear from the description of the output of the algorithm `PrimaryDecompZero` that property (1) holds. Thus, suppose that $\mathbf{u}_1 \neq \varnothing$ and let us look at one iteration of steps 10-15 in the algorithm. Let Q be the list from which we have obtained C and let $(A, B) \in Q$. We know that $(A) \subset k(\mathbf{u}_1)[\mathbf{x}\backslash\mathbf{u}_1]$ is a primary ideal with $(B) = \sqrt{(A)}$. It follows from Lemma 3.38 that the contraction $(A)^{\mathrm{c}}$ is a primary ideal with $\sqrt{(A)^{\mathrm{c}}} = (B)^{\mathrm{c}}$, where both contractions are taken with respect to the inclusion ι. This explanation clarifies property (1).

Secondly, we check that property (3) holds for the list C. Let $(G_1, H_1), (G_2, H_2) \in C$ be two different pairs in the list C. Then there exist two pairs (A_1, B_1) and (A_2, B_2) in the list Q from which we have obtained the pairs (G_1, H_1) and (G_2, H_2) respectively. In fact, the pairs (A_1, B_1) and (A_2, B_2) are two different elements of the list Q, because the two pairs (G_1, H_1) and (G_2, H_2) are different elements of the list C.

Moreover, the ideals (B_1) and (B_2) in $k(\mathbf{u}_1)[\mathbf{x}\backslash\mathbf{u}_1]$ are different, because we know that the algorithm `PrimaryDecompZero` returns a minimal primary decomposition of the ideal $(F) \subset k(\mathbf{u}_1)[\mathbf{x}\backslash\mathbf{u}_1]$. If $\mathbf{u}_1 = \varnothing$, then the sets H_1 and H_2 respectively are equal to B_1 and B_2 respectively. In the case that $\mathbf{u}_1 \neq \varnothing$, the sets H_1 and H_2 respectively are computed by a call of `Contraction` from B_1 and B_2 respectively.

Note that we know by Lemma A.1, applied to $R = k[\mathbf{x}]$, the multiplicatively closed set $S = M(\mathbf{u}_1)$ and the natural map ι with the natural identification $R_S \cong k(\mathbf{u}_1)[\mathbf{x}\backslash\mathbf{u}_1]$, that $(H_1)^{\mathrm{e}} = (B_1)$ and $(H_2)^{\mathrm{e}} = (B_2)$. Now, if the ideals (H_1) and (H_2) were equal, then we would thus get that $(B_1) = (B_2)$. However, we know that the ideals (B_1) and (B_2) are not equal, therefore the ideals (H_1) and (H_2) are not equal. We conclude that property (3) holds for the list C.

Next, we will show that the properties (1)-(3) hold for the complete list L, which we obtain by putting the lists L' and C together. It is clear that the list L satisfies property (1), because both lists L' and C satisfy this property. Notice that we have that

$$(F)^{\mathrm{ec}} = \left(\bigcap_{(A,B)\in Q} (A) \right)^{\mathrm{c}} = \bigcap_{(A,B)\in Q} (A)^{\mathrm{c}} = \bigcap_{(G,H)\in C} (G).$$

Thus, we see that the list L also satisfies property (2), because this property also holds for the set $F \cup \{f_1^{l_1}\}$ and the list L'. As both lists L' and C satisfy property (3) separately, we only need to check that for different pairs $(G_1, H_1) \in L'$ and $(G_2, H_2) \in C$ we have that $(H_1) \neq (H_2)$. Notice that $(H_2) \cap k[\mathbf{u}_1] = (0)$, because (H_2) is a contraction of a proper ideal $(B_2) \subset k(\mathbf{u}_1)[\mathbf{x}\backslash\mathbf{u}_1]$ for some pair $(A_2, B_2) \in Q$. The fact that (B_2) is a proper ideal of $k(\mathbf{u}_1)[\mathbf{x}\backslash\mathbf{u}_1]$ follows from the fact that it is a prime ideal. Thus, we see in particular that $f_1 \notin (H_2)$, because f_1 is a non-zero polynomial in $k[\mathbf{u}_1]$. On the other hand, we do have that $f_1 \in (H_1)$, because $(F, f_1^{l_1})$ is contained in (H_1) and (H_1) is a prime ideal of $k[\mathbf{x}]$. We see that $(H_1) \neq (H_2)$.

