UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Algoritmos de álgebra conmutativa en anillos de polinomios

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Santiago Jorge Laplagne

Director de tesis: Dra. Teresa Krick

Consejero de estudios: Dra. Teresa Krick

Buenos Aires, 2012

Algoritmos de álgebra conmutativa en anillos de polinomios

Resumen

En esta tesis nos enfocamos en los aspectos algorítmicos de algunos de los tópicos más importantes del álgebra conmutativa. Estudiamos el cálculo de radicales y primos y minimales, la normalización de anillos e ideales y otros problemas relacionados. En los últimos años, se desarrollaron varios programas de álgebra computacional con implementaciones muy eficientes de las herramientas básicas para trabajar con polinomios, ideales y anillos. Esto renovó el interés por algoritmos eficientes para resolver algunos problemas difíciles del área.

Proponemos nuevos algoritmos para algunos de estos problemas, basándonos en ideas matemáticas y resultados nuevos. Hemos implementado todos los algoritmos en esta tesis en SINGULAR (Decker et al., 2011), uno de los programas de álgebra computacional más comúnmente utilizados, y están actualmente disponibles para su uso por toda la comunidad matemática. Si bien para la mayoría de estos problemas ya existían algoritmos, los nuevos algoritmos propuestos los superan en la mayoría de los casos, siendo ahora los algoritmos por default en SINGULAR.

Palabras clave: ideales polinomiales, radical, primos minimales asociados, normalización, bases enteras

Commutative algebra algorithms in polynomial rings

Abstract

This thesis addresses the algorithmic aspects of some major topics of commutative algebra. We study the computation of radicals and minimal associated primes of ideals, the normalization of rings and ideals and other related problems. In recent years a number of computer algebra systems have been developed with very efficient implementations of some basic tools to work with polynomials, ideals and rings. This put on the spot the need for efficient algorithms to solve some difficult problems.

We propose new algorithms for some of these problems, based on new mathematical ideas and results. All the algorithms in this thesis have been implemented in SINGULAR (Decker et al., 2011), one of the most commonly used computer algebra systems, and are now available for use of the mathematical community. Although other algorithms already existed for most of these tasks, the new algorithms outperform them in most cases and are now the default algorithms in SINGULAR.

Keywords: polynomial ideals, radical, minimal associate primes, normalization, integral bases

Agradecimientos

A mi familia mamá, papá, Diego, Ignacio, Naty, Nico, Fede.

A Teresa por guiarme y aconsejarme a lo largo de ya tanto años.

A toda la gente del equipo Singular de Kaiserslautern: Gert-Martin Greuel, Wolfram Decker, Gerhard Pfister, Janko Böhm, Frank Seelisch, Hans Schönemann, Stefan Steidel, Andreas Steenpaß, Petra Bäsell, que siempre me trataron tan bien y son parte fundamental de esta tesis.

A los jurados Alicia Dickenstein, André Galligo y Thomas Markwig, por el laburo de leer la tesis y sus valiosos comentarios.

A toda la gente de la Olimpíada: Patricia, Flora, Ceci, Bibi, Elisita, Juanca, Graciela, Julia, Marita, Vero, Norma y Juan Carlos.

Y a todos mis amigos, con quienes compartí en estos años almuerzos, meriendas, oficinas y tantas cosas, Dano, Flor, Santi, Guille, Colo, Dani, Delpe, Caro, Eze, Ele, Vendra, Carla, Gabriela, Leandro, Sandra, Fede, Seba, Nico, Marce, Charly, Martín, Maxi, Nahuel, Sergio, Vicky, Magui, Mariana, Ani, Constanza, Cristian, Malena, Agustín, Dora, Gustavo, Pablo H, Eduardo, Matilde, Flavia, Gumu, Julián, Silvia, Fernando, Tada, Fede.

Contents

Capítulo 1

Introducción (Versión en español)

Los fundamentos del álgebra conmutativa fueron introducidos hace más de un siglo, a mediados del siglo XIX. Dedekind definió en 1879 la noción de ideal, que podemos considerar como el punto de partida de la teoría, en los suplementos que escribió al libro *Vorlesungen ber Zahlentheorie* (Dirichlet, 1968) que contenía las notas de las clases de Dirichlet sobre teoría de números. También probó un teorema de factorización de ideales para una clase especial de anillos que ahora llamamos anillos de Dedekind.

Unos años más tarde, Lasker (1905) generalizó estos resultados, desarrollando la teoría de descomposición primaria y demostrando la existencia de esta descomposición para ideales en anillos de polinomios.

Alrededor de 1920, Emmy Noether estudió estos trabajos, simplificándolos y reformulando la teoría en un contexto mucho más general. Su brillante trabajo (Noether, 1921) es considerado como el punto de partida del álgebra conmutativa moderna.

En esta tesis nos enfocamos en los aspectos algorítmicos de algunos de los tópicos más importantes del álgebra conmutativa. Estudiamos el cálculo de radicales y primos y minimales, la normalización de anillos e ideales y otros problemas relacionados. En los últimos años, se desarrollaron varios programas de álgebra computacional con implementaciones muy eficientes de las herramientas básicas para trabajar con polinomios, ideales y anillos. Esto renovó el interés por algoritmos eficientes para resolver algunos problemas difíciles del área.

Proponemos nuevos algoritmos para algunos de estos problemas, basándonos en ideas matemáticas y resultados nuevos. Hemos implementado todos los algoritmos en esta tesis en Singular (Decker et al., 2011), uno de los programas de álgebra computacional más comúnmente utilizados, y están actualmente disponibles para su uso por toda la comunidad matemática. Si bien para la mayoría de estos problemas ya existían algoritmos, los nuevos algoritmos propuestos los superan en la mayoría de los casos, siendo ahora los algoritmos por default en Singular.

1.1 Radical y primos minimales asociados

Dado un ideal $I \subset k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, k un cuerpo, el radical de I es el ideal

$$\sqrt{I} = \{f \in k[\boldsymbol{x}] \mid f^m \in I \text{ para algún } m \in \mathbb{N}\}.$$

El radical juega un papel importante en el álgebra conmutativa cuando nos interesan los aspectos geométricos, en virtud de la biyección que existe entre variedades e ideales radicales sobre cuerpos algebraicamente cerrados.

Aunque la definición es muy simple, calcular el radical de un ideal es generalmente muy difícil computacionalmente. En los últimos años, se propusieron varios algoritmos, entre los que mencionamos (Gianni et al., 1988), (Krick and Logar, 1991b) y (Eisenbud et al., 1992) para el caso general, (Kemper, 2002) para el caso cero–dimensional y (Matsumoto, 2001) para ideales en anillos sobre cuerpos de característica positiva.

En el Capítulo 4 proponemos un algoritmo para el cálculo del radical basado en las ideas de Gianni et al. (1988) y Krick and Logar (1991b), comparamos nuestra implementación del mismo con las implementaciones de otros algoritmos y analizamos la complejidad teórica. Los resultados de esta sección se encuentran publicados en (Laplagne, 2006a) y (Laplagne, 2006b).

En (Krick and Logar, 1991b), los autores usan la herramienta para descomposición de ideales $\sqrt{I} = \sqrt{I : h} \cap \sqrt{\langle I, h\rangle}$ (Proposición 4.2.1) para un h adecuado (Proposición 4.2.13). Encuentran h tal que $\sqrt{I : h}$ pueda calcularse reduciendo el problema al caso cero–dimensional y calculan $\sqrt{\langle I, h\rangle}$ por inducción en la dimensión. Al tomar el ideal $\langle I, h\rangle$, aparecen componentes redundantes (es decir, componentes que no forman parte de la descomposición del ideal original) que vuelven lento al algoritmo. En nuestro nuevo algoritmo (Algoritmo 4.2.1), evitamos usar el ideal $\langle I, h\rangle$, considerando en cambio la saturación $I : h^\infty$ para distintos polinomios h. Esto lleva a un algoritmo más eficiente en la mayoría de los casos.

Una tarea relacionada es calcular los primos minimales asociados de un ideal. Geométricamente, esto equivale a descomponer el conjunto de soluciones del sistema de ecuaciones polinomiales en sus componentes irreducibles. Es decir, podemos interpretarlo como resolver el sistema dado, cuando no nos interesan las multiplicidades de las soluciones, o más generalmente, la estructura algebraica de las mismas.

En la sección 4.3, mostramos como se pueden aplicar las mismas ideas que usamos para calcular el radical de un ideal al cálculo de los primos minimales. Hacemos una breve descripción del nuevo algoritmo y comparamos el rendimiento de la implementación que hicimos en Singular con la de otros algoritmos implementados.

Conjuntamente con Wolfram Decker, Gert-Martin Greuel y Hans Schönemann hemos implementado los algoritmos propuestos para el cálculo del radical de un ideal y de los primos minimales asociados en la biblioteca `primdec` (Decker et al., 2006) de Singular.

1.2 Normalización de anillos

En el Capítulo 5 nos dedicamos al problema de calcular la normalización de anillos de polinomios. Es otra herramienta importante del álgebra conmutativa, con aplicaciones en geometría algebraica y teoría de singularidades. El contenido de las Secciones 5.1 a 5.5 es un trabajo en conjunto con Gert-Martin Greuel y Frank Seelisch, presentado en (Greuel et al., 2010). El enfoque local propuesto en la Sección 5.6 es un trabajo en conjunto con Janko Böhm, Wolfram Decker, Gerhard Pfister, Andreas Steenpaßy Stefan Steidel, presentado en una versión más general en (Böhm et al., 2011a).

Sea A un anillo conmutativo Noetheriano reducido (es decir, sin elementos nilpotentes).

Sea $A \subset B$ una extensión de anillos. Decimos que $b \in B$ es entero sobre A si existen $a_i \in A$, $1 \leq i \leq s$, tales que

$$b^s + a_1 b^{s-1} + \cdots + a_{s-1} b + a_s = 0.$$

La *clausura entera* de A en B es el conjunto de todos los elementos de B enteros sobre A.

Definimos el anillo de fracciones $Q(A) = S^{-1}A$, donde S es el conjunto de elementos no divisores de cero de A y $S^{-1}A$ es la localización de A en S. La *normalización* $\bar{A}$ de A es la clausura entera de A en $Q(A)$. Un anillo A se dice *normal* si $A = \bar{A}$.

En nuestros algoritmos, consideramos el anillo $R = k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, con k un cuerpo e $I \subset R$ un ideal equidimensional (i.e., todas las componentes tienen la misma dimensión) radical y tomamos $A = k[\boldsymbol{x}]/I$. Abusando la notación, llamamos también $x_1, \ldots, x_n$ a las imágenes de $x_1, \ldots, x_n$ en A.

Queremos calcular la normalización de anillos A de este tipo.

Ejemplo 1.2.1. Sea $I = \langle y^3 - x^2 \rangle \subset k[x, y]$ y $A = k[x, y]/I$. Es decir, A es el anillo de coordenadas de la curva C en la Figura 1.1.

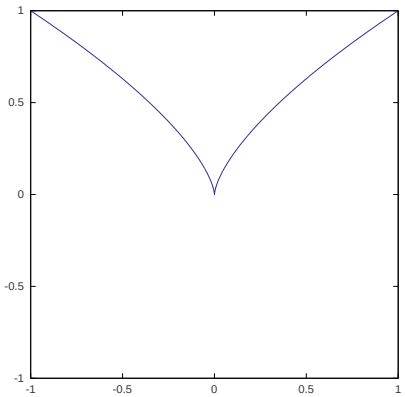

Figura 1.1: $y^3 - x^2 = 0$

En ese anillo, y^2/x satisface la ecuación entera

$$\left(\frac{y^2}{x}\right)^2 - y = 0,$$

por lo tanto es un elemento de $\overline{A}$. Mas aún, como veremos en el Capítulo 5, $\overline{A} = A[y^2/x]$.

Llamando $t = y^2/x$, t satisface las relaciones $t^2 - y = 0$ y $t^3 - x = 0$. Esto nos da la estructura de anillo de $\overline{A}$,

$$\overline{A} \cong k[x, y, t]/\langle y^3 - x^2, t^2 - y, t^3 - x\rangle \cong k[t].$$

Vemos que el resultado de la normalización es el anillo de coordenadas de una curva suave. Esto siempre sucede en el caso de curvas. Si A es el anillo de funciones polinomiales sobre una curva C, existe una curva no–singular $\widetilde{C}$ (contenida en algún k^m) con la propiedad de que la normalización $\overline{A} = k[\widetilde{C}]$ es el anillo de funciones polinomiales en $\widetilde{C}$ y la inclusión $A \subset \overline{A}$ corresponde a una función polinomial $\widetilde{C} \to C$ entre curvas algebraicas. Es decir, la normalización de A corresponde a una resolución de las singularidades de A. En el ejemplo anterior, obtenemos la función $t \mapsto (t^3, t^2)$ de $\widetilde{C} = k$ en $C = \{y^3 - x^2 = 0\} \subset k[x, y]$. (Para un tratamiento más detallado se puede consultar, por ejemplo, Reid 1995, Sección 4.5.)

Para variedades de dimensión mayor, la normalización del anillo de coordenadas no es necesariamente no–singular, pero es en general una mejora en las singularidades. Por ejemplo, la codimensión del conjunto de puntos singulares es siempre ≥ 2.

1.2.1 Trabajos previos

Los primeros algoritmos generales para calcular la normalización de anillos fueron propuestos por Stolzenberg (1968) y Seidenberg (1970, 1975). Sin embargo, las herramientas involucradas, tales como extensión de cuerpos y anillos, hacen que estos algoritmos sean muy costosos computacionalmente e inadecuados para la mayoría de las aplicaciones prácticas.

En los últimos años, diversos autores propusieron nuevos y más eficientes algoritmos, usando bases de Gröbner. El enfoque básico, continuando la línea de los trabajos anteriores, es calcular una cadena creciente de anillos entre el ideal original y su normalización. Entre estos trabajos, mencionamos (Traverso, 1986), (Vasconcelos, 1991, 1998), (Brennan and Vasconcelos, 2001). Hasta nuestro conocimiento, ninguno de estos algoritmos ha sido implementado y no es claro qué tan eficientes son. También de Jong (1998) y Decker et al. (1999a) siguen este camino, aplicando como nuevo ingrediente un criterio de normalidad propuesto por Grauert and Remmert (1971). En (Decker et al., 1999a), los autores reportan una implementación efectiva de su algoritmo en SINGULAR. Ese algoritmo se convirtió en el algoritmo estándar para normalización de anillos en los programas

de álgebra computacional, y fue implementado también en Macaulay2 (Grayson and Stillman, 2009) y Magma (Bosma et al., 1997). En (Swanson and Huneke, 2006, Chapter 15), se puede encontrar una buena reseña de la mayoría de estos algoritmos.

Otro enfoque, presentado en (Gianni and Trager, 1997), es usar normalización de Noether, reduciendo el problema al caso de dimensión uno, y aplicar algoritmos específicos para ese caso propuestos en (Ford, 1987; Cohen, 1993). Sin embargo, no conocemos ninguna implementación de estos algoritmos.

Un alternativa más reciente, propuesta en (Leonard and Pellikaan, 2003) y (Singh and Swanson, 2009) es calcular una cadena decreciente de módulos finitamente generados sobre el anillo original, que contengan a la normalización. Estos algoritmos funcionan sólo en el caso de anillos sobre cuerpos de característica positiva p, en donde es posible calcular la transformación de Frobenius de un ideal. Estos algoritmos fueron implementados en SINGULAR y Macaulay2, y resultan muy rápidos para primos pequeños. Sin embargo, para primos grandes el cálculo de la transformación de Frobenius es demasiado costoso, haciendo que el algoritmo sea inaplicable.

Existen también métodos muy eficientes para calcular normalizaciones de anillos en casos especiales. Por ejemplo, en (Bruns and Koch, 2001) se presentan algoritmos combinatorios para calcular la normalización de anillos teóricos.

1.2.2 El nuevo algoritmo

El algoritmo que proponemos en esta tesis es un algoritmo general, basado en los trabajos de de Jong (1998) y Decker et al. (1999a). En esos algoritmos, como comentamos antes, se construyen cadenas crecientes de anillos. Los anillos se agrandan calculando el anillo de endomorfismos de ciertos ideales de control, agregando nuevas variables para cada generador del anillo de endomorfismos considerado como módulo sobre el anillo original, y dividiendo por las relaciones entre las mismas. Luego, se aplica el algoritmo al nuevo anillo, en forma recursiva. Esto produce una disminución drástica en el rendimiento del algoritmo, debido a la cantidad creciente de nuevas variables y relaciones entre ellas. Cuando la cantidad de anillos intermedios es grande, el algoritmo se vuelve en la mayoría de los casos inútil, por el crecimiento exponencial de las bases de Gröbner involucradas. Nuestro enfoque evita la complejidad creciente de los anillos intermedios, aprovechando la estructura de A-módulo finitamente generado de la normalización. Realizamos la mayor parte de los cálculos sobre el anillo original, sin necesidad de incorporar nuevas variables ni relaciones.

En la Sección 5.2 presentamos los resultados principales y en la Sección 5.3 detallamos el algoritmo. La Sección 5.4 contiene varios ejemplos y comparaciones con otros algoritmos conocidos, mientras que la sección 5.5 está dedicada a una extensión del algoritmo a anillos locales. Conjuntamente con Gert-Martin Greuel y Gerhard Pfister, implementamos los algoritmos propuestos en la biblioteca `normal` (Greuel et al., 2009) de SINGULAR.

Una mejora interesante para el caso de curvas, que explicamos en la Sección 5.6, es descomponer el conjunto de singularidades en puntos, y calcular la contribución local en cada uno de esos puntos a la normalización para luego juntar todos los resultados locales. De esta forma obtenemos un algoritmo que resulta mucho mejor en la mayoría de los casos.

1.2.3 Aplicaciones

La normalización de anillos tiene varias aplicaciones, y estudiamos dos de ellas en el Capítulo 6. En la Sección 6.1 nos enfocamos en el cálculo de la clausura entera de ideales y en la Sección 6.2 estudiamos el cálculo de bases enteras usando los algoritmos de normalización. El contenido de la Sección 6.2 es parte de un trabajo en conjunto (en progreso) con Janko Böhm, Wolfram Decker y Frank Seelisch, presentado en (Böhm et al., 2012a).

Definición 1.2.2. Sea I un ideal en el anillo R. Un elemento $r \in R$ se dice *entero* sobre I si existe un entero s y elementos $a_i \in I^i$, $1 \leq i \leq s$, tales que se satisface la ecuación de dependencia entera

$$r^s + a_1 r^{s-1} + a_2 r^{s-2} + \cdots + a_{s-1} r + a_s = 0.$$

La clausura entera de I, que denotamos $\bar{I}$, es el conjunto de todos los elementos de R enteros sobre I. Si $I = \bar{I}$, decimos que I es integralmente cerrado.

A partir de un ideal I, podemos definir el álgebra de Rees de I,

$$R[It] = \oplus_{n \geq 0} I^n t^n = \left\{ \sum_{i=0}^{n} a_i t^i \mid n \in \mathbb{N}, a_i \in I^i \right\}.$$

con t una nueva variable.

Podemos obtener la normalización de I a partir de la normalización del anillo $R[It]$, como veremos en la Proposición 6.1.3.

Por lo tanto, las mejoras en los algoritmos para calcular la normalización de anillos producen inmediatamente mejoras en el cálculo de la clausura entera de ideales. Como el álgebra de Rees es un anillo con una estructura particular, resulta interesante estudiar como se aplica el nuevo algoritmo a este caso particular. La Sección 6.1 está dedicada a este tema.

Usualmente, el álgebra de Rees contiene una gran cantidad de variables con relaciones de grado alto entre ellas, y por lo tanto, en general este enfoque no resulta ser eficiente. Sin embargo, no se conoce ningún algoritmo directo para calcular la clausura entera de ideales. Esto es un tema para estudio futuro.

Como otra aplicación, en la Sección 6.2 estudiamos el cálculo de bases enteras usando los algoritmos de normalización.

Sea $R = k[x, y]$, $f \in R$ mónico como polinomio en y y sea $A = k[C] = k[x, y]/\langle f(x, y) \rangle$. Una *base entera* de $\overline{A}$ es un conjunto $b_0, \ldots, b_{n-1}$ de generadores libres de $\overline{A}$ sobre $k[x]$:

$$\overline{A} = k[x]b_0 \oplus \cdots \oplus k[x]b_{n-1}.$$

Aplicaciones típicas de bases enteras son el cálculo de ideal adjuntos (ver Mňuk, 1997; Böhm et al., 2012b), espacios de Riemann-Roch (ver Huang and Ieradi, 1994; Hess, 2002) y la parametrización de curvas racionales (ver van Hoeij 1997; Böhm et al. 2012c; la biblioteca de SINGULAR `paraplanecurves`, Böhm et al. 2011c).

En conjunto con Janko Böhm, Wolfram Decker y Frank Seelisch, hemos implementado los algoritmos propuestos en esta sección en la biblioteca `integralbasis` (Böhm et al., 2011b) de SINGULAR.

Como veremos en el Capítulo 7, podemos usar algoritmos específicos para calcular bases enteras. Sin embargo, la aplicación directa de los algoritmos de normalización es competitiva o incluso mejor que los algoritmos específicos, en algunos casos particulares.

1.2.4 Criterios de dependencia entera

En la Sección 6.3, estudiamos criterios que permitan determinar en forma algorítmica si un elemento dado pertenece a la normalización de un anillo o ideal.

Si bien una manera de hacerlo es calcular la normalización y luego verificar si el elemento dado pertenece a la misma, Vasconcelos (2005) pregunta por la existencia de criterios directos que no requieran calcular la normalización, debido al alto costo computacional de hacerlo (especialmente en el caso de ideales).

En (Greuel and Pfister, 2008, Proposición 3.1.3) se propone un criterio de dependencia entera para una extensión de la forma $R[f_1, \ldots, f_s] \hookrightarrow R$. En este trabajo, damos criterios similares para analizar la pertenencia a la normalización de anillos e ideales, y cuando la respuesta es positiva, podemos además calcular una ecuación de dependencia entera, la cual no se puede obtener directamente de los algoritmos de normalización.

Implementamos los algoritmos en SINGULAR y mostramos su aplicación en algunos ejemplos.

1.3 Bases enteras por Lema de Hensel

Finalmente, en el Capítulo 7 explicamos cómo calcular eficientemente bases enteras usando el Lema de Hensel. El contenido de este capítulo es un trabajo en conjunto (en progreso) con Janko Böhm, Wolfram Decker y Frank Seelisch, presentado en (Böhm et al., 2012a).

Desde un punto de vista teórico, nuestro enfoque es similar a (van Hoeij, 1994), donde se utilizan las llamadas series de Puiseux. Sin embargo, aplicando el Lema de Hensel, podemos agrupar las expansiones de Puiseux conjugadas o que coincidan en sus primeros términos, obteniendo un algoritmo mucho más eficiente.

Dado $f \in k[x, y]$ mónico de grado n en y, queremos calcular bases enteras locales de f en los puntos singulares. Podemos suponer por lo tanto que f tiene

una singularidad aislada en el origen, y calcular la base entera local para esa singularidad.

Sabemos que la base entera tiene la forma $b_0, \ldots, b_{n-1}$, donde $b_i = p_i/x^{e_i}$, con p_i mónico de grado i como polinomio en y, para $0 \leq i \leq n-1$.

Nos concentramos en calcular el último término de la base, $b = b_{n-1} = p/x^e$. (Para los otros elementos, el procedimiento es similar.)

El problema es entonces encontrar p mónico de grado $n-1$ en y con la máxima valuación posible en $x = 0$ (es decir, que pueda ser dividido por la mayor potencia de x y seguir siendo entero).

Sean $\gamma_1(x), \ldots, \gamma_n(x) \in \mathcal{P}(x)$ las expansiones de Puiseux de f en $x = 0$. Estudiamos cómo deben ser las expansiones de p en $x = 0$. Si escribimos

$$p = (y - \eta_1(x)) \cdots (y - \eta_{n-1}(x)), \tag{1.1}$$

queremos calcular las series $\eta_1(x), \ldots, \eta_{n-1}(x)$ que maximicen el valor de e.

Como se explica en (van Hoeij, 1994, Theorem 5.1), el mejor $\tilde{p} \in \mathcal{P}(x)[y]$ posible se puede obtener tomando $\{\eta_1(x), \ldots, \eta_{n-1}(x)\} \subset \{\gamma_1(x), \ldots, \gamma_n(x)\}$. En ese trabajo se muestra también cómo elegir ese subconjunto.

Sin embargo, $\tilde{p}$ en general no es un elemento de $k[x, y]$ como queremos, sino que puede contener coeficientes en una extensión algebraica del cuerpo de base o contener exponentes fraccionarios. Utilizando la traza, van Hoeij demuestra que existe $p \in k[x, y]$ mónico de grado $n-1$ en y con la misma valuación que $\tilde{p}$.

Estas ideas son usadas únicamente para obtener cotas en el algoritmo, y no son utilizadas para construir p. En nuestro trabajo, mostramos que p puede construirse fácilmente utilizando el Lema de Hensel para calcular $(y - \eta_1(x)) \cdots (y - \eta_{n-1}(x))$ eficientemente, o más precisamente el producto de estos factores truncados hasta un grado apropiado.

Podemos resumir nuestro algoritmo en los siguientes pasos,

(1) Calculamos e mirando las partes singulares de las expansiones de Puiseux de f, como se describe en (van Hoeij, 1994). Este paso es en general rápido.

(2) Determinamos cómo truncar las expansiones que aparecen en $\tilde{p}$ para obtener un elemento $p \in k[x, y]$ con la misma valuación que $\tilde{p}$. (Sección 7.3.)

(3) Utilizamos el Lema de Hensel para calcular el producto de las expansiones de Puiseux que no se anulan en el origen, hasta grado e en x. (Todas estas expansiones deben aparecer en p pues de lo contrario el máximo exponente para el cual p/x^e resulte entero sería $e = 0$.) Este paso ya representa una gran mejora comparado con el algoritmo de van Hoeij, puesto que no necesitamos calcular separadamente cada expansión de Puiseux fuera del origen. (Sección 7.4.)

(4) Aplicamos una transformación a los polinomios para poder utilizar el Lema de Hensel para calcular productos de expansiones de Puiseux conjugadas que se anulan en el origen. (Sección 7.5.)

(5) Calculamos p multiplicando los factores apropiados que obtuvimos utilizando el Lema de Hensel.

Comparado con el algoritmo de van Hoeij, estamos prediciendo los elementos de la base entera, en lugar de calcularlos resolviendo sistemas de ecuaciones.

Chapter 2

Introduction (English version)

The fundamentals of commutative algebra have been laid more than one century ago, in the middle of the 19th century. The notion of ideal, which can be considered as the origin of the theory, was introduced by Dedekind in the supplements he wrote in 1879 to the book *Vorlesungen ber Zahlentheorie* (Dirichlet, 1968) containing Dirichlet's lectures on number theory. He also proved a theorem of unique factorization of ideals in the special class of rings we now call Dedekind rings.

These results were generalized some years later by Lasker (1905), developing the theory of primary decomposition and proving the existence of this decomposition for ideals in rings of polynomials.

In the 1920's, Emmy Noether studied these works, simplified and reformulated them in a much more general setting. Her brilliant paper (Noether, 1921) is now considered the starting point of modern commutative algebra.

This thesis addresses the algorithmic aspects of some major topics of commutative algebra. We study the computation of radicals and minimal associated primes of ideals, the normalization of rings and ideals and other related problems. In recent years a number of computer algebra systems have been developed with very efficient implementations of some basic tools to work with polynomials, ideals and rings. This put on the spot the need for efficient algorithms to solve some difficult problems.

We propose new algorithms for some of these problems, based on new mathematical ideas and results. All the algorithms in this thesis have been implemented in Singular (Decker et al., 2011), one of the most commonly used computer algebra systems, and are now available for use of the mathematical community. Although other algorithms already existed for most of these tasks, the new algorithms outperform them in most cases and are now the default algorithms in Singular.

2.1 Radical and minimal associated primes

Given an ideal $I \subset k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, k a field, the radical of I is the ideal

$$\sqrt{I} = \{f \in k[\boldsymbol{x}] \mid f^m \in I \text{ for some } m \in \mathbb{N}\}.$$

The radical of an ideal plays an important role in commutative algebra, when we are concerned with the geometry aspects. This is due to the bijection existing between varieties and radical ideals for algebraic closed fields.

Although the definition is quite simple, computing the radical of a given ideal is usually very hard computationally. In recent years some algorithms for the computation of the radical have been proposed. Among these, we mention (Gianni et al., 1988), (Krick and Logar, 1991b) and (Eisenbud et al., 1992) for the general case, (Kemper, 2002) for the zero–dimensional case and (Matsumoto, 2001) for ideals over fields of positive characteristic.

In Chapter 4 we propose an algorithm for computing the radical based on the ideas of Gianni et al. (1988) and Krick and Logar (1991b), compare an implementation of it with the implementations of other known algorithms, and analyze its theoretical complexity. The results of this section are published in (Laplagne, 2006a) and (Laplagne, 2006b).

In (Krick and Logar, 1991b), the authors use the splitting tool $\sqrt{I} = \sqrt{I : h} \cap \sqrt{\langle I, h\rangle}$ (Proposition 4.2.1) for an appropriate h (Proposition 4.2.13). They find h such that $\sqrt{I : h}$ can be obtained by reduction to the zero–dimensional case and obtain $\sqrt{\langle I, h\rangle}$ by induction on the dimension. When taking $\langle I, h\rangle$, redundant components appear (that is, components that are not part of the original ideal) that slow down the algorithm performance. In our new algorithm (Algorithm 4.2.1), we avoid using $\langle I, h\rangle$ but instead we use repeatedly the saturation $I : h^\infty$ for appropriate h. This leads in many cases to a more efficient algorithm.

A related task is to compute the minimal associated primes of an ideal. Geometrically, this is equivalent to decompose the set of solutions of a system of polynomial equations into its irreducible components. That is, we can interpret it as solving the system, when we are not interested in multiplicities or, more specifically, in the algebraic structure of the solutions.

In Section 4.3, we show how the same ideas that we used for the computation of the radical of an ideal can be applied to the computation of the minimal associated primes of an ideal. We make a brief description of the new algorithm and we show some time comparisons with the existing algorithms in SINGULAR.

Together with Wolfram Decker, Gert-Martin Greuel and Hans Schönemann, we have implemented the proposed algorithms for the computation of the radical and the minimal associated primes of ideals in the SINGULAR library `primdec` (Decker et al., 2006).

2.2 Normalization of rings

In Chapter 5 we turn to the problem of computing the normalization of polynomial rings. It is another major tool in commutative algebra, with applications to algebraic geometry and singularity theory. The content of Sections 5.1 to 5.5 is a joint work with Gert-Martin Greuel and Frank Seelisch. It is presented in (Greuel et al., 2010). The local approach proposed in Section 5.6 is a joint work with Janko Böhm, Wolfram Decker, Gerhard Pfister, Andreas Steenpaßand Stefan Steidel, and is presented in a more general version in (Böhm et al., 2011a).

Let A be a reduced Noetherian ring. (All rings are assumed to be commutative with 1 and all ring morphisms map 1 to 1.)

Let $A \subset B$ be a ring extension. We say that $b \in B$ is *integral* over A if there exist $a_i \in A$, $1 \leq i \leq s$, such that

$$b^s + a_1 b^{s-1} + \cdots + a_{s-1} b + a_s = 0.$$

The *integral closure* of A in B is the set of all elements of B that are integral over A.

We define the total ring of fractions $Q(A) = S^{-1}A$, where $S \subseteq A$ is the set of non–zerodivisors of A and $S^{-1}A$ is the localization of A at S. The *normalization* $\bar{A}$ of A is the integral closure of A in $Q(A)$. A ring A is called *normal* if $A = \bar{A}$.

For our algorithms we will consider $R = k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, with k a field and $I \subset R$ an equidimensional (i.e., all the components have the same dimension) radical ideal and take $A = k[\boldsymbol{x}]/I$. Abusing the notation, we denote also by $x_1, \ldots, x_n$ the images of $x_1, \ldots, x_n$ in A.

We are interested in computing the normalization of such rings A.

Example 2.2.1. Let $I = \langle y^3 - x^2 \rangle \subset k[x, y]$ and $A = k[x, y]/I$. That is, A is the coordinate ring of the curve shown in Figure 2.1.

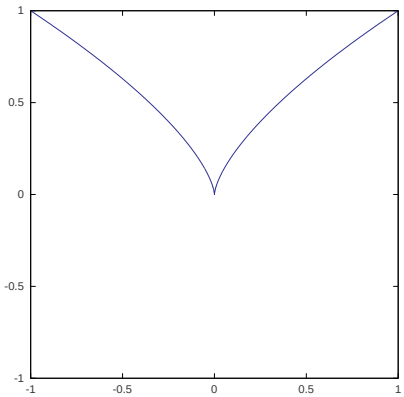

Figure 2.1: $y^3 - x^2 = 0$

Then, y^2/x satisfies the integral equation

$$\left(\frac{y^2}{x}\right)^2 - y = 0,$$

so it is an element of $\overline{A}$. Moreover, as we will see in Chapter 5, $\overline{A} = A[y^2/x]$.

If we call $t = y^2/x$, then t satisfies the relations $t^2 - y = 0$ and $t^3 - x = 0$. This gives the ring structure of $\overline{A}$,

$$\overline{A} \cong k[x, y, t]/\langle y^3 - x^2, t^2 - y, t^3 - x\rangle \cong k[t].$$

We see that the output of the normalization is the coordinate ring of a smooth curve. This always happens for the case of curves. If A is the ring of polynomial functions on a curve C, there is a non-singular curve $\widetilde{C}$ (contained in some k^m) with the property that the normalization $\overline{A} = k[\widetilde{C}]$ is the ring of polynomial functions on $\widetilde{C}$ and the inclusion $A \subset \overline{A}$ corresponds to a polynomial map $\widetilde{C} \to C$ between algebraic curves. That is, the normalization of A corresponds to a resolution of singularities. In the above example we get the map $t \mapsto (t^3, t^2)$ from $\widetilde{C} = k$ to $C = \{y^3 - x^2 \ = 0\} \subset k[x, y]$. (See, for example, Reid, 1995, Section 4.5)

For higher dimensional varieties, the normalization of the coordinate ring will not necessarily be non-singular, but an improvement of the singularities. For example, the codimension of the singular locus will be ≥ 2.

2.2.1 Previous work

The first general algorithms for computing the normalization of rings were proposed by Stolzenberg (1968) and Seidenberg (1970, 1975). However, the tools involved, such as extensions of the ground field and addition of new indeterminates, make them computationally too expensive and unsuitable for most practical applications.

In recent years several new and more practicable algorithms using Gröbner bases have been proposed. The basic approach, continuing the line of the works mentioned before, is to compute an increasing chain of rings from the original ring to its normalization. This is carried out in the works of Traverso (1986), Vasconcelos (1991, 1998), Brennan and Vasconcelos (2001). To our knowledge none of these algorithms has been implemented and it remains unclear how efficient they are. Also de Jong (1998) and Decker et al. (1999a) follow this path, applying as a new ingredient a criterion for normality due to Grauert and Remmert (1971). In (Decker et al., 1999a) they report an effective implementation of their algorithm in Singular (Decker et al., 2011). It became the standard algorithm for normalization in computer algebra systems, being now implemented also in Macaulay2 (Grayson and Stillman, 2009) and Magma (Bosma et al., 1997). A good review on most of these algorithms can be found in (Swanson and Huneke, 2006, Chapter 15).

Another approach, presented in (Gianni and Trager, 1997), is to use Noether normalization, reduce the problem to the one–dimensional case, and apply existing special algorithms for that case (Ford, 1987; Cohen, 1993). Unfortunately, we do not know of any implementation of these algorithms.

A more recent approach taken in (Leonard and Pellikaan, 2003) and (Singh and Swanson, 2009) is to compute a decreasing chain of finitely generated modules over the original ring containing the normalization. Their algorithm works only in the case when the base field is of positive characteristic p, where they can use the Frobenius map. It has been implemented in Macaulay2 and SINGULAR, and it turns out to be very fast for small p. However the computation of the Frobenius map makes it impracticable when p is large.

There are also very efficient methods for computing the normalization in some special cases. For example, for toric rings, one can apply fast combinatorial techniques, as explained in (Bruns and Koch, 2001).

2.2.2 The new algorithm

The algorithm that we propose in this thesis is a general algorithm and it is based on (de Jong, 1998) and (Decker et al., 1999a). In their algorithm, as we mentioned before, they construct an increasing chain of affine rings. They enlarge the rings by computing the endomorphism ring of a test ideal (see below), adding new variables for each module generator of the endomorphism ring and dividing out the relations among them. Then the algorithm is applied recursively to the new affine ring. This can produce a big slow-down in the performance of the algorithm, due to the increasing number of variables and relations among them. For a large number of intermediate rings, the algorithm is in most cases unusable, since the Gröbner bases of the ideals of relations grow extensively. Our approach avoids the increasing complexity when enlarging the rings, benefiting from the finitely generated A-module structure of the normalization. We are able to do most computations over the original ring without adding new variables or relations.

The main new results are presented in Section 5.2. In Section 5.3 we describe the algorithm. Section 5.4 contains several benchmark examples and a comparison with previously known algorithms, while Section 5.5 is devoted to an extension of the algorithm to local rings. Together with Gert-Martin Greuel and Gerhard Pfister, we have implemented the proposed algorithms in the SINGULAR library `normal` (Greuel et al., 2009).

A nice improvement for the case of curves, explained in Section 5.6, is to decompose the singular locus of the curve into its singular points, compute the local contribution to the normalization at each of these points and put the local results together. In this way, we get an algorithm that performs much better in most examples.

2.2.3 Applications

The normalization of rings have several applications, and we study two of them in Chapter 6. In Section 6.1 we focus on the computation of the integral closure of ideals and in Section 6.2 we study the computation of integral bases using the normalization algorithm. The content of Section 6.2 is part of a joint work (in progress) with Janko Böhm, Wolfram Decker and Frank Seelisch, presented in (Böhm et al., 2012a).

Definition 2.2.2. Let I be an ideal in a ring R. An element $r \in R$ is said to be *integral* over I if there exist an integer s and elements $a_i \in I^i$, $1 \leq i \leq s$, such that

$$r^s + a_1 r^{s-1} + a_2 r^{s-2} + \cdots + a_{s-1} r + a_s = 0.$$

Such an equation is called an equation of integral dependence of r over I (of degree n). The set of all elements that are integral over I is called the integral closure of I, and is denoted $\bar{I}$. If $I = \bar{I}$, then I is called integrally closed.

From I, we can define the Rees algebra

$$R[It] = \oplus_{n \geq 0} I^n t^n = \left\{ \sum_{i=0}^{n} a_i t^i \mid n \in \mathbb{N}, a_i \in I^i \right\},$$

where t is a new variable.

The normalization of I can be obtained from the normalization of the ring $R[It]$, as we explain in Proposition 6.1.3.

That is, an improvement in the algorithms to compute the normalization of rings immediately leads to better ways to compute the integral closure of ideals. Since the Rees algebra is a ring with a special structure, it is interesting to study how the new algorithms apply to this particular case. This is done in Section 6.1.

Usually the Rees algebra contains a large number of variables with high degree relations among them, and therefore this is not a good approach in general. However there is no known direct method to compute the integral closure of ideals up to date. This is a problem for further studying.