We conclude that in the case $RC(F) = N$, the output L of `PrimaryDecomp` satisfies properties (1)-(3). This concludes the proof for the correctness of the algorithm `PrimaryDecomp`. □

Remark 3.49. Let k be a field satisfying the conditions of Theorem 3.48 and let $F \subset k[\mathbf{x}]$ be a finite non-empty set with $F \neq \{0\}$. By applying the algorithm `PrimaryDecomp` to the field k and the set F, we receive a list L satisfying the properties of the output mentioned in the algorithm `PrimaryDecomp`. We know in particular that $(F) = \bigcap_{(G,H)\in L}(G)$ is a primary decomposition of (F), with the property that for two different pairs $(G_1, H_1), (G_2, H_2) \in L$ we have that $(H_1) \neq (H_2)$.

Therefore, in order to make this primary decomposition minimal, we only need to make the decomposition irredundant. This can be achieved by checking for every $(G_i, H_i) \in L$ whether for $L' := L\backslash\{(G_i, H_i)\}$ and $I_i := \bigcap_{(G,H)\in L'}(G)$, we have that I_i is contained in (G_i). To do this computationally, we can try to find generators of I_i and then check whether each generator is contained in (G_i). Finding generators of a finite intersection of ideals is not too complicated, see for instance [BW98, Proposition 6.19, p. 259].

Notice that by making this primary decomposition of (F) minimal, we know exactly what the associated prime ideals of $k[\mathbf{x}]/(F)$ are. In fact, we have generators for each associated prime ideal of $k[\mathbf{x}]/(F)$.

Remark 3.50. We wish to note that the field $\mathbf{Q}$ satisfies the conditions of Theorem 3.48. We refer for a proof of the fact that for any subset of variables $\mathbf{u} \subset \mathbf{x}$ we can computationally factorise squarefree univariate polynomials with coefficients in $\mathbf{Q}(\mathbf{u})$ to [BW98, Corollary 2.104, p. 114].

In fact, any algebraic number field ℓ satisfies the conditions of Theorem 3.48. The approach for computationally factoring, for any subset of variables $\mathbf{u} \subset \mathbf{x}$, squarefree univariate polynomials with coefficients in $\ell(\mathbf{u})$ is in essence the same as described in the reference in the previous paragraph. We will not explain the details in this thesis.

Remark 3.51. Notice that in the algorithm `PrimaryDecomp` there may be some free choice in picking a maximally independent set mod an ideal. As we will see in Example 3.52, a different choice may lead to a different primary decomposition.

Also, the output of the algorithm `ExtensionContraction` may be altered accordingly with Remark 3.44 and Remark 3.42. For an example of this phenomenon we refer to [BW98, end of p. 398]. This reflects the fact that a primary decomposition, even a minimal primary decomposition, of an ideal is not in general unique.

Example 3.52. We will exhibit an example of a calculation of a primary decomposition of an ideal in $k[\mathbf{x}]$ using the algorithm `PrimaryDecomp`. This example will illustrate that the primary decomposition the algorithm yields might not always be the same, because there is a lot of free choice in the algorithm. This again illustrates that a minimal primary decomposition of an ideal is not in general unique.

Let $k := \mathbf{Q}$, set $\mathbf{x} := \{x, y, z\}$, and consider for the set $F := \{yz^2, z(x^2 - y^2), zy(x + y), z^4\}$ the proper ideal defined by $I := (F) \subset k[\mathbf{x}]$. We now apply the algorithm `PrimaryDecomp` to the field k and the set F. Notice that by Remark 3.50, the field $k := \mathbf{Q}$ satisfies the conditions of this algorithm.

The only maximal independent set mod (F) is the set $\mathbf{u}_0 := \{x, y\}$, as the reader can check using either of the two procedures in Remark 3.9. In this case, there is no need to apply `PrimaryDecompZero` to the field $k(\mathbf{u}_0)$ and the set F, because we see by inspection that $(F)^{\mathrm{e}} = (z) \subset k(\mathbf{u}_0)[z]$ which is a prime ideal, where we take the extension with respect to the inclusion $\iota\colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u}_0)[z]$. The reader easily verifies that by applying the algorithm `Contraction` to the field k, the subset of variables $\mathbf{u}_0$ and the set $\{z\}$ yields the set $\{z\}$, thus we see that $(F)^{\mathrm{ec}} = (z)$.

Next, we apply `ExtensionContraction` to the field k, the subset of variables $\mathbf{u}_0$ and the set F. Notice that the set F is the reduced Gröbner basis of I with respect to the lexicographical monomial order on $M(\{x, y, z\})$ with $z > x > y$, which is an inverse block order on $M(\{x, y, z\})$ with respect to $\mathbf{u}_0$, as is mentioned in Example 3.3. In this case, we see that $f_1 := \mathrm{lcm}\{1, y, x^2 - y^2, (x + y)y\} = (x^2 - y^2)y$. Furthermore, the reader easily verifies using either of the methods in Remark 3.42 that for $l_1 = 1$ it holds that $I : f_1^l = I : f_1^\infty$, using that we have that $I : f_1^\infty = (z)$.

Thus, we see that the first iteration of the algorithm `PrimaryDecomp` yields that $I = (F \cup \{f_1\}) \cap (z)$. We now apply the algorithm `PrimaryDecomp` to the field k and the set $F_1 := F \cup \{f_1\}$. Let us define $I_1 = (F_1) \subset k[\mathbf{x}]$. The ideal I_1 has two maximally independent sets of variables mod I_1, namely $\mathbf{u}_1 := \{x\}$

and $\mathbf{u}_2 := \{y\}$. We will first pick $\mathbf{u}_1 := \{x\}$ and then proceed, and later we will see what happens if we had chosen $\mathbf{u}_2 := \{y\}$.

Let us first take $\mathbf{u}_1 = \{x\}$. We now apply the algorithm `PrimaryDecompZero` to the field $k(\mathbf{u}_1)$ and the set F_1, i.e., we will compute the minimal primary decomposition of I_1^{e} along with the associated prime ideals of $k(\mathbf{u}_1)[y,z]/I_1^{\mathrm{e}}$, where we take the extension with respect to $\iota_1 \colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u}_1)[y,z]$.

Define $J_1 := \sqrt{I_1^{\mathrm{e}}} \subset k(\mathbf{u}_1)[y,z]$. The set $H_2 := \{z, y(y^2 - x^2)\}$ is the reduced Gröbner basis of J_1 with respect to the lexicographical monomial order $<$ on $M(\{y,z\})$ with $z > y$. This can be verified by first computing generators of J_1 by applying the algorithm `ZeroRadical` to the field $k(\mathbf{u}_1)$ and the set F_1, and then by computing the reduced Gröbner basis of J_1 with respect to $<$. Next, we apply the algorithm `PrimaryDecompZeroRad` to the field $k(\mathbf{u}_1)$ and the set H_2. Notice that using Lemma 3.30 we see that J_1 is already in normal position with respect to y. Moreover, we see that for $h = y(y^2 - x^2)$ we have that $J_1 \cap k(\mathbf{u}_1)[y] = (h)$, where we factorise $h = y(y-x)(y+x)$.

Therefore, we see that the ideals $N_1 := (H_2, y)$, $N_2 := (H_2, y - x)$ and $N_3 := (H_2, y + x)$ are the primary components of the ideal J_1, i.e., these are the associated prime ideals of $k(\mathbf{u}_1)[y,z]/I_1^{\mathrm{e}}$, where a small calculation shows that $B_1 := \{z, y\}, B_2 := \{z, y - x\}$ and $B_3 := \{z, y + x\}$ are the reduced Gröbner bases, with respect to the lexicographical monomial order $<$ on $M(\{y,z\})$ with $z > y$, of N_1,N_2 and N_3 respectively.