As another application, in Section 6.2 we study the computation of integral bases using the normalization algorithm.

Let $R = k[x, y]$, $f \in R$ monic in y and $A = k[C] = k[x, y]/\langle f(x, y) \rangle$. An *integral basis* for $\overline{A}$ is a set $b_0, \ldots, b_{n-1}$ of free generators for $\overline{A}$ over $k[x]$:

$$\overline{A} = k[x]b_0 \oplus \cdots \oplus k[x]b_{n-1}.$$

Typical applications of integral bases are the computation of adjoint ideals (see Mňuk, 1997; Böhm et al., 2012b), the computation of Riemann-Roch spaces (see Huang and Ieradi, 1994; Hess, 2002), and the parametrization of rational curves (see van Hoeij 1997; Böhm et al. 2012c; the SINGULAR library `paraplanecurves`, Böhm et al. 2011c).

Together with Janko Böhm, Wolfram Decker and Frank Seelisch, we have implemented the algorithms proposed in this section in the library `integralbasis` (Böhm et al., 2011b).

As we show in Chapter 7, we can also use special algorithms for computing integral bases, based on the special structure of the ring. However, this general algorithm is competitive in many cases and even better than the special algorithm in some particular examples.

2.2.4 Criteria for integral dependence

In Section 6.3, we study criteria for integral dependence. That is, we want to decide algorithmically if a given element belongs to the normalization of a ring or an ideal.

Although a way to do this is to first compute the normalization and then check if the given element belongs to it, Vasconcelos (2005) asks for the existence of direct criteria that do not require to compute it, due to the high computational cost of doing so (especially in the case of normalization of ideals).

In (Greuel and Pfister, 2008, Proposition 3.1.3), the authors propose an integral dependence criterion for an extension of type $R[f_1, \ldots, f_s] \hookrightarrow R$. In our work, we give similar criteria for checking if any given element belongs to the normalization of rings and ideals. When the element is integral, we get as part of the output an equation of integral dependence, which is not possible to obtain directly from the normalization algorithms.

We have implemented the tests in SINGULAR, and we give some examples of applications.

2.3 Integral bases via Hensel's Lemma

Finally, in Chapter 7 we explain how to compute efficiently the integral bases by using Hensel's lemma. The content of this chapter is a joint work (in progress) with Janko Böhm, Wolfram Decker and Frank Seelisch, presented in Böhm et al. (2012a).

Theoretically, the approach is similar to (van Hoeij, 1994), where the Puiseux Expansions are used. However, by using Hensel's lemma we can group together conjugate or similar Puiseux expansions and obtain a much faster algorithm.

Given $f \in k[x, y]$ monic of degree n in y, we want to compute the local integral bases of f at the singular points. We therefore assume that f has an isolated singularity at the origin, and we compute the local integral basis for this singularity.

We know that the basis will have the form $b_0, \ldots, b_{n-1}$, where $b_i = p_i/x^{e_i}$, with p_i monic of degree i as polynomial in y.

We focus on computing the last term $b = b_{n-1} = p/x^e$. (For the other terms, the

procedure is similar, and we explain it afterwards.)

The problem is then to find p monic of degree $n-1$ in y with the highest vanishing order at $x = 0$ (that is, that can be divided by the largest power of x and still be integral).

Let $\gamma_1(x), \ldots, \gamma_n(x) \in \mathcal{P}(x)$ be the Puiseux expansions of f at $x = 0$. We consider how the Puiseux expansions of p at $x = 0$ must be. That is, we write

$$p = (y - \eta_1(x)) \cdots (y - \eta_{n-1}(x)) \tag{2.1}$$

and we want to compute appropriate $\eta_1(x), \ldots, \eta_{n-1}(x)$ to maximize e.

As noted in (van Hoeij, 1994, Theorem 5.1), the best $\tilde{p} \in \mathcal{P}(x)[y]$ can be obtained by taking $\{\eta_1(x), \ldots, \eta_{n-1}(x)\}$ a subset of $\{\gamma_1(x), \ldots, \gamma_n(x)\}$. In that paper it is also explained how to compute which subset to take.

However $\tilde{p}$ is usually not in the ground field and may contain fractional exponents. By using the trace map, van Hoeij proves that there exists $p \in k[x, y]$ monic of degree $n - 1$ in y with the same vanishing order as $\tilde{p}$.

These ideas are only used there to get bounds for his algorithm, and are not used to construct p. In this work, we show that p can be easily constructed, using Hensel's Lemma to efficiently compute $(y-\eta_1(x)) \cdots (y-\eta_{n-1}(x))$ or more precisely the product of the truncated expansions of these factors up to the appropriate degree.

Our new algorithm can be sketched as follows:

(1) We compute e by looking at the singular part of the Puiseux expansions of f, as described in (van Hoeij, 1994). This step is usually fast.

(2) We determine how to truncate the expansions appearing in $\tilde{p}$ to get an element p in the ground field with the same vanishing order as $\tilde{p}$. (Section 7.3.)

(3) We use Hensel's Lemma to compute the product of the Puiseux expansions that do not vanish at the origin, up to degree e in x. (All these expansions must appear in p or otherwise the maximum exponent such that p/x^e is integral will be $e = 0$.) This step is already a major improvement compared to van Hoeij's algorithm, as we do not need to compute the different Puiseux expansions outside the origin separately. (Section 7.4.)

(4) We apply a transformation to the polynomials so that Hensel's Lemma can be used to compute the products of conjugate Puiseux Expansions that vanish at the origin. (Section 7.5.)

(5) We multiply the appropriate factors obtained using Hensel's Lemma to compute p.

Compared to van Hoeij's algorithm, we are predicting the elements of the integral basis instead of computing them by solving systems of equations.

Chapter 3

Preliminaries

3.1 Ideals and varieties

In this chapter we introduce the basic notions of commutative algebra. Some proofs will be omitted, they can be found in (van der Waerden, 1949), (Atiyah and Macdonald, 1969), (Lang, 2002) or (Cox et al., 1996).

We set k any field and $k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$ the ring of polynomials in n variables with coefficients in k. We start by studying the common zeros of sets of polynomials.

Definition 3.1.1. We note k^n the n–dimensional affine space over k, that is, the set of n-uples $\boldsymbol{p} := (p_1, \ldots, p_n)$ with $p_i \in k$, with the affine vector space structure.

For any set $X \subseteq k[\boldsymbol{x}]$ of polynomials, we define

$$V = \mathbf{V}(X) = \{\boldsymbol{p} \in k^n \mid f(\boldsymbol{p}) = 0 \quad \forall\ f \in X\}.$$

We call V the *affine variety* defined by X.

We say that a given set of points $V \subseteq k^n$ is an affine variety if there exists $X \subseteq k[\boldsymbol{x}]$ such that $V = \mathbf{V}(X)$.

Example 3.1.2. In $\mathbb{R}^3$, let $U = \mathbf{V}(\{(x^2 + y^2 - z)z^2\})$. The picture of U is shown in Figure 3.1.[1]

If k is not algebraically closed, we are usually interested in varieties over the algebraic closure of k, $\bar{k}$. In this case, we note $\mathbf{V}_{\bar{k}}$ and $\mathbf{V}_k$ to distinguish both varieties, or we indicate explicitly the field: $\mathbf{V}_{\mathbb{C}}, \mathbf{V}_{\mathbb{R}}, \ldots$.

Example 3.1.3.

$$\mathbf{V}_{\mathbb{R}}(\{x^2 + y^2\}) = \{(0, 0)\}$$

and

$$\mathbf{V}_{\mathbb{C}}(\{x^2 + y^2\}) = \{(x, y) \mid y = ix\} \cup \{(x, y) \mid y = -ix\}.$$

[1] Picture made using Surfer software, from `http://www.imaginary-exhibition.com/`.

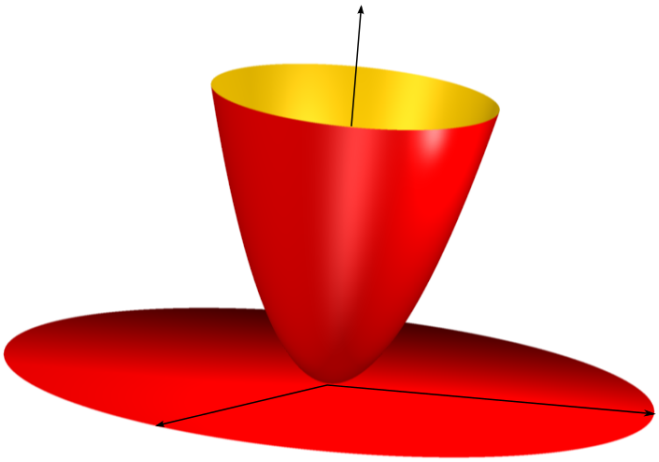

Figure 3.1: $\mathbf{V}_{\mathbb{R}}(\{(x^2+y^2-z)z^2\})$

The following notion is useful for dealing with set of polynomials.

Definition 3.1.4. A set $I \subseteq k[\boldsymbol{x}]$ is called an *ideal* if it satisfies the following conditions:

(1) $0 \in I$.

(2) If $f, g \in I$, then $f + g \in I$.

(3) If $f \in I$ and $g \in k[\boldsymbol{x}]$, then $gf \in I$.

We next see a way to construct ideals.

Definition 3.1.5. Let $X \subseteq k[\boldsymbol{x}]$. The *ideal generated* by X is the ideal

$$I = \langle f \mid f \in X \rangle = \left\{ \sum_{f_\lambda \in X} h_\lambda f_\lambda : h_\lambda \in k[\boldsymbol{x}] \right\},$$

where all the sums contain only a finite number of terms.

Given an ideal, we can construct the variety associated to it.

Definition 3.1.6. Let $I \subseteq k[\boldsymbol{x}]$ be an ideal, we define the variety of the ideal I as

$$\mathbf{V}(I) = \{\boldsymbol{p} \in k^n \mid f(\boldsymbol{p}) = 0 \quad \forall f \in I\}$$

We have the following property.

Proposition 3.1.7. *Let $X \subseteq k[\boldsymbol{x}]$ and let $I = \langle f \mid f \in X \rangle$. Then $\mathbf{V}(I) = \mathbf{V}(X)$.*

If $X = \{f_1, \ldots, f_s\}$ is finite, we write $I = \langle f_1, \ldots, f_s \rangle$ and we say that I is a *finitely generated* ideal. We next mention an important property, asserting that all the ideals in $k[\boldsymbol{x}]$ are finitely generated.

Definition 3.1.8. A ring R is called *Noetherian* if all ideals in R are finitely generated.

The following fundamental theorem is known as the *Hilbert basis theorem.*

Theorem 3.1.9. *Let k be a field. The ring of polynomials $k[\boldsymbol{x}]$ is Noetherian.*

We have seen before how to define a variety from any set of polynomials. By Proposition 3.1.7, $V = \mathbf{V}(X) = \mathbf{V}(I)$, where $I = \langle f \mid f \in X \rangle$. Since $k[\boldsymbol{x}]$ is Noetherian, the ideal I is finitely generated, that is, $I = \langle f_1, \ldots, f_s \rangle$ for some $f_1, \ldots, f_s \in k[\boldsymbol{x}]$. Therefore $V = \mathbf{V}(\{f_1, \ldots, f_s\})$. This means that in the definition of a variety we can restrict to finite sets of polynomials.

The Noetherian condition is equivalent to the ascending chain condition, which we next define.

Proposition 3.1.10. *Let R be a ring. The following conditions are equivalents:*

(1) R is Noetherian.

(2) (Ascending chain condition) For every ascending chain

$$I_1 \subseteq I_2 \subseteq \ldots$$

of ideals in R, there exists $N \geq 1$ such that $I_N = I_{N+1} = I_{N+2} = \ldots$ In this case, we say that the chain of ideals stabilizes.

Proof. (1) $\Rightarrow$ (2) Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be an ascending chain. Consider the set $I = \bigcup_{i=1}^{\infty} I_i$. We want to prove that I is an ideal.

(1) $0 \in I$ because 0 is in any ideal I_i.

(2) If $f, g \in I$, there exists N_1 and N_2 such that $f \in I_{N_1}$ and $g \in I_{N_2}$. We assume $N_2 > N_1$, then $I_{N_1} \subseteq I_{N_2}$ and $f, g \in I_{N_2}$. Therefore $f + g \in I_{N_2}$ and $f + g \in I$.

(3) Let $f \in I$ and $h \in k[\boldsymbol{x}]$. There exists N such that $f \in I_N$. Therefore, $hf \in I_N$ and we get $hf \in I$.

Since R is Noetherian, the ideal I is finitely generated. This says that there exist $f_1, \ldots, f_s$ which generate I. For each f_i, $1 \leq i \leq s$, there exists N_i such that $f_i \in I_{N_i}$. Let N the maximum of all N_i, $1 \leq i \leq s$. Since the ideals I_i are an ascending chain, $f_i \in I_N$ for all $1 \leq i \leq s$. Therefore $\langle f_1, \ldots, f_s \rangle \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I = \langle f_1, \ldots, f_s \rangle$. Then, all the inclusions are identities, and the ascending chain stabilizes.

(2) $\Rightarrow$ (1) We assume that R is not Noetherian. Let I be an ideal in R that does not have any finite set of generators.

We can construct a chain $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \cdots \subsetneq \langle f_1, f_2, \ldots, f_s \rangle \subsetneq \ldots$ with $f_i \in I$ $\forall i \in \mathbb{N}$ and $f_i \notin \langle f_1, f_2, \ldots, f_{i-1} \rangle$. None of these ideals can be equal to I because I is not finitely generated. Therefore we can extend the chain infinitely, and we conclude that R does not satisfy the ascending chain condition. $\square$

From the Hilbert basis theorem, we conclude that all ideals in $k[\boldsymbol{x}]$ satisfy the ascending chain condition.

We next study the ideals obtained from varieties.

Definition 3.1.11. Let $V \subseteq k^n$ be a variety. We define

$$\mathbf{I}(V) = \{f \in k[\boldsymbol{x}] \mid f(\boldsymbol{p}) = 0 \quad \forall\, \boldsymbol{p} \in V\}.$$

$\mathbf{I}(V)$ is an ideal, which we call *the ideal of* V. When necessary, we will indicate over which ring is the ideal generated $(\mathbf{I}_{k[\boldsymbol{x}]}(V), \mathbf{I}_{\bar{k}[\boldsymbol{x}]}(V), \dots)$.

Lemma 3.1.12. *For any variety $V \subseteq k^n$, it holds $\mathbf{V}(\mathbf{I}(V)) = V$.*

Proof. If $\boldsymbol{p} \in V$, all the polynomials in $\mathbf{I}(V)$ vanish at $\boldsymbol{p}$ and therefore $\boldsymbol{p} \in \mathbf{V}(\mathbf{I}(V))$.

For the reverse inclusion, we have seen that there exist polynomials $f_1, \dots, f_s$ such that

$$V = \mathbf{V}(\{f_1, \dots, f_s\}) = \{\boldsymbol{p} \in k^n \mid f_i(\boldsymbol{p}) = 0 \quad \forall i, 1 \leq i \leq s\}.$$

Therefore $f_1, \dots, f_s \in \mathbf{I}(V)$. If $\boldsymbol{p} \in \mathbf{V}(\mathbf{I}(V))$, $f_1(\boldsymbol{p}) = f_2(\boldsymbol{p}) = \cdots = f_s(\boldsymbol{p}) = 0$ and $\boldsymbol{p} \in V$. □

If we do the converse operation, that is, given an ideal $I \subseteq k[\boldsymbol{x}]$, we compute $\mathbf{I}(\mathbf{V}(I))$, we do not always obtain the original ideal. For example, if $I = \langle x^2, y^2 \rangle \subset \mathbb{C}[x, y]$, then $\mathbf{V}(I) = \{(0, 0)\}$ and $\mathbf{I}(\mathbf{V}(I)) = \langle x, y \rangle$.

However, over algebraically closed fields, there exists an easy relation between both ideals.

To state the relation, we define the *radical* of an ideal (which we study in deeper detail in Chapter 4).

Definition 3.1.13. Let $I \subseteq k[\boldsymbol{x}]$ be an ideal. The *radical* of I is the ideal $\sqrt{I} = \{f \mid f^m \in I \text{ for some } m \in \mathbb{N}\}$. We say that an ideal I is *radical* if $I = \sqrt{I}$.

Theorem 3.1.14. *Let k be an algebraically closed field and $I \subseteq k[\boldsymbol{x}]$ an ideal. Let $f \in I$. There exists $m \in \mathbb{N}$ such that $f^m \in \mathbf{I}(\mathbf{V}(I))$. That is,*

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

This theorem is of great importance in the development of algebraic geometry. It is usually mentioned with the original German name *Nullstellensatz*, which means "the theorem of the zeros".

Example 3.1.15. In Example 3.1.2, $U = \mathbf{V}(\langle (x^2 + y^2 - z)z^2 \rangle$ and $\mathbf{I}(U) = \langle (x^2 + y^2 - z)z \rangle$.

The following corollary is known as the weak Nullstellensatz.

Theorem 3.1.16. *Let k be an algebraically closed field and $I \subseteq k[\boldsymbol{x}]$ an ideal. If $\mathbf{V}(I) = \emptyset$, then $I = \langle 1 \rangle$.*

Proof. $\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\emptyset) = \langle 1 \rangle$. □

We see next the analog for varieties of the ascending chain condition for ideals. We use the following lemma.

Lemma 3.1.17 (Reversion of inclusions)**.**

(1) Let $I \subseteq J \subseteq k[\boldsymbol{x}]$ be ideals. Then $\mathbf{V}(I) \supseteq \mathbf{V}(J)$.

(2) Let $U \subseteq V \subseteq k^n$ be varieties. Then $\mathbf{I}(U) \supseteq \mathbf{I}(V)$.

Proof.

(1) Let $\boldsymbol{p} \in \mathbf{V}(J)$. Then $g(\boldsymbol{p}) = 0 \ \forall g \in J$. Since $I \subseteq J$, $f(\boldsymbol{p}) = 0 \ \forall f \in I$ and $\boldsymbol{p} \in \mathbf{V}(I)$.

(2) Let $f \in \mathbf{I}(V)$. Then $f(\boldsymbol{p}) = 0 \ \forall \boldsymbol{p} \in V$. Since $U \subseteq V$, $f(\boldsymbol{p}) = 0 \ \forall \boldsymbol{p} \in U$ and $f \in \mathbf{I}(U)$.

□

Proposition 3.1.18. *Let*

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \dots$$

be a descending chain of varieties in k^n. There exists $N \geq 1$ such that

$$V_N = V_{N+1} = V_{N+2} = \dots$$

Proof. If we consider the ideals of the varieties, we obtain from Lemma 3.1.17,

$$\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \mathbf{I}(V_3) \subseteq \dots$$

From the ascending chain condition, this chain stabilizes. This means, $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \dots$ for some $N \in \mathbb{N}$. Considering now the varieties defined by these ideals, we get

$$\mathbf{V}(\mathbf{I}(V_1)) \supseteq \mathbf{V}(\mathbf{I}(V_2)) \supseteq \mathbf{V}(\mathbf{I}(V_3)) \supseteq \dots$$

But we have already seen that $\mathbf{V}(\mathbf{I}(V)) = V$. Therefore

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \dots$$ □

Definition 3.1.19. Let $I \subsetneq A$ be an ideal. I is called *prime* if given $f, g \in k[\boldsymbol{x}]$ such that $fg \in I$ then either $f \in I$ or $g \in I$. I is called *maximal* if it is maximal with respect to inclusion (i.e., if $I \subseteq I' \subsetneq k[\boldsymbol{x}]$, then $I = I'$).

The ring A itself is not considered prime (but the null ideal is, when A is an integral domain).

Prime ideals allow us to give an algebraic definition of the dimension of rings and ideals.

Definition 3.1.20. The *Krull dimension* (or *dimension*) of a ring A is the maximal length m of chains $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_m$ of prime ideals in A.

Definition 3.1.21. Let $I \subset A$ be an ideal. The *dimension* of I is the dimension of the ring A/I.

Since there exists a one-to-one correspondence between prime ideals of A/I and ideals of A containing I, the dimension of an ideal I can be defined also as the maximal length of a chain of prime ideals of A containing I.

Example 3.1.22. The ring $k[x_1, \ldots, x_n]$ has dimension n (see, for example, Eisenbud, 1995). If $I = \langle x \rangle \subset k[x, y, z]$, then $k[x, y, z]/\langle x \rangle \cong k[y, z]$ and therefore $\dim(I) = \dim(k[y, z]) = 2$.

3.1.1 Localization of rings

In this section we explain the process of localization, which will be used in the algorithms in the next chapters.

We recall the definition of quotient field given in Section 2.2.

Definition 3.1.23. Let A be an integral domain, the quotient field of A is

$$Q(A) = \left\{ \frac{a}{b} \mid a, b \in A, b \neq 0 \right\},$$

where $\dfrac{a}{b} = \dfrac{c}{d} \iff ad = bc$.

To extend this construction to general rings, we make first the following definition.

Definition 3.1.24. Let A be a ring. A set $S \subseteq A$ is called *multiplicatively closed* if

(1) $1 \in S$

(2) $a \in S, b \in S \Rightarrow ab \in S$

We can now define the localization.

Definition 3.1.25. Let A be a ring and $S \subseteq A$ a multiplicatively closed set. The *localization* of A with respect to S is the ring

$$S^{-1}A = \left\{ \frac{a}{b} \mid a \in A, b \in S \right\},$$

where $\dfrac{a}{b} = \dfrac{c}{d}$ iff there exists $s \in S$ such that $s(ad - bc) = 0$.

We will use special notations for some particular cases.

Example 3.1.26.

(1) $A \setminus P$ is multiplicatively closed for any prime ideal P. The ring

$$A_P = \left\{ \frac{a}{b} \mid a \in A, b \notin P \right\}$$

is called the *localization of A at P*. It is a local ring with maximal ideal PA_P. In particular, if $\mathfrak{m}$ is a maximal ideal, $A_\mathfrak{m}$ is a local ring with maximal ideal $\mathfrak{m}A_\mathfrak{m}$.

(2) For any $f \in A$, the set $S = \{1, f, f^2, \dots\}$ is multiplicatively closed. The localization with respect to S is noted

$$A_f = \left\{ \frac{a}{f^n} \mid a \in A, n \geq 0 \right\}.$$

(3) The set S of all non–zerodivisors of A is also multiplicatively closed. We note

$$Q(A) = \left\{ \frac{a}{b} \mid a \in A, b \text{ a non–zerodivisor of } A \right\},$$

the total ring of fractions of A. This extends the previous definition for integral domains.

3.2 Operations on ideals

We define now some operations among ideals that we will use through all this work.

3.2.1 Sum of ideals

Definition 3.2.1. If I and J are ideals in $k[\boldsymbol{x}]$, we define the sum of I and J as the set

$$I + J = \{f + g \mid f \in I, g \in J\}$$

This set is an ideal. If I and J are generated by polynomials $I = \langle f_1, \dots, f_s \rangle$ and $J = \langle g_1, \dots, g_t \rangle$ then $I + J = \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle$.

We will usually use the notation $\langle I, J \rangle$ instead of $I + J$ and $\langle I, g_1, \dots, g_t \rangle$ instead of $I + \langle g_1, \dots, g_t \rangle$.

Regarding the varieties defined by the ideals, we have the following property.

Proposition 3.2.2. *Let $I = \langle f_1, \dots, f_s \rangle$ and $J = \langle g_1, \dots, g_t \rangle$ be ideals in $k[\boldsymbol{x}]$. Then*

$$\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J).$$

Proof. Let $\boldsymbol{p} \in \mathbf{V}(I+J)$. Then $f_1(\boldsymbol{p}) = \cdots = f_s(\boldsymbol{p}) = g_1(\boldsymbol{p}) = \cdots = g_t(\boldsymbol{p}) = 0$. Therefore, $\boldsymbol{p} \in \mathbf{V}(I)$ and $\boldsymbol{p} \in \mathbf{V}(J)$. Conversely, let $f \in \mathbf{V}(I) \cap \mathbf{V}(J)$. Then $f_1(\boldsymbol{p}) = \cdots = f_s(\boldsymbol{p}) = 0$ and $g_1(\boldsymbol{p}) = \cdots = g_t(\boldsymbol{p}) = 0$. We conclude that $\boldsymbol{p} \in \mathbf{V}(I+J)$. □

3.2.2 Product of ideals

Let $I, J \subseteq k[\boldsymbol{x}]$ be ideals, and consider the set $\{fg \mid f \in I, g \in J\}$. This set is not always an ideal, as we see in the following example.

Example 3.2.3. Let $I = \langle x, y\rangle, J = \langle z, w\rangle \subset k[x, y, z, w]$, and set $H = \{fg \mid f \in I, g \in J\}$. It holds $xz \in H$ and $yw \in H$, but $xz + yw \notin H$ (the polynomial is irreducible).

Taking this into account, we make the following definition.

Definition 3.2.4. Let $I, J \subseteq k[\boldsymbol{x}]$ be ideals. We define the product of I and J as the ideal

$$IJ = \langle fg \mid f \in I, g \in J\rangle.$$

If I and J are generated by polynomials, $I = \langle f_1, \ldots, f_s\rangle$ and $J = \langle g_1, \ldots, g_t\rangle$ then

$$IJ = \langle f_1 g_1, \ldots, f_1 g_t, f_2 g_1, \ldots, f_s g_t\rangle.$$

When I is generated by a unique polynomial, $I = \langle f\rangle$, we will use the notation fJ for the product of I and J.

We will also use the exponential notation to note the product of an ideal with itself: $I^n = I \cdots I$ (n times).

In this case, we have the following property concerning the varieties defined by the ideals:

Proposition 3.2.5. *Let I and J be ideals in $k[\boldsymbol{x}]$. Then*

$$\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$$

Proof. Let $\boldsymbol{p} \in \mathbf{V}(I) \cup \mathbf{V}(J)$. We can assume that $\boldsymbol{p} \in \mathbf{V}(I)$. Then $(fg)(\boldsymbol{p}) = 0$ for all $f \in I$ and $g \in J$ because $f(\boldsymbol{p}) = 0$ for all $f \in I$.

Conversely, let $\boldsymbol{p} \notin \mathbf{V}(I) \cup \mathbf{V}(J)$. There exists $f \in \mathbf{V}(I)$ such that $f(\boldsymbol{p}) \neq 0$ and $g \in \mathbf{V}(J)$ such that $g(\boldsymbol{p}) \neq 0$. We conclude that $(fg)(\boldsymbol{p}) \neq 0$ and therefore $\boldsymbol{p} \notin \mathbf{V}(IJ)$. □

3.2.3 Intersection of ideals

Let $I, J \subseteq k[\boldsymbol{x}]$ be ideals. Their intersection

$$I \cap J = \{f \in k[\boldsymbol{x}] \mid f \in I \text{ and } f \in J\}.$$

is also an ideal.

When taking varieties, we get a similar result as in the case of products of ideals.

Proposition 3.2.6. *Let $I = \langle f_1, \ldots, f_s \rangle$ and $J = \langle g_1, \ldots, g_t \rangle$ be ideals in $k[\boldsymbol{x}]$. Then*

$$\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(IJ).$$

Proof. Let $\boldsymbol{p} \in \mathbf{V}(I) \cup \mathbf{V}(J)$. We assume $\boldsymbol{p} \in \mathbf{V}(I)$. Then $f(\boldsymbol{p}) = 0$ for all $f \in I$. Since $I \cap J \subseteq I$, $f(\boldsymbol{p}) = 0$ for all $f \in I \cap J$. Therefore, $\boldsymbol{p} \in \mathbf{V}(I \cap J)$.

Conversely, let $\boldsymbol{p} \notin \mathbf{V}(I) \cup \mathbf{V}(J)$. There exist $f \in \mathbf{V}(I)$ such that $f(\boldsymbol{p}) \neq 0$ and $g \in \mathbf{V}(J)$ such that $g(\boldsymbol{p}) \neq 0$. The polynomial fg is in I and J, so $fg \in I \cap J$ and $fg(\boldsymbol{p}) \neq 0$. Therefore $\boldsymbol{p} \notin \mathbf{V}(I \cap J)$. □

Although the varieties of IJ and $I \cap J$ are equal, the ideals may be different. However, the following inclusion always holds.

Lemma 3.2.7. *Let $I, J \subseteq k[\boldsymbol{x}]$ be ideals. Then $IJ \subseteq I \cap J$.*

Proof. Let $f \in IJ$, $f = \sum_{i=1}^{s} g_i h_i$ with $g_i \in I$ and $h_i \in J$, $1 \leq i \leq s$. Then $g_i h_i \in I$ and $g_i h_i \in J$ for all i, $1 \leq i \leq s$. Therefore, $f \in I \cap J$. □

The other inclusion does not always hold, as we see in the following easy example.

Example 3.2.8. Let $I = J = \langle x \rangle \subset k[x]$. Then $IJ = \langle x^2 \rangle$ and $I \cap J = \langle x \rangle$.

3.2.4 Quotient and saturation of ideals

Definition 3.2.9. Let $I, J \subseteq k[\boldsymbol{x}]$ be ideals. We define the *quotient ideal* of I and J as

$$I : J = \{f \in k[\boldsymbol{x}] \mid fJ \subseteq I\}.$$

We define also the *saturation* of I and J as

$$I : J^{\infty} = \{f \in k[\boldsymbol{x}] \mid fJ^m \subseteq I \text{ for some } m \in \mathbb{N}\}.$$

The sets $I : J$ and $I : J^{\infty}$ are easily seen to be ideals.

When the ideal J is principal, $J = \langle f \rangle$, we use the notations $I : f$ and $I : f^{\infty}$.

Observation 3.2.10. We have the following chain of ideals:

$$I : f \subseteq I : f^2 \subseteq \cdots \subseteq I : f^j \subseteq \cdots \subseteq I : f^{\infty}.$$

Since $k[\boldsymbol{x}]$ satisfies the ascending chain condition, there exists m such that $I : f^m = I : f^{m+1} = I : f^{\infty}$.

We have the following relation between intersections and quotients.

Proposition 3.2.11. *Let I_1, I_2 and J be ideals in $k[\boldsymbol{x}]$. Then*

$$(I_1 \cap I_2) : J = (I_1 : J) \cap (I_2 : J).$$

Proof. If $f \in (I_1 \cap I_2) : J$, then $fJ \subseteq I_1$ and $fJ \subseteq I_2$. Therefore, $f \in (I_1 : J) \cap (I_2 : J)$.

Conversely, if $f \in (I_1 : J) \cap (I_2 : J)$, then $fJ \subseteq I_1$ and $fJ \subseteq I_2$. Therefore, $fJ \subseteq I_1 \cap I_2$ and $f \in (I_1 \cap I_2) : J$. □

3.3 Gröbner bases

We have up to now seen some topics of commutative algebra and algebraic geometry from the theoretical point of view. Our main goal in this thesis is to provide effective algorithms for some problems in these areas. In this section we introduce the well–known Gröbner bases, that allow us to answer questions and perform operations between ideals algorithmically. They are a basic tool that we use in most of this thesis. The proofs that are omitted can be found in (Cox et al., 1996).

As usual, we work over $R = k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, where k is a field.

Definition 3.3.1. We call $\mathrm{Mon}(x_1, \ldots, x_n)$ the set of monomials in $x_1, \ldots, x_n$. If $\boldsymbol{a} \in \mathbb{Z}^n_{\geq 0}$, $a = (a_1, \ldots, a_n)$, we note by $\boldsymbol{x}^{\boldsymbol{a}}$ the monomial $x_1^{a_1} \ldots x_n^{a_n}$. A *(global) monomial order* in $k[\boldsymbol{x}]$ is a relation $>$ in $\mathrm{Mon}(x_1, \ldots, x_n)$ such that

(1) $>$ is a strict total ordering.

(2) $\boldsymbol{x}^{\boldsymbol{a}} > \boldsymbol{x}^{\boldsymbol{b}} \Rightarrow \boldsymbol{x}^{\boldsymbol{a}} \cdot \boldsymbol{x}^{\boldsymbol{c}} > \boldsymbol{x}^{\boldsymbol{b}} \cdot \boldsymbol{x}^{\boldsymbol{c}}$ for all $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{N}^n_0$.

(3) $>$ is a well–ordering.

When the last condition is not satisfied, we call $>$ a *non–global* monomial order.

Definition 3.3.2. Given $f \in k[\boldsymbol{x}]$, $f \neq 0$, and a fixed monomial order $>$, we write

$$f = c\,\boldsymbol{x}^{\boldsymbol{a}} + f'$$

with $c \in k$, $c \neq 0$, and $\boldsymbol{x}^{\boldsymbol{a}'} < \boldsymbol{x}^{\boldsymbol{a}}$ for all non–zero terms $c'\boldsymbol{x}^{\boldsymbol{a}'}$ of f'.

We define

$$\begin{aligned} \mathrm{lt}(f) &= c\boldsymbol{x}^{\boldsymbol{a}}, \text{ the leading term of } f \\ \mathrm{lc}(f) &= c, \text{ the leading coefficient of } f \\ \mathrm{lm}(f) &= \boldsymbol{x}^{\boldsymbol{a}}, \text{ the leading monomial of } f \end{aligned}$$

(We will also use the definition for polynomials over rings.)

Definition 3.3.3. Given a term $\tau = c\,\boldsymbol{x}^{\boldsymbol{a}}$, the *total degree* (or simply, the *degree*) of τ is $\deg(\tau) = |\boldsymbol{a}| = a_1 + \cdots + a_n$. We define the *total degree* (or *degree*) of a non–zero polynomial $f \in k[\boldsymbol{x}]$ as the maximum of all the degrees of its terms.

For a set $F \subseteq k[\boldsymbol{x}]$ and a monomial order $>$, we set

$$\mathrm{Lt}(F) = \langle \mathrm{lt}(f) \mid f \in F \rangle$$

the *leading ideal* of F, generated by all the leading terms of the polynomials in F.

We define $\mathrm{lt}(0) = 0$, $\mathrm{lc}(0) = 0$ and $\deg(0) = -\infty$.

One of the most commonly used orderings is the lexicographical order.

Definition 3.3.4. Let $\boldsymbol{a} = (a_1, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{Z}^n_{\geq 0}$. We say that $\boldsymbol{x}^{\boldsymbol{a}} > \boldsymbol{x}^{\boldsymbol{b}}$ in the *lexicographical* order if there exists $m \leq n$ such that $a_i = b_i$ for $i < m$ and $a_m > b_m$.

For example, $xy^3z > xy^2z^2$ in $k[x, y]$ and $x_1 > x_2 > \ldots > x_n$ in $k[x_1, \ldots, x_n]$. In some cases, we will use the lexicographical order with a different ordering on the variables. For example, if we set $z > y > x$, then $xy^2z^2 > xy^3z$.

Definition 3.3.5. We say that a polynomial $f \in k[\boldsymbol{x}]$ is *reduced* modulo $F \subseteq k[\boldsymbol{x}]$ if $f \neq 0$ and no monomial of f is in $\mathrm{Lt}(F)$ (or equivalently, no monomial of f is divisible by any monomial $\mathrm{lt}(g)$, $g \in F$). If not, we say that f is *reducible* modulo F.

When f is reducible, we can reduce it and obtain a reduced polynomial, as we see in the following theorem, whose proof can be found in (Cox et al., 1996, Theorem 2.3.3).

Theorem 3.3.6 (Existence of Division Algorithm in $k[\boldsymbol{x}]$)**.** *Let $>$ be a monomial order in $k[\boldsymbol{x}]$. Let $F = \{f_1, \ldots, f_s\} \subseteq k[\boldsymbol{x}]$ and $f \in k[\boldsymbol{x}]$, then f can be written as*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where a_i, $r \in k[\boldsymbol{x}]$, $1 \leq i \leq s$, and $r = 0$ or r is reduced modulo F. The polynomials a_i and r can be computed algorithmically and so that $\mathrm{lm}(f) \geq \mathrm{lm}(a_i f_i)$ if $a_i f_i \neq 0$.

The theorem suggests the following definition.

Definition 3.3.7. With the notation of the previous theorem, if $f \in k[\boldsymbol{x}]$ can be written as

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where a_i, $r \in k[\boldsymbol{x}]$ and $r = 0$ o r is reduced modulo $\{f_1, \ldots, f_s\}$, we say that r is a *remainder* of f on division by F.

We remark that the remainder r is not unique in general.

Example 3.3.8. Let $f = x^2 + y^2 \in k[x, y]$ and let $F = \{x + y, x^2 + 3\}$. Then $f = (x-y)(x+y) + 2y^2 = 1(x^2+3) + y^2 - 3$, giving two different remainders $2y^2$ and $y^2 - 3$.

Definition 3.3.9. A finite subset G of an ideal $I \subseteq k[\boldsymbol{x}]$ is called a *Gröbner basis* of I with respect to a monomial order $>$ if $\mathrm{Lt}(G) = \mathrm{Lt}(I)$.

The name *basis* suggests that G generates I. Indeed, the following property holds.

Proposition 3.3.10. *Let G be a Gröbner basis of I w.r.t. a monomial order $>$, then G is a set of generators of I.*

Proof. Let $f \in I$ and $G = \{g_1, \ldots, g_t\}$. The polynomial f can be written as

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

where $r = 0$ or r is reduced modulo G. Then $r = f - a_1 g_1 + \cdots + a_t g_t \in I$. This implies that $\mathrm{lt}(r) \in \mathrm{Lt}(I)$. But $\mathrm{Lt}(I) = \mathrm{Lt}(G)$, so we conclude that $r = 0$ and $f \in \langle G \rangle$. □

Corollary 3.3.11. *If G is a Gröbner basis of I with respect to a monomial order $>$, every non–zero element of I is reducible modulo G.*

Proof. It is a direct corollary of the last proposition. □

Moreover, the remainder of a polynomial on division by a Gröbner basis is always unique.

Proposition 3.3.12. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and let G be a Gröbner basis of I with respect to an ordering $>$. Given $f \in k[\boldsymbol{x}]$, the remainder of f on division by G is uniquely determined.*

Proof. We assume that there are two different remainders r_1 and r_2. That is, $f = \sum a_i g_i + r_1 = \sum b_i g_i + r_2$. Then $r_1 - r_2 \in I$. But the monomials of $r_1 - r_2$ are not divisible by any of the leading monomials of g_1 or g_2. Therefore, we conclude that $r_1 - r_2 = 0$. □

Definition 3.3.13. If G is a Gröbner basis of an ideal, we write $\overline{f}^G$ for the remainder of f on division by G.

Every ideal in a ring of polynomials over a field has a Gröbner basis.

Proposition 3.3.14. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and $>$ a monomial order. There exists $G = \{g_1, \ldots, g_t\}$, a Gröbner basis of I with respect to $>$.*

Proof. Since $k[\boldsymbol{x}]$ is Noetherian, there exists a finite set of generators of $\mathrm{Lt}(I)$. By definition, $\mathrm{Lt}(I)$ is the set of the leading monomials of the polynomials in I. Therefore, there exist $g_1, \ldots, g_t \in I$ such that $\mathrm{Lt}(I) = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$. The set $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis of I. □

However, in practice, computing the Gröbner basis of a given ideal is a much more difficult task. The first solution to this problem was given by Buchberger in 1965 in his doctoral thesis.

Proposition 3.3.15. *Given any set of generators of an ideal $I \subseteq k[\boldsymbol{x}]$, it is possible to algorithmically compute a Gröbner basis of it.*

The original algorithm for computing Gröbner bases, proposed by Buchberger, can be found in his works (Buchberger, 1970) and (Buchberger, 1976).