Moreover, the reader easily verifies that the univariate exponent of I_1^{e} is equal to 2. Thus, the primary components of I_1^{e} are given by $Q_1 := (F_1, B_1^2)$, $Q_2 := (F_1, B_2^2)$ and $Q_3 := (F_1, B_3^2)$, where the associated prime ideals of $k(\mathbf{u}_1)[y,z]/I_1^{\mathrm{e}}$ are given by $\sqrt{Q_1} = (B_1)$, $\sqrt{Q_2} = (B_2)$ and $\sqrt{Q_3} = (B_3)$. In fact, the sets B_1, B_2 and $B_4 := \{z^2, y + x\}$ are the reduced Gröbner bases of Q_1, Q_2 and Q_3 respectively with respect to the lexicographical monomial order on $M(\{y,z\})$ with $z > y$.

Furthermore, the reader easily verifies using the algorithm `Contraction` that the ideals $(B_1), (B_2)$ and (B_4) in $k[\mathbf{x}]$ are the primary components of I_1^{ec}, where the associated prime ideals of $k[\mathbf{x}]/I_1^{\mathrm{ec}}$ are given by $\sqrt{(B_1)} = (B_1)$, $\sqrt{(B_2)} = (B_2)$ and $\sqrt{(B_4)} = (B_3)$.

Next, we apply the algorithm `ExtensionContraction` to the field k and the set F_1, which yields $f_2 := x^2$ and $l_2 := 1$. The reduced Gröbner basis of the ideal $I_2 := (F_1 \cup \{f_2\}) \subset k[\mathbf{x}]$ with respect to the lexicographical monomial order $<$ on $M(\{\mathbf{x}\})$ with $x > y > z$ is given by $G_2 := \{x^2, xyz, y^2z, yz^2, y^3, z^4\}$. In fact, the ideal I_2 is (x,y,z)-primary, which we will leave to the reader to verify; this can be checked by applying the algorithm `PrimaryDecomp` to the field k and the set $F_1 \cup \{f_2\}$.

Putting the results of the second iteration together, we see that

$$I_1 = I_2 \cap I_1^{\mathrm{ec}} = (y,z) \cap (x - y, z) \cap (x + y, z^2) \cap (x^2, xyz, y^2z, yz^2, y^3, z^4)$$

is a primary decomposition of I_1.

In conclusion, we have found that

$$I = (z) \cap (y,z) \cap (x - y, z) \cap (x + y, z^2) \cap (x^2, xyz, y^2z, yz^2, y^3, z^4)$$

is a primary decomposition of I. In fact, this decomposition is not minimal. We see that the primary decomposition of I given by

$$I = (z) \cap (x + y, z^2) \cap (x^2, xyz, y^2z, yz^2, y^3, z^4)$$

is in fact minimal, where the associated prime ideals of $k[\mathbf{x}]/I$ are $(z), (x + y, z)$ and (x, y, z).

Let us now consider what the output of the algorithm `PrimaryDecomp` would have been if we had chosen the subset of variables $\mathbf{u}_2 = \{y\}$ in the second iteration.

As in the case of $\mathbf{u}_1 = \{x\}$, we would apply the algorithm `PrimaryDecompZero` to field $k(\mathbf{u}_2)$ and the set F_1, in order to compute the minimal primary decomposition of I_1^{e}, where we take the extension of I_1 with respect to the inclusion $\iota_2 \colon k[\mathbf{x}] \hookrightarrow k(\mathbf{u}_2)[x,z]$. For the sake of brevity, we will gloss over this calculation, as it is similar to what we have done as in the case of $\mathbf{u}_1 = \{x\}$. In fact, we have that $I_1^{\mathrm{ec}} = (x+y, z^2) \cap (x-y, z)$ is a primary decomposition of I_1^{ec}, where $(x + y, z^2)$ is a $(x + y, z)$-primary ideal and where $(x - y, z)$ is a prime ideal.

The algorithm `ExtensionContraction` applied to the field k and the set F_1 yields $f_3 := y$ and $l_3 := 1$. Set $I_3 := (F_1 \cup \{f_3\})$, then we see that $I_3 = (x^2z, y, z^4)$ by inspection. Thus, in this case we have that $I_1 = (x^2z, y, z^4) \cap (x + y, z^2) \cap (x - y, z)$. In fact, the reader easily verifies that $I_3 = (x^2, y, z^4) \cap (y, z)$ is a primary decomposition of I_3, where (x^2, y, z^4) is a (x, y, z)-primary ideal and where (y, z) is a prime ideal; this can be done by hand, using a similar approach as in Nonexample 2.39 to prove that the intersection of the two stated ideals is equal to I_3, and then separately checking that both ideals are primary. To conclude, in this case we have found that

$$I = (z) \cap (y, z) \cap (x - y, z) \cap (x + y, z^2) \cap (x^2, y, z^4)$$

is also a primary decomposition of I. Moreover, the reader again easily verifies that the primary decomposition given by

$$I = (z) \cap (x + y, z^2) \cap (x^2, y, z^4)$$

is minimal.

A Localisation of commutative rings and modules

In this section, we briefly discuss localisations of commutative rings and modules over commutative rings. Let R be a commutative ring and let M be an R-module throughout this section. We will follow Section 4 of Chapter 2 in [Mat89].

A subset $S \subset R$ is called *multiplicatively closed* if $1 \in S$ and it is closed under multiplication. The localisation of R with respect to a multiplicatively closed set S is defined to be the set of equivalence classes $(R \times S)/\sim$, where $\sim$ is an equivalence relation on $R \times S$ which is defined as follows. For elements $(r, s_1), (t, s_2) \in R \times S$ we define $(r, s_1) \sim (t, s_2)$ if and only if there exists an element $s_3 \in S$ such that $s_3 \cdot (s_2 r - s_1 t) = 0 \in R$. For our convenience, we write R_S instead of $(R \times S)/\sim$ and r/s for the equivalence class of (r, s) in R_S.

For $r/s_1, t/s_2 \in R_S$ we have well-defined operations in R_S defined by

$$r/s_1 + t/s_2 := (rs_2 + ts_1)/s_1 s_2 \quad \text{and} \quad (r/s_1) \cdot (t/s_2) := rt/s_1 s_2,$$

which turn R_S into a commutative ring. Furthermore, we have a canonical ring homomorphism $\iota \colon R \to R_S$ defined by $r \mapsto r/1$. We suggestively denote this morphism with ι, but note that ι is injective if and only if S does not contain any zero-divisors of R.

The localisation of M with respect to S is similar. We define the same equivalence relation on $M \times S$ and we denote the set of equivalence classes by M_S. We write m/s for the equivalence class of (m, s) in M_S.

We define for $m/s_1, n/s_2 \in M_S$ and $r/s_3 \in R_S$ the following well-defined operations

$$m/s_1 + n/s_2 := (s_2 m + s_1 n)/s_1 s_2 \quad \text{and} \quad (r/s_3) \cdot (m/s_1) := rm/s_3 s_1,$$

with which M_S is a R_S-module. In this case, we also have a canonical R-linear homomorphism $\tau \colon M \to M_S$ defined by $m \mapsto m/1$.

The multiplicatively closed set $R \backslash P$ for a prime ideal $P \subset R$ is often used. To shorten the notation we write R_P and M_P instead of $R_{R\backslash P}$ and $M_{R\backslash P}$ respectively.

We can in fact characterise the localisation of R and M with respect to S with a universal property, but the current construction is sufficient for our purposes. We will now state and prove some results concerning R_S and M_S. The first goal is to characterise prime ideals in R_S. This characterisation is stated in Proposition A.4, which we prove using Lemma A.1 and A.3.