In general, the Gröbner bases of an ideal are not unique, not even for a fixed monomial order. However, under certain hypotheses, we can get uniqueness results.

Definition 3.3.16. Let $I \subseteq k[\boldsymbol{x}]$ and let $>$ be a monomial order. A Gröbner basis G of I is called reduced if

- $\mathrm{lc}(g) = 1$ for all $g \in G$.
- For all $g \in G$, no monomial of g belongs to $\mathrm{Lt}(G - \{g\})$.

We get the following theorem of uniqueness (Cox et al., 1996, Proposition 2.7.6).

Theorem 3.3.17. *Let $I \subseteq k[\boldsymbol{x}]$, $I \neq \{0\}$, and let $>$ be a monomial order. Then I has a unique reduced Gröbner basis with respect to that ordering.*

We state now an important property of Gröbner bases, which is a corollary of Buchberger's algorithm for computing Gröbner bases. It will be of great importance in the proofs of several theorems.

Proposition 3.3.18. *Let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[\boldsymbol{x}]$. Let $k' \subseteq k$ be a subfield of k such that all f_i have all their coefficients in k'. Let G be a reduced Gröbner basis of I. Then, all the coefficients of the polynomials in G are actually in k'.*

3.4 Applications of Gröbner bases

The following applications of Gröbner bases are extensively used in the algorithms we propose in the next chapters.

3.4.1 Ideal membership

This is certainly one of the most important applications of Gröbner bases.

We want to know if a given polynomial belongs to some ideal. The following property holds.

Proposition 3.4.1. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and let $f \in k[\boldsymbol{x}]$. Let G be a Gröbner basis of I with respect to a monomial order $>$. Then*

$$f \in I \iff \overline{f}^G = 0.$$

Proof. Given $f \in I$, since G generates I, $f = \sum_{i=1}^{s} a_i g_i + 0$, with $a_i \in k[\boldsymbol{x}]$, $1 \leq i \leq s$. This means that 0 is a remainder of f on division by G. But G is a Gröbner basis and therefore the remainder is unique, so $\overline{f}^G = 0$. The converse is immediate. □

This means that we can solve the ideal membership problem by using the division algorithm we have mentioned in Theorem 3.3.6.

3.4.2 Elimination of variables

Given $I \subseteq k[\boldsymbol{x}]$, we want to compute $I' = I \cap k[x_{s+1}, \ldots, x_n]$ (the polynomials in I in the variables $x_{s+1}, \ldots, x_n$). The problem is reduced to compute a Gröbner basis of I with respect to an appropriate monomial order.

Definition 3.4.2. We say that a monomial order $>$ in $k[\boldsymbol{x}]$ is an *elimination order* for $x_1, \ldots, x_s$ ($s < n$) if any monomial that contains some of the variables $x_1, \ldots, x_s$ is bigger than any monomial that does not contain any of them. Equivalently,

$$\forall f \in k[\boldsymbol{x}],\ \mathrm{lt}(f) \in k[x_{s+1}, \ldots, x_n] \Rightarrow f \in k[x_{s+1}, \ldots, x_n].$$

Note that the lexicographical order with $x_1 > \ldots > x_n$ is an elimination order for $x_1, \ldots, x_s$, $s < n$, hence elimination orders exist.

Lemma 3.4.3. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and $>$ an elimination order for $x_1, \ldots, x_s$. If $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis of I, then*

$$G' = \{g \in G \mid g \in k[x_{s+1}, \ldots, x_n]\}$$

is a Gröbner basis of $I' = I \cap k[x_{s+1}, \ldots, x_n]$ in the order induced by $>$.

Proof. Given $f \in I'$, since $I' \subseteq I$, there exists $g_i \in G$ such that $\mathrm{lt}(g_i) \mid \mathrm{lt}(f)$. Since $\mathrm{lt}(f) \in k[x_{s+1}, \ldots, x_n]$, also $\mathrm{lt}(g_i) \in k[x_{s+1}, \ldots, x_n]$ and $g_i \in G'$. Therefore $\mathrm{Lt}(G') = \mathrm{Lt}(I')$ and G' is a Gröbner basis of I'. □

When $>$ is an elimination order for a set $\boldsymbol{u}$ of variables ($\boldsymbol{u} \subset \{x_1, \ldots, x_n\}$), we use the notation $\boldsymbol{u} \gg \boldsymbol{x} \setminus \boldsymbol{u}$.

3.4.3 Intersection of ideals

We explain now how to compute the intersection of ideals.

Lemma 3.4.4. *Let $I_1 = \langle f_1, \ldots, f_s \rangle$ and $I_2 = \langle g_1, \ldots, g_r \rangle$ be ideals in $k[\boldsymbol{x}]$. Let*

$$J = \langle tf_1, \ldots, tf_s, (1-t)g_1, \ldots, (1-t)g_r \rangle = tI_1 + (1-t)I_2 \subseteq k[\boldsymbol{x}, t],$$

where t is a new variable.

Then, $I_1 \cap I_2 = J \cap k[\boldsymbol{x}]$.

Proof. If $f \in I_1 \cap I_2$, then $tf+(1-t)f \in J$ and hence $f \in J \cap k[\boldsymbol{x}]$. For the reverse inclusion, let $h \in J \cap k[\boldsymbol{x}]$. Then $h = tq_1(\boldsymbol{x}, t)h_1 + (1-t)q_2(\boldsymbol{x}, t)h_2$, with $h_1 \in I_1$ and $h_2 \in I_2$. Since t does not appear in h, taking $t = 1$, $h = q_1(\boldsymbol{x}, 1)h_1 \in I_1$ and taking $t = 0$, $h = q_2(\boldsymbol{x}, 0)h_2 \in I_2$. □

We can therefore compute the intersection of ideals by computing a Gröbner basis of $tI_1 + (1-t)I_2 \subseteq k[\boldsymbol{x}, t]$ with respect to an elimination order for t.

3.4.4 Quotient and saturation of ideals

The following lemma shows that computing the quotient of and ideal and a polynomial can be done by computing intersections.

Lemma 3.4.5. *Let $I \subseteq k[\boldsymbol{x}]$, and let $h \in k[\boldsymbol{x}]$, $h \neq 0$. Let $f_1, \ldots, f_s \in k[\boldsymbol{x}]$ be such that $I \cap \langle h \rangle = \langle f_1 h, \ldots, f_s h \rangle$. Then $I : h = \langle f_1, \ldots, f_s \rangle$.*

Proof. If $f \in \langle f_1, \ldots, f_s \rangle$, then $hf \in I$ and therefore $f \in I : h$.

Conversely, let $f \in I : h$. Then $hf \in I \cap \langle h \rangle$. Therefore, $hf = \sum_{i=1}^{s} \alpha_i h f_i$. Dividing out h, $f \in \langle f_1, \ldots, f_s \rangle$, as wanted. □

We see next how to compute the quotient of two ideals.

Lemma 3.4.6. *Let I and H be ideals in $k[\boldsymbol{x}]$. If $H = \langle h_1, \ldots, h_r \rangle$, then*

$$I : H = \bigcap_{i=1}^{r} (I : h_i).$$

Proof. If $f \in I : H$, clearly $h_i f \in I$ because $h_i \in H$ for all $1 \leq i \leq r$. Conversely, if $f \in \bigcap_{i=i}^{r} (I : h_i)$ and $h \in H$, writing $h = \sum_{i=1}^{r} \alpha_i h_i$ we get that $hf \in I$. □

To compute the saturation $I : h^\infty$, we can use two different methods. The first one relies on the observation we made in Section 3.2.4.

Let I and H be ideals in $k[\boldsymbol{x}]$. We can compute

$$I : H \subseteq I : H^2 \subseteq \ldots$$

until we find m such that $I : H^m = I : H^{m+1}$. For this value of m, we know that $I : H^m = I : H^\infty$.

A more efficient algorithm to find m can be obtained from the next lemma.

Lemma 3.4.7. *Let I, H_1 and H_2 be ideals in $k[\boldsymbol{x}]$. Then $I : (H_1 \cdot H_2) = (I : H_1) : H_2$.*

Proof. Let $f \in I : (H_1 \cdot H_2)$ and let $h_1 \in H_1$ and $h_2 \in H_2$. Then $f h_2 h_1 \in I$. Therefore, $f h_2 \in I : H_1$ and we conclude that $f \in (I : H_1) : H_2$.

Conversely, let $f \in (I : H_1) : H_2$ and $h = h_1 h_2 \in H_1 \cdot H_2$. Then $f h_2 \in I : H_1$. Therefore $f h_2 h_1 \in I$ and we conclude that $f \in I : (H_1 \cdot H_2)$. □

Based on this lemma, we take $I_0 = I$ and compute $I_j = I_{j-1} : H$ until we find m such that $I_m = I_{m+1}$.

In this way we avoid computing powers of H, which can grow very fast.

A drawback of the above method is that we do not have an a priori bound for m.

For the special case of a principal ideal $H = \langle h \rangle$, we can compute $I : h^\infty$ directly.

Proposition 3.4.8. *Let $I \subseteq k[\boldsymbol{x}]$ and $h \in k[\boldsymbol{x}]$. Then*

$$I : h^\infty = \langle I, ht - 1 \rangle k[\boldsymbol{x}, t] \cap k[\boldsymbol{x}],$$

where t is a new variable.

Proof. We note first that $(ht)^j - 1 \in \langle I, ht-1 \rangle k[\boldsymbol{x}, t]$ for all j, because $(ht)^j - 1 = (ht - 1)\left((ht)^{j-1} + (ht)^{j-2} + \cdots + 1\right)$.

Let $f \in I : h^\infty$. There exists $m \in \mathbb{N}$ such that $fh^m = g$, with $g \in I$. We get

$$fh^m t^m = gt^m \Rightarrow f \cdot ((ht)^m - 1) = gt^m - f \Rightarrow f = gt^m - f \cdot ((ht)^m - 1).$$

Therefore, $f \in \langle I, ht - 1 \rangle k[\boldsymbol{x}, t] \cap k[\boldsymbol{x}]$.

Conversely, let $f \in \langle I, ht - 1 \rangle k[\boldsymbol{x}, t] \cap k[\boldsymbol{x}]$. Then $f = \alpha_1 g + \alpha_2(ht - 1)$ with $\alpha_1, \alpha_2 \in k[\boldsymbol{x}, t]$ and $g \in I$. Since $f \in k[\boldsymbol{x}]$, we can take $t = 1/h$ and get

$$f = \alpha_1(\boldsymbol{x}, 1/h) g(\boldsymbol{x}).$$

Taking m large enough, $h^m \alpha_1(\boldsymbol{x}, 1/h) \in k[\boldsymbol{x}]$. Therefore $h^m f \in I : h^\infty$. □

Chapter 4

Radical and Minimal Associated Primes

In this chapter we propose new algorithms for computing the radical and minimal associated primes of polynomial ideals.

4.1 Preliminaries

4.1.1 Irreducible varieties and prime ideals

Definition 4.1.1. An affine variety $V \subseteq k^n$ is called *irreducible* if given V_1 and V_2 such that $V = V_1 \cup V_2$ then $V_1 = V$ or $V_2 = V$.

Proposition 4.1.2. *Let $V \subseteq k^n$ be an affine variety. Then V can be written as a finite union*

$$V = V_1 \cup \cdots \cup V_t,$$

where each V_i is an irreducible variety.

Proof. We assume that there exists a variety V that cannot be decomposed as the union of irreducible varieties. This implies that V is not irreducible and it can be decomposed as $V_1 \cup V_1'$, ($V_1 \neq V$ and $V_1' \neq V$). If we could decompose V_1 and V_1' as union of irreducible varieties, this would give us a decomposition of V into irreducible varieties. Therefore, we can assume that V_1 is not the union of irreducible varieties. That is, $V_1 = V_2 \cup V_2'$ ($V_2 \neq V$ y $V_2' \neq V$), and by the same argument, we can assume that V_2 is not a union of irreducible varieties. Carrying on with this process, we would get an infinite sequence of varieties

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \dots$$

Since the inclusions are strict, this contradicts the Descending Chain condition (Proposition 3.1.18). □

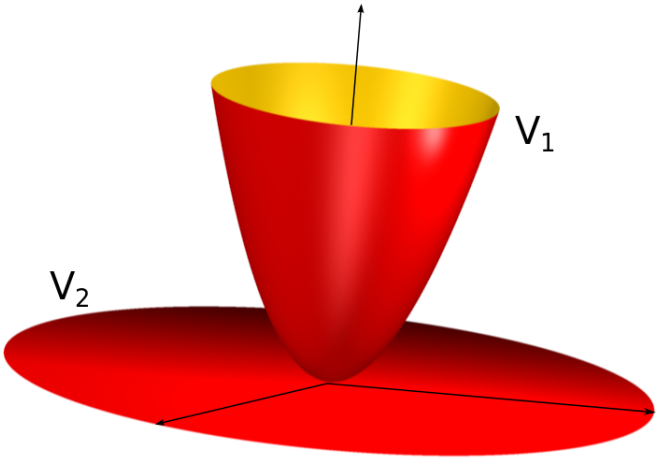

Figure 4.1: $U = V_1 \cup V_2$

Example 4.1.3. Carrying on with Example 3.1.2, $U = \mathbf{V}((x^2 + y^2 - z)z^2)$ is not irreducible because it can be decomposed as the union of the paraboloid and the plane. To prove this, we take $V_1 = \mathbf{V}(x^2+y^2-z)$ and $V_2 = \mathbf{V}(z^2)$ whose pictures are shown in figure 4.1.1. We have $U = V_1 \cup V_2$.

We focus now on decomposing ideals. Our goal is to write the ideal I as intersection of ideals $I_1, \ldots, I_t$, so that each of $I_1, \ldots, I_t$ corresponds to an irreducible component of the variety of I.

In the previous example, we can write $I = \langle x^2+y^2-z\rangle \cap \langle z^2\rangle$. This decomposition of the ideal I separates $\mathbf{V}(I)$ into its irreducible varieties.

The algebraic analogous of irreducible varieties are prime ideals. The relation is given in next proposition.

We use the following lemma.

Lemma 4.1.4. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and $f, g \in k[\boldsymbol{x}]$ polynomials. Then*

$$\mathbf{V}(\langle I, f\rangle) \cup \mathbf{V}(\langle I, g\rangle) = \mathbf{V}(\langle I, fg\rangle).$$

Proof. Let $\boldsymbol{p} \in \mathbf{V}(\langle I, f\rangle) \cup \mathbf{V}(\langle I, g\rangle)$. We can assume $\boldsymbol{p} \in \mathbf{V}(\langle I, f\rangle)$. Therefore $f(\boldsymbol{p}) = 0$ and the polynomials in I also vanish at $\boldsymbol{p}$. Then, $\boldsymbol{p} \in \mathbf{V}(\langle I, fg\rangle)$.

Conversely, let $\boldsymbol{p} \in \mathbf{V}(\langle I, fg\rangle)$. Then $f(\boldsymbol{p}) = 0$ or $g(\boldsymbol{p}) = 0$. Assuming $f(\boldsymbol{p}) = 0$, we have $\boldsymbol{p} \in \mathbf{V}(\langle I, f\rangle)$ and then, $\boldsymbol{p} \in \mathbf{V}(\langle I, f\rangle) \cup \mathbf{V}(\langle I, g\rangle)$. □

Proposition 4.1.5. *Let $V \subseteq k^n$ be an affine variety. Then V is irreducible if and only if $\mathbf{I}(V)$ is a prime ideal.*

Proof. We assume that $\mathbf{I}(V)$ is not prime. There exist f and g in $k[\boldsymbol{x}]$ such that $fg \in \mathbf{I}(V)$ but $f \notin \mathbf{I}(V)$ and $g \notin \mathbf{I}(V)$. This means that there exist points $\boldsymbol{p}$ and $\boldsymbol{q}$ in V such that $f(\boldsymbol{p}) \neq 0$ and $g(\boldsymbol{q}) \neq 0$.

From the previous lemma, we have

$$V = \mathbf{V}(\langle \mathbf{I}(V), f\rangle) \cup \mathbf{V}(\langle \mathbf{I}(V), g\rangle),$$

but V is not equal to any of the two varieties, then V is not irreducible.

For the reverse statement, we assume that V is not irreducible. Then $V = V_1 \cup V_2$, with $V_1 \subsetneq V$ and $V_2 \subsetneq V$. This implies $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$ and $\mathbf{I}(V) \subsetneq \mathbf{I}(V_2)$. Let $f \in \mathbf{I}(V_1) \setminus \mathbf{I}(V)$ and let $g \in \mathbf{I}(V_2) \setminus \mathbf{I}(V)$. If we consider fg, we see that fg vanishes at all the points of V, because f vanishes at V_1 and g vanishes at V_2. Then $fg \in \mathbf{I}(V)$, but $f \notin \mathbf{I}(V)$ and $g \notin \mathbf{I}(V)$. Therefore, $\mathbf{I}(V)$ is not prime. □

By what we have seen, given $V \subseteq k^n$ and a decomposition into irreducible varieties $V = V_1 \cup \cdots \cup V_t$, we have the following decomposition of $\mathbf{I}(V)$:

$$\mathbf{I}(V) = \mathbf{I}(V_1) \cap \cdots \cap \mathbf{I}(V_t),$$

where $\mathbf{I}(V_i)$ are prime ideals.

Example 4.1.6. Carrying on with Example 4.1.3, $\mathbf{I}(V_1) = \langle x^2+y^2-z\rangle$ and $\mathbf{I}(V_2) = \langle z\rangle$. These ideals are prime and give a decomposition of $\mathbf{I}(U)$ as intersection of prime ideals.

4.1.2 Primary decomposition and associated primes

When we work with integer numbers, every number can be written as a product of prime numbers. We will see next how to extend this to ideals. We can think of the integer numbers as ideals in $\mathbb{Z}$, associating to each integer a the ideal $\langle a\rangle$, and replacing the product of numbers by the intersection of ideals. Then, for example, the identity $6 = 2.3$ in translated into $\langle 6\rangle = \langle 2\rangle \cap \langle 3\rangle$.

The ideal $\langle 9\rangle$ cannot be written as intersection of prime ideals, because the only prime ideals that contain it are $\langle 1\rangle$ and $\langle 3\rangle$, but $\langle 3\rangle \cap \langle 3\rangle = \langle 3\rangle$. However, we can write it as the square of the prime ideal $\langle 3\rangle$ (using the product of ideals we have defined before).

As in the case of varieties, an ideal is called *irreducible* if whenever $I = I_1 \cap I_2$, then $I = I_1$ or $I = I_2$. Every ideal can be decomposed as a finite intersection of irreducible ideals, by the ascending chain condition.

Prime ideals are always irreducible, but the converse is not true in general. We have just seen that the irreducible ideals in $\mathbb{Z}$ are the prime ideals and the powers of prime ideals. The ideal $\langle p_1^{m_1} \cdots p_s^{m_s}\rangle$ can be decomposed as $\langle p_1\rangle^{m_1} \cap \cdots \cap \langle p_s\rangle^{m_s}$.

To generalize this to the ring of polynomials, a natural question is whether any ideal can be written as the intersection of prime ideals or powers of prime ideals.

Unfortunately, this is not true, as we see in the following example.

Example 4.1.7. Let $I = \langle x, y^2\rangle \subset k[x, y]$. To write it as intersection of ideals, we look for ideals that contain it. The only possible ideals are $\langle 1\rangle$ and $\langle x, y\rangle$, but I cannot be written as intersection of those ideals. Then I is irreducible, but it is

not prime (because $y^2 \in I$ and $y \notin I$) and it is not a power of a prime (because $\langle x, y\rangle^2 = \langle x^2, xy, y^2\rangle$, which does not contain I).

To decompose any ideal, we have to work with a broader class of ideals than the powers of prime ideals.

Definition 4.1.8. An ideal $I \subseteq k[\boldsymbol{x}]$ is called *primary* if given two polynomials f and g such that $fg \in I$, then $f \in I$ or $g^m \in I$ for some $m > 0$.

Before studying further these ideals, we come back to the radical ideals. We recall that the radical of an ideal I is the set $\sqrt{I} = \{f \in k[\boldsymbol{x}] \mid f^m \in I \text{ for some } m \in \mathbb{N}\}$.

Lemma 4.1.9. *Let $I \subseteq k[\boldsymbol{x}]$. Then $\sqrt{I}$ is a radical ideal.*

Proof. We show first that $\sqrt{I}$ is an ideal.

(1) $0 \in \sqrt{I}$.

(2) Let $f \in \sqrt{I}$ and $g \in k[\boldsymbol{x}]$. There exists $m > 0$ such that $f^m \in I$. Then $g^m f^m \in I$ and therefore $gf \in \sqrt{I}$.

(3) Let $f, g \in \sqrt{I}$. There exist m_1 and m_2 such that $f^{m_1} \in I$ and $g^{m_2} \in I$. We consider $(f+g)^{m_1+m_2} = f^{m_1+m_2} + f^{m_1+m_2-1}g + \cdots + g^{m_1+m_2}$. All the terms of this sum are in I, then $(f+g)^{m_1+m_2} \in I$ and $f + g \in \sqrt{I}$.

To prove that it is radical, let f be such that $f^m \in \sqrt{I}$. Then $(f^m)^l \in I$ for some $l \in \mathbb{N}$ and $f \in \sqrt{I}$, as required. □

Proposition 4.1.10. *Let $I_1, \ldots, I_t$ be ideals in $k[\boldsymbol{x}]$ and let $I = I_1 \cap \cdots \cap I_t$. Then*

$$\sqrt{I} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_t}.$$

Proof. Let $f \in \sqrt{I}$. There exists $m \in \mathbb{N}$ such that $f^m \in I$. Then $f^m \in I_i$ $\forall i$, $1 \leq i \leq t$, and therefore $f \in \sqrt{I_i}$ $\forall i$, $1 \leq i \leq t$.

Conversely, if $f \in \sqrt{I_i}$, $1 \leq i \leq t$, there exist m_i such that $f^{m_i} \in \sqrt{I_i}$. Taking m the maximum of all m_i, $1 \leq i \leq t$, we conclude that $f \in \sqrt{I}$. □

The following corollary is immediate.

Proposition 4.1.11. *Let $I_1, \ldots, I_t$ be radical ideals and let $I = I_1 \cap \cdots \cap I_t$. Then I is a radical ideal.*

Clearly, a prime ideal is radical. Moreover,

Lemma 4.1.12. *If I is a primary ideal, then $\sqrt{I}$ is prime and it is the smallest prime ideal containing I.*

Proof. We assume $fg \in \sqrt{I}$. Then $(fg)^m \in I$ for some m. Since I is primary, $f^m \in I$ or $(g^m)^l \in I$ for some $l \in \mathbb{N}$. Then $f \in \sqrt{I}$ or $g \in \sqrt{I}$. Therefore, $\sqrt{I}$ is prime.

To prove the second part, let J be a prime ideal such that $I \subseteq J$. We want to show that $\sqrt{I} \subseteq J$. Let $f \in \sqrt{I}$. By definition $f^m \in I$ for some $m \in \mathbb{N}$. Then $f^m \in J$ because $I \subseteq J$. Since J is prime, we conclude that $f \in J$, which proves the inclusion. □

Definition 4.1.13. If I is primary and $\sqrt{I} = P$, we say that I is *P-primary.*

In general, checking if a given ideal is primary is not easy, but the following special case is sometimes useful.

Proposition 4.1.14. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal such that $\sqrt{I}$ is maximal. Then I is primary.*

Proof. Let $f, g \in k[\boldsymbol{x}]$ be such that $fg \in I$. We assume that $g^m \notin I$ for any $m > 0$. We want to prove that $f \in I$. Since $g \notin \sqrt{I}$ and $\sqrt{I}$ is maximal, $\langle \sqrt{I}, g \rangle = \langle 1 \rangle$. Therefore, there exist $p \in \sqrt{I}$ and $q \in k[\boldsymbol{x}]$ such that $1 = p + qg$. Let $l \in \mathbb{N}$ be such that $p^l \in I$. Taking powers in the last identity, $1 = p^l + lp^{l-1}qg + \cdots + (qg)^l$. Multiplying by f, we get $f = fp^l + lp^{l-1}qgf + \cdots + (qg)^l f$, where all the terms in the right side are in I. Therefore, $f \in I$. □

Example 4.1.15. The ideal $I = \langle x, y^2 \rangle \subset k[x, y]$ is not prime ($y^2 \in I$ but $y \notin I$), but it is primary because the radical of I is $\langle x, y \rangle$, that is maximal. The ideal I is $\langle x, y \rangle$-primary.

Example 4.1.16. The ideal $I = \langle xy, y^2 \rangle \subset k[x, y]$ is not primary, because $xy \in I$, but $y \notin I$ and $x^m \notin I$ for any $m \in \mathbb{N}$.

Primary ideals allow us to decompose any ideal in $k[\boldsymbol{x}]$.

Proposition 4.1.17. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal. Then I admits a primary decomposition. That is, there exist primary ideals $Q_1, \ldots, Q_t$ such that*

$$I = \bigcap_{i=1}^{t} Q_i$$

Proof. Since every ideal can be written as the intersection of irreducible ideals, it is enough to show that an irreducible ideal is primary.

We assume that I is irreducible and that $fg \in I$ with $f \notin I$. We have to prove that some power of g is in I. We consider the ideals $I : g^m$, $m \geq 1$. We have the following chain of ideals:

$$I : g \subseteq I : g^2 \subseteq \ldots$$

By the ascending chain condition, there exists $N \geq 1$ such that $I : g^N = I : g^{N+1} = \ldots$ We claim that $\langle I, g^N \rangle \cap \langle I, f \rangle = I$. The inclusion $\supseteq$ is clear. To prove $\subseteq$, let $h \in \langle I, g^N \rangle \cap \langle I, f \rangle$. Then $h = i + \alpha g^N = j + \beta f$, with $i, j \in I$ y $\alpha, \beta \in k[\boldsymbol{x}]$.

Multiplying by g, $ig + \alpha g^{N+1} = jg + \beta fg$, where $fg \in I$. Thus $ig + \alpha g^{N+1} \in I$ and $\alpha g^{N+1} \in I$. Now $I : g^N = I : g^{N+1}$ implies that $\alpha g^N \in I$ and therefore $h \in I$.

Since I is irreducible, then $I = \langle I, g^N \rangle$ or $I = \langle I, f \rangle$. But the later is impossible because $f \notin I$. Therefore $I = \langle I, g^N \rangle$ and we conclude that $g^N \in I$. □

Example 4.1.18. A primary decomposition of $I = \langle xy, y^2 \rangle$ is

$$I = \langle y \rangle \cap \langle x, y^2 \rangle.$$

Example 4.1.19. The ideal $I = \langle (x^2 + y^2 - z)z^2 \rangle$ can be decomposed as $I = \langle x^2 + y^2 - z \rangle \cap \langle z^2 \rangle$. We have seen that the variety of I is the union of a paraboloid and the plane. These varieties correspond to the varieties of the ideals $\langle x^2+y^2-z \rangle$ and $\langle z^2 \rangle$ respectively. Therefore, from the primary decomposition of I, we obtained the components of I corresponding to irreducible varieties.

Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and let $I = Q_1 \cap \cdots \cap Q_t$, be its primary decomposition. Taking radicals,

$$\sqrt{I} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_t}.$$

If Q_i is P_i-primary, we get the decomposition

$$\sqrt{I} = P_1 \cap \cdots \cap P_t.$$

If we consider the corresponding varieties, we get

$$\mathbf{V}(I) = \mathbf{V}(P_1) \cup \cdots \cup \mathbf{V}(P_t),$$

where we have used that $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$. Since P_i, $1 \leq i \leq t$, are prime ideals, we obtain a decomposition of $\mathbf{V}(I)$ into irreducible varieties.

Now that we know that ideals and varieties can be decomposed into irreducible components, a natural question is how to obtain their decompositions algorithmically. This problem will be studied in the following sections.

We need to study first some properties of the primary decomposition.

Definition 4.1.20. Let $I = Q_1 \cap \cdots \cap Q_t$ be a primary decomposition of I. The decomposition is called irredundant if

(1) $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $1 \leq i, j \leq t$ and $i \neq j$.

(2) $Q_i \not\supseteq \cap_{j \neq i} Q_j$ for $1 \leq i \leq t$.

Given any primary decomposition of an ideal, we can obtain from it a primary decomposition satisfying the second property by simply removing the redundant components.

To fulfill the first condition, we use the following lemma.

Lemma 4.1.21. *Let P be a prime ideal and let $Q_1, \ldots, Q_t$ be P-primary ideals. Let $Q = Q_1 \cap \cdots \cap Q_t$. Then Q is a P-primary ideal.*

Proof. Clearly $\sqrt{Q} = \sqrt{Q_1 \cap \cdots \cap Q_t} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_t} = P$. Let $f\,g \in Q$, with $f \notin Q$. We need to show that $g^m \in Q$ for some $m \in \mathbb{N}$. There exists k, $1 \leq k \leq t$, such that $f \notin Q_k$ and therefore, $g^u \in Q_k$, for some $u \in \mathbb{N}$. Then $g \in P$ and $g^m \in Q$ for some $m \in \mathbb{N}$, as required. □

Hence, when for some prime ideal P the decomposition has more than one P-primary ideal we take the intersection of all of them and get a new P-primary ideal.

In this way, any primary decomposition can be transformed into an irredundant primary decomposition. We conclude that every ideal $I \subseteq k[\boldsymbol{x}]$ has an irredundant primary decomposition.

Example 4.1.22. We have seen that a primary decomposition of $I = \langle xy, y^2 \rangle$ is $I = \langle y \rangle \cap \langle x, y^2 \rangle$. Another primary decomposition of I is $I = \langle y \rangle \cap \langle x^2, xy, y^2 \rangle$. This means that there is no uniqueness in the primary decomposition, not even when considering irredundant primary decompositions.

If we take radicals, we get $\sqrt{\langle x, y^2 \rangle} = \sqrt{\langle x^2, xy, y^2 \rangle} = \langle x, y \rangle$. That is, the corresponding prime ideals are equal.

The property of the later example always holds and we prove it next. We use the following lemmas.

Lemma 4.1.23. *Let $I_1, \ldots, I_t$ be ideals in $k[\boldsymbol{x}]$ and let P be a prime ideal such that $I_1 \cap \cdots \cap I_t \subseteq P$. Then there exists i, $1 \leq i \leq t$, such that $I_i \subseteq P$. If $P = I_1 \cap \cdots \cap I_t$, then $P = I_i$ for some i, $1 \leq i \leq t$.*

Proof. We assume $I_i \not\subseteq P$ for any i, $1 \leq i \leq t$. Then for all i, $1 \leq i \leq t$, there exists $f_i \in I_i$ such that $f_i \notin P$. Taking $f = f_1 f_2 \cdots f_t$, we get $f \in I_1 \cap \cdots \cap I_t$, but $f \notin P$ because P is prime. This contradicts the hypothesis $I_1 \cap \cdots \cap I_t \subseteq P$.

For the second part, if $P = I_1 \cap \cdots \cap I_t$, $P \subseteq I_i$ for all i, $1 \leq i \leq t$. If $I_j \subseteq P$, then $P = I_j$. □

Lemma 4.1.24. *Let $Q \subseteq k[\boldsymbol{x}]$ be a P-primary ideal and let $f \in k[\boldsymbol{x}]$. Then*

(1) If $f \in Q$, $Q : f = \langle 1 \rangle$.

(2) If $f \notin Q$, $Q : f$ is P-primary.

(3) If $f \notin P$, $Q : f = Q$.

Proof. (1) If $f \in Q$, $gf \in Q$ for all $g \in k[\boldsymbol{x}]$, then $Q : f = \langle 1 \rangle$.

(2) If $f \notin Q$ and $gf \in Q$, $g \in \sqrt{Q} = P$. Then $Q \subseteq Q : f \subseteq P$. Taking radicals, we get that $\sqrt{Q : f} = P$. To see that it is a primary ideal, let $gh \in Q : f$, such that $g^m \notin Q : f$ for any $m \in \mathbb{N}$. Then $g^m \notin Q$ for any $m \in \mathbb{N}$. But $ghf \in Q$ and since Q is primary, we get that $hf \in Q$. Therefore, $h \in Q : f$ as required.

(3) If $f \notin P$ and $g \in Q : f$ we get that $gf \in Q$. Since $f^m \notin Q$ for any $m \in \mathbb{N}$, $g \in Q$. For the other inclusion, let $g \in Q$. Then, $gf \in Q$ and therefore $g \in Q : f$. □

We obtain the following uniqueness theorem:

Theorem 4.1.25. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and let $I = Q_1 \cap \cdots \cap Q_t$ be an irredundant primary decomposition of I. Let $P_i = \sqrt{Q_i}$, $1 \leq i \leq t$. The number of primary components and the prime ideals P_i, $1 \leq i \leq t$, do not depend on the chosen primary decomposition.*

Proof. To prove the theorem, we will prove that the prime ideals P_i, $1 \leq i \leq t$ are exactly the *prime* ideals that appear in the set of ideals $\sqrt{I : f}$, $f \in k[\boldsymbol{x}]$.

If $f \in k[\boldsymbol{x}]$, $I : f = (\bigcap Q_i) : f = \bigcap (Q_i : f)$. Then $\sqrt{I : f} = \bigcap_{i=1}^{t} \sqrt{Q_i : f} = \bigcap_{f \notin Q_j} P_j$ by Lemma 4.1.24.

Since the primary decomposition is irredundant, for any i, $1 \leq i \leq t$, $\exists\, g_i \in \bigcap_{j \neq i} Q_j \setminus Q_i$. For these g_i, $\sqrt{I : g_i} = P_i$. Then, all the prime ideals P_i, $1 \leq i \leq t$, appear in the set of ideals $\sqrt{I : f}$.

Conversely, let P be a prime ideal such that $P = \sqrt{I : f}$ for some $f \in k[\boldsymbol{x}]$. Then $P = \bigcap_{f \notin Q_j} P_j$. By Lemma 4.1.23, it holds $P = P_j$ for some j, $1 \leq j \leq t$. □

Definition 4.1.26. Let $I \subseteq k[\boldsymbol{x}]$ and let $I = Q_1 \cap \cdots \cap Q_t$ be an irredundant primary decomposition. The prime ideals $P_i = \sqrt{Q_i}$ are called *associated* primes of I. The minimal elements (with respect to inclusion) of the set of associated primes are called *minimal* or *isolated* associated primes. The other associated primes are called *embedded*.

Example 4.1.27. In the example $I = \langle xy, y^2 \rangle = \langle y \rangle \cap \langle x, y^2 \rangle$, the associated prime ideals are $P_1 = \langle y \rangle$ y $P_2 = \langle x, y \rangle$. P_1 is isolated and P_2 is embedded because $P_1 \subseteq P_2$. If we look at the varieties, $\mathbf{V}(P_1)$ is the line $\{y = 0\}$ and $\mathbf{V}(P_2)$ is the point $\{(0, 0)\}$. We observe that $\mathbf{V}(P_2)$ is included in $\mathbf{V}(P_1)$, and that is where the name *embedded* comes from.

Remark 4.1.28. If we take an irredundant primary decomposition $I = Q_1 \cap \cdots \cap Q_t$ (with Q_i P_i-primary, $1 \leq i \leq t$) and take radicals, we obtain $\sqrt{I} = P_1 \cap \cdots \cap P_t$. If there are embedded primes, some of the components P_i are redundant. By removing them, we get a decomposition of $\sqrt{I}$ as intersection of prime ideals. These are exactly the minimal associated primes, which by Theorem 4.1.25, are uniquely determined. Since the variety of a prime ideal is irreducible, and $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$, this gives a decomposition of $\mathbf{V}(I)$ into its irreducible components.

That is, when we are only interested in decomposing the set of solutions of a system of polynomial equations into its irreducible components, it is enough to compute the minimal associated primes of the corresponding ideal, instead of computing the full primary decomposition, which is usually slower.

In the last example, we have seen that there is no uniqueness for the general primary decomposition. However, the primary components associated to isolated prime ideals are uniquely determined.

Theorem 4.1.29. *Let $I \subseteq k[\boldsymbol{x}]$ and let $P_1, \ldots, P_t$ be the associated prime ideals of I. Let $I = Q_1 \cap \cdots \cap Q_t$ be a primary decomposition of I such that $\sqrt{Q_i} = P_i$, $1 \leq i \leq t$. If P_i is a minimal prime ideal of I, then Q_i is independent of the chosen primary decomposition.*

The proof of this theorem can be found in (Atiyah and Macdonald, 1969).

In the next section, we will see that for zero–dimensional ideals, all the associated prime ideals are minimal, and therefore the primary decomposition is unique.

We conclude this section with a property of minimal prime ideals.

Proposition 4.1.30. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and let P be a prime ideal such that $I \subseteq P$. Then P contains a minimal associated prime ideal of I.*

Proof. If $P \supseteq I = Q_1 \cap \cdots \cap Q_t$, then $P = \sqrt{P} \supseteq \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_t} = P_1 \cap \cdots \cap P_t$. By Lemma 4.1.23, $P \supseteq P_i$ for some i, $1 \leq i \leq s$, and therefore P contains a minimal prime associated to I. □

Observation 4.1.31. By this property, all the minimal prime ideals in the set of ideals that contain an ideal I are always associated prime ideals of I.

4.2 Computation of the radical of an ideal

In this section we study an algorithm for computing the radical based on the ideas of Gianni et al. (1988) and Krick and Logar (1991b), compare an implementation of it with the implementations of other known algorithms, and analyze its theoretical complexity.

4.2.1 Theoretical aspects

We state some results that will be used as splitting tools in the algorithms.

Proposition 4.2.1. *Let $I \subset R$ be an ideal, and $f, g, h \in R$ polynomials. Then*

(1) $\sqrt{\langle I, fg\rangle} = \sqrt{\langle I, f\rangle} \cap \sqrt{\langle I, g\rangle}$.

(2) If $\langle f, g\rangle = \langle 1\rangle$, *then* $\langle I, fg\rangle = \langle I, f\rangle \cap \langle I, g\rangle$.

(3) For $m \in \mathbb{N}$ *such that* $I : h^\infty = I : h^m$, $I = \langle I, h^m\rangle \cap (I : h^m)$.

Proof. (1) The inclusion $\sqrt{\langle I, fg\rangle} \subseteq \sqrt{\langle I, f\rangle} \cap \sqrt{\langle I, g\rangle}$ is clear. For the reverse inclusion, let $h \in \sqrt{\langle I, f\rangle} \cap \sqrt{\langle I, g\rangle}$. There exist $u, v \in \mathbb{N}$ such that $h^u = p + \alpha f$ and $h^v \in q + \beta g$, where $p, q \in I$ and $\alpha, \beta \in R$. Therefore $h^{u+v} = pq + \beta gp + \alpha fq + \alpha\beta fg \in \langle I, fg\rangle$ and hence $h \in \sqrt{\langle I, fg\rangle}$.

(2) The inclusion $\langle I, fg\rangle \subseteq \langle I, f\rangle \cap \langle I, g\rangle$ is clear. For the reverse inclusion, let $h \in \langle I, f\rangle \cap \langle I, g\rangle$ and $r, s \in R$ be such that $rf + sg = 1$. There exist $p, q \in I$ and $\alpha, \beta \in R$ such that $h = p + \alpha f = q + \beta g$. Therefore $h = (sg + rf)h = sgp + \alpha sgf + rfq + \beta rfg$ and hence $h \in \langle I, fg\rangle$.

(3) The inclusion $I \subseteq \langle I, h^m\rangle \cap (I : h^m)$ is clear. For the reverse inclusion, let $g \in \langle I, h^m\rangle \cap (I : h^m)$. Then $g = p + \alpha h^m$, for some $p \in I$ and $\alpha \in R$, and $h^m g \in I$. Hence $ph^m + \alpha h^{2m} \in I$ and therefore $\alpha h^{2m} \in I$. Since $I : h^\infty = I : h^m$, $\alpha h^m \in I$ and we conclude that $g \in I$, as wanted. □

Although computing the radical of an ideal requires complex algorithms, deciding whether a given polynomial belongs to the radical of an ideal requires only one Gröbner basis computation, as we see in the next lemma.

Lemma 4.2.2 (Radical membership)**.** *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and $f \in k[\boldsymbol{x}]$. Then*

$$f \in \sqrt{I} \iff 1 \in \langle I, tf - 1\rangle_{k[x_1,\ldots,x_n,t]},$$

where t is a new variable.

Proof. Since $(tf)^N - 1 \in \langle tf - 1\rangle$ for all $N \in \mathbb{N}$, if $f^m \in I$ then clearly $1 \in \langle I, tf - 1\rangle$.

Conversely, if $1 = \alpha p + \beta(tf - 1)$, with $\alpha, \beta \in k[x_1, \ldots, x_n, t]$, replacing t by $1/f$, we get $1 = \alpha(x_1, \ldots, x_n, 1/f)p(x_1, \ldots, x_n)$. Multiplying by a large enough power of f, f^m, we conclude that $f^m \in I$ as wanted. □

We study first the computation of the radical of zero–dimensional ideals, which correspond to ideals such that $\mathbf{V}_{\bar{k}}(I)$ has only a finite number of points.

The following is an important characterization of zero–dimensional ideals, that will be used in the algorithms.

Proposition 4.2.3. *An ideal $I \subset k[x_1, \ldots, x_n]$ is zero–dimensional if and only if for every i, $1 \leq i \leq n$, the set $I \cap k[x_i]$ contains non–zero elements.*

Proof. If I is zero–dimensional, $V = \mathbf{V}(I)$ is finite. For $1 \leq i \leq n$, the polynomial $f_i = \prod_{\boldsymbol{p} \in V}(x_i - p_i)$, with p_i the i-th coordinate of $\boldsymbol{p}$, is in $\mathbf{I}(V)$ and therefore $f_i^m \in I$ for some $m \in \mathbb{N}$. For the converse, let $f_i \in I \cap k[x_i]$. Then $\mathbf{V}(I) \subseteq \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \text{ a root of } f_i\}$. □

In particular, since $k[x_i]$ is a principal ideal domain, if I is zero–dimensional, for every i, $1 \leq i \leq n$, there exists $f_i \in k[x_i] \setminus \{0\}$ such that $I \cap k[x_i] = \langle f_i\rangle$.

We show next that all associated primes of a zero–dimensional ideal are minimal, as mentioned in Section 4.1.2.

Proposition 4.2.4. *Let $I \subset k[\boldsymbol{x}]$ be a zero–dimensional ideal and let P be an associated prime of I. Then P is a maximal ideal of $k[\boldsymbol{x}]$, and is therefore a minimal associated prime of I.*

Proof. If $Q \subset k[\boldsymbol{x}]$ is a maximal ideal (and therefore, prime) such that $P \subseteq Q$, we obtain the chain $I \subseteq P \subseteq Q$. Since I is zero–dimensional, it must be $P = Q$. Therefore P is maximal, and a minimal associated prime of I. □

In (Gianni et al., 1988) and (Krick and Logar, 1991b) the computation of the radical of a general ideal is reduced to the zero–dimensional case. For the computation of the radical of a zero–dimensional ideal, a special algorithm is used.

Before stating the algorithm, we make the following definitions.

Definition 4.2.5. Given a field k, an irreducible polynomial $f = a_n x^n + \cdots + a_1 x + a_0$ is called *separable* if all the roots of f in $\bar{k}$ are simple. A field k is called *perfect* if every irreducible polynomial $f \in k[x]$ is separable.

Example 4.2.6. The polynomial $g = x^3 - t \in \mathbb{Q}(t)[x]$ is separable, because it has three different roots in $\overline{\mathbb{Q}(t)}$, but $h = x^3 - t \in \mathbb{Z}_3(t)[x]$ is not separable, it can be factorized as $(x - \alpha)^3$ in $\overline{\mathbb{Z}_3(t)}[x]$, where we can think of α as $\sqrt[3]{t}$. The field $\mathbb{Z}_3(t)$ is not perfect.

It is a classical result that finite fields, fields of characteristic 0 and algebraically closed fields are perfect.

When k is perfect, there exists a simple algorithm to compute the radical of a zero–dimensional ideal.

Proposition 4.2.7. *(Seidenberg Lemma, 1974) Let $I \subset k[\boldsymbol{x}]$ (with k a perfect field) be a zero–dimensional ideal and $I \cap k[x_i] = \langle f_i \rangle$, $1 \leq i \leq n$. Let $g_i = \sqrt{f_i} = f_i / \gcd(f_i, f_i')$, the square free part of f_i. Then*

$$\sqrt{I} = \langle I, g_1, \ldots, g_n \rangle.$$

We will need to compute the radical of zero–dimensional ideals over $k(\boldsymbol{u})$, with $\boldsymbol{u}$ a set of variables. When k has characteristic 0, $k(\boldsymbol{u})$ is still perfect, and we can use this lemma. However, if the characteristic of k is not 0, we have seen in Example 4.2.6 that $k(\boldsymbol{u})$ might not be perfect. In that case, more elaborated algorithms (Kemper, 2002; Matsumoto, 2001) can be used. We will restrict to the case of characteristic 0.

The general algorithm is based on the following well–known properties (see, for example, Greuel and Pfister, 2008, Chapters 3 and 4).

Lemma 4.2.8. *Let $I = Q_1 \cap \cdots \cap Q_t \subset k[\boldsymbol{x}]$ be a primary decomposition of the ideal I, and $J \subset k[\boldsymbol{x}]$ another ideal. Then $I : J^\infty = \bigcap_{J \not\subset P_i} Q_i$, where $P_i = \sqrt{Q_i}$.*

Proof. If Q is a P-primary ideal, and $g \in P$ then $Q : g^\infty = \langle 1 \rangle$. If $g \notin P$, then $Q : g^\infty = Q$. Hence $I : J^\infty = (Q_1 \cap \cdots \cap Q_t) : J^\infty = (Q_1 : J^\infty) \cap \cdots \cap (Q_t : J^\infty) = \bigcap_{J \not\subset P_i} Q_i$ □

We say that a set of variables $\boldsymbol{u} \subset \boldsymbol{x}$ is *independent* (with respect to I) if $I \cap k[\boldsymbol{u}] = \{0\}$. If I is zero–dimensional, for all $1 \leq i \leq n$ there exists a polynomial $f_i \in I$ such that $f_i \in k[x_i]$, and hence the only independent set is the empty set. In general, if $\boldsymbol{u}$ is independent, then $Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ is not the whole ring and has dimension at most $\dim(I) - \#\boldsymbol{u}$. Therefore $\#\boldsymbol{u}$ can be at most equal to $\dim(I)$. We say that an independent set is *maximal* if it has $\dim(I)$ elements.

Using maximal independent sets we can reduce the problem of computing the radical of an ideal to the zero–dimensional case.

Lemma 4.2.9. *Let $I \subset k[\boldsymbol{x}]$ be a proper ideal and $\boldsymbol{u} \subset \boldsymbol{x}$ a maximal independent set of variables with respect to I. Then $Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \subset k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ is a zero–dimensional ideal.*

Proof. If $Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ is not zero–dimensional, there exists a variable $t \in \boldsymbol{x} \smallsetminus \boldsymbol{u}$ such that $Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ contains no non–zero polynomial in t. Hence $\boldsymbol{u} \cup \{t\}$ is also independent, which contradicts the maximality of $\boldsymbol{u}$. □

For the proof of the next proposition, we use the following lemmas.

Lemma 4.2.10. *Let $Q \subset k[\boldsymbol{x}]$ be a primary ideal and $\boldsymbol{u}$ a set of variables such that $Q \cap k[\boldsymbol{u}] = \{0\}$. Then $Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] \cap k[\boldsymbol{x}] = Q$.*

Proof. Clearly $Q \subseteq Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] \cap k[\boldsymbol{x}]$. For the reverse inclusion, let $f \in Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] \cap k[\boldsymbol{x}]$, $f = g(\boldsymbol{x})/h(\boldsymbol{u})$, with $g \in Q$ and $h \neq 0$. Then $hf \in Q$ and, since Q is primary and $h(\boldsymbol{u}) \notin \sqrt{Q}$ (because $Q \cap k[\boldsymbol{u}] = \{0\}$), $f \in Q$ as wanted. □

Lemma 4.2.11. *Let $Q \subset k[\boldsymbol{x}]$ be a primary ideal and $\boldsymbol{u}$ a set of variables such that $Q \cap k[\boldsymbol{u}] = \{0\}$. Then $Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ is a primary ideal.*

Proof. We assume first that Q is prime. If $f \in Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ and $f = \frac{g_1(\boldsymbol{x})}{h_1(\boldsymbol{u})}\frac{g_2(\boldsymbol{x})}{h_2(\boldsymbol{u})}$, with $g_1, g_2 \in k[\boldsymbol{x}]$, $h_1, h_2 \in k[\boldsymbol{u}]$, then by the previous lemma, $h_1h_2f = g_1g_2 \in Q$. Hence either g_1 or g_2 belong to Q, and therefore either $\frac{g_1(\boldsymbol{x})}{h_1(\boldsymbol{u})}$ or $\frac{g_2(\boldsymbol{x})}{h_2(\boldsymbol{u})}$ belong to $Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$.

If Q is primary, then $\sqrt{Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]} = \sqrt{Q}k(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ is prime and therefore maximal (because it is zero–dimensional). This proves that $Qk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ is primary. □

Proposition 4.2.12. *Let $I \subseteq k[\boldsymbol{x}]$ be an ideal and $\boldsymbol{u} \subseteq \boldsymbol{x}$ a maximal independent set of variables with respect to I. Let $I = Q_1 \cap \cdots \cap Q_t$ be an irredundant primary decomposition of I, such that $Q_i \cap k[\boldsymbol{u}] = \{0\}$ for $1 \leq i \leq s$ and $Q_i \cap k[\boldsymbol{u}] \neq \{0\}$ for $s+1 \leq i \leq t$. Then, for $1 \leq i \leq s$, Q_i is an isolated primary component of I (that is, it corresponds to a minimal prime) and is therefore uniquely determined.*

Moreover $Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] = (Q_1k(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]) \cap \cdots \cap (Q_sk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}])$ is the unique irredundant primary decomposition of the zero–dimensional ideal $Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ and $\sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]} \cap k[\boldsymbol{x}] = P_1 \cap \cdots \cap P_s$, with $P_i = \sqrt{Q_i}$.

Proof. For the first claim, fix Q_i, $1 \leq i \leq s$. Clearly, $\boldsymbol{u}$ is a maximal independent set with respect to Q_i since if $\boldsymbol{u} \subsetneq \boldsymbol{u}'$ with $Q_i \cap k[\boldsymbol{u}'] = \{0\}$, $\boldsymbol{u}$ would not be independent maximal with respect to I. Therefore $Q_ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ is a zero–dimensional ideal.

Suppose now that there exist $1 \leq i < j \leq s$ such that $\sqrt{Q_i} =: P_i \subsetneq P_j := \sqrt{Q_j}$. This would imply the strict inclusion $P_ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] \subsetneq P_jk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$, of prime ideals, which is a contradiction since they are both zero–dimensional.

For the second claim,

$$\begin{aligned} Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] &= (Q_1 \cap \cdots \cap Q_t)k(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] \\ &= (Q_1k(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]) \cap \cdots \cap (Q_sk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]) \end{aligned}$$

is an irredundant primary decomposition by the previous lemma.

Finally, since $\sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}]} = \sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}]} = \sqrt{Q_1 \cap \cdots \cap Q_s}$, the last claim is clear. □

To apply the ideas above in the algorithms, we need to study the computational aspects of contractions and extensions.

Proposition 4.2.13. *Let $\boldsymbol{u} \subset \boldsymbol{x}$ be a set of variables and $J \subset k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ an ideal. Let $\{g_1, \ldots, g_s\}$ be a Gröbner basis of J with respect to a monomial order $>$ in $k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ consisting of polynomials in $k[\boldsymbol{x}]$. Let*

$$h = \gcd\{\mathrm{lc}(g_i), 1 \leq i \leq s\} \in k[\boldsymbol{u}],$$

where $\mathrm{lc}(g_i)$ denotes the leading coefficient of g_i regarded as a polynomial in $k[\boldsymbol{u}][\boldsymbol{x} \setminus \boldsymbol{u}]$.

Then

$$J \cap k[\boldsymbol{x}] = \langle g_1, \ldots, g_s \rangle : h^\infty,$$

where $\langle g_1, \ldots, g_s \rangle$ is the ideal generated in $k[\boldsymbol{x}]$.

Proof. Let $I = \langle g_1, \ldots, g_s \rangle$ in $k[\boldsymbol{x}]$ and $f \in I : h^\infty$. There exists $m \in \mathbb{N}$ such that $h^m f \in I$. Since $h \in k[\boldsymbol{u}]$, $f \in Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}] = J \cap k[\boldsymbol{x}]$. Therefore, $I : h^\infty \subset J \cap k[\boldsymbol{x}]$.

For the reverse inclusion, let $f \in J \cap k[\boldsymbol{x}]$. Since $\{g_1, \ldots, g_s\}$ is a Gröbner basis of J, $f = \sum_{i=1}^{s} \alpha_i g_i$, with $\alpha_i \in k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$. In Buchberger's algorithm for computing Gröbner bases, the coefficients α_i are obtained by divisions only by the coefficients $\mathrm{lc}(g_i)$ of g_i, $1 \leq i \leq s$. Therefore, we can write $\alpha_i = \frac{\beta_i}{h^{m_i}}$, with $\beta_i \in k[\boldsymbol{x}]$. Taking m the maximum m_i, $1 \leq i \leq s$, we get $h^m f \in k[\boldsymbol{x}]$ and therefore, $f \in I : h^\infty$. □

Remark 4.2.14. Recall from Property 3.4.8 that the saturation ideal $\langle g_1, \ldots, g_s \rangle : h^\infty$ can be computed by the formula $I : h^\infty = \langle I, th - 1 \rangle \cap k[\boldsymbol{x}]$, t a new variable.

Remark 4.2.15. A Gröbner basis of $Jk(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ can be obtained by computations in $k[\boldsymbol{x}]$ taking $\{f_1, \ldots, f_s\}$, a set of generators of J consisting of polynomials in $k[\boldsymbol{x}]$, and computing a basis of $\langle f_1, \ldots, f_s \rangle k[\boldsymbol{x}]$ with respect to an elimination order with $\boldsymbol{x} \setminus \boldsymbol{u} \gg \boldsymbol{u}$.

The generators of J in $k[\boldsymbol{x}]$ can be obtained from any set of generators of J simply by multiplying the polynomials by its denominators in $k[\boldsymbol{u}]$.

4.2.2 Algorithms

Our new algorithm is stated in Algorithm 4.2.1. Correctness of the algorithm is given by the following proposition.

Proposition 4.2.16. *Let $I \subset k[\boldsymbol{x}]$ be a proper ideal, let $\mathcal{P}$ be a subset of the minimal primes of I and let $\tilde{P} := \bigcap_{P \in \mathcal{P}} P$ be the intersection of these minimal primes.*

Algorithm 4.2.1 RADICAL1, radical of an ideal

Input: $I \subset k[\boldsymbol{x}]$.
Output: $\sqrt{I}$, the radical of I.

1: $\tilde{P} \leftarrow \langle 1 \rangle$.
2: **loop**
3: Look for $g \in \tilde{P} \setminus \sqrt{I}$. To find it, search over the generators of $\tilde{P}$ and check if they are in $\sqrt{I}$. (Lemma 4.2.2.)
4: If there does not exist such g, it means that $\tilde{P} \subset \sqrt{I}$. Since we always have $\sqrt{I} \subset \tilde{P}$, we conclude that $\tilde{P} = \sqrt{I}$. Exit the cycle.
5: If there exists $g \in \tilde{P} \setminus \sqrt{I}$, this means that there exists at least one minimal prime P associated to I such that $g \notin P$.
$J \leftarrow I : g^\infty$.
6: Reduction to the zero–dimensional case:
Take a maximal independent set $\boldsymbol{u}$ with respect to J and compute the radical of the zero–dimensional ideal $Jk(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ (Proposition 4.2.7).
7: Contract $\sqrt{Jk(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]}$ to $k[\boldsymbol{x}]$.
8: $\tilde{P} \leftarrow \tilde{P} \cap (\sqrt{Jk(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}])$.
9: **end loop**
10: **return** $\tilde{P}$.

We assume that there exists $g \in \tilde{P} \setminus \sqrt{I}$. If $I : g^\infty = \cap_{i=1}^s Q_i$ is an irredundant primary decomposition and $\boldsymbol{u}$ is a maximal independent set with respect to $I : g^\infty$ then, for all $1 \leq i \leq s$ such that $Q_i \cap k[\boldsymbol{u}] = \{0\}$, $\sqrt{Q_i}$ is a minimal prime of I, and moreover $\sqrt{Q_i} \notin \mathcal{P}$.

Proof. Let Q_i be a primary component of $I : g^\infty$ such that $Q_i \cap k[\boldsymbol{u}] = \{0\}$. By Lemma 4.2.8, Q_i is a primary component of I and $P_i = \sqrt{Q_i} \notin \mathcal{P}$.

Since $\boldsymbol{u}$ is a maximal independent set with respect to $I : g^\infty$ and $Q_i \cap k[\boldsymbol{u}] = \{0\}$, $Q_i k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ is a primary component of the zero–dimensional ideal $(I : g^\infty)k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ and therefore $P_i k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ is a minimal prime. Hence P_i is a minimal prime of $I : g^\infty$. (Clearly, P_i cannot contain any prime ideal P such that $P \cap k[\boldsymbol{u}] \neq \{0\}$.)

To prove that P_i is a minimal prime of I, suppose that there exists a component Q of I with $\sqrt{Q} \subsetneq P_i$. We would have $g \notin \sqrt{Q}$ and therefore Q would appear in the primary decomposition of $I : g^\infty$, contradicting the fact that P_i is a minimal prime of $I : g^\infty$. □

Remark 4.2.17. The algorithm terminates because, in each iteration, we add to $\tilde{P}$ at least one new minimal prime ideal associated to I.

Remark 4.2.18. In this algorithm there is no redundancy. All the ideals that we intersect in $\tilde{P}$ are intersection of minimal prime ideals associated to I.

Example 4.2.19. As an example, we apply the algorithm to the ideal

$$I = \langle y + z, x\, z^2 w, x^2 z^2 \rangle \subset \mathbb{Q}[x, y, z, w].$$

In the first iteration, we take $g := 1$ and $J := I : 1^\infty = I$. We find that $\boldsymbol{u} = \{x, w\}$ is a maximal independent set with respect to J. Making the reduction step, we obtain that $\sqrt{J(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}] = \langle y, z\rangle$. We take $\tilde{P} := \langle y, z\rangle$.

In the second iteration, we look for $g \in \tilde{P}$ such that $g \notin \sqrt{I}$. We obtain that $z \notin \sqrt{I}$ and compute $J = I : z^\infty = \langle y + z, xw, x^2\rangle$. Now $\boldsymbol{u} = \{z, w\}$ is a maximal independent set with respect to J. We compute $\sqrt{Jk(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}] = \langle y+z, x\rangle$. We take $\tilde{P} := \langle y, z\rangle \cap \langle y + z, x\rangle = \langle y + z, xz\rangle$.

If we search for $g \in \tilde{P}$ such that $g \notin \sqrt{I}$, we obtain that $y + z$ and xz are both in $\sqrt{I}$. Therefore, the algorithm terminates. We obtain that $\sqrt{I} = \langle y + z, xz\rangle$.

We now apply Krick-Logar algorithm to the same ideal, to compare it with ours. We start with $I = \langle y+z, x\, z^2 w, x^2 z^2\rangle$ and we take the independent set $\boldsymbol{u} = \{x, w\}$. Making the reduction step, we obtain that $\sqrt{I(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}] = \langle y, z\rangle$. Up to now, there is no difference with the algorithm we propose.

The next step is different. We look for h such that $\sqrt{I} = (\sqrt{I(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}]) \cap \langle I, h\rangle$. We can take $h = xz$. Now, $\sqrt{I} = \langle y, z\rangle \cap \sqrt{\langle I, xz\rangle}$. So it remains to be computed the radical of $\langle I, xz\rangle$. Carrying on with the algorithm, we get $\sqrt{\langle I, xz\rangle} = \sqrt{\langle y + z, x\rangle} \cap \sqrt{\langle w, y + z, z^2\rangle} = \langle y + z, x\rangle \cap \langle w, y, z\rangle$.

The last component is redundant, it contains the component $\langle y, z\rangle$ that was already obtained. This redundant component is not an embedded component of I, it is a new component that appeared when we added xz to I.

This is a situation that repeats often in the examples. The polynomials that the algorithm adds to I make it more and more complex. The polynomials added are usually large, since they are the product of coefficients of polynomials in a Gröbner basis and the size of the Gröbner basis of the new ideal can increase drastically.

This does not happen in our proposed algorithm. We compute instead the saturation with respect to polynomials that are usually simple, and this saturation does not increase the complexity of the ideal since it only takes some components away from it. No new components can appear.

4.2.3 Complexity analysis

We shall now compute the theoretical complexity of the algorithm. We remark that we will be analyzing the worst-case-complexity. In the applications, the bounds that we will get are usually not achieved and this is what gives the algorithm practical interest. The modifications to the algorithm that we will introduce in this section (such as random coordinate changes) are only for the purpose of improving the worst-case complexity but are not good in practice.

As presented in the last section, in each step of the algorithm we intersect $\tilde{P}$ with at least one new prime component of $\sqrt{I}$. Therefore, the number of iterations is bounded by the number of prime components of $\sqrt{I}$, which is in time bounded by the Bézout number d^n (see, for example, Heintz, 1983). Since the degrees of

the polynomials in a Gröbner basis can be doubly exponential in the number of variables, if we carry out the complexity estimate with the previous algorithm, we would obtain an estimate triply exponential in the number of variables.

To get a better theoretical complexity, we introduce some modifications in the algorithm that will allow us to reduce the *dimension* of the ideal in each iteration and therefore perform at most n iterations. This will lead to a doubly exponential complexity bound. We insist that although this modifications improve the theoretical complexity, in practice they are not efficient, since they destroy the good properties, such as sparsity, that the ideal might have.

Definition 4.2.20. We say that an ideal $I \subset k[\boldsymbol{x}]$ of dimension e is in *Noether position* if the set $\boldsymbol{u} = \{x_1, \ldots, x_e\}$ is a maximal independent set with respect to I and for each i, $e+1 \leq i \leq n$, there exists a non–zero polynomial $p \in I \cap k[x_1, \ldots, x_e, x_i]$, monic as a polynomial in $k[x_1, \ldots, x_e][x_i]$.

If the ideal I is not in Noether position, we can put it in Noether position by a linear coordinate change. We can use a random coordinate change (Krick et al., 2001, Proposition 4.5), or we can do it deterministically with complexity $s^5 d^{O(n^2)}$, where s is the number of polynomials of I and d the maximum degree of the polynomials (Dickenstein et al., 1991).

When the ideal I is in Noether position, we have the following lemma.

Lemma 4.2.21. *(Krick and Logar, 1991b, Lemma 2.3) Let I be an ideal of dimension e in Noether position, and*

$$I = (Q_{e_1 1} \cap \ldots Q_{e_1 a_1}) \cap \cdots \cap (Q_{e_t 1} \cap \cdots \cap Q_{e_t a_t})$$

the primary decomposition of I, where $Q_{e_i j}$ are primary ideals of dimension e_i and $0 \leq e_1 < \ldots < e_t = e$. Let $P_{e_i j}$ be the associated primes. Then

$$k[x_1, \ldots, x_e] \cap P_{e_t j} = (0), \quad 1 \leq j \leq a_t.$$

If we take $\boldsymbol{u} := \{x_1, \ldots, x_e\}$, we obtain that $Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}] = Q_{e_t 1} \cap \cdots \cap Q_{e_t a_t}$. Therefore, in Step 5, when we take $J = I : g^\infty$ with $g \in (P_{e_t 1} \cap \cdots \cap P_{e_t a_t}) \setminus \sqrt{I}$, all the primary components of I of dimension e are killed.

To get a good complexity bound we want to kill only the prime components of $\sqrt{I}$ of maximal dimension. We can use a random combination of the polynomials in $\tilde{P}$ as g or we can do it deterministically in the following way.

Proposition 4.2.22. *Let I be an ideal of dimension e, as in Lemma 4.2.21. Let $J = Q_{e_t 1} \cap \cdots \cap Q_{e_t a_t}$. Then $I : J^\infty$ has dimension at most $e-1$ and $\sqrt{I} = \sqrt{J} \cap \sqrt{I : J^\infty}$.*

Therefore we can bound the number of iterations of the algorithm by e.

Remark 4.2.23. The ideal $I : J^\infty$ is not exactly $(Q_{e_1 1} \cap \cdots \cap Q_{e_1 a_1}) \cap \cdots \cap (Q_{e_{t-1} 1} \cap \cdots \cap Q_{e_{t-1} a_{t-1}})$, since some primary components corresponding to embedded primes can also be killed.

The ideal $I : J^\infty$ can be computed in the following way (see Vasconcelos, 1998, Proposition 1.2.6):

Proposition 4.2.24. *Let I, J be ideals in $k[\boldsymbol{x}]$, with J generated by $f_1, \ldots, f_r$. Let*

$$f := f_1 + tf_2 + \cdots + t^{r-1} f_r \in k[t, \boldsymbol{x}].$$

Then $I : J^\infty = (I : f^\infty) \cap k[\boldsymbol{x}]$.

Proof. Let $I = Q_1 \cap \cdots \cap Q_s$ be a primary decomposition of I and $P_i = \sqrt{Q_i}$. By Proposition 4.2.8, $I : J^\infty = \bigcap_{J \not\subset P_i} Q_i$ and $(I : f^\infty) \cap k[\boldsymbol{x}] = (\bigcap_{f \notin P_i k[t,\boldsymbol{x}]} Q_i k[t, \boldsymbol{x}]) \cap k[\boldsymbol{x}]$. Therefore we need to prove that $J \subset P_i \iff f \in P_i k[t, \boldsymbol{x}]$. If $J \subset P_i$, clearly, $f \in P_i k[t, \boldsymbol{x}]$. For the converse, let $f = a_1 p_1 + \cdots + a_s p_s$, with $p_j \in P_i$ and $a_j \in k[t, \boldsymbol{x}]$. If we replace t by r different values, we obtain that $f_1 + t_j f_2 + \cdots + {t_j}^{r-1} f_r \in P_i$ for $t_1, \ldots, t_r \in k$. We deduce that $f_i \in P_i$ for $1 \leq i \leq r$, and therefore $J \subset P_i$ as wanted. □

We get Algorithm 4.2.2.

Algorithm 4.2.2 RADICAL2, radical of an ideal

Input: $I \subset k[\boldsymbol{x}]$.
Output: $\sqrt{I} = P$, the radical of I.

1: Make a linear coordinate change of variables so that I is in Noether position
2: Let $\boldsymbol{u} := \{x_1, \ldots, x_e\}$, with $e = \dim I$. Compute the radical of the zero–dimensional ideal $Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ using Proposition 4.2.7.
3: Contract $\sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]}$ to $k[\boldsymbol{x}]$. $J \leftarrow \sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}]$.
4: **return** $J \cap$ RADICAL2$(I : J^\infty)$.

To estimate the complexity we work over $k = \mathbb{Q}$. We analyze the arithmetic complexity, that is, the number of operations performed in $\mathbb{Q}$. We use the notation $\mathrm{CG}(d, n, s)$, $\mathrm{DG}(d, n)$ and $\mathrm{NG}(d, n, s)$ for the complexity, maximum degree and number of polynomials in a Gröbner basis of an ideal in n variables over $\mathbb{Q}$, generated by s polynomials of maximum degree d. In (Giusti, 1984; Krick and Logar, 1991a; Dubé, 1990) they prove bounds for the complexity and the number of polynomials in the general case doubly exponential in the number of variables. The bounds are of order $s^{O(1)} d^{2^{O(n)}}$.

For the maximum degree, the following bound is given in (Dubé, 1990):

$$\deg(g) \leq 2 \left(\frac{d^2}{2} + d \right)^{2^{n-1}}.$$

We approximate it by d^{2^n}.

We estimate the complexity of each step of the algorithm, without considering the intersection of the ideals in the last step. We assume that $I \subset \mathbb{Q}[\boldsymbol{x}]$ is an ideal generated by s polynomials of maximum degree d.

(1) The Noether position can be achieved by a linear coordinate change. This does not affect the theoretical complexity.

(2) To compute the radical $\sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]}$, following Proposition 4.2.7, we need to compute at most n Gröbner bases of I. This has complexity at most $ns^{O(1)}d^{2^{O(n)}}$. The n polynomials that appear have degree at most d^{2^n}.

(3) The degree of the polynomial h used for the contraction can be bounded by the number of polynomials in the basis times the maximum degree of the polynomials:

$$s^{O(1)}d^{2^{O(n)}}d^{2^n} = s^{O(1)}d^{2^{O(n)}},$$

since the degree of the lcm is bounded by the degree of the product of all the polynomials.

Now, the complexity of the contraction is the complexity of the computation of the Gröbner basis of $\langle I, th-1\rangle$:

$$\mathrm{CG}(s^{O(1)}d^{2^{O(n)}}, n+1, s^{O(1)}d^{2^{O(n)}}) =$$
$$(s^{O(1)}d^{2^{O(n)}})^{O(1)}(s^{O(1)}d^{2^{O(n)}})^{2^{O(n)}} = (sd)^{2^{O(n)}}.$$

The number of polynomials in J and their degrees can also be approximated by $(sd)^{2^{O(n)}}$.

(4) To compute $I : J^\infty$, by Proposition 4.2.24 and Remark 4.2.14, we need to compute a Gröbner basis of $\langle I, tf-1\rangle$. The degree of f is bounded by $(sd)^{2^{O(n)}} + d^{2^{O(n)}} = (sd)^{2^{O(n)}}$. This has complexity

$$CG((sd)^{2^{O(n)}}, n+1, (sd)^{2^{O(n)}}) = (sd)^{2^{O(n)}}.$$

The number of polynomials and the maximum degree can also be approximated by $(sd)^{2^{O(n)}}$.

We can estimate the complexity of the whole call by $(sd)^{2^{O(n)}} = (sd)^{2^{cn}}$ for some universal constant c.

In each call, the dimension of the ideal considered decreases. Therefore we need at most n calls, since the dimension cannot be greater than the number of variables.

In the second call we start with $(sd)^{2^{cn}}$ polynomials of degree $(sd)^{2^{cn}}$. The complexity of this call is

$$((sd)^{2^{cn}}, n, (sd)^{2^{cn}}) = ((sd)^{2\,2^{cn}})^{2^{cn}} = (sd)^{2^{2cn+1}}.$$

The same bounds are valid for the number of polynomials and their degrees.

Therefore, after n calls we get the bound

$$(sd)^{2^{n(cn)+n-1}} = (sd)^{2^{O(n^2)}},$$

for the complexity, the number of polynomials and their degrees in the last call.

Finally, to compute the intersection of the outputs in each call, we use that $I_1 \cap I_2 = \langle I_1 \cdot t, I_2 \cdot (1-t)\rangle \cap k[\boldsymbol{x}]$, which can be done by a Gröbner basis computation. This does not modify the obtained estimates.

We have shown that the theoretical complexity of the algorithm is doubly exponential in the number of variables.

4.2.4 Performance evaluation

In this section, we apply the proposed algorithm to several examples given in (Decker et al., 1999b; Caboara et al., 1997) and evaluate its performance. (We only consider those ideals that are not zero–dimensional.) We implemented the algorithm in SINGULAR (Decker et al., 2011). Our routine uses the subroutine for the reduction to the zero–dimensional case that was already implemented in the library `primdec` (Decker et al., 2006) for the computation of the radical by Krick-Logar-Kemper algorithm (Krick and Logar, 1991b; Kemper, 2002). We compare the times obtained by our algorithm with the algorithms implemented in `primdec`: Krick-Logar-Kemper (KLK) and Eisenbud-Huneke-Vasconcelos (EHV) (Eisenbud et al., 1992).

The results are shown in Table 4.1. All the computations are done over $\mathbb{Q}$. The ordering of the monomials is always the degree reverse lexicographical ordering with the underlying ordering of the alphabet.

The codes for the examples in the first column are the ones given in (Decker et al., 1999b) and (Caboara et al., 1997). The second column indicates the dimension of the ideal, the third column the total number of primary components and the fourth column the number of primary components corresponding to embedded primes. Timing is measured in hundredth of seconds. The entry * means that after one day of computations, the algorithm did not terminate.

In the implementation of KLK in Singular, the original ideal is first decomposed using factorizing Gröbner bases algorithm and then the radical of each component is computed. We do the same decomposition in our algorithm.

We see that for time consuming computations, our proposed algorithm is always faster. We explain briefly the differences that appear.

In example DGP-29, both KLK and our algorithm obtain the radical in the first step. Because of the structure of them, our algorithm stops after that step, but KLK algorithm goes on computing redundant components. In examples DGP-16, CCT-83 and CCT-C, after the first step, the saturations computed by our algorithm are simple and the algorithm terminates quickly, while in KLK algorithm, the polynomials added are large, and the resulting Gröbner bases are huge and impossible to handle.

4.3 Minimal Associated Primes

In this section we show how the ideas presented in last section can be applied to the computation of the minimal associated primes of an ideal. We show some time comparisons using an implementation in SINGULAR (Decker et al., 2011).

Table 4.1: Timing results

Code	Dim	Prim. comps.	Emb. comps.	EHV	KLK	new algorithm
DGP-1	3	4	0	*	104	90
DGP-2	3	16	1	*	86	158
DGP-3	2	11	7	240	8	13
DGP-4	6	4	1	53	23	21
DGP-5	3	9	2	*	4271	627
DGP-6	3	3	0	*	158	185
DGP-7	3	6	0	*	45	153
DGP-9	1	12	0	11	*	229
DGP-12	1	25	0	329	5597	247
DGP-14	1	8	6	5	7	10
DGP-16	8	4	0	*	3214	3402
DGP-20	4	2	1	589	74	38
DGP-21	9	9	8	4	39	13
DGP-22	2	9	2	*	63	84
DGP-23	2	18	6	*	111	157
DGP-24	8	6	1	*	14	29
DGP-25	5	7	2	*	225	273
DGP-27	4	3	0	199	5	9
DGP-28	7	2	0	2380	46	56
DGP-29	2	12	11	*	61714	3598
DGP-30	1	14	0	*	132	163
DGP-31	1	1	0	1	6	8
DGP-32	2	17	9	25814	66	265
DGP-33	2	3	0	2	11	16
CCT-M	5	3	0	*	119	129
CCT-83	5	3	0	*	*	250
CCT-C	5	4	0	*	*	326
CCT-O	2	5	0	1	217	29

4.3.1 Algorithms

As in the case of the computation of the radical of an ideal, the computation of the minimal associated primes of a general ideal can be reduced to the zero dimensional case. For the computation of the minimal associated primes of a zero–dimensional ideals, the following algorithm, also based in an algorithm proposed in (Gianni et al., 1988), can be used.

Given a zero–dimensional ideal $I \subset k[\boldsymbol{x}]$, we say that a polynomial $f \in k[\boldsymbol{x}]$ separates points of $\mathbf{V}_{\bar{k}}(I)$ if $f(p)$ is different for every $p \in \mathbf{V}_{\bar{k}}(I)$.

Proposition 4.3.1. *Let $\langle g \rangle = I \cap k[x_n]$ and $g = g_1^{m_1} \dots g_t^{m_t}$, the factorization. Then*

$$I = \cap_{i=1}^{t} \langle I, g_i^{m_i} \rangle.$$

If x_n separates points of $\mathbf{V}_{\bar{k}}(I)$, then

- $\langle I, g_i^{m_i}\rangle$ *is primary*
- $\sqrt{\langle I, g_i^{m_i}\rangle} = \langle I, g_i\rangle$*, and these are the minimal associated primes of* I*.*

For radical zero–dimensional ideals, a classical result called the *Shape lemma* gives a criterion to check if x_n separates points.

Proposition 4.3.2 (Shape lemma)**.** *Let $I \subseteq k[\boldsymbol{x}]$ be a zero–dimensional ideal. Let G be a reduced Gröbner basis of $\sqrt{I}$ under a lexicographical ordering $\boldsymbol{x} \setminus x_n \gg x_n$. Then x_n separates points of $\mathbf{V}_{\bar{k}}(I)$ if and only if G has the following shape:*

$$G = \{x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\}$$

with g_n containing no multiple roots in $\overline{k}$.

Proof. ($\Rightarrow$) We assume first $k = \overline{k}$. Let $g_n \in k[x_n]$ be the monic generator of $\sqrt{I} \cap k[x_n]$. Let $V = \mathbf{V}_{\bar{k}}(I) = \mathbf{V}_{\bar{k}}(\sqrt{I})$ and let $\boldsymbol{p} = (p_1, \ldots, p_n) \in V$. Then $V \subset \mathbf{V}(g_n)$ implies $g(p_n) = 0$. Since the last coordinates p_n of each $\boldsymbol{p} \in V$ are all different, $\prod_{\boldsymbol{p}\in V}(x_n - p_n) \mid g_n$. On the other hand, $\prod_{\boldsymbol{p}\in V}(x_n - p_n) \in \mathbf{I}(V) \cap k[x_n] = \sqrt{I} \cap k[x_n] = \langle g_n\rangle$, which implies that $g_n \mid \prod_{\boldsymbol{p}\in V}(x_n - p_n)$. Therefore the two polynomials are equal (and, since $\sqrt{I}$ is radical, g_n has no multiple roots).

Now, let $g_i(x_n)$ be the unique polynomial of degree smaller than $\#V$ satisfying $g_i(p_n) = p_i$ for all $\boldsymbol{p} = (p_1, \ldots, p_n) \in V$. Then $x_i - g_i(x_n) \in \mathbf{I}(V) = \sqrt{I}$. We conclude that

$$\langle x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\rangle \subseteq \sqrt{I}.$$

Since the corresponding varieties have the same number of points, equality holds. Moreover, it is clear that the generators form a reduced Gröbner basis of $\sqrt{I}$ with respect to $>$.

If k is not algebraically closed, the conclusion still holds, since all the computations used for computing the Gröbner basis are done over the base field k.

($\Leftarrow$) Conversely, if $G = \{x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\}$, let $V = V_{\bar{k}}(\sqrt{I})$. Hence

$$V = \{\boldsymbol{p} = (p_1, \ldots, p_n) \in \overline{k}^n \mid g_n(p_n) = 0, p_i = g_i(p_n), 1 \leq i \leq n-1\},$$

and clearly x_n separates points of V since g_n has no multiple roots. □

When the ideal is not radical, in (Greuel and Pfister, 2008) [Criterion 4.2.4], an algorithm is given for checking if x_n separates points, by looking at the shape that the ideals $\langle I, g_i^{m_i}\rangle$ must have in that case.