Lemma A.1. *Let R be a commutative ring, $S \subset R$ a multiplicatively closed set, $\iota \colon R \to R_S$ the canonical ring homomorphism and let $J \subset R_S$ be an ideal. Then there exists an ideal $I \subset R$ such that $J = I^{\mathrm{e}}$, where we take the extension of I with respect to ι.*

Proof. We claim that $I := J^{\mathrm{c}}$ is the desired ideal, where we take the contraction of J with respect to ι. We now argue that $J = I^{\mathrm{e}}$. Notice that $\iota(I) \subset J$, and hence $I^{\mathrm{e}} \subset J$. To prove the other inclusion, let $r/s \in J$. This means that $\iota(r) = r/1$ is an element of J, hence $r \in I$, and therefore $\iota(r) \in \iota(I)$. We conclude that $r/s = (1/s) \cdot (r/1) \in I^{\mathrm{e}}$. This concludes the proof. □

From the previous lemma we can easily deduce that if R is a Noetherian ring, i.e., if every ideal in R is finitely generated, then R_S is also a Noetherian ring.

Proposition A.2. *Let R be a Noetherian ring and let $S \subset R$ be a multiplicatively closed set. Then R_S is a Noetherian ring.*

Proof. For the proof, see [Eis95, Corollary 2.3, p. 62]. □

Lemma A.3. *Let R be a commutative ring, $S \subset R$ a multiplicatively closed set, $\iota\colon R \to R_S$ the canonical ring homomorphism and let $I \subset R$ be an ideal. Then for any $c \in R$ and $q \in S$ with $c/q \in I^{\mathrm{e}}$ there exists an element $t \in S$ such that $t \cdot c \in I$, where we take the extension of I with respect to ι.*

Proof. There exist elements $r_k \in R, s_k \in S$ and $c_k \in I$ with $1 \leq k \leq n$ such that

$$\frac{c}{q} = \sum_{k=1}^{n} \frac{r_k}{s_k} \cdot \frac{c_k}{1}.$$

Set $s := \prod_{k=1}^{n} s_k$ and define also $d := \sum_{j=1}^{n} \left(\prod_{k \neq j} s_k \right) r_j c_j$. Then we have that

$$\frac{c}{q} = \frac{d}{s}.$$

Moreover, notice that $s \in S$ and $d \in I$. Therefore, there exists an element $t' \in S$ such that $t's \cdot c = t'q \cdot d$, where we have that $t'q \cdot d \in I$. Hence, $t := t's \in S$ is the sought after element. □

We shall now state and prove Proposition A.4.

Proposition A.4. *Let R be a commutative ring, $S \subset R$ a multiplicatively closed set, $\iota\colon R \to R_S$ the canonical ring homomorphism. Define $\mathscr{P}_S := \{P : P \in \operatorname{Spec}(R) \text{ such that } P \cap S = \varnothing\}$. Then the maps*

$$\begin{aligned} \mathscr{P}_S &\longleftrightarrow \operatorname{Spec}(R_S) \\ P &\longmapsto P^{\mathrm{e}} \\ J^{\mathrm{c}} &\longmapsfrom J \end{aligned}$$

are each other's inverse, where we take the extensions and contractions of ideals with respect to ι.

Proof. We first have to check that both maps are well-defined. Let us denote the map from left to right by φ and the map from right to left by ψ. The well-definedness of ψ follows immediately from the fact that ι is a ring homomorphism.

In order to prove the well-definedness of φ, we need to show that for $P \in \mathscr{P}_S$, the ideal $P^{\mathrm{e}} \subset R_S$ is prime. Therefore, let $a/r, b/s \in R_S$ be such that $(a/r) \cdot (b/s) = ab/rs \in P^{\mathrm{e}}$. By Lemma A.3, we know that there exists an element $t_1 \in S$ such that $t_1 \cdot ab \in P$. Because $S \cap P = \varnothing$ and P is a prime ideal, we have that either $a \in P$ or $b \in P$. Hence, either $a/r \in P^{\mathrm{e}}$ or $b/s \in P^{\mathrm{e}}$. Note also that $P^{\mathrm{e}} \neq R_S$, because $S \cap P = \varnothing$. We conclude that φ is well-defined.

We now argue why the maps are each other's inverse. The proof of the fact that $\varphi \circ \psi = 1_{\operatorname{Spec}(R_S)}$ uses the same arguments as the proof of Lemma A.1. We only show that $\psi \circ \varphi = 1_{\mathscr{P}_S}$. We want to show that for $P \in \mathscr{P}_S$, we have that $P = P^{\mathrm{ec}}$. Note that for any $r \in P$, we have that $\iota(r) \in P^{\mathrm{e}}$ and hence $r \in P^{\mathrm{ec}}$. To prove the other inclusion, let $r \in R$ such that $\iota(r) = r/1 \in P^{\mathrm{e}}$. Then by Lemma A.3 there exists an element $t \in S$ such that $t \cdot r \in P$. Because $S \cap P = \varnothing$ and P is a prime ideal, we have that $r \in P$. □

Now, let $S \subset R$ be a fixed multiplicatively closed set. Then for any R-modules M and N and for any given R-linear homomorphism $g\colon M \to N$, we have an induced R_S-linear homomorphism $g_S\colon M_S \to N_S$ defined for $m/s \in M_S$ by $g_S(m/s) := g(m)/s$. In fact, the assignment $g \mapsto g_S$ is functorial in g.

Furthermore, the functor $M \mapsto M_S$ with the previously defined assignment on the R-linear homomorphisms is an exact functor, i.e., it maps an exact sequence of R-modules to an exact sequence of R_S-modules. This is the content of Lemma A.5, which is the second-to-last result of this section.

Lemma A.5. *Let R be a commutative ring and let $S \subset R$ be a multiplicatively closed set. The assignment given by $M \mapsto M_S$ forms an exact functor from the abelian category of R-modules to the abelian category of R_S-modules.*

Proof. For the proof, see [Mat89, Theorem 4.5, p. 26]. □

Moreover, localisations of R-modules commute with taking intersections of modules. This is the content of the following lemma.

Lemma A.6. *Let R be a commutative ring, M an R-module, $N, L \subset M$ submodules and let $S \subset R$ be a multiplicatively closed set. Then $N_S \cap L_S = (N \cap L)_S$.*

Proof. For the proof, see [AM69, Corollary 3.4 (ii), p. 39]. □

References

[AM69] M. Atiyah and I. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[BvLT24] M. Bright, R. van Luijk, and D. Testa. Geometry and arithmetic of surfaces. Draft version, 2024.

[BW98] T. Becker and V. Weispfenning. *Gröbner Bases: a Computational Approach to Commutative Algebra*. Springer, 1998. doi:10.1007/978-1-4612-0913-3.

[CLO18] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, fourth edition, 2018. doi:10.1007/978-3-319-16721-3.

[Con] K. Conrad. Noetherian modules. Accessed at 01-04-2024. URL: https://kconrad.math.uconn.edu/blurbs/linmultialg/noetherianmod.pdf.

[EGSS13] D. Eisenbud, D. Grayson, M. Stillman, and B. Sturmfels. *Computations in Algebraic Geometry with Macaulay 2*. Springer, 2013. doi:10.1007/978-3-662-04851-1.

[EHV92] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Inventiones Mathematicae*, 110:207–235, 1992. doi:10.1007/BF01231331.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 1995. doi:10.1007/978-1-4612-5350-1.

[GTZ88] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6:149–167, 1988.

[Har77] R. Hartshorne. *Algebraic Geometry*. Springer, 1977. doi:10.1007/978-1-4757-3849-0.

[KR08] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1*. Springer, 2008. doi:10.1007/978-3-540-70628-1.

[Lan02] S. Lang. *Algebra*. Springer, 2002. doi:10.1007/978-1-4613-0041-0.

[Mat89] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1989. doi:10.1017/CBO9781139171762.

[MS05] E. Miller and B. Sturmfels. *Combinatorial Commutative Algebra*. Springer, 2005. doi:10.1007/b138602.

[SY96] T. Shimoyama and K. Yokoyama. Localization and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 22:247–277, 1996. doi:10.1006/jsco.1996.0052.

[SZ65] P. Samuel and O. Zariski. *Commutative Algebra*, volume 1. D. Van Nostrand, 1965.

[vzGG14] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, third edition, 2014. doi:10.1017/CBO9781139856065.