We give a slightly modified version of the criterion.

Proposition 4.3.3. *Let $I \subset k[\boldsymbol{x}]$ be a proper ideal. The following conditions are equivalent.*

(1) I is zero–dimensional, primary and x_n separates points of $\mathbf{V}(I)$.

(2) Let G be a reduced Gröbner basis of I with respect to the lexicographical ordering $x_1 > \ldots > x_n$. There exist

$$g_1(x_1,\ldots,x_n), g_2(x_2,\ldots,x_n),\ldots,g_n(x_n) \in G,$$

$$\tilde{g}_1(x_n), \tilde{g}_2(x_n),\ldots,\tilde{g}_n(x_n) \in k[x_n],$$

with $\tilde{g}_n$ irreducible, and $m_1,\ldots,m_n \in \mathbb{N}$ such that

(a) $g_n(x_n) = \tilde{g}_n(x_n)^{m_n}$,

(b) For $1 \leq j \leq n-1$,

$$g_j(x_j,\ldots,x_n) \equiv (x_j - \tilde{g}_j)^{m_j} \pmod{M_{j+1}k[x_j,\ldots,x_n]},$$

where $M_{j+1} = \langle x_{j+1} - \tilde{g}_{j+1},\ldots,x_{n-1} - \tilde{g}_{n-1}, \tilde{g}_n\rangle$.

Proof. (1) $\Rightarrow$ (2) The conditions in (2) imply inductively that the polynomials $\tilde{g}_n$, $x_{n-1} - \tilde{g}_{n-1},\ldots,x_1 - \tilde{g}_1$ belong to $\sqrt{I}$. Therefore, since I is proper,

$$\sqrt{I} = \langle x_1 - \tilde{g}_1,\ldots,x_{n-1} - \tilde{g}_{n-1}, \tilde{g}_n\rangle$$

is a maximal zero–dimensional ideal, and x_n separates points of $\mathbf{V}(\sqrt{I})$.

Hence, by Proposition 4.1.14, I is primary. Moreover, since $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$, I is zero–dimensional and x_n separates points of $\mathbf{V}(I)$.

(2) $\Rightarrow$ (1) Since I is zero–dimensional, primary, and x_n separates points of $\mathbf{V}(I)$, $\sqrt{I}$ is maximal and, by the Shape Lemma, we can find generators

$$\sqrt{I} = \langle x_1 - \tilde{g}_1(x_n),\ldots,,x_{n-1} - \tilde{g}_{n-1}(x_n), \tilde{g}_n(x_n)\rangle,$$

with g_n irreducible.

For $1 \leq j \leq n$, we define $I_j := I \cap k[x_j,\ldots,x_n]$ and $M_j := \sqrt{I_j} \subseteq k[x_j,\ldots,x_n]$.

We observe that $M_j = \langle x_j - \tilde{g}_j(x_n),\ldots,x_{n-1} - \tilde{g}_{n-1}(x_n), \tilde{g}_n(x_n)\rangle$ since the latter is a maximal ideal contained in M_j. Hence, I_j is zero–dimensional, primary and x_n separates points of $\mathbf{V}(I_j)$.

Now, $I_n = I \cap k[x_n] = \langle g_n(x_n)\rangle$ for some $g_n \in G$, since I_n is principal and $G \cap k[x_n]$ is a Gröbner basis of I_n by the ordering we are using. Moreover, since M_n is maximal, $\sqrt{I_n} = M_n = \langle \tilde{g}_n\rangle$ for some $\tilde{g}_n$ irreducible. Hence, $g_n = \tilde{g}_n^{m_n}$ for some $m_n \in \mathbb{N}$ (since the radical is generated by the square free part), which proves the first claim.

We prove now that for $j < n$ and once M_{j+1} is defined, there exist $g_j(x_j,\ldots,x_n) \in G$, $\tilde{g}_j(x_n) \in k[x_n]$ and $m_j \in \mathbb{N}$ such that

$$g_j(x_j,\ldots,x_n) \equiv (x_j - \tilde{g}_j)^{m_j} \pmod{M_{j+1}k[x_j,\ldots,x_n]}.$$

Since I_j is zero–dimensional in $k[x_j,\ldots,x_n]$ and $G \cap k[x_j,\ldots,x_n]$ is a reduced Gröbner basis of I_j, there exist a unique polynomial $g_j \in G$ with leading term pure in x_j.

We claim that

$$I_j + M_{j+1}k[x_j, \ldots, x_n] = \langle g_j \rangle + M_{j+1}k[x_j, \ldots, x_n]. \tag{4.1}$$

The inclusion $\supseteq$ is trivial. For $\subseteq$ it is enough to prove that any $g \in G \cap k[x_j, \ldots, x_n]$, $g \neq g_j$, belongs to $M_{j+1}k[x_j, \ldots, x_n]$. We prove something the stronger result that if $g = p_s x_j^s + \cdots + p_0$ with $p_i \in k[x_{j+1}, \ldots, x_n]$, then $p_i \in M_{j+1}$, $0 \leq i \leq s$.

We observe that since G is reduced, $s \leq m_j := \deg_{x_j} g_j$. We prove first that $p_s \in M_{j+1}$:

Let J be the set of all the leading coefficients with respect to x_j (lc_{x_j}) of polynomials in I_j with degree x_j smaller than m_j, together with the 0 element. That is,

$$J := \{\, p \in k[x_{j+1}, \ldots, x_n] : \exists\, f \in I_j \text{ with } \deg_{x_j} f < m_j \text{ s.t. } lc_{x_j} f = p \,\} \cup \{0\}.$$

The set J is a proper ideal of $k[x_{j+1}, \ldots, x_n]$, and $I_{j+1} \subseteq J$ since $I_{j+1} \subseteq I_j$. This implies that $M_{j+1} \subseteq \sqrt{J}$, that is $\sqrt{J} = M_{j+1}$, and therefore $J \subseteq M_{j+1}$.

Hence, since for $g = p^s x_j^s + \cdots + p_0 \in G$, $g \neq g_j$, it holds $s < m_j$, therefore $p_s \in J \subseteq M_{j+1}$.

Looking at the polynomial $x_j^{m_j - s} g - p_s g_j$, the leading terms vanish and the result is in I_j, hence its leading coefficient belongs to $J \subseteq M_{j+1}$. But this coefficient is of the form $p_{s-1} - p_s p'$ where p' is a coefficient of g_j, and we deduce that p_{s-1} also belongs to J. We apply the reasoning successively for p_{s-2}, etc. We conclude that for $0 \leq i \leq s$, $p_s \in M_{j+1}$ and therefore $g \in M_{j+1}k[x_j, \ldots, x_n]$ as claimed. This proves the equality (4.1).

Let now k' be the field $k' := k[x_{j+1}, \ldots, x_n]/M_{j+1}$ and the natural projection morphism:

$$\Phi : k[x_j, \ldots, x_n] \longrightarrow k'[x_j].$$

First, $\Phi(I_j) = \Phi(I_j + M_{j+1}k[x_j, \ldots, x_n]) = \Phi(\langle g_j \rangle) = \langle \Phi(g_j) \rangle$ and second, as $\sqrt{\Phi(I_j)} = \Phi(\sqrt{I_j}) = \Phi(M_j)$ since $M_{j+1} \subseteq M_j$, we conclude that $\sqrt{\Phi(I_j)} = \langle \Phi(x_j - \tilde{g}_j(x_n)) \rangle$.

Therefore, there exists $r \in \mathbb{N}$ such that $\Phi(g_j) = \Phi(x_j - \tilde{g}_j(x_n))^r$, that is

$$g_j(x_j, \ldots, x_n) \equiv (x_j - \tilde{g}_j(x_n))^r \pmod{M_{j+1}k[x_j, \ldots, x_n]}.$$

Here, clearly $r = m_j$ since both polynomials are monic in x_j. □

If x_n does not separate points, a random coordinate change must be performed. If k is infinite a suitable coordinate change always exists.

In (Gianni et al., 1988), the authors use the splitting tool $I = (I : h^\infty) \cap \langle I, h \rangle$ (for h such that $I : h = I : h^2$). They find h such that the minimal associated primes of $I : h$ can be obtained by reduction to the zero–dimensional case and the ones corresponding to $\langle I, h \rangle$ can be obtained by induction.

As in the computation of the radical, when taking $\langle I, h\rangle$ there may appear redundant components (that is, components that were not part of the original ideal) that slow down the algorithm performance.

In the algorithm that we proposed for computing the radical of an ideal, we avoided using $\langle I, h\rangle$ and instead we used repeatedly the saturation $I : h^\infty$ for appropriate h, yielding in some cases a more efficient algorithm.

The same ideas can be used for computing the minimal associated primes of an ideal, obtaining Algorithm 4.3.1

Algorithm 4.3.1 minAssPrimes, minimal associated primes of an ideal

Input: $I \subset k[\boldsymbol{x}]$.

Output: $P_1, \ldots, P_t$, the minimal associated primes of I.

1: $\tilde{P} \leftarrow \langle 1\rangle$ ($\tilde{P}$ will be the intersection of the minimal associated primes already obtained).
2: **loop**
3: Look for $g \in \tilde{P} \setminus \sqrt{I}$. To find it, search over the generators of $\tilde{P}$ and check if they are in $\sqrt{I}$.
4: If there does not exist such g, it means that $\tilde{P} \subset \sqrt{I}$. Since we always have $\sqrt{I} \subset \tilde{P}$, we conclude that $\tilde{P} = \sqrt{I}$. Exit the cycle.
5: If there exists $g \in \tilde{P} \setminus \sqrt{I}$, this means that there exists at least one minimal prime P associated to I such that $g \notin P$.
$J \leftarrow I : g^\infty$.
6: Reduction to the zero–dimensional case:
Take a maximal independent set $\boldsymbol{u}$ with respect to J and compute $P'_1, \ldots, P'_s$, the minimal associated primes of the zero–dimensional ideal $Jk(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$.
7: Contract the ideals $P'_i \subset k(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ to $P_i \subset k[\boldsymbol{x}]$, $1 \leq i \leq s$.
8: $\tilde{P} \leftarrow \tilde{P} \cap P_1 \cap \cdots \cap P_s$.
9: $\mathcal{P} \leftarrow \mathcal{P} \cup \{P_1, \ldots, P_s\}$.
10: **end loop**
11: **return** $\mathcal{P}$, the minimal associated primes of I.

The correctness and termination of the algorithm can be proven in exactly the same way as for the radical.

Remark 4.3.4. As before, in this algorithm there is no redundancy. All the ideals that we add to $\mathcal{P}$ are minimal associated primes of I.

Example 4.3.5. We apply the algorithm to the ideal

$$I = \langle y + z, xz^2w, x^2z^2\rangle \subset \mathbb{Q}[x, y, z, w].$$

In the first iteration, we take $g := 1$ and $J := I : 1^\infty = I$. We find that $\boldsymbol{u} = \{x, w\}$ is a maximal independent set with respect to J. Making the reduction step, we obtain that the only minimal associated prime of $J(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}]$ is $\langle y, z\rangle$, which contracted to $k[\boldsymbol{x}]$ is $P_1 = \langle y, z\rangle$. We take $\tilde{P} := P_1$ and $\mathcal{P} := \{P_1\}$.

In the second iteration, we look for $g \in \tilde{P}$ such that $g \notin \sqrt{I}$. We obtain that $z \notin \sqrt{I}$ and compute $J = I : z^\infty = \langle y + z, xw, x^2\rangle$. Now $\boldsymbol{u} = \{z, w\}$ is a

maximal independent set with respect to J. The only minimal associated prime of $Jk(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ is $\langle y+z, x\rangle$, which contracted to $k[\boldsymbol{x}]$ gives $P_1 = \langle y+z, x\rangle$. We take $\tilde{P} := \langle y, z\rangle \cap \langle y+z, x\rangle = \langle y+z, xz\rangle$ and $\mathcal{P} = \{\langle y, z\rangle, \langle y+z, x\rangle\}$.

If we search for $g \in \tilde{P}$ such that $g \notin \sqrt{I}$, we obtain that $y+z$ and xz are both in $\sqrt{I}$. Therefore, the algorithm terminates. We obtain that the minimal associated primes of I are $\langle y, z\rangle$ and $\langle y+z, xz\rangle$.

We now apply GTZ algorithm (Gianni et al., 1988) to the same ideal, to compare it with ours. We start with $I = \langle y+z, x\,z^2w, x^2z^2\rangle$. The first step is the same, we obtain $P_1 = \langle y, z\rangle$ $\tilde{P} := P_1$ and $\mathcal{P} = \{P_1\}$.

The next step is different. We look for h such that $I = (I(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}]) \cap \langle I, h\rangle$. We can take $h = xz$. Now, $\sqrt{I} = \langle y, z\rangle \cap \sqrt{\langle I, xz\rangle}$. So it remains to compute the minimal associated primes of $\langle I, xz\rangle$. Carrying on with the algorithm, we get that they are $\langle y+z, x\rangle$ and $\langle w, y, z\rangle$.

The last prime is not a minimal associated prime of I (not even an associated prime of I). It is a new component that appeared when we added xz to I.

This is a situation that repeats often in the examples. The polynomials that the algorithm adds to I make it more and more complex. The polynomials added are usually large, since they are the product of coefficients of polynomials in a Gröbner basis and the size of the Gröbner basis of the new ideal can increase drastically.

This does not happen in our proposed algorithm. We compute instead the saturation with respect to polynomials that are usually simple, and this saturation does not increase the complexity of the ideal since it only takes some components away from it. No new components can appear.

4.3.2 Performance evaluation

In this section, we evaluate the performance of our proposed algorithm using several examples given in (Decker et al., 1999b; Caboara et al., 1997) and other new examples. (We only consider ideals that are not zero–dimensional.) We implemented the algorithm in SINGULAR (Decker et al., 2011). We compare it with other algorithms implemented in the SINGULAR library `primdec`: Gianni-Trager-Zacharias (GTZ) (Gianni et al., 1988) and via Characteristic Sets (Char).

We created some new examples where the differences are more significant, which we detail below.

$p_1 = a+c+d+e+f+g+h+j-1, p_2 = -b+c+e+g+j, q_1 = 59ad+59ah+59dh-705d-1199h, q_2 = -54acf-54adf+a+d, q_3 = adfg+a+d$
$I_1 = \langle p_1, p_2\rangle \cap \langle q_1, q_2, q_3\rangle$ (polynomials taken from DGP25 and DGP28)

$p_1 = x^2+y^2+z^2-t^2, p_2 = xy+z^2-1, q_1 = w^2xy+w^2xz+w^2z^2, q_2 = tx^2y+x^2yz+x^2z^2, q_3 = twy^2+ty^2z+y^2z^2, q_4 = t^2wx+t^2wz+t^2z^2$
$I_2 = \langle p_1, p_2\rangle \cap \langle q_2, q_3, q_4\rangle, I_3 = \langle p_1, p_2\rangle \cap \langle q_1, q_3, q_4\rangle$ (polynomials taken from DGP31 and DGP32)

The results are shown in Table 4.2. All the computations are done over $\mathbb{Q}$. The ordering of the monomials is always the degree reverse lexicographical ordering with the underlying ordering of the alphabet.

Table 4.2: Timing results

Source	Code	Dim	Prim. comps.	Min. ass.	Emb. comps.	Equidim?	new	GTZ	Char
DGP	1	3	4	4	0	Yes	39	37	1037
DGP	2	3	16	15	1	No	57	40	86
DGP	3	2	11	4	7	No	6	4	2
DGP	4	6	4	3	1	No	18	17	14
DGP	7	3	6	6	0	Yes	26	20	76
DGP	14	1	8	2	6	No	9	7	5
DGP	20	4	2	1	1	No	15	14	3185
DGP	21	9	9	1	8	No	3	2	1
DGP	22	2	9	7	2	No	33	25	370
DGP	23	2	18	12	6	No	91	71	22750
DGP	24	8	6	5	1	No	14	9	12
DGP	25	5	7	5	2	No	101	81	1615
DGP	27	4	3	3	0	Yes	13	9	11
DGP	28	7	2	2	0	Yes	30	27	18
DGP	29	2	12	1	11	No	4	2	9
DGP	30	1	14	14	0	Yes	283	259	12145
DGP	31	1	1	1	0	Yes	10	10	3
DGP	32	2	17	8	9	No	21	15	34
DGP	33	2	3	3	0	No	10	8	5
CCT	M	5	3	3	0	No	58	48	2268
CCT	83	5	3	3	0	No	133	603	98
CCT	O	2	5	5	0	Yes	26	209	3
New	1	9	4	4	0	No	281	*	2383
New	2	3	11	8	3	No	120	*	32065
New	3	3	11	8	3	No	69	*	27088

The codes for the examples in the firsts columns are the ones given in (Decker et al., 1999b) and (Caboara et al., 1997). "Dim" indicates the dimension of the ideal; "Prim. comps.", the total number of primary components; "Min. ass.", the number of minimal associated primes; "Emb. comps.", the number of embedded components and "Equidim?" if the ideal is equidimensional (i.e., all the components have the same dimension). The last three columns show the timings. Column "new" stands for the new algorithm and the other two columns for the existing algorithms, as explained before. Timing is measured in hundredths of seconds. The entry * means that after one day of computations, the algorithm did not terminate.

In the implementation of GTZ in SINGULAR, the original ideal is first decomposed using factorizing Gröbner bases algorithm and then the minimal associated primes of each component are computed. We do the same decomposition in our algorithm.

We see that for time consuming computations, our proposed algorithm is always faster than GTZ algorithm.

Chapter 5

Normalization of rings

The content of Sections 5.1 to 5.5 is a joint work with Gert-Martin Greuel and Frank Seelisch. It is published in (Greuel et al., 2010). The local approach proposed in Section 5.6 is a joint work with Janko Böhm, Wolfram Decker, Gerhard Pfister, Andreas Steenpaßand Stefan Steidel, and is presented in a more general version in Böhm et al. (2011a).

5.1 Basic definitions and tools

In this section we assume that A is a commutative Noetherian ring. We recall the definitions from Section 2.2 and state some basic properties.

Definition 5.1.1. Let $A \subseteq B$ be a ring extension. We say that $b \in B$ is *integral* over A if there exist $a_i \in A$, $1 \leq i \leq s$, such that

$$b^s + a_1 b^{s-1} + \cdots + a_{s-1} b + a_s = 0.$$

The *integral closure* of A in B is the set of all elements of B that are integral over A.

Proposition 5.1.2. *If B is a finitely generated A-algebra of the form $B = A[b_1, \ldots, b_t]$, with b_i integral over A, then B is module–finite over A (i.e., B is a finitely generated A–module).*

Proof. We proceed by induction in the number of elements considering

$$A[b_1, \ldots, b_t] = A[b_1, \ldots, b_{t-1}][b_t]$$

and using the transitivity of the finiteness condition.

Suppose now that B is generated by only one element, $B = A[b_1]$, and that this element satisfies an integral equation of degree s. Then for any $s' \geq s$, $b_1^{s'}$ is a linear combination of $b_1^0, \ldots, b_1^{s-1}$. Hence B is generated as an A-module by these s elements, and is therefore finitely generated. □

Definition 5.1.3. The ring $S^{-1}A$, with S the set of non–zerodivisors of A, is called the *total ring of fractions* of A and denoted $Q(A)$. The *normalization* $\bar{A}$ of A is the integral closure of A in $Q(A)$. A ring A is called *normal* if $A = \bar{A}$.

Observation 5.1.4. Every element of A is integral over A, and therefore $A \subseteq \overline{A}$.

The normalization $\overline{A}$ is a subalgebra of $Q(A)$, but it is not in general module–finite over A. The following theorem by Emmy Noether proves finiteness in an important case. (For the proof, see for example, Greuel and Pfister 2008, Theorem 3.5.10.)

Theorem 5.1.5. *Let $P \subset k[x_1, \ldots, x_n]$ be a prime ideal and $A = k[x_1, \ldots, x_n]/P$. Then $\overline{A}$ is a finite A-module.*

The finiteness of $\overline{A}$ is equivalent to the existence of a common denominator for all its elements, as we will show in the next lemma. We need first a definition.

Definition 5.1.6. The *conductor* of A in $\bar{A}$ is $\mathcal{C} = \{a \in Q(A) \mid a\bar{A} \subseteq A\} = \mathrm{Ann}_{Q(A)}(\bar{A}/A)$.

Since $1 \in \overline{A}$, it turns out that $\mathcal{C} \subseteq A$. If $c \in \mathcal{C}$, then any element $b \in \overline{A}$ can be written as $b = f/c$, for some $f \in A$. That is, $\mathcal{C}$ is the set of common denominators of the normalization.

Lemma 5.1.7. *$\bar{A}$ is module–finite over A if and only if $\mathcal{C}$ contains a non–zerodivisor of A.*

Proof. If $p \in \mathcal{C}$ is a non–zerodivisor then $\bar{A} \cong p\bar{A} \subseteq A$ is module-finite over A, since A is Noetherian. Conversely, if $\bar{A}$ is module-finite over A then any common multiple of the denominators of a finite set of generators is a non–zerodivisor of A contained in $\mathcal{C}$. □

As a first ingredient for the normalization algorithms, we need to be able to check whether a given ring is normal or not. We observe that normality is a local property, in the following sense.

Lemma 5.1.8. *Let A be an integral domain. The following conditions are equivalent*

(1) A is normal;

(2) A_P is normal for every prime ideal P;

(3) $A_{\mathfrak{m}}$ is normal for every maximal ideal $\mathfrak{m}$.

Proof. See, for example, (Greuel and Pfister, 2008, Proposition 3.2.5). □

This motivates the next definition. We call spectrum of A, $\mathrm{Spec}(A)$, the set of prime ideals of the ring A and the variety of I, $V(I) = \{P \in \mathrm{Spec}\, A \mid P \supseteq I\}$, the set of prime ideals containing I. This definition is common in Algebraic Geometry, and is more general than our previous definition. Note that when k is algebraically closed, maximal ideals containing I correspond to points in the variety, so we are now looking at all the prime ideals instead of only the maximal ones.

Definition 5.1.9. The *non-normal locus* of A is defined as

$$N(A) = \{P \in \mathrm{Spec}\, A \mid A_P \text{ is not normal}\}.$$

By the previous lemma, a ring is normal if and only if the non-normal locus is empty.

There is a close relation between the non–normal locus and the conductor ideal.

Lemma 5.1.10. *If $\overline{A}$ is module-finite over A then $N(A) = V(\mathcal{C})$.*

Proof. If $P \in N(A)$, then $A_P \subsetneq \overline{A_P}$ and $\mathcal{C}_P = \mathrm{Ann}_{A_P}(\overline{A_P}/A_P) \subsetneq A_P$. This implies that $1 \notin \mathcal{C}_P$ and therefore $P \supseteq \mathcal{C}$. For the converse inclusion, if $\overline{A}$ is generated by $H = \{h_1, \ldots, h_s\}$ and we set $\mathcal{C}_h := \{a \in A \mid ah \in A\}$ for $h \in A$ then $\mathcal{C} = \cap_{h \in H} C_h$. We show that $V(\mathcal{C}_h) \subseteq N(A)$, for any $h \in \overline{A}$. Let $P \notin N(A)$. Since $\overline{A} \subset \overline{A_P} = A_P$, there exist $f \in A$ and $g \in A \setminus P$ such that $h \equiv f/g$ in A_P and therefore also in $Q(A)$. This implies $gh \in A$, that is, $g \in \mathcal{C}_h$. Therefore $\mathcal{C}_h \nsubseteq P$ and $P \notin V(\mathcal{C}_H)$. □

Another notion closely related to normality is that of regularity.

Definition 5.1.11. Let $A = k[x_1, \ldots, x_n]/I$, with $I = \langle f_1, \ldots, f_s\rangle$ equidimensional radical of dimension d. We say that a point $p \in V(I)$ is *regular* (or *smooth* or *non-singular*) if $\mathrm{rank}\left(\frac{\partial f_i}{\partial x_j}\right)_{\substack{1\le i\le s\\ 1\le j\le n}} = n - d$, that is, if the tangent space has the expected dimension. More generally, a Noetherian local ring A is regular if the minimal number of generators of its maximal ideal is equal to its dimension, and an arbitrary Noetherian ring A is regular if A_P is regular for every prime ideal P. We define the *singular locus* of A as the set $\mathrm{Sing}(A) := \{P \in \mathrm{Spec}(A) \mid A_P \text{ is not regular }\}$.

The relation between normality and regularity is given by the following theorem.

Theorem 5.1.12. *Let A be a regular local ring, then A is normal.*

Proof. See, for example, (Greuel and Pfister, 2008, Theorem 5.7.14). □

We say that a ring A is *reduced* if it contains no nilpotent elements. When $A = k[\boldsymbol{x}]/I$, A is reduced if and only if I is a radical ideal.

We can now give a normality criterion proved by Grauert and Remmert (1971).

Proposition 5.1.13. *Let A be a Noetherian reduced ring and $J \subseteq A$ an ideal satisfying the following conditions:*

(1) J contains a non–zerodivisor of A,

(2) J is a radical ideal,

(3) $N(A) \subseteq V(J)$.

Then A is normal if and only if $A \cong \mathrm{Hom}_A(J, J)$, via the canonical map which maps $a \in A$ to the multiplication by a.

Definition 5.1.14. An ideal $J \subseteq A$ satisfying properties (1)–(3) is called a *test ideal* (for the normalization) of A. A pair (J, p) with J a test ideal and $p \in J$ a non–zerodivisor of A is called a *test pair* for A.

By Lemmas 5.1.7 and 5.1.10, test pairs exist if and only if $\bar{A}$ is module-finite over A. Theoretically, we can take any non–zerodivisor p of A in $\mathcal{C}$ and any radical ideal J such that $p \in J \subseteq \sqrt{\mathcal{C}}$, but the conductor ideal is not known a priori.

Our algorithm computes the normalization of A when a test pair for A is known. If A is a reduced, finitely generated k-algebra with k a perfect field, a non–zerodivisor can be computed by using the Jacobian ideal and J can be taken, following Theorem 5.1.12, as the radical of the Jacobian ideal or any radical ideal included in it containing a non–zerodivisor (cf. Lemma 5.3.1 and Remark 5.3.7).

If A is not normal, we get a proper ring extension $A \subsetneq \mathrm{Hom}_A(J, J) =: A_1$.

If A_1 is not normal, which is checked by applying Proposition 5.1.13 to A_1, we obtain a new ring A_2 by that same proposition, which then has to be tested for normality, and so on. That is, we get a chain of inclusions of rings

$$A \subseteq A_1 \subseteq A_2 \subseteq \ldots$$

(with $A_i = A[t_1, \ldots, t_{s_i}]/I_i$, I_i ideal in A_i, and natural maps $\psi_i : A \hookrightarrow A_i$).

If at some point, we get a normal ring A_N, since this ring is integral over A and isomorphic to a subring of $Q(A)$, the next lemma proves that $A_N \cong \overline{A}$. This guarantees that if $\bar{A}$ is module–finite over A, the chain will become stationary with A_N normal, giving an algorithm to compute the normalization.

Lemma 5.1.15. *Let $\psi : A \to B$ be a map between reduced Noetherian rings satisfying the following conditions:*

(1) ψ is injective,

(2) B is integral over A,

(3) B is contained in $Q(\psi(A))$.

Then ψ induces isomorphisms $Q(A) \xrightarrow{\cong} Q(B)$ and $\overline{A} \xrightarrow{\cong} \overline{B}$. In particular, if B is integrally closed, then $\overline{A}$ is isomorphic to B.

Proof. Since $A \hookrightarrow B$ is injective, so is $Q(A) \hookrightarrow Q(B)$ and hence $\overline{A} \hookrightarrow \overline{B}$. The isomorphism $Q(A) \to Q(B)$ is clear by (3). Since $A \hookrightarrow B$ is integral, also $A \hookrightarrow \bar{B}$ is integral. Since $\psi(A) \subseteq B \subseteq \bar{B} \subseteq Q(B) = Q(\psi(A))$, we conclude that $\bar{B}$ is the normalization of $\psi(A)$, which immediately implies the isomorphism $\overline{A} \to \bar{B}$. $\square$

The fact which makes the whole algorithm practicable is the isomorphism

$$\mathrm{Hom}_A(J, J) \cong 1/p \cdot (pJ :_A J),$$

allowing us to compute $\mathrm{Hom}_A(J, J)$. This fact, not contained in (de Jong, 1998), was first published in (Decker et al., 1999a) (see also Greuel and Pfister 2008, Lemma 3.6.1 and Gianni and Trager 1997 for related statements). We prove a generalization of this isomorphism -which will be needed in the new algorithm- in 5.2.1 below.

Finally, to compute the normalization of A recursively, we describe the A-algebra structure of $1/p \cdot (pJ :_A J)$. We need to compute the ideal of relations among a system of A-module generators of it. Given s elements $f_1, \ldots, f_s$ of an A-module, an s-tupple $(g_1, \ldots, g_s) \in A^s$ satisfying $g_1 f_1 + \cdots + g_s f_s = 0$ is called a *syzygy* or linear relation. The set of all syzygies between $f_1, \ldots, f_s$ is a submodule of A^s, which is finitely generated since A is Noetherian. A system of generators of this module can be computed using Gröbner bases for modules (see, for example, Greuel and Pfister, 2008, Algorithm 2.5.4). For higher degree relations, note that the A-module structure of $1/p \cdot (pJ :_A J)$ implies that the product of two elements $u_1/p \cdot u_2/p$ can also be written in the form u/p, with $u \in (pJ :_A J)$. This implies that no relations of degree higher than 2 are needed to generate the ideal of relations, as we show in the following lemma (Greuel and Pfister, 2008, Lemma 3.6.7).

Lemma 5.1.16. *Let A be a reduced Noetherian ring, and (J, p) a test pair for A. Let $\{u_0 = p, u_1, \ldots, u_s\}$ be a system of generators for the A-module $pJ :_A J$. Let $\{(\eta_0^k, \ldots, \eta_s^k) \in A^{s+1},\ 1 \leq k \leq m\}$ generate the module of syzygies of $u_0, \ldots, u_s$ and let $\xi_k^{ij} \in A$, $0 \leq k \leq s$, $1 \leq i \leq j \leq s$ be such that*

$$(u_i/p) \cdot (u_j/p) = \sum_{k=0}^{s} \xi_k^{ij} (u_k/p),\ 1 \leq i \leq j \leq s.$$

Let $t_1, \ldots, t_s$ denote new variables. The map $\phi : t_j \mapsto u_j/p$, $1 \leq j \leq s$ defines an isomorphism of A-algebras

$$A_1 := A[t_1, \ldots, t_s]/I_1 \xrightarrow{\cong} \frac{1}{p}(pJ :_A J),$$

where $I_1 = \langle \{\sum_{\nu=0}^{s} \eta_\nu^k t_\nu\}_{1 \leq k \leq m}, \{t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k\}_{1 \leq i \leq j \leq s} \rangle$ is the ideal of linear and quadratic relations.

Proof. By construction, $I_1 \subseteq \ker(\phi)$. For the reverse inclusion, let $h \in \ker(\phi)$. Using the relations $t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k$, $1 \leq i \leq j \leq s$, we can write $h \equiv h_0 +$

$\sum_{i=1}^{s} h_i t_i \mod I_1$, for some $h_0, h_1, \ldots, h_s \in A[t_1, \ldots, t_s]$. Now $\phi(h) = 0$ implies $h_0 + \sum_{i=1}^{s} h_i \cdot (u_i/p) = 0$, hence $(h_0, \ldots, h_s)$ is s syzygy of $u_0, \ldots, u_s$ and therefore $h \in I$. □

Example 5.1.17. Let $I = \langle x^2 - y^3 \rangle \subset k[x, y]$ and $A = k[x, y]/I$. We take the test pair (J, p), with $J := \langle x, y \rangle_A$ (the radical of the singular locus of A) and $p := x$ (see Algorithm 5.3.1). Then $pJ :_A J = \langle x, y^2 \rangle_A$ and $1/p \cdot (pJ :_A J) = 1/x \cdot \langle x, y^2 \rangle_A \cong A_1 := A[t]/I_1$ where $I_1 = \langle t^2 - y, yt - x, y^2 - xt \rangle_{A[t]}$. The isomorphism is given by $t \mapsto y^2/x$.

5.2 Computing over the original ring

It has already been noticed by many authors (see for example the comments preceding Vasconcelos 2005, Prop. 6.65) that algorithms relying on the chain of rings mentioned in last section, or similar constructions where the number of variables and relations increase in each step, behave poorly in practice. (See also Remark 5.4.1.)

There has been therefore a search for algorithms carrying out most of the computations in the original ring. In (Vasconcelos, 2000) the author proposes to use

$$B = \bigcup_{n \geq 1} \mathrm{Hom}_S(I^n, I^n),$$

where S is a hypersurface ring over which A is finite and birational and I is the annihilator of the S-module A/S. However, as mentioned in that same paper, computing B is still the hard part of the algorithm and there is no indication on how to do it.

In this section we show that a chain of rings as used in (Decker et al., 1999a) can be constructed doing most of the computations in the original ring. In this way we obtain an algorithm that is usually much faster in practice.

The purpose of this section is not only to show that computations in the original ring are possible. The proofs that we provide also show how these computations can be done and thus prepare the algorithms presented in the next section.

We start with a generalization of the isomorphism from the previous section, expressing $\mathrm{Hom}_A(J, J)$ as an ideal quotient, to be used later. We formulate a more general version than needed. For a related statement see (Swanson and Huneke, 2006).

Lemma 5.2.1. *Let A be a reduced (not necessarily Noetherian) ring, $Q(A)$ its total ring of fractions, and I, J two A-submodules of $Q(A)$. Assume that I contains a non–zerodivisor p of $Q(A)$.*

(1) The map

$$\Phi : \mathrm{Hom}_A(I, J) \to \frac{1}{p}(pJ :_{Q(A)} I) = J :_{Q(A)} I, \quad \varphi \mapsto \frac{\varphi(p)}{p},$$

is independent of the choice of p and is an isomorphism of A-modules.

(2) If $J \subseteq A$ then

$$pJ :_{Q(A)} I = pJ :_A I.$$

Proof. (1) Let $q \in I$ be another non–zerodivisor of $Q(A)$. Write $p = p_1/p_0$ and $q = q_1/q_0$, with $p_0, q_0, p_1, q_1 \in A$ and p_0, q_0 non–zerodivisors of A.

Also $c := p_0 q_0 \in A$ is a non–zerodivisor, and $cp, cq \in A$ with $cpq \in I$. Since $\varphi \in \mathrm{Hom}_A(I, J)$ is A-linear, we can write

$$cp\varphi(q) = \varphi(cpq) = cq\varphi(p),$$

hence $\varphi(p)/p = \varphi(q)/q$ in $Q(A)$, showing that Φ is independent of p.

Note that p_1 must also be a non–zerodivisor of $Q(A)$. Then, for any $f = f_1/f_0 \in I$, with $f_0, f_1 \in A$ and f_0 a non–zerodivisor of A, we have

$$\frac{\varphi(p)}{p} \cdot \frac{f_1}{f_0} = \frac{\varphi(p_1)}{p_1} \cdot \frac{f_1}{f_0} = \frac{\varphi(p_1 f_1)}{p_1 f_0} = \frac{\varphi(p_1 f_0 f_1/f_0)}{p_1 f_0} = \varphi(f_1/f_0) = \varphi(f) \in J,$$

in particular $\varphi(p) \cdot f \in pJ$. This shows that the image $\Phi(\varphi)$ is in $1/p \cdot (pJ :_{Q(A)} I)$. It also shows that $\varphi(p) = 0 \Leftrightarrow \varphi(f) = 0, \forall f \in I \Leftrightarrow \varphi = 0$, and hence that Φ is injective.

To see that Φ is surjective, let $q \in Q(A)$ satisfy $qI \subseteq J$. Denote by $m_q \in \mathrm{Hom}_A(I, J)$ the multiplication by q. Then $\Phi(m_q) = qp/p = q$ showing that Φ is surjective.

(2) During the proof of (1) we saw that

$$pJ :_{Q(A)} I = \{\varphi(p) \mid \varphi \in \mathrm{Hom}_A(I, J)\}.$$

Hence, the claimed equality holds if and only if $\varphi(p) \in A$ for all $\varphi \in \mathrm{Hom}_A(I, J)$, which is clearly true if $J \subseteq A$. □

Recall the chain of extension rings from last section $A \subseteq A_1 \subseteq A_2 \subseteq \ldots$ We have seen that we can compute the normalization of A by computing the normalization of A_i (Lemma 5.1.15). The next proposition explains how to obtain a test pair in A_i from a given test pair in A. This is the only computation to be carried out in A_i.

Proposition 5.2.2. *Let A be a reduced Noetherian ring, $A' = A[t_1, \ldots, t_s]/I'$ a finite extension ring, with natural inclusion $\psi : A \hookrightarrow A'$. If (J, p) is a test pair for A then $(J', \psi(p))$ is a test pair for A', where $J' = \sqrt{\langle \psi(J) \rangle_{A'}}$.*

Proof. Clearly, every non–zerodivisor of A is also a non–zerodivisor of $Q(A)$. In particular, it is a non–zerodivisor of A'. Furthermore, if $\mathcal{C}_{A'}$ is the conductor of A' in $\overline{A'} = \overline{A}$, then $\mathcal{C}_{A'} \supseteq \mathcal{C}_A$. It follows that every prime ideal $Q \in N(A') = V(\mathcal{C}_{A'})$ contracts to a prime ideal $P \in N(A) = V(\mathcal{C}_A)$. Hence, if (J, p) is a test pair for A, then $P \supseteq J$, which implies that $Q \supseteq \sqrt{JA'} = J'$. We conclude that (J', p) is a test pair for A'. □

Example 5.2.3. Recall Example 5.1.17. We started with $A = k[x,y]/\langle x^2 - y^3\rangle$ and test pair $(J,p) = (\langle x,y\rangle, x)$ and obtained $A_1 := A[t]/I_1 \cong 1/d_1 \cdot U_1$ where $I_1 = \langle t^2 - y, yt - x, y^2 - xt\rangle$, $d_1 = x$ and $U_1 = \langle x, y^2\rangle_A$.

We now compute $J_1 = \sqrt{\langle \psi_1(J)\rangle_{A_1}} = \sqrt{\langle x,y\rangle_{A_1}} = \langle x,y,t\rangle_{A_1} = \langle t\rangle_{A_1}$ (since $t^2 = y$ and $t^3 = x$ in A_1). Therefore $(\langle t\rangle, x)$ is a test pair for A_1.

For the rest of this section, let R be a Noetherian ring, $I \subseteq R$ a radical ideal and $A = R/I$. We are mainly interested in $R = k[\boldsymbol{x}] = k[x_1,\ldots,x_n]$ with k a field (which the reader may assume in the following). However, as mentioned before, the proposed method works quite generally, whenever a test pair is known.

In the new algorithm, we will compute ideals $U_1, U_2, \ldots, U_N$ of A and non–zerodivisors $d_i \in U_i$, $1 \leq i \leq N$, of A such that

$$A \subseteq \frac{1}{d_1}U_1 \subseteq \frac{1}{d_2}U_2 \subseteq \cdots \subseteq \frac{1}{d_N}U_N = \bar{A}.$$

From the construction we know that $1/d_i \cdot U_i$ is a finitely generated R-algebra and hence there is a surjection

$$R_i := R[t_1,\ldots,t_{s_i}] \twoheadrightarrow \frac{1}{d_i}U_i, \quad t_j \mapsto u_j,$$

where $\{d_i, u_1, \ldots, u_{s_i}\}$ is a set of R-module generators of U_i. If I_i denotes the kernel of this map, we get a ring map

$$\varphi_i : A_i := R_i/I_i \xrightarrow{\cong} \frac{1}{d_i}U_i \subseteq Q(A).$$

Example 5.2.4. Carrying on with Example 5.2.3, we compute $\varphi_1(J_1) = \varphi_1(\langle t\rangle)$.

Note that $\varphi_1(t) = y^2/x$. However the A-module $\langle y^2/x\rangle_A \subsetneq \varphi_1(\langle t\rangle)$. For example, we have seen that $y \in \langle t\rangle_{A_1}$ and clearly $\varphi_1(y) = yx/x$, but $yx \notin \langle y^2\rangle_A$.

This shows that in order to obtain A-module generators of $\varphi_i(J_i)$ it is not enough to compute the images of the generators of J_i. In Algorithm 5.3.2 we will show how to compute the generators. In this example, it turns out that $\varphi_1(\langle t\rangle) = \langle yx/x, y^2/x\rangle$ as A-module.

Once we have computed a test pair (J_i, p_i) in A_i, the next step is to compute the quotient $pJ_i :_{A_i} J_i$. The following theorem shows that this computation can be carried out in the original ring A.

Theorem 5.2.5. *Let $A = R/I$, $A' = A[t_1,\ldots,t_s]/I'$ a finite ring extension and maps $\psi : A \hookrightarrow A'$, $\varphi : A' \hookrightarrow Q(A)$. Let (J,p) be a test pair for A and (J',p') a test pair for A', with $p' = \psi(p)$. Let U, H be ideals of A and $d \in A$ such that $\varphi(A') = \frac{1}{d}U$ and $\varphi(J') = \frac{1}{d}H$. Then*

$$(p'J') :_{A'} J' = \frac{1}{d}(dpH :_A H).$$

Proof. The proof is an easy consequence of Lemma 5.2.1. Omitting φ and ψ in the following notations and applying Lemma 5.2.1 to $p \in J \subseteq A$ we get

$$(p'J') :_{A'} J' = (p'J') :_{Q(A)} J' = pH :_{Q(A)} H,$$

since $Q(A') = Q(A)$ and $J' = 1/d \cdot H$.

On the other hand, we can apply Lemma 5.2.1 to $dp \in H \subseteq A$ and get

$$\frac{1}{d}(dpH :_A H) = \frac{1}{d}(dpH :_{Q(A)} H) = pH :_{Q(A)} H.$$

□

Using Theorem 5.2.5 together with the previous results, once we have computed an intermediate ring A_i, we can compute A_{i+1}, the next ring in the chain. If $A_i = A_{i+1}$, we have finished and A_i is the normalization of the original ring A, by Lemma 5.1.15. If not, we proceed by induction to compute the normalization.

We continue with the example.

Example 5.2.6. We have $p = d_1 = x$ and $H_1 = \langle xy, y^2 \rangle_A$. We compute $d_1 p H_1 :_A H_1 = x^2\langle xy, y^2\rangle :_A \langle xy, y^2\rangle = \langle x^2, xy^2\rangle$.

Then

$$\mathrm{Hom}_{A_1}(J_1, J_1) \cong \frac{1}{x^2}\langle x^2, xy^2\rangle = \frac{1}{x}\langle x, y^2\rangle.$$

This is equal to A_1. Therefore, the ring A_1 was already normal, and hence equal to the normalization of A.

Modification 5.2.7. We have seen that the only computation performed in A_i is the radical of $\psi_i(J)$. However, when the characteristic of the base field is $q > 0$ it is possible to compute also this radical over the original ring. For this, we use the Frobenius map, as described in (Matsumoto, 2001).

Let $G = \psi_i(J) \subseteq A_i$. By definition,

$$J_i = \sqrt{G} = \{f \in A_i \mid f^m \in G \text{ for some } m \in \mathbb{N}\}.$$

Mapping to $Q(A)$, we obtain

$$\varphi_i(J_i) = \left\{ \tilde{f}/d_i \;\middle|\; \tilde{f} \in U_i,\ \left(\tilde{f}/d_i\right)^m \in \varphi_i(G) \text{ for some } m \in \mathbb{N} \right\} = \bigcup_{m \geq 1} G_m,$$

where $G_m := \left\{ \tilde{f}/d_i \;\middle|\; \tilde{f} \in U_i,\ \left(\tilde{f}/d_i\right)^m \in \varphi_i(G) \right\}$. Then

$$d_i G_q = \{\tilde{f} \in U_i \mid \tilde{f}^{\,q} \in d_i^q \varphi_i(G)\}.$$

Now $d_i^q \varphi_i(G)$ is an ideal of A and $d_i G_q$ is the so-called q-th root of $d_i^q \varphi_i(G)$. This ideal can be computed over A using the Frobenius map (see Matsumoto, 2001).

By iteratively computing the q-th root of the output, until no new polynomials are added, we obtain $\varphi_i(J_i)$ as desired.

Computing the radical in this way, we get another algorithm (in positive characteristic) which is similar to the one proposed in (Singh and Swanson, 2009). In their algorithm they start with the inclusion $\bar{A} \subseteq \frac{1}{c}A$, where c is an element of the conductor and compute a decreasing chain of A-modules

$$\frac{1}{c}A = \frac{1}{c}U_0' \supseteq \frac{1}{c}U_1' \supseteq \cdots \supseteq \frac{1}{c}U_N' = \bar{A}.$$

In our algorithm we compute an increasing chain

$$A \subseteq \frac{1}{d_1}U_1 \subseteq \cdots \subseteq \frac{1}{d_N}U_N = \bar{A}.$$

The most difficult computational task for both algorithms is the Frobenius map. However, in our algorithm we start with a small denominator d_1 and therefore the computations might be in some cases easier. This modification has not yet been tested.

5.3 Algorithms

We describe the algorithm in general terms. Since we compute an increasing sequence of subrings of the integral closure the algorithm terminates, for a Noetherian ring A, if and only if $\bar{A}$ is module–finite over A. By Lemma 5.1.7 this is equivalent to the existence of a test pair. We now deal with the problem of constructing an initial test pair.

Lemma 5.3.1. *Let k be a perfect field, and $A = k[x_1, \ldots, x_n]/I$ a reduced equidimensional ring of dimension r (that is, I is radical and all the associated primes have dimension r). Let M be the Jacobian ideal of $I = \langle f_1, \ldots, f_t \rangle$, defined as the ideal in A generated by the images of the $(n-r) \times (n-r)$-minors of the Jacobian matrix $(\partial f_i/\partial x_j)_{i,j}$. Then M is contained in the conductor of A and contains a non–zerodivisor of A.*

Proof. Let $I = P_1 \cap \ldots \cap P_s$ with $P_1, \ldots, P_s$ the minimal associated primes of I. Since A is equidimensional, $\dim(A) = \text{height}(P_i) = r$ for $1 \leq i \leq s$. Hence, the image of M in $A_i = k[x_1, \ldots, x_n]/P_i$ is contained in the Jacobian ideal M_i of P_i. By the Lipman-Sathaye theorem (see Swanson and Huneke 2006 and Singh and Swanson 2009, Remark 1.5) M_i and hence M is contained in the conductor of A_i. Since $\bar{A} = \bar{A}_1 \oplus \cdots \oplus \bar{A}_s$, M is then also contained in the conductor of A. Moreover, the image of M in A_i is not zero since A_i is reduced. This follows from the Jacobian criterion and by Serre's condition for reducedness (see Greuel and Pfister, 2008, Section 5.7). As a consequence, M is not contained in the union of the minimal primes of A and hence contains a non–zerodivisor of A. □

Note that both the Lipman-Sathaye theorem and the Jacobian criterion require k to be perfect.

The ideal $J := \sqrt{M}$ from last lemma can be used as an initial test ideal. To construct a test pair, we need to find in addition a non–zerodivisor of A in J. An element $p \in A$ is a non–zerodivisor if and only if $0 :_A p = 0$, hence the non–zerodivisor test is effective. However, it is not sufficient to apply the test to the generators of J. (E.g., if $I = \langle xy \rangle$, the polynomials x, y generate J and are zerodivisors of A, but $x + y$ is not.) Since we cannot test all elements of J there seems to be a problem to find a test pair if I is not prime. We address this problem as well as the perfectness and the equidimensionality assumptions in Remark 5.3.7.

We first describe in Algorithm 5.3.1 how to compute the initial test pair (J, p) in A, assuming that we are able to find a non–zerodivisor.

Remark 5.3.2. Only for this step we need the assumption that $R = k[\boldsymbol{x}]$ with k perfect and that I is equidimensional. All further steps do not require this assumption.
If, by whatever means, an initial test pair (J, p) for A is known, we can start with the computation of U_1 and then all further steps are correct, and the loop terminates with the computation of $\bar{A}$. Hence, for any reduced ring $A = R/I$ with given test pair (J, p), the algorithm is effective when Gröbner bases, ideal quotients, and radicals can be computed in rings of the form $R[t_1, \ldots, t_s]$.

Algorithm 5.3.1 Initial test pair (J, p)

Input: $I \subseteq R$, an equidimensional radical ideal, with $R = k[x_1, \ldots, x_n]_>$ and k a perfect field.

Output: (J, p) a test pair for $A := R/I$.

1: $r := \dim(I)$
2: $M' :=$ the Jacobian ideal of I, i.e., the ideal in R generated by the $(n-r) \times (n-r)$-minors of the Jacobian matrix of I
3: $M :=$ the image of M' in A
4: $J := \sqrt{M} \subseteq A$
5: choose $p \in J$ such that p is a non–zerodivisor of A
6: **return** (J, p).

We now explain how to perform some auxiliary tasks, that will be needed in the main algorithm.

We have seen in the previous section that if $A = R/I$ and $A' = R[t_1, \ldots, t_n]/I'$ is a finite extension ring with $I \subseteq I'$, then there exist a non–zerodivisor $d \in A$, an ideal $U \subseteq A$ and a map $\varphi : A' \to 1/d \cdot U$ such that $A' \xrightarrow{\cong} 1/d \cdot U$. For computations, we need to know how to move from one representation to the other.

Remark 5.3.3. If we know d and generators $\{d, u_1, \ldots, u_s\}$ of U, we can explicitly compute $\varphi(q)$ for any $q \in A'$. Let $\tilde{q} \in R'$ be a representative, and substitute all the variables t_j in $\tilde{q}$ by the corresponding fraction u_j/d. This gives an element $f/d^e \in Q(A)$ for some $f \in A$ and $e \in \mathbb{Z}_{\geq 0}$. Now we need to find $f' \in A$ such that $f/d^e = f'/d$ in $Q(A)$, which is equivalent to $f = f'd^{e-1} + g$ in R, with $g \in I$. We can find f' by solving the (extended) ideal membership problem $f \in I + \langle d^{e-1} \rangle$

in R, e.g. by using the SINGULAR command `lift` (see Greuel and Pfister, 2008, Example 1.8.2).

More generally, if f/c is an element of $1/d \cdot U \subseteq Q(A)$, with c a non–zerodivisor, we can find f' such that $f/c = f'/d$ by solving the ideal membership problem $df \in \langle I, c\rangle$.

We will need also to compute A-module generators of ideals $J' \subseteq A'$ given by generators in A'. It is clear that for any such J' there exists an ideal $H \subseteq A$ such that $\varphi(J') = 1/d \cdot H$. So the problem is equivalent to finding elements $h_1, \ldots, h_l$ in A that generate H as an A-ideal. In Algorithm 5.3.2 we explain how to do it.

Algorithm 5.3.2 A-module generators

Input: $A = R/I$, with $R = k[x_1, \ldots, x_n]$ and $I \subseteq R$ ideal; $A' = R'/I'$ a ring extension of A, with $R' = R[t_1, \ldots, t_s]$ and $I' \subseteq R'$ an ideal, $d \in A'$ a non–zerodivisor and $U' = \langle u_0 = d, u_1, \ldots, u_s\rangle_A$ such that $A' \overset{\varphi}{\cong} \frac{1}{d}U$, $J' = \langle f_1, \ldots, f_m\rangle_{A'}$ an ideal of A'.

Output: $H = \langle h_1, \ldots, h_l\rangle_A$ such that $\varphi(J') = 1/d \cdot H$.

1: **for** $j = 1, \ldots, m$ **do**
2: compute h_j such that $\varphi_i(f_j) = h_j/d$ (cf. Remark 5.3.3)
3: **end for**
4: set $S = \{h_1, \ldots, h_m\}$
5: **for** $j = 1, \ldots, m$; $k = 1, \ldots, s$ **do**
6: compute $h_{j,k} \in A$ such that $\dfrac{h_{j,k}}{d} = \dfrac{u_k}{d}\dfrac{h_j}{d}$ in $Q(A)$ (again by Remark 5.3.3)
7: **if** $h_{j,k} \notin \langle S\rangle_A$ **then**
8: $S = S \cup \{h_{j,k}\}$
9: **end if**
10: **end for**
11: **return** $H := \langle S\rangle$.

Lemma 5.3.4. *Let $A = R/I$, with $R = k[x_1, \ldots, x_n]$ and $I \subseteq R$ ideal; $A' = R'/I'$ a ring extension of A, with $R' = R[t_1, \ldots, t_s]$ and $I' \subseteq R'$ an ideal, $d \in A'$ a non–zerodivisor and $U' = \langle u_0 = d, u_1, \ldots, u_s\rangle_A$ such that $A' \overset{\varphi}{\cong} \frac{1}{d}U$, $J' = \langle f_1, \ldots, f_m\rangle_{A'}$ an ideal of A'. The output ideal $H = \langle h_1, \ldots, h_l\rangle_A$ of Algorithm 5.3.2 satisfies $\varphi(J') = 1/d \cdot H$.*

Proof. This follows since the A-module $\langle 1 = u_0/d, u_1/d_i, \ldots, u_s/d\rangle_A = \varphi(A')$ and the A'-module $\langle h_1/d, h_2/d, \ldots, h_m/d\rangle_{A'} = \varphi(J')$ ($h_1, \ldots, h_m$ as in the algorithm). Therefore the products $(u_k/d)(h_j/d)$, $0 \leq k \leq s$, $1 \leq j \leq m$, generate $\varphi(J')$ as A-module. Hence $\{h_j\}_{1 \leq j \leq l}$ generates H as A-module, or equivalently as A-ideal. □

Example 5.3.5. We apply the algorithm to compute the A-module generators of $\varphi_1(J_1)$ from Example 5.2.4. Recall that $J_1 = \langle t\rangle_{A_1}$, $U_1 = \langle x, y^2\rangle_A$ and $d = x$. We start with $h_1 = \varphi_1(t) = y^2/x$ and $S = \{h_1\}$. In the first step, we compute

$(x/x)(y^2/x) = y^2/x$, therefore $h_{1,0} = y^2$. Since $y^2 \in \langle y^2 \rangle$, we do not do anything. In the second step we compute $(y^2/x)(y^2/x) = y^4/x^2 = x^2y/x^2 = xy/x$, therefore $h_{1,1} = xy$. Since $xy \notin \langle y^2 \rangle$, we add it to S. We finish with $H = \langle xy, y^2 \rangle$, as mentioned in Example 5.2.4.

We are now ready to present in Algorithm 5.3.3 the main algorithm to compute the normalization.

Termination follows from Lemma 5.1.7 and the discussion after Definition 5.1.14, correctness follows from Lemma 5.1.15.

Algorithm 5.3.3 Normalization of R/I

Input: $I \subseteq R$, an equidimensional radical ideal.

Output: generators of an ideal $U \subseteq R$, and $d \in R$ such that $\overline{A} = \frac{1}{d}U \subseteq Q(A)$, with $A := R/I$.

1: compute (J, p), an initial test ideal
2: $U_1 := (pJ :_A J) \subseteq A$
3: $d_1 := p$
4: **if** $\langle d_1 \rangle = U_1$ **then**
5: **return** $(\langle 1 \rangle, 1)$
6: **end if**
7: $i := 1$
8: **loop**
9: write $U_i = \left\langle d_i, u_1^{(i)}, u_2^{(i)}, \ldots, u_s^{(i)} \right\rangle_A$
10: set $R_i := R[t_1, \ldots, t_s]$, $\pi_i : R_i \to \frac{1}{d_i}U_i \subseteq \frac{1}{d_i}A$ the map $t_j \mapsto u_j^{(i)}/d_i$
11: $I_i := \ker(\pi_i)$ (cf. Lemma 5.1.16)
12: set $A_i = R_i/I_i$
13: $J_i := \sqrt{\psi_i(J)} \subseteq A_i$, with $\psi_i : A \hookrightarrow A_i$
14: compute $\{f_1, \ldots, f_k\} \subseteq A$ such that $H_i := \langle f_1, \ldots, f_k \rangle_A = d_i\varphi_i(J_i)$, with $\varphi_i : A_i \xrightarrow{\cong} \frac{1}{d_i}U_i$ (cf. Lemma 5.3.4)
15: compute generators of $U_{i+1} := (pd_iH_i) :_A H_i$
16: **if** $d_iU_i \subseteq U_{i+1}$ **then**
17: **return** (U_i, d_i)
18: **end if**
19: $d_{i+1} := pd_i$
20: $i := i + 1$
21: **end loop**

We give another complete example, applying the given algorithm.

Example 5.3.6. For

$$A = k[x, y]/\langle x^5 - y^2\,(y-1)^3 \rangle,$$

the radical of the Jacobian ideal is

$$J := \langle x, y\,(y-1) \rangle_A\,,$$

and we can take $p := x \in J$ as a non–zerodivisor of A. In its first step, starting with the initial test pair (J, x), the normalization algorithm produces the following

data:

$$U^{(1)} := xJ \ :_A \ J = \left\langle x, y(y-1)^2 \right\rangle_A \text{ and}$$
$$A_1 := A[t_1]/I_1 \cong \frac{1}{x}U^{(1)} \ ,$$

with relations and isomorphism given by

$$I_1 = \left\langle -t_1 x + y(y-1)^2, -t_1 y(y-1) + x^4, t_1^2 - x^3(y-1) \right\rangle \text{ and}$$
$$t_1 \mapsto \frac{y(y-1)^2}{x}, \textit{ respectively.}$$

In the next step, since $t_1^2 = x^3(y-1)$ and $t_1 x = y(y-1)^2$, we find

$$J_1 := \sqrt{\langle x, y(y-1) \rangle_{A_1}} = \langle x, y(y-1), t_1 \rangle_{A_1}$$
$$= \frac{1}{x} \left\langle x^2, xy(y-1), y(y-1)^2 \right\rangle_A =: \frac{1}{x} H_1.$$

Using the test pair (J_1, x), in the next step we compute

$$\frac{1}{x}(xJ_1 \ :_{A_1} \ J_1) = \frac{1}{x^2}(x^2 H_1 \ :_A \ H_1)$$
$$= \frac{1}{x^2} \left\langle x^2, xy(y-1), y(y-1)^2 \right\rangle_A =: \frac{1}{x^2} U^{(2)}$$

and

$$A_2 = A[t_2, t_3]/I_2 \cong \frac{1}{x^2}U^{(2)} \ ,$$

with relations and isomorphism given by

$$I_2 = \big\langle t_2 x - t_3(y-1), -t_3 x + y(y-1), -t_2 y(y-1) + x^3,$$
$$-t_2 y^3 (y-1)^2 + t_3 x^4, t_2^2 - x(y-1), t_2 t_3 - x^2, t_3^2 - t_2 y \big\rangle$$

and

$$t_2 \mapsto \frac{y(y-1)}{x}, \ t_3 \mapsto \frac{y(y-1)^2}{x^2},$$

respectively. Now,

$$J_2 := \sqrt{\langle x, y(y-1) \rangle_{A_2}} = \langle x, y(y-1), t_2, t_3 \rangle = \langle x, t_2, t_3 \rangle$$
$$= \frac{1}{x^2} \left\langle x^3, xy(y-1), y(y-1)^2 \right\rangle_A =: \frac{1}{x^2} H_2.$$

Continuing with the test pair (J_2, x), we get

$$\frac{1}{x}(xJ_2 \ :_{A_2} \ J_2) = \frac{1}{x^3}(x^3 H_2 \ :_A \ H_2)$$
$$= \frac{1}{x^3} \left\langle x^3, x^2 y(y-1), xy(y-1)^2, y^2(y-1)^2 \right\rangle_A =: \frac{1}{x^3} U^{(3)}$$

and

$$A_3 := A[t_4, t_5, t_6]/I_3 \cong \frac{1}{x^3}U^{(3)},$$

where I_3 is generated by 11 relations. In the final step, we find that A_3 is normal and, hence, equal to $\overline{A}$.

Remark 5.3.7. Let us comment on some variations and generalizations of Algorithm 5.3.3. We let k be *any* field, $R = k[x_1, \ldots, x_n]_>$, and $I \subseteq R$ a radical ideal.
(1) If I is not (or not known to be) equidimensional we can start with an algorithm to compute its minimal associated primes (see Greuel and Pfister, 2008, Algorithm 4.3.4, Algorithm 4.4.3)) or its equidimensional decomposition (see Greuel and Pfister, 2008, Algorithm 4.4.9), where the latter is often faster. The corresponding ideals $I_1, I_2, \ldots, I_r$ are equidimensional and we have $\overline{R/I} \cong \overline{R/I_1} \oplus \overline{R/I_2} \oplus \cdots \oplus \overline{R/I_r}$. Hence the problem is reduced to the case of I being prime or equidimensional.
(2) If I is equidimensional, we let M be its Jacobian ideal. Since regular rings are normal, it follows from the Jacobian criterion that $N(R/I) \subseteq V(M)$. Let us assume that $M \neq 0$ and choose $p \in M \setminus \{0\}$.
a) If $I_1 := I :_R \langle p \rangle \subseteq I$ then p is a non–zerodivisor of A and $J = \sqrt{M}$ is a test ideal. This is always the case if I is prime.
b) If $I_1 \not\subseteq I$ we compute $I_2 := I :_R I_1$ and obtain a splitting $I = I_1 \cap I_2$ (see Greuel and Pfister, 2008, Lemma 1.8.14(3)) and $\overline{R/I} \cong \overline{R/I_1} \oplus \overline{R/I_2}$. Hence we can continue with the ideals I_1 and I_2 separately which have both fewer minimal associated primes than I. Consequently, after finitely many splittings, the corresponding ideal is prime or we have found a non–zerodivisor. This provides us with test ideals as in case a).
(3) The above arguments show that (even if k is not perfect) Algorithm 5.3.3 works for prime ideals if and only if the Jacobian ideal M is not zero. This is always the case for k perfect. However, if k is not perfect, $M = 0$ may occur. For example, consider $k = (\mathbb{Z}/q)(t)$ with q a prime number, and $I = \langle x^q + y^q + t \rangle \subset k[x, y]$. For a method to compute a non–zero element in the conductor of R/I if I is prime and if $Q(R/I)$ is separable over k, see (Swanson and Huneke, 2006, Exercise 12.12).

5.4 Examples and comparisons

In Table 5.1 we present a comparison of the implementations in SINGULAR of the new algorithm `normal` and other existing algorithms. `normalC` is an implementation based on the algorithm (Decker et al., 1999a) (see also Greuel and Pfister, 2008, Section 3.6) and `normalP` is an implementation of the algorithm in (Leonard and Pellikaan, 2003; Singh and Swanson, 2009) for positive characteristic. All these implementations are now available in the SINGULAR library `normal` (Greuel et al., 2009). Computations were performed on a compute server running a 1.60GHz Dual AMD Opteron 242 with 8GB ram.
$*$ indicates that the algorithm had not finished after 20 minutes,

Table 5.1: Timings

No.	char	`normal` data		seconds		
		non–zerodivisor	steps	`normal`	`normalP`	`normalC`
1	0	y	7	0	-	72
1	2	y	7	0	0	0
1	5	y	7	1	73	0
1	11	$x-2y$	7	1	12	$*$
1	32003	y	7	0	$*$	1
2	0	y	7	1	-	$*$
2	3	y	8	0	0	3
2	13	y	7	0	$*$	10
2	32003	y	7	0	$*$	10
3	0	y	6	2	-	$*$
3	2	y	13	1	0	$*$
3	5	y	6	1	7	$*$
3	11	$x+4y$	6	1	$*$	$*$
3	32003	y	6	1	$*$	$*$
4	0	$2x^2y-y^3+y$	1	0	-	0
4	5	x^2y+2y^3-2y	1	0	3	0
4	11	x^2y+5y^3-5y	1	0	$*$	0
4	32003	$x^2y+16001y^3-16001y$	1	0	$*$	0
5	0	y	1	0	-	0
5	5	x^3y+xy	3	1	$*$	$*$
5	11	y	1	0	0	0
5	32003	y	1	1	$*$	0
6	2	v	2	6	24	172
7	0	y	6	12	-	582
7	2	y	6	11	0	35
7	5	y	6	12	3	358
7	11	y	6	11	43	503
7	32003	y	6	11	$*$	617

- indicates that the algorithm is not applicable (i.e., using `normalP` in characteristic 0).

We show the timings for several examples over the fields $k = \mathbb{Q}$ and $k = \mathbb{Z}_p, p \in \{2, 3, 5, 11, 13, 32003\}$, when the ideal is prime in the corresponding ring. We see that the new algorithm is extremely fast compared to the other algorithms. Only the algorithm `normalP` is sometimes faster for very small characteristic.

In columns 3 and 4 we give additional information on how the new algorithm works. The column "non–zerodivisor" indicates which non–zerodivisor is chosen. The column "steps" indicates how many loop steps are needed to compute the normalization. We see that our new algorithm performs well compared to the classic algorithm especially when the number of steps needed is large.

We used the following examples:

- $I_1 = \langle (x-y)x(y+x^2)^3 - y^3(x^3+xy-y^2)\rangle \subset k[x,y]$,
- $I_2 = \langle 55x^8 + 66y^2x^9 + 837x^2y^6 - 75y^4x^2 - 70y^6 - 97y^7x^2\rangle \subset k[x,y]$,
- $I_3 = \langle y^9 + y^8x + y^8 + y^5 + y^4x + y^3x^2 + y^2x^3 + yx^8 + x^9\rangle \subset k[x,y]$,
- $I_4 = \langle (x^2+y^2-1)^3 + 27x^2y^2\rangle \subset k[x,y]$,
- $I_5 = \langle -x^{10} + x^8y^2 - x^6y^4 - x^2y^8 + 2y^{10} - x^8 + 2x^6y^2 + x^4y^4 - x^2y^6 - y^8 + 2x^6 - x^4y^2 + x^2y^4 + 2x^4 + 2x2y^2 - y^4 - x^2 + y^2 - 1\rangle \subset k[x,y]$,
- $I_6 = \langle z^3 + zyx + y^3x^2 + y^2x^3, uyx + z^2, uz + z + y^2x + yx^2, u^2 + u + zy + zx, v^3 + vux + vz^2 + vzyx + vzx + uz^3 + uz^2y + z^3 + z^2yx^2\rangle \subset k[x,y,z,u,v]$.
- $I_7 = \langle x^2 + zw, y^3 + xwt, xw^3 + z^3t + ywt^2, y^2w^4 - xy^2z^2t - w^3t^3\rangle \subset k[x,y,z,w,t]$.

Remark 5.4.1. As mentioned before, the main drawback of the algorithm (Decker et al., 1999a) is the increasing complexity of computing the intermediate rings. A direct implementation of the algorithm turns out to be so slow that it does not even finish for most of the examples analyzed in this paper (after 1 hour). For example, in the second example, I_2, over $\mathbb{Z}_3$, the fifth ring constructed in the chain has 12 variables and 76 generators for the ideal of relations. The sixth ring could not be computed using this direct approach.

A partial solution to this problem, used in implementations, is to eliminate as far as possible redundant variables, that is, variables than can be expressed in term of the others through the relations in the ring. This is what is done in `normalC`, and it is sometimes a good improvement. However detecting the redundant variables becomes more and more difficult as the relations get more and more complex, adding a new expensive task to the computation, that does not always succeeds in detecting all the relations.

The algorithm proposed in this paper avoids this problem in a natural way.

We have also compared our implementation with the normalization procedures in Macaulay2 (they use the algorithms (Decker et al., 1999a) and (Singh and Swanson, 2009)) and in Magma (they say that they use (Decker et al., 1999a)

for the general case; however it seems to work only in characteristic 0 and the code is not accessible). Our new algorithm is always faster and succeeds where the other implementations do not finish. We do not know of implementations in other computer algebra systems.

5.5 Normalization of local rings

In this section, let $I \subseteq R = k[\boldsymbol{x}]$ be an equidimensional radical ideal and P a prime ideal of $A = R/I$. We want to compute the normalization of the local ring A_P.

Note that since normalization commutes with localization (see, for example, Eisenbud, 1995, Proposition 4.13), the normalization of the ring A_P is module–finite over A_P.

We can extend Algorithm 5.3.3 from Section 5.3 to this general situation in two different ways.

The first method is to do all computations locally. This can be done by using an appropriate non-global monomial ordering. (See Greuel and Pfister 2008, where the theory of standard basis for such monomial orders is developed.)

This algorithm is correct (by applying Proposition 5.1.15 to A_P) and terminates because $\overline{A_P}$ is module–finite over A_P.

The second method is to compute the normalization of A as in the previous section, and then mapping the result to A_P. The method is also correct since normalization commutes with localization.

If we start with an equidimensional decomposition $I = \bigcap_{i=1}^{r} I_i$, then of course we only need to compute the normalization for those ideals I_i for which the localization $(R/I_i)_P$ is not $\langle 1 \rangle$.

Example 5.5.1. To see the difference between both methods, let

$$I = \langle y^2 - x^2(x+1)^2(x+2) \rangle \subset R = k[x, y]$$

In Figure 5.1 we can see the real part of the curve $\mathbf{V}(I)$. This curve has two singularities, at the points $P_1 = (0, 0)$ and $P_2 = (-1, 0)$.

We want to compute the normalization of $A' = (R/I)_{\langle x,y \rangle}$.

We carry out the first method, setting $I' = IA'$. The singular locus of I' is $J = \langle x, y \rangle$, which is radical. This is the first test ideal. We take as non–zerodivisor $p := y$ and compute the quotient

$$U_1 := yJ :_{A'} J = \langle x, y \rangle.$$

Since $U_1 \neq \langle y \rangle$ we go on. The ring structure of $1/y \cdot U_1$ is $A_1 = (k[t, x, y]/I_1)_{\langle x,y \rangle}$, with $I_1 = \langle tx^4 + 4tx^3 + 5tx^2 + 2tx - y, -ty + x, t^2(x+1)^2(x+2) - 1, x^5 + 4x^4 + 5x^3 + 2x^2 - y^2 \rangle$.

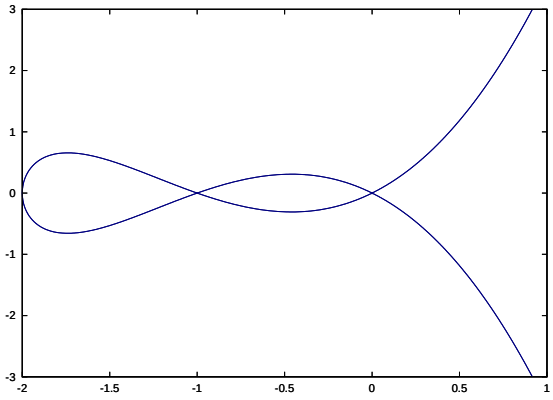

Figure 5.1: $y^2 - x^2(x+1)^2(x+2) = 0$

We compute $J_1 := \sqrt{\varphi_1(\langle x, y\rangle)} = \langle x, y, 2t^2 - 1\rangle_{A_1}$.

Mapping J_1 to $Q(A')$ using $d_1 = y$ as denominator, we get $J_1 \cong 1/y \cdot H_1$, with $H_1 := \langle yx, y^2\rangle$. (The image of $2t^2 - 1$ in $Q(A')$ is $(-10xy - 8x^2y - 2x^3y)/y$, which is already in $1/y \cdot \langle yx, y^2\rangle$.) We compute the quotient

$$U_2 := y^2\langle yx, y^2\rangle :_{A'} \langle yx, y^2\rangle = \langle xy, y^2\rangle.$$

We see that $yU_1 = U_2$. This means that A_1 was already normal and isomorphic to the normalization of A', which is therefore $1/y \cdot \langle x, y\rangle_{A'}$.

Let us now apply the second method. The singular locus of I is $J = \langle x^2 + x, y\rangle$, which is radical. J serves as first test ideal. As non–zerodivisor we choose $p := y$ and compute the quotient

$$U_1 := yJ :_A J = \langle y, x^3 + 3x^2 + 2x\rangle.$$

As $U_1 \neq \langle y\rangle$, we continue. We compute A_1, the ring structure of $1/y \cdot U_1$, $A_1 = k[t, x, y]/\langle tx^2 + tx - y, -ty + x^3 + 3x^2 + 2x, t^2 - x - 2, x^5 + 4x^4 + 5x^3 + 2x^2 - y^2\rangle$, and $J_1 = \sqrt{\varphi_1(\langle x^2 + x, y\rangle)} = \langle x^2 + x, y\rangle$.

Mapping J_1 to $Q(A)$ using $d_1 = y$ as denominator, we obtain $J_1 \cong 1/y \cdot H_1$, with $H_1 := \langle y(x^2 + x), y^2\rangle$. We compute the quotient

$$U_2 := y^2\langle y(x^2 + x), y^2\rangle :_A \langle y(x^2 + x), y^2\rangle = \langle y^2, y(x^3 + 3x^2 + 2x)\rangle.$$

Now we have $yU_1 = U_2$, and thus A_1 was already normal and isomorphic to the normalization of A. Therefore, the normalization $\overline{A'}$ equals $1/y \cdot \langle y, x^3 + 3x^2 + 2x\rangle_{A'} = 1/y \cdot \langle y, x\rangle_{A'}$, as before.

Remark 5.5.2. In the previous example, using the first method yields simpler test ideals and quotients. However, our experience is that in general, computations with non-global orderings are often slower than computations with global orderings, and therefore the second method should be preferred at least if the input ideal is prime. On the other hand the computation should be faster with the first method if the ideal, or its Jacobian ideal, has complicated components which vanish in the localization.

5.6 Normalization via localization

As suggested in last section, local computations can sometimes reduce the problem to a simpler one. This motivates a local-global approach for computing the normalization of a ring that we propose in this section. Our starting point for combining local results is the following result:

Proposition 5.6.1. *Let A be a reduced Noetherian ring and set* $\mathrm{Sing}(A) = \{P_1, \ldots, P_s\}$ *the singular locus. Let $S_i = A \setminus P_i$, $1 \leq i \leq s$, and suppose that an intermediate ring $A \subseteq A^{(i)} \subset \overline{A}$ is given such that $S_i^{-1}A^{(i)} = \overline{S_i^{-1}A}$ for $1 \leq i \leq s$. Then*

$$\sum_{i=1}^{s} A^{(i)} = \overline{A}.$$

Proof. By construction, $B := \sum_{i=1}^{s} A^{(i)} \subset \overline{A}$. We wish to show equality. It suffices to show that if $P \in \mathrm{Spec}(A)$ is a prime ideal and $S = A \setminus P$, then $S^{-1}B = S^{-1}\overline{A}$. If $P \in \mathrm{Sing}(A)$, then $P = P_i$ for some i, and the local equality is obtained from the chain of inclusions

$$S_i^{-1}A^{(i)} \subseteq S_i^{-1}B \subseteq S_i^{-1}\overline{A} = \overline{S_i^{-1}A}.$$

Indeed, $S_i^{-1}A^{(i)} = \overline{S_i^{-1}A}$ by assumption. If $P \notin \mathrm{Sing}(A)$, then $S^{-1}A$ is normal, and the local equality follows likewise from the chain of inclusions

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

□

Definition 5.6.2. We call any ring $A^{(i)}$ as in Proposition 5.6.1 a *local contribution* to $\overline{A}$ at P_i.

If $P \in \mathrm{Sing}(A)$ is minimal with respect to inclusion, the modification of the Grauert and Remmert criterion below will allow us to find a local contribution to $\overline{A}$ at P along the lines of the global algorithm.

Proposition 5.6.3. *Let A be a reduced Noetherian ring, let $A \subseteq A'$ be a module-finite ring extension, let $P \in \mathrm{Sing}(A)$ be minimal with respect to inclusion, and let $J' = \sqrt{PA'}$. Suppose that P contains a non–zerodivisor p of A. If*

$$A' \cong \mathrm{Hom}_{A'}(J', J')$$

via the map which sends a' to multiplication by a', then the localization $S^{-1}A'$ is normal.

Proof. Since localization commutes with taking homomorphisms (see Eisenbud, 1995, Proposition 2.10), we get

$$S^{-1}A' \cong S^{-1}(\mathrm{Hom}_{A'}(J', J')) \cong \mathrm{Hom}_{S^{-1}A'}(S^{-1}J', S^{-1}J').$$

Hence, the result will follow from the Grauert and Remmert Criterion 5.1.13 applied to $S^{-1}A'$ once we show that the localized ideal $S^{-1}J'$ satisfies the three conditions of the criterion.

First, since taking radicals commutes with localization, $S^{-1}J'$ is a radical ideal. Second, the image of p in $S^{-1}A'$ is a non–zerodivisor on $S^{-1}A'$ contained in $S^{-1}J'$. Third, we show that $V(\mathcal{C}_{S^{-1}A'}) = N(S^{-1}A') \subseteq V(S^{-1}J'_P)$. For this, we first note that by the minimality assumption on P, we have $V(\mathcal{C}_{S^{-1}A}) = N(S^{-1}A) = \{S^{-1}P\}$ since prime ideals in $S^{-1}A$ correspond to prime ideals in A contained in P. Let now $Q \in N(S^{-1}A')$. Then, as mentioned in the proof of Lemma 5.2.2, Q contracts to P in A. This implies that

$$Q \supseteq \sqrt{(S^{-1}P)(S^{-1}A')} = \sqrt{S^{-1}(PA')} = S^{-1}(\sqrt{PA'}) = S^{-1}J',$$

as desired. □

In the situation of the proposition, suppose that we know a non–zerodivisor of A, $p \in P$. Then, we may use P together with p instead of a test pair as in Definition 5.1.14. Proceeding as in Section 5.3, we get a chain of rings

$$A \subseteq A_1 \subset \cdots \subseteq A_m \subset \overline{A}$$

such that $S^{-1}(A_m)$ is normal and, hence, equal to $S^{-1}\overline{A} = \overline{S^{-1}A}$.

Adding up, we are lead to Algorithms 5.6.1 and 5.6.2 below.

Algorithm 5.6.1 Local contribution to the normalization

Input: An affine domain $A = k[x_1, \ldots, x_n]/I$ over a perfect field k and a prime ideal $P \in \mathrm{Sing}(A)$ which is minimal with respect to inclusion.
Output: $U \subseteq A$ ideal and $d \in A$ with $1/d \cdot U \subset \overline{A}$ and $S^{-1}(1/d \cdot U) = \overline{S^{-1}A}$.
1: Choose $0 \neq p \in P$
2: **return** the result of Algorithm 5.3.3 applied to (P, p).

Algorithm 5.6.2 Normalization via localization

Input: An affine domain $A = k[x_1, \ldots, x_n]/I$ over a perfect field k such that there are no strict inclusions between the prime ideals in $\mathrm{Sing}(A)$.
Output: $U \subseteq A$ ideal and $d \in A$ such that $\overline{A} = 1/d \cdot U \subseteq Q(A)$.
1: $J := \sqrt{M}$, where M is the Jacobian ideal of I
2: Choose $0 \neq p \in J$
3: Compute $\mathrm{Sing}(A) = \{P_1, \ldots, P_s\}$ by decomposing J
4: **for all** P_i **do**
5: Apply Algorithm 5.6.1 using the test pair (P_i, p) to find ideals $U_i \subseteq A$ and powers $d_i = p^{m_i}$ with $A \subseteq 1/d_i \cdot U_i \subset \overline{A}$ and $S^{-1}(1/d_i \cdot U_i) = \overline{S^{-1}A}$
6: **end for**
7: $m := \max\{m_1, \ldots, m_s\}$, $d := p^m$, $U := \sum_i p^{m-m_i} U_i$
8: **return** (U, d).

Remark 5.6.4. In Algorithm 5.6.2, it may be more efficient to choose test pairs (P_i, p_i), with possibly different non–zero elements $p_i \in P_i$. The algorithm computes, then, pairs (U_i', d_i) with ideals $U_i' \subseteq A$ and powers $d_i = p_i^{m_i}$. As explained in Remark 5.3.3, we can always find a denominator $d \in M$ and ideals $U_i \subseteq A$ such that $1/d \cdot U_i = 1/d_i \cdot U_i'$ for all i. Hence, the desired result is $(\sum_i U_i, d)$.

Example 5.6.5. We come back to the coordinate ring A of the curve C defined by $f(X,Y) = X^5 - Y^2(Y-1)^3$ from Example 5.3.6 to discuss normalization via localization. The curve C has a double point of type A_4 at $(0,0)$ and a triple point of type E_8 at $(0,1)$. We illustrate Algorithm 5.6.2 in two ways:

(1) First, we use for both singular points the non–zerodivisor $p = x$. For the A_4-singularity, consider

$$P_1 = \langle x, y \rangle_A \quad \text{and} \quad S_1 = A \setminus P_1.$$

The local normalization algorithm yields $\overline{S_1^{-1}A} = S_1^{-1}\left(\frac{1}{d_1}U_1\right)$, where

$$d_1 = x^2 \quad \text{and} \quad U_1 = \left\langle x^2,\ y(y-1)^3 \right\rangle_A.$$

For the E_8 singularity, considering

$$P_2 = \langle x, y-1 \rangle_A \quad \text{and} \quad S_2 = A \setminus P_2,$$

we get $\overline{S_2^{-1}A} = S_2^{-1}\left(\frac{1}{d_2}U_2\right)$, where

$$d_2 = x^3 \quad \text{and} \quad U_2 = \left\langle x^3,\ x^2y^2\,(y-1),\ y^2\,(y-1)^2 \right\rangle_A.$$

Combining the local contributions, we get

$$\frac{1}{d}U = \frac{1}{d_1}U_1 + \frac{1}{d_2}U_2$$

with $d = x^3$ and

$$U = \left\langle x^3,\ xy(y-1)^3,\ x^2y^2\,(y-1),\ y^2\,(y-1)^2 \right\rangle_A.$$

A moments thought shows that U coincides with the ideal $U^{(3)}$ computed in Example 5.3.6.

(2) Now we choose $p_1 = y \in P_1$ and $p_2 = y - 1 \in P_2$. Then the normalization algorithm yields $\overline{A_{P_i}} = \frac{1}{d_i}(U_i)_{P_i}$, with

$$\begin{array}{lll} d_1 = y & \text{and} & U_1 = \langle y,\ x^3 \rangle_A, \\ d_2 = (y-1)^2 & \text{and} & U_2 = \left\langle (y-1)^2,\ x^2\,(y-1),\ x^4 \right\rangle_A. \end{array}$$

Combining the local contributions, we get $\overline{A} = \frac{1}{d}U$ with

$$\begin{array}{l} d = y\,(y-1)^2 \quad \text{and} \\ U = \left\langle y\,(y-1)^2,\ x^2y\,(y-1),\ x^3\,(y-1)^2,\ x^4y \right\rangle_A. \end{array}$$

One easily checks that both representations describe the same ring.

The approach presented in this section implies a big improvement in the normalization algorithm for the special case of curves in the plane. Moreover, in this case we can combine the local approach with a special algorithm for computing the normalization of curves which we present in Chapter 7. The performance of this approach will be analyzed in that chapter.

Chapter 6

Applications of the normalization and related tasks

6.1 Integral closure of ideals

A direct application of the normalization of rings is the computation of the integral closure of an ideal, which we explain in this section.

6.1.1 Preliminaries

Let I be an ideal in a ring R. Recall from Section 2.2.3 that an element $r \in R$ is called integral if it satisfies an integral dependence equation $r^s + a_1 r^{s-1} + a_2 r^{s-2} + \cdots + a_{s-1} r + a_s = 0$, with $a_i \in I^i$, $1 \leq i \leq s$. The integral closure of I, $\bar{I}$, is the set of all integral elements of R over I.

Example 6.1.1. Let $I = \langle x^3, y^3 \rangle \subset \mathbb{Q}[x, y]$. The polynomial xy^2 satisfies the integral dependence equation

$$(xy^2)^3 - x^3 y^6 = 0,$$

where $x^3 y^6 = x^3 y^3 y^3 \in I^3$, and therefore xy^2 is integral over I.

Note that computing the integral closure of I is not equivalent to computing the normalization of the ring R/I. For example, a radical ideal is always integrally closed.

Lemma 6.1.2. *If $r \in \bar{I}$, then $r \in \sqrt{I}$.*

Proof. If $r^n + a_1 r^{n-1} + a_2 r^{n-2} + \cdots + a_{n-1} r + a_n = 0$, with $a_i \in I^i$, $1 \leq i \leq n$, in particular $a_i \in I$ for all $1 \leq i \leq n$. Therefore $r^n \in I$ and $r \in \sqrt{I}$. □

However, there is a relation between the integral closure of ideals and the normalization of rings, via the Rees algebra of I,

$$R[It] = \bigoplus_{n \geq 0} I^n t^n = \left\{ \sum_{i=0}^{n} a_i t^i \mid n \in \mathbb{N}, a_i \in I^i \right\} \subset R[t].$$

Proposition 6.1.3. *Let R be a ring and t a free variable over R. For any ideal I in R, the integral closure of $R[It]$ in $R[t]$ equals the graded ring*

$$R \oplus \bar{I}t \oplus \overline{I^2}t^2 \oplus \overline{I^3}t^3 \oplus \dots$$

That is, the integral closure of I is the component of degree 1 of the integral closure of $R[It]$ in $R[t]$. We are interested in the case $R = k[x_1, \dots, x_n]$. In this situation, $R[t]$ is integrally closed in $Q(R[t])$ and since $Q(R[t]) = Q(R[It])$, we conclude that the integral closure of $R[It]$ in $R[t]$ is exactly the normalization of $R[It]$. We can therefore apply the normalization algorithms studied in Chapter 5 to compute the integral closure of an ideal.

6.1.2 Algorithm

Given an ideal $I \subset R$, to compute the normalization of the Rees algebra $R[It]$ we must first present it as a ring of the form S/J, S a polynomial ring and $J \subset S$ an ideal.

We use the following general result:

Proposition 6.1.4. *Let R be a ring and $p_1, \dots, p_s$ elements of R. Let $t_1, \dots, t_s$ be new free variables. Consider the morphism $\varphi : R[t_1, \dots, t_s] \to R$, $\varphi(t_i) = p_i$. Then*

$$R[p_1, \dots, p_s] \cong R[t_1, \dots, t_s]/\ker(\varphi).$$

In our case, given $I = \langle f_1, \dots, f_s \rangle$, we take $\varphi : R[t_1, \dots, t_s] \to R[t]$, $\varphi(t_i) = f_i t$, $1 \leq i \leq s$. Let $S = R[t_1, \dots, t_s]$ and $K = \ker(\varphi)$. We can apply Algorithm 5.3.3 to compute the normalization of $R[It] \cong S/K$. We obtain $d \in S$ and $U \subset S$ such that $\overline{S/K} = \dfrac{1}{d}U \subset Q(S/K)$.

That is, if $U = \langle u_1, \dots, u_m \rangle$, then u_j/d, $1 \leq j \leq m$, generate the normalization of S/K and $\tilde{u}_j = u_j(f_1 t, \dots, f_s t)/d(f_1 t, \dots, f_s t)$, $1 \leq j \leq m$, generate the integral closure of $R[It]$ in $Q(R[t])$ as an $R[It]$-ring. Recall that the integral closure of $R[It]$ in $Q(R[t])$ is actually included in $R[t]$. This means that $\mathcal{U} = \{\tilde{u}_1, \dots, \tilde{u}_m\} \subset R[t]$.

Example 6.1.5. The Rees algebra of $I = \langle x^3, y^3 \rangle \subset \mathbb{Q}[x, y]$ is

$$\mathbb{Q}[x, y][x^3 t, y^3 t] \cong \mathbb{Q}[x, y, z_1, z_2]/\langle y^3 z_1 - x^3 z_2 \rangle.$$

Here, z_1 represents $x^3 t$ and z_2 represents $y^3 t$.

The last step is to compute the component of t–degree 1 of the integral closure. It is generated by all the elements of t–degree 1 in $\mathcal{U}$ and all the elements $\tilde{u}p$ where $\tilde{u} \in \mathcal{U}$ is an element of t–degree 0 and $p \in \{f_1 t, \dots, f_s t\}$. However, since the component of degree 0 is R, we always add $\{f_1 t, \dots, f_s t\}$ to the generators.

Example 6.1.6. The normalization of $\mathbb{Q}[x, y, z_1, z_2]/\langle y^3 z_1 - x^3 z_2 \rangle$ is

$$\frac{1}{y^2}\langle xyz_2, x^2 z_2, y^2 \rangle.$$

Replacing z_2 by y^3t and simplifying the denominator, we get the ring generators $\{xy^2t, x^2yt, 1\}$. The component of degree 1 is $\langle xy^2t, x^2yt, x^3t, y^3t\rangle$ and therefore, the integral closure of I is $\langle x^3, x^2y, xy^2, y^3\rangle$.

In Algorithm 6.1.1 we summarize the steps for computing the integral closure of an ideal.

Algorithm 6.1.1 Integral closure of an ideal

Input: $I = \langle f_1, \ldots, f_s\rangle \subset R$, an ideal, with $R = k[x_1, \ldots, x_n]$, with k a perfect field.

Output: $\bar{I}$, the integral closure of I.

1: Set $S = R[t_1, \ldots, t_s]$
2: Compute K, the kernel of the map $\varphi : S \to R[t]$, $t_i \mapsto f_it$
3: Using Algorithm 5.3.3, compute $d \in S$ and $U = \langle u_1, \ldots, u_m\rangle \subset S$ such that $\overline{S/K} = \frac{1}{d}U \subset Q(S/K)$
4: Compute $\mathcal{U} = \{\tilde{u}_1, \ldots, \tilde{u}_m\}$, where $\tilde{u}_j = u_j(f_1t, \ldots, f_st)/d(f_1t, \ldots, f_st) \in R[t]$, $1 \leq j \leq m$
5: Set $\mathcal{U}_0 = \{\tilde{u} \in \mathcal{U} \text{ s.t. } \deg_t(\tilde{u}) = 0\}$ and $\mathcal{U}_1 = \{\tilde{u} \in \mathcal{U} \text{ s.t. } \deg_t(\tilde{u}) = 1\}$
6: Set $\mathcal{N} = \{\tilde{u}f_i : \tilde{u} \in \mathcal{U}_0, 1 \leq i \leq s\} \cup \{\tilde{u}/t : \tilde{u} \in \mathcal{U}_1\}$
7: **return** $\mathcal{N}$.

6.1.3 Performance evaluation

We apply the proposed algorithm to several examples. The algorithm is implemented in SINGULAR. We compare the timings with the procedure available in the SINGULAR library `reesclos` (Hirsch, 2001), that uses an independent implementation of (Decker et al., 1999a) algorithm.

We use the following examples:

- $I_1 = \langle x^{12}, y^{12}\rangle \subset k[x, y]$.
- $I_2 = \langle x^5, y^5, z^5\rangle \subset k[x, y, z]$.
- $I_3 = \langle x^2 + xy^3 - 5z, z^3 + y^2 - xzy, x^2y^3z^5 + y^3 - y^5\rangle \subset k[x, y, z]$.
- $I_4 = \langle yz^2, y^3 + z^3 - z^2, xz^2, xy^2 + z^2\rangle \subset k[x, y, z]$.
- $I_5 = \langle x^4, y^2 + x^2, z^3 + x^3\rangle \subset k[x, y, z]$.
- $I_6 = \langle x^4, y^2 + x^3, z^5 + x^3\rangle \subset k[x, y, z]$.

The results are shown in Table 4.1. All the computations are done over $\mathbb{Q}$. The ordering of the monomials is always the degree reverse lexicographical ordering with the underlying ordering of the alphabet.

Timing is measured in seconds. The entry * means that after three hours of computations, the algorithm did not terminate.

Table 6.1: Timing results

Code	New	Old
I_1	182	459
I_2	1	5
I_3	20	*
I_4	0	0
I_5	3	1
I_6	68	*

We see that for time consuming computations, our proposed algorithm is always faster.

Although the simple examples shown here were feasible for the new algorithm, computing the integral closure of an ideal is usually very hard, since the ideal of relations appearing in the construction of the Rees algebra can be quite big. There is a need to find direct algorithms that do not use the Rees algebra as an intermediate step. However, no such algorithm is known for the general case. For the case of monomial ideals, the problem is much easier and very fast and simple algorithms are known, based on combinatorial techniques, see for example (Swanson and Huneke, 2006, Section 1.4).

6.2 Integral bases via normalization

Another important application of the normalization algorithms is to compute *integral bases*. The content of this section is part of a joint work (in progress) with Janko Böhm, Wolfram Decker and Frank Seelisch, presented in (Böhm et al., 2012a).

6.2.1 Basic definitions

As usual, given a ring A, we write $\overline{A}$ for the normalization and call A *normal* if $A = \overline{A}$. In this section, we are mainly interested in the case where A is the coordinate ring of an algebraic curve defined over a field k of characteristic zero. More precisely, let $f \in k[x, y]$ be an irreducible polynomial in two variables, let $C \subset \mathbb{A}^2(\bar{k})$ be the affine plane curve defined by f, and let

$$A = k[C] = k[x, y]/\langle f(x, y)\rangle$$

be the coordinate ring of C. We write $\bar{x}$ and $\bar{y}$ for the residue classes of x and y in A. Throughout the paper, we suppose that f is monic in y (due to Noether normalization, this can always be achieved by a linear change of coordinates). Then the function field of C is of type

$$k(C) = \mathrm{Q}(A) = k(\bar{x}, \bar{y}) = k(x)[y]/\langle f(x, y)\rangle,$$

$\bar{x}$ is a separating transcendence basis of $k(C)$ over k, and $\bar{y}$ is integral over $k[\bar{x}]$, with integral equation $f(\bar{x}, \bar{y}) = 0$.

From now on we will use x and y instead of $\bar{x}$ and $\bar{y}$, as no confusion will arise.

The ring A is integral over $k[x]$, which implies that $\overline{A}$ coincides with the integral closure $\overline{k[x]}$ of $k[x]$ in $k(C)$. Furthermore, $\overline{A} = \overline{k[x]}$ is a free $k[x]$-module of rank

$$n := \deg(f) = [k(C) : k(x)].$$

Definition 6.2.1. An *integral basis* for $\overline{A}$ is a set $b_0, \ldots, b_{n-1}$ of free generators of $\overline{A}$ over $k[x]$:

$$\overline{A} = k[x]b_0 \oplus \cdots \oplus k[x]b_{n-1}.$$

Remark 6.2.2. Viewing the elements of $k(C)$ as polynomials in y of degree $< n$, there always exists an integral basis $b_0, \ldots, b_{n-1}$ such that $\deg(b_i) = i$ for all i. In fact, as pointed out in (van Hoeij, 1994), such a basis can be obtained from any given integral basis by means of Gaussian elimination.

6.2.2 Algorithm

Given $A = k[x, y]/\langle f \rangle$, with $f \in k[x, y]$ irreducible, we explain how to obtain an integral basis of $\overline{A}$ from the output of the normalization algorithms.

The basic idea is to multiply the generators of the normalization $\overline{A}$ by suitable powers of y to get a system of generators of $\overline{A}$ over $k[x]$, and then eliminate the redundant elements.

Applying to A the normalization algorithm described in Chapter 5, we can compute $f_1, \ldots, f_s \in Q(A)$ such that

$$\overline{A} = Af_1 + \cdots + Af_s.$$

with $f_1 = \dfrac{p_1}{q}, \ldots, f_{s-1} = \dfrac{p_{s-1}}{q}, f_s = \dfrac{q}{q} = 1$ and q a power of a polynomial in the radical of the singular locus of $\langle f \rangle$.

We need to compute an integral basis of $\overline{k[x]}$ from the elements $f_1, \ldots, f_s$.

Without further requirements, we can use as basis $y^i f_j(x, y)$, $0 \leq i \leq n-1$, $1 \leq j \leq s$. To get an integral basis as described earlier (one generator of each degree in y), we need to reduce the system of generator and eliminate the redundant elements.

Before giving the details of the algorithm, we show an example.

Example 6.2.3. Let $A = k[x, y]/\langle y^3 - x^2 \rangle$. The output of the normalization algorithm is $\overline{A} = A\dfrac{y^2}{x} + A$.

If we want to generate $\overline{A}$ as a $k[x]$-module, we get

$$\overline{A} = k[x]\frac{y^2}{x} + k[x]\frac{y^3}{x} + k[x]\frac{y^4}{x} + k[x] + k[x]y + k[x]y^2.$$

Note that $y^3 = x^2$, and $k[x]y^2 \subset k[x]\dfrac{y^2}{x}$. Therefore

$$\overline{A} = k[x]\frac{y^2}{x} + k[x] + k[x]y,$$

and $1, y, \dfrac{y^2}{x}$ is the integral basis.

Note that since the singular locus is 0–dimensional, we can always take q as a polynomial in x.

To do the reduction systematically, let A be a ring as before and $p_1, \ldots, p_s$ the numerators of a system of generators of the normalization. We write $p_i = a_{i,n-1}y^{n-1} + \cdots + a_{i,1}y + a_{i,0}$, $a_{i,j} \in k[x]$, $1 \leq i \leq s$, and construct the matrix of coefficients

$$M = \begin{pmatrix} a_{1,n-1} & \ldots & a_{1,0} \\ \vdots & \ddots & \vdots \\ a_{s,n-1} & \ldots & a_{s,0} \end{pmatrix}.$$

The entries of M are polynomials in $k[x]$, a principal ideal domain (PID). By the same algorithm used to compute the Smith normal form of a matrix (Smith, 1861), we can triangulate the matrix M in such a way that the rows of the output matrix generate the same space as the rows of M. (The algorithm to compute the Smith normal form is a generalization of Gaussian elimination.) The non–zero rows of the output matrix are therefore the coefficients of the basis we are looking for. We get Algorithm 6.2.1.

Algorithm 6.2.1 Integral basis from normalization

Input: $f \in k[x, y]$, an irreducible polynomial of degree n in y.
Output: $b_0, \ldots, b_{n-1}$, an integral basis of $k[x, y]/\langle f \rangle$.

1: Applying Algorithm 5.3.3, compute polynomials $p_1, \ldots, p_s, q \in k[x, y]$ such that $\overline{A} = \frac{1}{q}\langle p_1, \ldots, p_s \rangle_A$
2: Write $p_i = a_{i,n-1}y^{n-1} + \cdots + a_{i,1}y + a_{i,0}$, $1 \leq i \leq s$) and define

$$A = \begin{pmatrix} a_{1,n-1} & \ldots & a_{1,0} \\ \vdots & \ddots & \vdots \\ a_{s,n-1} & \ldots & a_{s,0} \end{pmatrix}$$

3: Apply Smith normal form algorithm to compute an upper triangular matrix B such that the rows of B generate the same module as the rows of A
4: **return** $b_{n-1}, \ldots, b_1, b_0$, the rows of $\frac{1}{q}B[y^{n-1} \ldots y\ 1]^t$.

We note that in general the polynomials in the output of the normalization algorithm are already monic as polynomials in y. In that case we can apply Gaussian elimination directly.

In Chapter 7 we will compare this algorithm with a special method for computing integral bases.

6.3 Criteria for integral dependence

Computing the normalization of a ring or an ideal is not always feasible using the known algorithms. In many cases, however, we are only interested in deciding whether a given element belongs to the normalization of a ring or the integral closure of an ideal, and in that case, to know an integral dependence equation. In this section, we propose algorithms for that tasks.

6.3.1 Integral dependence over rings

As usual, we take $R = k[x_1, \ldots, x_n]$, $I \subseteq R$ an ideal and $A = R/I$. We note $Q(A)$ the total ring of fractions of A, $Q(A) = S^{-1}A$, where S is the set of non–zerodivisors of A. For an element $p \in R$, we denote also by p its image in A.

We first mention a criterion of integral dependence given in (Decker et al., 2011, Section 3.1).

Lemma 6.3.1. *Let b, $g_1, \ldots, g_r \in R$, $I = \langle f_1, \ldots, f_s \rangle \subset R$ and $t, y_1, \ldots, y_r$ new variables. Consider the ideal*

$$J = \langle t - b, y_1 - g_1, \ldots, y_r - g_r, f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n, t, y_1, \ldots, y_r].$$

Let $>$ be an ordering in $k[x_1, \ldots, x_n, t, y_1, \ldots, y_r]$ with $x_i \gg t \gg y_j$, $1 \leq i \leq n$, $1 \leq j \leq r$, and let G be a Gröbner basis of J with respect to this ordering. Then b is integral over $k[g_1, \ldots, g_r]/I$ if and only if G contains an element g with leading monomial $\mathrm{lm}(g) = t^p$ for some $p > 0$.

That is, given the ring extension $k[g_1, \ldots, g_s]/I \hookrightarrow k[\boldsymbol{x}]/I$, we can check whether an element of the second ring is integral over the first one.

Since $Q(A)$ is not a finitely generated A-algebra, this criterion cannot be used directly to check whether an element of $Q(A)$ belongs to the normalization of A. In the next lemma, we propose a criterion for that task.

Lemma 6.3.2. *Let $I = \langle f_1, \ldots, f_s \rangle \subset R = k[\boldsymbol{x}]$ and $A = R/I$. Let $r = p/q \in Q(A)$, with $p, q \in R$ and $R' = k[\boldsymbol{x}, t]$, t a new variable. Then*

$$r \in \overline{A} \iff 1 \in (\langle I, pt - q \rangle : p^\infty) + \langle t \rangle \subset R'$$

Proof. Assume $r \in \overline{A}$. Then r satisfies an equation

$$r^m + a_1 r^{m-1} + \cdots + a_m = 0, \quad a_i \in R$$

in $Q(A)$. Hence $q^m(p^m + a_1 p^{m-1} q + \cdots + a_m q^m) = 0$ in A. Since q is a non–zerodivisor, we obtain

$$p^m + a_1 p^{m-1} q + \cdots + a_m q^m \in I.$$

Therefore,

$$p^m + a_1 p^m t + \cdots + a_m p^m t^m \in \langle I, pt - q \rangle,$$

which implies

$$1 + a_1 t + \cdots + a_m t^m \in \langle I, pt - q\rangle : p^\infty.$$

This proves that $1 \in (\langle I, pt - q\rangle : p^\infty) + \langle t\rangle$.

Conversely, assume $1 = g + \alpha t$, with $g \in \langle I, pt - q\rangle : p^\infty$ and $\alpha \in R'$. Then $p^m = h + \alpha p^m t$, for $m \in \mathbb{N}$ large enough and $h \in \langle I, pt - q\rangle$.

Replacing t by q/p, we obtain

$$p^m = \left(\sum_{i=1}^{s} \beta_i(x, q/p) f_i(x)\right) + \alpha(x, q/p) p^{m-1} q,$$

for some $\beta_i \in R'$. Assuming m greater than the degrees in t of α and β_i, $1 \leq i \leq s$, so that the denominators cancel,

$$p^m = \left(\sum_{i=1}^{s} \beta_i'(x, q) f_i(x)\right) + \alpha(x, q/p) p^{m-1} q,$$

and therefore

$$p^m - \alpha(x, q/p) p^{m-1} q = \sum_{i=1}^{s} \beta_i'(x, q) f_i(x) \in I.$$

Expanding α, we conclude that

$$p^m + a_1 p^{m-1} q + \cdots + a_m q^m \in I,$$

for some $a_i \in R$, as needed. □

Example 6.3.3. Let $I = \langle x^2 - y^3\rangle \subset R = k[x, y]$, and $A = R/I$. We check if $\frac{x}{y} \in \overline{A}$. Computing the saturation $S = \langle I, xt - y\rangle : x^\infty$, we find that $yt^2 - 1 \in S$ and $(yt^2 - 1)x^2 \in \langle I, xt - y\rangle$. Therefore $\frac{x}{y} \in \overline{A}$, and replacing t by y/x, we get the equation $(\frac{x}{y})^2 - y = 0$ in A.

Since there are no other implementations of integral dependence criteria, instead of showing timings comparisons, we show how this criterion can be used to find integral elements, when the normalization algorithm is too slow.

Example 6.3.4. Let $f = (y^2 + x^2y^2 + 2x^5)(y^3 + 7z^5)(z^3 + 2x^4) + x^3y^3z^3 \in R = \mathbb{Q}[x, y, z]$. If we apply the normalization algorithm to $R/\langle f\rangle$, it does not finish after two hours of computation. A common technique is to consider the problem in the ring of polynomials over a prime field. For example, if we consider $S = \mathbb{Z}_{32003}[x, y, z]$, the normalization of $S/\langle f\rangle$ takes 2 seconds, and gives the output

$$\left\langle 1, \frac{2x^7y + x^4y^3 + x^2y^3}{z}, \frac{2x^7z^2 + x^3z^5}{y}, \frac{2x^8y^2 + x^5y^4 + x^3y^4}{z^2}, \frac{2x^9y^2 + x^6y^4 + x^4y^4}{z^3}\right\rangle_{S/\langle f\rangle}$$

In principle, these elements considered as elements of $Q(R/\langle f\rangle)$ need not be integral over $R/\langle f\rangle$, but we can test it using the criterion. In this example, the test is fast, giving a positive answer for all the generators in a few seconds.

6.3.2 Integral dependence over ideals

The same idea can be used to check if a polynomial r belongs to the integral closure of an ideal $I \subset R = k[x_1, \ldots, x_n]$.

The criterion is based on the next lemma, which can be deduced from the proof of (Swanson and Huneke, 2006, Proposition 6.8.2).

Lemma 6.3.5. *Let $I \subset R$ be an ideal and $r \in I$ a polynomial. Then $r \in \bar{I}$ iff $1 \in \frac{I}{r}R[\frac{I}{r}]$, where $R[\frac{I}{r}]$ is the ring generated over R by the elements $\frac{x}{r}$, $x \in I$.*

Proof. If $1 \in \frac{I}{r}R[\frac{I}{r}]$, we can write

$$1 = \sum_{i=1}^{m} \frac{a_i}{r^i},$$

for some $a_i \in I^i$. Multiplying this equation by r^m yields an equation of integral dependence of r over I of degree m, so that r is integral over I.

Conversely, if $r \in \bar{I}$, r satisfies an equation

$$r^m = a_1 r^{m-1} + \cdots + a_{m-1} r + a_m, \quad a_i \in I^i.$$

Dividing by r^m,

$$1 = \frac{a_1}{r} + \cdots + \frac{a_{m-1}}{r^{m-1}} + \frac{a_m}{r^m}, \quad a_i \in I^i.$$

Writing each a_i as polynomial combination of the generators of I^i, we obtain that each $\frac{a_i}{r^i} \in \frac{I}{r}R[\frac{I}{r}]$. Therefore, $1 \in \frac{I}{r}R[\frac{I}{r}]$. □

We obtain the following criterion.

Lemma 6.3.6. *Let $I = \langle f_1, \ldots, f_s \rangle \subset R$ be an ideal and $R' = R[t_1, \ldots, t_s]$, with t_j, $1 \leq j \leq s$, new variables. For $r \in R$, set $J = \langle t_1 r - f_1, \ldots, t_s r - f_s \rangle$. Then*

$$r \in \bar{I} \iff 1 \in (J : r^\infty) + \langle t_1, \ldots, t_s \rangle.$$

Proof. Assume $r \in \bar{I}$. Then r satisfies a relation

$$r^m + a_1 r^{m-1} + \cdots + a_m = 0, \quad a_i \in I^i.$$

We can consider each a_i as an homogeneous polynomial $A_i \in R[z_1, \ldots, z_s]$ of degree i, evaluated in $(f_1, \ldots, f_s)$. Since $t_j r - f_j \in J$ for all j, $1 \leq j \leq s$,

$$r^m + A_1(t_1 r, \ldots, t_s r) r^{m-1} + \cdots + A_{m-1}(t_1 r, \ldots, t_s r) r + A_m(t_1 r, \ldots, t_s r) \in J.$$

Then

$$r^m + A_1(t_1, \ldots, t_s) r^m + \cdots + A_{m-1}(t_1, \ldots, t_s) r^m + A_m(t_1, \ldots, t_s) r^m \in J,$$

and

$$1 + A_1(t_1, \ldots, t_s) + \cdots + A_{m-1}(t_1, \ldots, t_s) + A_m(t_1, \ldots, t_s) \in J : r^\infty.$$

This implies

$$1 \in (J : r^\infty) + \langle t_1, \ldots, t_s \rangle$$

as claimed.

Conversely, assume $1 = g + \sum_{j=1}^{s} \alpha_j t_j$ with $\alpha_j \in R'$ and $g \in J : r^\infty$. Then, there exists m_0 such that $gr^m \in J$ for $m \geq m_0$. For any such m, $r^m = h + \sum_{i=j}^{s} \alpha_j t_j r^m$, for $m \in \mathbb{N}$ large enough and some $h \in J$.

Replacing t_j by f_j/r, the polynomial h vanishes and we obtain

$$r^m = \sum_{j=1}^{s} \alpha_j(\boldsymbol{x}, f_1/r, \ldots, f_s/r) f_j r^{m-1}.$$

We can always take m greater than the degree in the variables $\{t_1, \ldots, t_s\}$ of the polynomials α_j, and so

$$\alpha_j(\boldsymbol{x}, f_1/r, \ldots, f_s/r) f_j r^{m-1} = \sum_{i=1}^{m-1} \tilde{\alpha}_{ij}(\boldsymbol{x}) r^{m-i},$$

for some $\tilde{\alpha}_{ij} \in I^i$

Grouping together all the powers of r with the same exponent, we obtain an equation of integral dependence of r over I,

$$r^m = a_1 r^{m-1} + \cdots + a_m, \quad a_i \in I^i.$$

□

Observation 6.3.7. The first criterion can be seen as a special case of the second. Indeed, p/q belongs to the normalization of R/I iff $p \in \overline{\langle q \rangle}$ in R.

Example 6.3.8. Let $I = \langle x^2, y^2, z^2 - xy \rangle$. We can easily compute $\sqrt{I} = \langle x, y, z \rangle$ and we want to find elements in $\sqrt{I}$ which are integral over I. We use the criterion to check if $r = zx \in \bar{I}$. We set $J = \langle t_1 xz - x^2, t_2 xz - y^2, t_3 xz - (z^2 - xy) \rangle$. Computing $J : r^\infty$, we find that $p = t_1^3 t_2 - t_1^2 t_3^2 + 2t_1 t_3 - 1 \in J : r^\infty$, and $pr^4 \in J$. Therefore, $r \in \bar{I}$, with integral equation

$$r^4 - 2(x^2)(z^2 - xy)r^2 + ((x^2)^2(z^2 - xy)^2 - (x^2)^3(y^2)) = 0$$

Chapter 7

Integral bases via Hensel's lemma

The content of this chapter is a joint work (in progress) with Janko Böhm, Wolfram Decker and Frank Seelisch, presented in (Böhm et al., 2012a).

In this section, we consider the coordinate ring

$$A = k[x, y]/\langle f(x, y)\rangle$$

of an irreducible plane curve C. We present a new algorithm to compute an integral basis of A via Puiseux expansions and Hensel's lemma. To simplify our presentation, we suppose first that C has only one singularity, located at the origin. At the end of the chapter, we will show how to handle the case of several singularities.

From a theoretical point of view, our approach is similar to (van Hoeij, 1994), where the Puiseux expansions of f over all the x-coordinates of singular points are computed, including those that do not pass through the singular point. However, the use of Hensel's lemma allows us to handle, in particular, groups of conjugate Puiseux expansions simultaneously without computing each individual expansion explicitly. In this way, we obtain a much faster algorithm.

7.1 Basic Remarks on Puiseux Series

We fix our notation and recall a few results in the context of Puiseux series.

7.1.1 Puiseux Series

As usual, let k be a field. We write $k[[x]]$ for the ring of formal power series in x over k and $k((x)) = Q(k[[x]])$, the field of formal Laurent series. The *field of Puiseux series* over k is the field

$$k\{\{x\}\} = \bigcup_{m=1}^{\infty} k((x^{1/m})).$$

Example 7.1.1. Let $\gamma, \delta \in \mathbb{Q}\{\{x\}\}$, $\gamma(x) = 3x^{-1/3} - 2x^{4/3} + \ldots$, $\delta = x^{1/2} + 2x^{2/2} + \ldots$ To compute the sum $\gamma + \delta$ we use a common denominator $\gamma + \delta = 3x^{-2/6} + x^{3/6} + 2x^{6/6} - 2x^{8/6} + \ldots$

If L is the algebraic closure of k, then $L\{\{x\}\}$ is the algebraic closure of $k((x))$ and $L[[x^{1/m}]]$ is the integral closure of $k[[x]]$ in $L((x^{1/m}))$ (see Eisenbud, 1995, Corollary 13.15).

We have a canonical *valuation map*

$$v : L\{\{x\}\} \setminus \{0\} \to \mathbb{Q},\ \gamma \mapsto v(\gamma),$$

where $v(\gamma)$ is the smallest exponent appearing in a term of γ. By convention, $v(0) = \infty$. If $p \in L\{\{x\}\}[y]$ is any polynomial in y with coefficients in $L\{\{x\}\}$, the *valuation* of p at $\gamma \in L\{\{x\}\}$ is defined to be $v_\gamma(p) := v(p(\gamma))$.

Since $L\{\{x\}\}$ is algebraically closed, a polynomial $f \in k[x, y] = k[x][y]$ has $n = \deg_y(f)$ roots $\gamma_1, \ldots, \gamma_n$ in $L\{\{x\}\}$. These roots are called the *Puiseux expansions* of f (at $x = 0$). We are interested in the case f monic in y, for which we have a factorization

$$f = (y - \gamma_1) \cdots (y - \gamma_n) \in L\{\{x\}\}[y].$$

It follows, that each γ_i is integral over $L[[x]]$ and, thus, contained in some $L[[x^{1/m}]]$. In other words, the terms of γ_i have only non–negative exponents. We denote $\mathcal{P}_x$ the subring of $L\{\{x\}\}$ of Puiseux series with non-negative valuation.

Definition 7.1.2 (Conjugate Puiseux series)**.** Two Puiseux series in $\mathcal{P}_x$ are called *conjugate* if they are conjugate as field elements over $k((x))$.

Definition 7.1.3 (Rational Part)**.** Let $\gamma = a_1x^{t_1} + a_2x^{t_2} + \cdots + a_lx^{t_l} + a_{l+1}x^{t_{l+1}} + \ldots$ be a Puiseux series in $\mathcal{P}_x$, with $0 \le t_1 < t_2 < \ldots$. For $1 \le i \le l$, suppose that $a_i \in k$ and $t_i \in \mathbb{Z}_{\ge 0}$. Furthermore, suppose that either $a_{l+1} \notin k$ or $t_{l+1} \notin \mathbb{Z}$. We call $a_1x^{t_1} + \cdots + a_lx^{t_l}$ the *rational part* of γ, and $a_{l+1}x^{t_{l+1}}$ the *first nonrational term* of γ.

Definition 7.1.4 (Characteristic exponents)**.** For $\gamma \in \mathcal{P}_x$, let $m \in \mathbb{N}$ be minimal with $\gamma \in L[[x^{1/m}]]$, and write $\gamma = \sum_{i \ge 0} b_i x^{i/m}$, with coefficients $b_i \in L$. If $m \ge 2$, the *characteristic exponents* of γ are defined inductively by

$$\begin{aligned} e_1 &:= \min\{i \mid b_i \neq 0 \text{ and } m \nmid i\} \text{ and} \\ e_\nu &:= \min\{i \mid b_i \neq 0,\ \gcd(e_1, \ldots, e_{\nu-1}) \nmid i\} \text{ for } \nu > 1. \end{aligned}$$

Then $e_1 < e_2 < \ldots$, there are only finitely e_ν, and they are coprime (but not necessarily pairwise coprime).

(If $m = 1$, there is no characteristic exponent.)

Example 7.1.5. If $\gamma = 2x^{1/2} + x^{3/4} + 6x^{5/4} - 5x^{17/8}$, the common denominator is $m = 8$. Writing $\gamma = 2x^{4/8} + x^{6/8} + 6x^{10/8} - 5x^{17/8}$, we see that the characteristic exponents are $e_1 = 4$, $e_2 = 6$, and $e_3 = 17$.

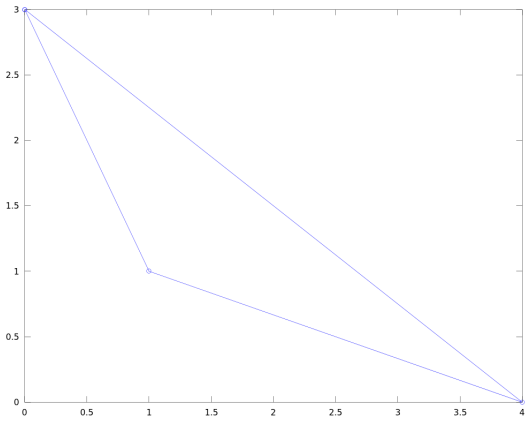

Figure 7.1: Newton polygon of $f = y^3 + xy + x^4$

Definition 7.1.6 (Regularity Index and Singular Part)**.** If $\gamma = a_1 x^{t_1} + a_2 x^{t_2} + \ldots$ is a Puiseux expansion of f, with $0 \leq t_1 < t_2 < \ldots$, we define the *regularity index* of γ to be the smallest exponent t_j such that no other Puiseux expansion of f has the same initial part $a_1 x^{t_1} + \cdots + a_j x^{t_j}$. This initial part is called the *singular part* of γ.

7.1.2 The Newton-Puiseux Algorithm

The Puiseux expansions of f can be computed recursively up to any given order using the Newton-Puiseux algorithm. A detailed description of the method, together with historical notes, can be found in (Brieskorn and Knorrer, 1986, Section 8.3). To present the basic ideas, we apply the method to an example.

Example 7.1.7. Let $f = y^3 + xy + x^4$. Since f has degree 3 in y, we can find Puiseux series γ, η, μ such that $f = (y-\gamma)(y-\eta)(y-\mu)$. We construct recursively a solution $\gamma \in \mathcal{P}_x$, which must verify the equation $f(x, \gamma(x)) = 0$. Taking $x = 0$ in the factorization, we see that γ has no constant term. We write

$$\gamma(x) = c_1 x^{t_1} + c_2 x^{t_2} + \ldots = c_1 x^{t_1} + \gamma_1(x).$$

with $c_j \neq 0$, $t_j \in \mathbb{Q}$, $t_j < t_{j+1}$ for all j, and $\gamma_1(x) \in \mathcal{P}_x$. After substitution, we get the equation

$$f(x, \gamma(x)) = x^4 + x(c_1 x^{t_1} + \gamma_1(x)) + (c_1 x^{t_1} + \gamma_1(x))^3 = 0.$$

We want the term of lowest degree to vanish, so we must choose t_1 such that at least two terms in the sum have the same initial exponent. To find the possible values of t_1 we consider the Newton polygon of the monomials of f and look at the faces for which all the other points of the polygon lie on or above the corresponding line (Figure 7.1).

If the slope of a face is s, a simple verification shows that $-1/s$ is a possible value of t_1. In our case, the slopes of the faces are -2 and $-1/3$ and therefore

the possible values of t_1 are $1/2$ and 3. We choose $t_1 = 1/3$ and replace it in the equation

$$f(x, \gamma(x)) = x^4 + x(c_1 x^{1/2} + \gamma_1(x)) + (c_1 x^{1/2} + \gamma_1(x))^3 = 0.$$

The term of lowest degree is $(c_1 + c_1^3)x^{3/2}$. We want the coefficient to be 0. Since $c_1 \neq 0$, we get $c_1 = \pm i$. If we choose $c_1 = i$, we get $\gamma = ix^{1/2} + \gamma_1$, and γ_1 can be computed recursively substituting y by this last expression in f. The Newton-Puiseux theorem (see Walker, 1950), guarantees that any initial part obtained by the Newton polygon method can be extended to a solution of $f(x, \gamma(x)) = 0$.

If we carry on the method for the different values of t_1 and c_1, we get the three solutions

$$\begin{aligned}
\gamma &= ix^{1/2} + 1/2x^3 + \dots \\
\eta &= -ix^{1/2} + 1/2x^3 + \dots \\
\mu &= -x^3 + x^8 + \dots
\end{aligned}$$

We note that in the process of building the solution, we need to extend the base field. Most computer algebra systems can handle field extensions, although it can be sometimes time-consuming.

7.1.3 Puiseux Blocks

We partition the set of all Puiseux expansions of f into *Puiseux blocks*. A Puiseux block represented by an expansion γ with $\gamma(0) = 0$ is obtained by collecting all expansions whose rational part agrees with that of γ and whose first nonrational term is conjugate to that of γ over $k((x))$. A *Puiseux segment* is by definition the union of all blocks having the same initial exponent. That is, we have one Puiseux segment for each face of the Newton polygon of f. In addition, all Puiseux expansions γ of f with $\gamma(0) \neq 0$ are grouped together to a single Puiseux block of an extra Puiseux segment. In this way, the Puiseux expansions of f are divided into Puiseux segments, each segment consists of Puiseux blocks, and each block is the union of classes of conjugate expansions.

Example 7.1.8. Let the Puiseux expansions of a given polynomial in $k[x][y]$ be

$$\begin{aligned}
\gamma_1 &= 1 + x^2 + \dots\ , & \gamma_6 &= x + b_1 x^{5/2} + x^3 + \dots\ , \\
\gamma_2 &= -1 + 3x + \dots\ , & \gamma_7 &= x + b_2 x^{5/2} + x^3 + \dots\ , \\
\gamma_3 &= a_1 x^{3/2} + 2x^2 + \dots\ , & \gamma_8 &= x + b_1 x^{5/2} + x^4 + \dots\ , \\
\gamma_4 &= a_2 x^{3/2} + 2x^2 + \dots\ , & \gamma_9 &= x + b_2 x^{5/2} + x^4 + \dots\ , \\
\gamma_5 &= x + 3x^2 + \dots\ ,
\end{aligned}$$

where a_i and b_i satisfy $a_i^2 = 2$ and $b_i^2 = -1$, $i = 1, 2$. Then $\{\gamma_1, \gamma_2\}$ is the segment of expansions γ with $\gamma(0) \neq 0$. Another segment is $\{\gamma_3, \gamma_4\}$ (which consists of one block containing a single class of conjugate expansions). All the other expansions form a single segment, consisting of the blocks $\{\gamma_5\}$ and $\{\gamma_6, \gamma_7, \gamma_8, \gamma_9\}$. The last block contains two classes of conjugate expansions, namely $\{\gamma_6, \gamma_7\}$ and $\{\gamma_8, \gamma_9\}$.

7.1.4 Maximal Integrality Exponents

Let $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ be the set of Puiseux expansions of f at $x = 0$ and let $p \in \mathcal{P}_x[y]$ be a polynomial in y with coefficients in the integrally closed field $\mathcal{P}_x$. The *valuation* of p at f is defined to be $v_f(p) = \min_{1 \le i \le n} v_{\gamma_i}(p)$. Note that if p is monic of degree $1 \le d := \deg(p) \le n-1$, and

$$p = (y - \eta_1(x)) \cdots (y - \eta_d(x)),\ \eta_i \in \mathcal{P}_x$$

is the factorization of p over $\mathcal{P}_x[y]$, then

$$v_f(p) = \min_{1 \le i \le n} \sum_{j=1}^{d} v(\gamma_i - \eta_j).$$

Lemma 7.1.9. *Let $p \in k[x,y] = k[x][y]$ be monic in y of degree d. Then $\lfloor v_f(p) \rfloor$ is the maximal exponent e such $p(x,y)/x^e$ is integral over $A = k[x,y]$. We call $\lfloor v_f(p) \rfloor$ the* integrality exponent *of p, written*

$$e(p) = \lfloor v_f(p) \rfloor.$$

Proof. See (van Hoeij, 1994, Section 2.4). □

To construct an integral basis, we can look for polynomials with maximal integrality exponent in each y-degree.

Lemma 7.1.10. *For $1 \le i \le n-1$, let $p_i \in k[x,y] = k[x][y]$ be monic in y of degree i. For each i, suppose that $e(p_i)$ is maximal among all $e(p)$, $p \in k[x][y]$ monic of degree i. Then $\{1, p_1(x,y)/x^{e(p_1)}, \ldots, p_{n-1}(x,y)/x^{e(p_{n-1})}\}$ is an integral basis of $\overline{A}$.*

Proof. Let $\tilde{A} = \langle 1, p_1(x,y)/x^{e(p_1)}, \ldots, p_{n-1}(x,y)/x^{e(p_{n-1})} \rangle_{k[x]}$. By Lemma 7.1.9, $A \subseteq \tilde{A} \subseteq \bar{A}$. Any element of $\overline{A}$ can be represented by an element of the form $q(x,y)/x^e \in \overline{A}$ with $q \in k[x,y]$, since we are assuming that the origin is the only singular point and hence some power of x is in the Jacobian ideal. We prove by induction on j that if

$$\tilde{A}_j = \langle 1, p_1(x,y)/x^{e(p_1)}, \ldots, p_j(x,y)/x^{e(p_j)} \rangle$$

and $q(x,y)/x^e \in \overline{A}$ is monic of degree j in y, then $q(x,y)/x^e \in \tilde{A}_j$. (Note that it is enough to consider monic polynomials q since, as shown in (van Hoeij, 1994), there exists an integral basis consisting of monic polynomials in each degree.) The claim is trivial for $j = 0$. We fix $j > 0$. By definition of p_j, $e \le e(p_j)$ and therefore $p_j(x,y)/x^e \in \tilde{A}_j$. The difference $q/x^e - p_j(x,y)/x^e$ is integral and has degree at most $j-1$ in y, hence it belongs to $\tilde{A}_{j-1} \subset \tilde{A}_j$. Therefore, $q(x,y)/x^e \in \tilde{A}_j$ as wanted. □

If we consider the broader class of polynomials in $\mathcal{P}_x[y]$, maximal integrality exponents can be computed by exhaustive search.

Lemma 7.1.11. *With notation as above, if $\mathcal{A} \subseteq \{1, \ldots, n\}$ is a subset of cardinality d, then set*

$$\mathrm{Int}_{\mathcal{A}} = \min_{j \notin \mathcal{A}} \left(\sum_{i \in \mathcal{A}} v(\gamma_i - \gamma_j) \right).$$

Choose $\widetilde{\mathcal{A}} \subseteq \{1, \ldots, n\}$ of cardinality d such that $\mathrm{Int}_{\widetilde{\mathcal{A}}}$ is maximal among all $\mathrm{Int}_{\mathcal{A}}$ as above, and set $\widetilde{p} = \prod_{i \in \mathcal{A}}(y - \gamma_i)$. Then $v_f(\widetilde{p}) = \mathrm{Int}_{\widetilde{\mathcal{A}}}$, and this number is the maximal valuation $v_f(p)$, for all $p \in \mathcal{P}_x[y]$ monic of degree d. We write $o(\Gamma, d) = v_f(\tilde{p})$.

Proof. It is clear from the definitions that $v_f(\widetilde{p}) = \mathrm{Int}_{\widetilde{\mathcal{A}}}$. The claim that this number is maximal among all $p \in \mathcal{P}_x[y]$ monic of degree d is a direct generalization of (van Hoeij, 1994, Theorem 5.1). □

In the case where $d = n - 1$, we also use the notation

$$\mathrm{Int}_i = \mathrm{Int}_{\{1,\ldots,i-1,i+1,n\}} = \sum_{j \neq i} v(\gamma_i - \gamma_j).$$

and call $E(f) := o(\Gamma, n-1)$ the maximal integrality exponent of f. We will see in the next section that for $f \in k[x][y]$, the maximal integrality over polynomials of any degree d in $k[x][y]$ is the same as the maximal integrality exponent over polynomials of degree d in $\mathcal{P}_x[y]$.

We compute the maximal integrality exponent of polynomials in two examples.

Example 7.1.12. Let $f = (y^2 + 2x^3) + y^3 \in \mathbb{Q}[x, y]$. The Puiseux expansions of f are

$$\begin{aligned} \gamma_1 &= a_1 x^{3/2} + x^3 + \ldots, \\ \gamma_2 &= a_2 x^{3/2} + x^3 + \ldots, \\ \gamma_3 &= -1 - 2x^3 + \ldots, \end{aligned}$$

where the a_i satisfy $a_i^2 = -2$. Then $\mathrm{Int}_1 = 3/2 + 0 = 3/2$, $\mathrm{Int}_2 = 3/2 + 0 = 3/2$, and $\mathrm{Int}_3 = 0 + 0 = 0$, so that both $i = 1$ and $i = 2$ are valid choices. For $i = 1$, we have $\widetilde{p} = (y - \gamma_2)(y - \gamma_3)$, which gives $e(\widetilde{p}) = \lfloor 3/2 \rfloor = 1$.

Example 7.1.13. Let $f = (y^3 - x^7)(y^2 - x^3) + y^6 \in \mathbb{Q}[x, y]$. The Puiseux expansions of f at $x = 0$ are

$$\begin{aligned} \gamma_1 &= x^{7/3} + \ldots, & \gamma_4 &= x^{3/2} + \ldots, \\ \gamma_2 &= \xi_1 x^{7/3} + \ldots, & \gamma_5 &= -x^{3/2} + \ldots, \\ \gamma_3 &= \xi_2 x^{7/3} + \ldots, & \gamma_6 &= -1 + x^3 + \ldots, \end{aligned}$$

where ξ_1, ξ_2 are the complex roots of $x^3 - 1 = 0$.

Now $\mathrm{Int}_1 = \mathrm{Int}_2 = \mathrm{Int}_3 = 7/3 + 7/3 + 3/2 + 3/2 + 0 = 23/3$, $\mathrm{Int}_4 = \mathrm{Int}_5 = 3/2 + 3/2 + 3/2 + 3/2 + 0 = 6$ and $\mathrm{Int}_6 = 0$. Therefore, the maximum integrality exponent is $e = \lfloor 23/3 \rfloor = 7$.

7.2 Sketch of the algorithm

Let $f \in k[x,y]$ be monic of y–degree n. We describe how to compute an integral basis of $A = k[x,y]/\langle f \rangle$, assuming that f has only a singularity at the origin.

The basis will have the form $b_0, \ldots, b_{n-1}$, where $b_i = p_i/x^{e_i}$, with p_i monic of y–degree i.

We focus on computing the last element $b = b_{n-1} = p/x^e$. For the other elements the procedure is similar and will be explained afterwards. The problem is then to find $p \in k[x,y]$ monic of y–degree $n-1$ such that its integrality exponent $e(p)$ is maximal. By Lemma 7.1.10, for such p, $p/x^{e(p)}$ is valid as the last element b of the integral basis of $\overline{A}$.

For $p \in k[x,y]$ of degree $n-1$ in y, write

$$p = (y - \eta_1(x)) \cdots (y - \eta_{n-1}(x)) \tag{7.1}$$

with η_i, $1 \leq i \leq n-1$, the Puiseux expansions of p at $x = 0$. We want to compute $\eta_1(x), \ldots, \eta_{n-1}(x)$ such that the integrality exponent $e(p)$ of p is maximal.

Denote by $\gamma_1(x), \ldots, \gamma_n(x)$ the Puiseux expansions of f at $x = 0$. As we explained in Section 7.1.4, if we allow a more general $\tilde{p} \in \mathcal{P}_x[y]$, the maximal integrality exponent can be obtained by choosing $\{\eta_1(x), \ldots, \eta_{n-1}(x)\}$ to be an appropriate subset of $\{\gamma_1(x), \ldots, \gamma_n(x)\}$.

The coefficients of $\tilde{p}$ may not lie in the ground field k, and furthermore $\tilde{p}$ may contain fractional exponents. By using the trace map, van Hoeij proves that there exists $p \in k[x,y]$ monic of y–degree $n-1$ with $e(p) = e(\tilde{p})$.

In (van Hoeij, 1994) these ideas are only used to fix bounds for the algorithm but not for constructing p. In this work, we show that p can be easily constructed, using Hensel's Lemma to efficiently compute the product $(y - \eta_1(x)) \cdots (y - \eta_{n-1}(x))$, or more precisely, the product of the truncated expansions of these factors up to appropriate degrees.

Our new algorithm can be sketched as follows:

(1) We determine $\tilde{p}$ of y–degree $n-1$ such that $e := e(\tilde{p})$ is maximal, by considering the singular parts of the Puiseux expansions of f. This step is usually fast.

(2) We determine how to truncate the expansions of $\tilde{p}$ to get a polynomial $p \in k[x,y]$ with $e(p) = e$.

(3) We use Hensel's Lemma to compute the product of the Puiseux expansions that do not vanish at the origin, up to x–degree e. (All these expansions must appear in p or otherwise the integrality exponent e will be zero.) Compared to van Hoeij's algorithm, this step is already a major improvement as we do not need to compute the different Puiseux expansions outside the origin separately.

(4) We apply a transformation to the polynomials such that Hensel's Lemma can be used to compute products of conjugate Puiseux expansions that vanish at the origin.

(5) We compute p by multiplying the appropriate factors obtained in steps 3 and 4.

Compared to van Hoeij's algorithm, we are predicting the elements of the integral basis instead of computing them by solving systems of linear equations.

In the following sections we explain these steps in more detail and how to extend this to compute the integral elements of lower y–degrees.

7.3 The element of largest degree of the integral basis

As explained in Section 7.1.4, to find an element $\tilde{p} \in \mathcal{P}_x[y]$ of degree $n-1$ in y with maximal integrality exponent $e(\tilde{p})$, we choose j, $1 \leq j \leq n$, such that Int_j is maximal among all Int_l, $1 \leq l \leq n$. Then we can take $\tilde{p} = \prod_{i \neq j}(y - \gamma_i)$, for which $e(\tilde{p}) = \lfloor \mathrm{Int}_j \rfloor$. However, the element $\tilde{p}$ may not be an element of $k[x, y]$.

We explain how the expansions γ of $\tilde{p}$ can be truncated to $\bar{\gamma}$ so that $p = \prod_{i \neq j}(y - \bar{\gamma}_i) \in k[x, y]$ is a polynomial over the ground field with $e(p) = e(\tilde{p}) = e$. Then we can take $b = \frac{p}{x^e}$ as the highest degree element of the integral basis.

Suppose that Int_1 is maximal among all Int_k, $1 \leq k \leq n$. We discard γ_1, and set $e = \lfloor \mathrm{Int}_1 \rfloor$. Denote by $\gamma_2, \ldots, \gamma_s$ the conjugate expansions of γ_1. For $s < i \leq n$, let $\bar{\gamma}_i$ be the truncation of γ_i after order e and

$$h = \prod_{i=s+1}^{n} (y - \bar{\gamma}_i) \in k[x, y].$$

(In Section 7.4 we will explain how to use Hensel's lemma to compute h in an efficient way by avoiding to compute all expansions.)

In the following paragraphs we show how to truncate the expansions $\gamma_2, \ldots, \gamma_s$ to compute $g \in k[x, y]$ such that $p = gh$ is the desired numerator of the last element of the integral basis. It is clear that the truncation to order e of the expansions appearing in h does not reduce the integrality exponent of p.

7.3.1 Expansions with one or no characteristic exponents

We assume that $\gamma_1, \ldots, \gamma_s$ are conjugate over $k((x))$ and that they have one or no characteristic exponents.

Note that for any $p \in k\,[x, y]$we have

$$v_{\gamma_i}(p) = v_{\gamma_j}(p)$$

for all $1 \leq i, j \leq s$.

Example 7.3.1. We carry on Example 7.1.12, $\tilde{p} = (y - \gamma_2)(y - \gamma_3)$, where the conjugacy class $\{\gamma_1, \gamma_2\}$ has one characteristic exponent. The factor $y - \gamma_3$ is already in $k[x, y]$, so we do not need to truncate it. However, as $e(\tilde{p}) = 1$, we can truncate γ_3 up to order 1, that is, $\bar{\gamma}_3 = -1$. For $\gamma_2 = a_2 \cdot x^{3/2} + x^3 + \dots$ the only truncation leading to an element over $\mathbb{Q}$ is $\bar{\gamma}_2 = 0$. For $p = (y - \bar{\gamma}_2)(y - \bar{\gamma}_3) = y(y - 1)$ we have $v_f(p) = 3/2 = v_f(\tilde{p})$, hence $e(p) = e(\tilde{p})$ and

$$b = \frac{y(y-1)}{x}$$

In general, the expansions γ_k will agree in the terms of degree lower than $t \in \mathbb{Q}$, and have conjugate coefficients $c_i \in \overline{k}$ at the monomial x^t, that is, for $1 \leq i \leq s$,

$$\gamma_i = a_1 x^{d_1} + a_2 x^{d_2} + \cdots + a_k x^{d_k} + c_i x^t + \dots$$

where $a_i \in k$, $d_i \in \mathbb{N}$. Truncating γ_i to $\bar{\gamma}_i$ for $2 \leq i \leq s$ after order d_k we obtain

$$g = (y - \bar{\gamma}_2) \cdots (y - \bar{\gamma}_s) \in k[x, y]$$

Lemma 7.3.2. *For $p = gh$ it holds $e(p) = e$.*

Proof. We have by construction

$$e = \mathrm{Int}_1 = \sum_{j=2}^{n} v(\gamma_1 - \gamma_j) = \sum_{j=2}^{n} v(\gamma_1 - \bar{\gamma}_j) = v_{\gamma_1}(p).$$

Since $\gamma_1, \dots, \gamma_s$ are conjugate and $p \in k[x, y]$, $v_{\gamma_j}(p) = v_{\gamma_1}(p) = e$ for $2 \leq j \leq s$. For $s < j \leq n$, $v(\gamma_i - \bar{\gamma}_i) \geq e$, so $v_{\gamma_j}(p) \geq e$.

Recall that $e(p) = \min_{1 \leq j \leq n} v_{\gamma_j}(p)$. So $e(p) = e$, as wanted. □

We illustrate this process with another example:

Example 7.3.3. Let $f = y^6 - (y^2 + 2x^3)((y + 2x^2)^2 + x^5)$. The Puiseux expansions at 0 are

$$\begin{aligned}
\gamma_1 &= a_1 x^{3/2} - a_1 x^{9/2} + 4x^5 + \dots \\
\gamma_2 &= a_2 x^{3/2} - a_2 x^{9/2} + 4x^5 + \dots \\
\gamma_3 &= -2x^2 + b_1 x^{5/2} - 16 b_1 x^{13/2} + \dots \\
\gamma_4 &= -2x^2 + b_2 x^{5/2} - 16 b_2 x^{13/2} + \dots \\
\gamma_5 &= 1 + 2x^2 + x^3 - 4x^4 - 7/2x^5 + \dots \\
\gamma_6 &= -1 + 2x^2 - x^3 + 4x^4 - 9/2x^5 + \dots
\end{aligned}$$

with a_1, a_2 the roots of $x^2 + 8$ and b_1, b_2 the roots of $x^2 + 1$.

The maximum of Int_i, $1 \leq i \leq s$ is attained for $\mathrm{Int}_3 = \mathrm{Int}_4 = 3/2 + 3/2 + 5/2 + 0 + 0 = 11/2$. We choose $i = 3$. Then $\tilde{p} = (y - \gamma_1)(y - \gamma_2)(y - \gamma_4)(y - \gamma_5)(y - \gamma_6)$ and

$e(\tilde{p}) = e(p) = 5$. The expansions γ_1 and γ_2 are conjugate, so $(y-\gamma_1)(y-\gamma_2) \in k((x))[y]$. Since $e(\tilde{p}) = 5$, we can truncate them after order 5 to get a product in $k[x,y]$. Similarly, γ_5 and γ_6 can be truncated after order 5. To obtain a polynomial over the ground field, we have to truncate γ_4 to $\bar{\gamma}_4 = -2x^2$.

We get $p = (y-\bar{\gamma}_1)(y-\bar{\gamma}_2)(y-\bar{\gamma}_4)(y-\bar{\gamma}_5)(y-\bar{\gamma}_6) \in k[x,y]$, with

$$\begin{aligned}
\bar{\gamma}_1 &= a_1 x^{3/2} - a_1 x^{9/2} + 4x^5 \\
\bar{\gamma}_2 &= a_2 x^{3/2} - a_2 x^{9/2} + 4x^5 \\
\bar{\gamma}_4 &= -2x^2 \\
\bar{\gamma}_5 &= 1 + 2x^2 + x^3 - 4x^4 - 7/2x^5 \\
\bar{\gamma}_6 &= -1 + 2x^2 - x^3 + 4x^4 - 9/2x^5
\end{aligned}$$

We observe that $e(\tilde{p}) = e(p)$.

7.3.2 Expansions with several characteristic exponents

Now suppose that the Puiseux expansions of the conjugacy class have several characteristic exponents. In this case the truncation has to be done iteratively. We describe a recursive process to obtain g, starting from $g_0 = \prod_{j=1}^{n}(y-\gamma_j)$.

The singular parts

$$\gamma_j^{\text{sing}} = a_1^j x^{t_1} + \cdots + a_k^j x^{t_k},\ t_1 < \ldots < t_k$$

of the expansions γ_j, $1 \le j \le s$, are pairwise different and conjugate over $k((x))$.

Since $\gamma_1^{\text{sing}} \neq \gamma_j^{\text{sing}}$, if we truncate the expansions γ_j after order t_{k-1} to

$$\gamma_{1,j} = a_1^j x^{t_1} + \cdots + a_{k-1}^j x^{t_{k-1}}$$

$(1 \le j \le s)$ and define

$$p_1 = \textstyle\prod_{j=2}^{s}(y-\gamma_{1,j}),$$

we have

$$v_{\gamma_1}(p_1) = v_{\gamma_1}(\tilde{p}).$$

That is, the valuation at γ_1 does not decrease.

We define $\overline{g_0} = \prod_{j=1}^{n}(y-\gamma_{1,j})$. Some of the expansions $\gamma_{1,j}$ will coincide. Denote by $\bar{\eta}_1, \ldots, \bar{\eta}_r$ the mutually distinct expansions, and set $g_1 = \prod_{j=1}^{r}(y-\bar{\eta}_j) \in k[x,y]$. By construction $\overline{g_0} = g_1^{u_1}$, with $u_1 = s/r \in \mathbb{N}$.

We start the i-th step by applying the whole procedure inductively to g_{i-1}, computing $\overline{g_{i-1}}$, g_i and u_i such that $\overline{g_{i-1}} = g_i^{u_i}$ and $\overline{g_{i-1}}$ comes from truncating the expansions of g_{i-1}. In each step the degree of g_i (and the number of characteristic exponents in the expansions) drops, hence the process terminates after a finite number of steps with $u_s = 1$ (that is, all the truncated expansions are different and hence $s_i = r_i$). The following lemma shows that

$$g = g_1^{u_1-1} g_2^{u_2-1} \cdots g_s \in k[x,y]$$

has the desired properties:

Lemma 7.3.4. *For $p = gh$ it holds $e(p) = e$.*

Proof. Since $g \in k[x, y]$, by the same arguments of Lemma 7.3.2, we only need to show that $v_{\gamma_1}(p) = e$. However, since all the truncations occur in terms that are different from the terms of γ_1, it is clear that $v_{\gamma_1}(p) = v_{\gamma_1}(\tilde{p}) = e$. □

We summarize our observations in Algorithm 7.3.1.

Algorithm 7.3.1 Truncated Factor

Input: $\{\bar{\gamma}_i = a_1^i x^{t_1} + \cdots + a_k^i x^{t_k}\}_{1 \le i \le s}$, a conjugacy class of Puiseux series with a finite number of terms.

Output: $p \in k[x, y]$ of degree $s - 1$ in y such that $v_f(p) = v_f(\tilde{p})$, with $\tilde{p} = (y - \gamma_2) \cdots (y - \gamma_s)$.

1: Set $\eta_1, \ldots, \eta_r$ the different expansions in the set $\{\overline{\gamma_1}^{t_{k-1}}, \ldots, \overline{\gamma_s}^{t_{k-1}}\}$
2: $g_0 = (y - \eta_1) \cdots (y - \eta_r)$
3: $u = s/r$
4: **if** $u > 1$ **then**
5: $\quad g_1 = \text{TruncatedFactor}(\{\eta_1, \ldots, \eta_r\})$
6: $\quad$ **return** $g_0^{u-1} g_1$.
7: **else**
8: $\quad$ **return** g_0.
9: **end if**

The following example illustrates the algorithm:

Example 7.3.5. Consider the polynomial

$$\begin{aligned} f = {} & y^8 + (-4x^3 + 4x^5)y^7 + (4x^3 - 4x^5 - 10x^6)y^6 + (4x^5 - 6x^6)y^5 + \\ & + (6x^6 - 8x^8)y^4 + (8x^8 - 4x^9)y^3 + (4x^9 + 4x^{10})y^2 + 4x^{11}y + x^{12} \\ & \in \mathbb{Q}(x, y) \end{aligned}$$

The singular parts of the Puiseux expansions of f are

$$\begin{aligned} \gamma_1^{\text{sing}} &= ix^{3/2} + (-1/2i - 1/2)x^{7/4} + 1/4ix^2 \\ \gamma_2^{\text{sing}} &= ix^{3/2} + (-1/2i - 1/2)x^{7/4} - 1/4ix^2 \\ \gamma_3^{\text{sing}} &= ix^{3/2} + (1/2i + 1/2)x^{7/4} + 1/4ix^2 \\ \gamma_4^{\text{sing}} &= ix^{3/2} + (1/2i + 1/2)x^{7/4} - 1/4ix^2 \\ \gamma_5^{\text{sing}} &= -ix^{3/2} + (1/2i - 1/2)x^{7/4} + 1/4ix^2 \\ \gamma_6^{\text{sing}} &= -ix^{3/2} + (1/2i - 1/2)x^{7/4} - 1/4ix^2 \\ \gamma_7^{\text{sing}} &= -ix^{3/2} + (-1/2i + 1/2)x^{7/4} + 1/4ix^2 \\ \gamma_8^{\text{sing}} &= -ix^{3/2} + (-1/2i + 1/2)x^{7/4} - 1/4ix^2 \end{aligned}$$

with $i^2 = -1$.

Truncating γ_i^{sing} after order $7/4$ we obtain

$$\overline{\gamma_1}^{7/4} = \overline{\gamma_2}^{7/4} = ix^{3/2} + (-1/2i - 1/2)x^{7/4}$$

$$\begin{aligned}
\overline{\gamma_3}^{7/4} &= \overline{\gamma_4}^{7/4} = ix^{3/2} + (1/2i + 1/2)x^{7/4} \\
\overline{\gamma_5}^{7/4} &= \overline{\gamma_6}^{7/4} = -ix^{3/2} + (1/2i - 1/2)x^{7/4} \\
\overline{\gamma_7}^{7/4} &= \overline{\gamma_8}^{7/4} = -ix^{3/2} + (-1/2i + 1/2)x^{7/4},
\end{aligned}$$

hence $u_1 = 2$ and

$$\begin{aligned}
g_1 &= (y - \overline{\gamma_1}^{7/4})(y - \overline{\gamma_3}^{7/4})(y - \overline{\gamma_5}^{7/4})(y - \overline{\gamma_7}^{7/4}) \\
&= y^4 + 2x^3y^2 + 2x^5y + x^6 + 1/4x^7.
\end{aligned}$$

Applying the whole procedure inductively to g_1 we drop the Puiseux expansion $\overline{\gamma_1}^{7/4}$ and truncation yields $g_2 = y(y^2 + x^3)$. Combining the factors, we get

$$g = g_1^{u_1 - 1} g_2 = y(y^2 + x^3)(y^4 + 2x^3y^2 + 2x^5y + x^6 + 1/4x^7).$$

7.4 Hensel's Lemma

In this section and the following, we explain how to use Hensel's lemma to compute the products $(y-\gamma_1)\cdots(y-\gamma_s)$ up to any x–degree, with $\gamma_1, \ldots, \gamma_s$ conjugate expansions belonging to a Puiseux segment or block, without computing each individual expansion. Computing all the expansions separately and then computing the product of the corresponding factors is usually much slower.

We recall Hensel's Lemma.

Lemma 7.4.1. *Let $f \in k[[x]][y]$ be a monic polynomial over the power series ring, and assume that $f(0, y) = g_0 h_0$ for monic polynomials $g_0, h_0 \in k[y]$ such that $\langle g_0, h_0 \rangle = k[y]$. Then there exist monic polynomials $g, h \in k[[x]][y]$ such that*

(1) $f = gh$

(2) $g(0, y) = g_0$, $h(0, y) = h_0$.

Moreover, for each $m \in \mathbb{N}$, there exist unique $g_m, h_m \in k[x, y]$ of x–degree m such that

(1) $f \equiv g_m h_m$ in $(k[[x]]/\langle x^{m+1} \rangle)[y]$

(2) $g_m \equiv g_i$, $h_m \equiv h_i$ in $(k[[x]]/\langle x^{i+1} \rangle)[y]$, $0 \leq i \leq m-1$.

These last conditions imply that the polynomials g_m and h_m can be computed inductively along the x–degree, solving for each m a determined system of n linear equations on n unknowns, where n is the y–degree of f. (For each i, $0 \leq i \leq n-1$, we get an equation by comparing the coefficients of $x^m y^i$ in f and in $g_m h_m$.) For further reference in the paper, we present this well–known procedure as Algorithm 7.4.1, omitting the actual computation steps. (This algorithm has been made available in SINGULAR since version 3.1.3 via the command `factmodd`.)

Algorithm 7.4.1 Hensel's lifting

Input: $f \in k[x,y]$ irreducible polynomial, monic in y; $g_0, h_0 \in k[y]$ such that $f(0,y) = g_0 h_0$ and $\langle g_0, h_0 \rangle = k[y]$; $d \in \mathbb{Z}_{\geq 0}$.

Output: $g, h \in k[x,y]$ such that $g(0,y) = g_0$, $h(0,y) = h_0$ and $f \equiv gh$ in $(k[[x]]/\langle x^{d+1} \rangle)[y]$.

We will usually use Hensel's lifting to separate the component that vanishes at the origin from the component that vanishes outside. Alternatively, we could perform this decomposition by means of the Weierstrass Division Theorem. (See for example, de Jong and Pfister 2000, Theorem 3.2.3.) However, the use of Hensel's Lemma allows for more generality, since we do not need to move the singularity to the origin. This is particularly useful when the singularity has no rational coordinates, as we avoid to move to an algebraic extension. Also the linear algebra techniques involved in Hensel's Lemma are usually faster than computing division with remainders of polynomials.

In the following example, we show how to use the lemma to decompose a polynomial and compute the integral basis in a simple case.

Example 7.4.2. Let $f = (y-x)(y+x)(y+2x)+y^7$. There are 3 Puiseux expansions at $y = 0$ and 4 expansions outside $y = 0$. (The degree of f in y is 7, so there must be a total of 7 expansions.) We call $\gamma_1 = x + \ldots, \gamma_2 = -x + \ldots, \gamma_3 = -2x + \ldots$ the expansions at the origin and $\gamma_4, \ldots, \gamma_7$ the expansions outside the origin. We want to compute $(y-\gamma_4)\cdots(y-\gamma_7)$ up to a given order in x without computing each expansion separately.

Here $\mathrm{Int}_i = 2$ for $i = 1, 2, 3$ and this is maximum. So $e(\tilde{g}) = 2$ and we need to compute the product up to degree 2 in x. Since $f(0,y) = y^3+y^7$, we take $g_0 = y^3$, $h_0 = 1 + y^4$, and apply Hensel's lemma to lift these factors up to degree 2. We obtain $g_2 = y^3 + 2xy^2 - 2x^2y$ and $h_2 = 5x^2y^2 - 2xy^3 + y^4 + 1$, and we conclude that $(y-\gamma_4)\cdots(y-\gamma_7) \equiv 5x^2y^2 - 2xy^3 + y^4 + 1$ modulo x^3.

Taking $i = 1$, to compute p, we still have to compute γ_2 and γ_3 up to degree 2. We obtain $\bar{\gamma}_2 = -x$ and $\bar{\gamma}_3 = -2x$. Combining all this we compute $p = \prod_{i=2}^{7}(y - \bar{\gamma}_i) = (y+x)(y+2x)(5x^2y^2 - 2xy^3 + y^4 + 1)$.

7.5 A local version of Hensel's Lemma

When we want to lift two factors g, h that vanish at $y = 0$ (for example, to compute $(y-\gamma_1)(y-\gamma_2)$ as in Example 7.3.3 up to any given order), the condition $\langle g(0,y), h(0,y) \rangle = k[y]$ is not satisfied.

We explain how to transform the polynomials so that Hensel's lemma can still be applied.

Let f have the following Puiseux expansions at 0:

$$\gamma_1 = a_1^1 x^{t_1^1} + a_2^1 x^{t_2^1} + \ldots$$

$$\gamma_2 = a_1^2 x^{t_1^2} + a_2^2 x^{t_2^2} + \dots$$
$$\vdots$$
$$\gamma_s = a_1^s x^{t_1^s} + a_2^s x^{t_2^s} + \dots$$

and assume $t = t_1^1 = \min_{1 \le i \le s} t_1^i$. We define $f_0 = (y-\gamma_1)\cdots(y-\gamma_s)$, $f_0 \in k[[x]][y]$.

We would like to replace y by $x^t y$, so that we can factor out x^t in all factors. But this will introduce fractional exponents in f_0, so we write $t = u/v$ and replace instead x by x^v and y by $x^u y$. We define

$$\begin{aligned}\tilde{f}_0(x,y) = f_0(x^v, x^u y) &= \left(x^u y - (a_1^1 x^{v t_1^1} + \dots)\right) \cdots \left(x^u y - (a_1^s x^{v t_1^s} + \dots)\right) \\ &= x^{su} \left(y - (a_1^1 + \dots)\right) \cdots \left(y - (a_1^s x^{\tilde{t}_1^s} + \dots)\right)\end{aligned}$$

and

$$F(x,y) = \tilde{f}_0(x,y)/x^{su} = \left(y - (a_1^1 + \dots)\right) \cdots \left(y - (a_1^s x^{\tilde{t}_1^s} + \dots)\right),$$

with $F(x,y) \in k[[x]][y]$.

So we can first use Hensel's lemma to compute the factor f_0 up to the required degree, and then compute F as defined above.

Now F has factors that do not vanish at the origin. So we can use again Hensel's lemma to separate the factors that vanish at the origin from the factors that do not. We get $F = GH$. We obtain the factors g and h by reversing the transformations, $g(x,y) = G(x^{1/v}, y/x^{u/v})$, and likewise for h.

We thus obtain Algorithm 7.5.1.

Algorithm 7.5.1 Segment splitting

Input: $f \in k[x,y]$ irreducible polynomial, monic of degree s in y, with no Puiseux expansions vanishing outside the origin; $d \in \mathbb{Z}_{\ge 0}$.

Output: $g_1, \dots, g_k \in k[x,y]$ such that the expansions of g_i correspond to the i-th Puiseux segment of f, developed up to degree d.

1: $t_1, \dots, t_k$ the different initial exponents of the Puiseux expansions of f (which are obtained from the Newton polygon of f)
2: **if** $l = 1$ **then**
3: **return** f
4: **end if**
5: $t = u/v = \min\{t_1, \dots, t_k\}$, with $u, v \in \mathbb{N}$
6: $\tilde{f}(x,y) = f(x^v, x^u y)$
7: $F = \tilde{f}/x^{su}$
8: Compute $G_0, H_0 \in k[y]$ such that $F(0,y) = G_0 H_0$, $G_0 = y^w$, for some $w \in \mathbb{N}$ and $y \nmid H_0$
9: $(G,H) = \text{Hensel}(F, G_0, H_0, vd)$
10: $g_1 = G(x^{1/v}, y/x^{u/v})$, $h = G(x^{1/v}, y/x^{u/v})$
11: **return** $\{g_1\} \cup \text{SegmentSplitting}(h)$.

See also (de Jong and Pfister, 2000, Theorem W) for an alternative approach extending the Weierstrass Division Theorem.

Example 7.5.1. We return to Example 7.3.3, $f = y^6 - (y^2 + 2x^3)((y + 2x^2)^2 + x^5)$. We want to compute $(y - \gamma_1)(y - \gamma_2)$ up to order 5. We first use Hensel's lemma to lift the factors y^4 and $1 + y^2$ up to degree 8 (we must lift up to this degree so that no information from f is lost). We obtain

$$\begin{aligned} f_0 &= 48x^8y^3 + 46x^8y^2 - 8x^7y^3 - 16x^8y - 8x^7y^2 + 32x^6y^3 + 2x^8 - 4x^6y^2 \\ &\quad - 8x^5y^3 + 8x^7 + x^5y^2 + 8x^5y + 4x^4y^2 + 2x^3y^2 + 4x^2y^3 + y^4, \\ f_1 &= -48x^8y + 210x^8 + 8x^7y - 56x^7 - 32x^6y + 4x^6 + 8x^5y - x^5 + 12x^4 - 2x^3 - 4x^2y + y^2 - 1. \end{aligned}$$

(Note that $f_1 = (y - \gamma_5)(y - \gamma_6)$ up to order 8, so we can truncate it up to order 5 to get the product of the expansions outside the origin.)

The smallest t is $t = u/v = 3/2$. We compute $\tilde{f}_0 = f_0(x^2, x^3y) = x^{12}(48x^{13}y^3 - 8x^{11}y^3 + 46x^{10}y^2 + 32x^9y^3 - 8x^8y^2 - 8x^7y^3 - 16x^7y - 4x^6y^2 + x^4y^2 + 2x^4 + 4x^2y^2 + 4xy^3 + y^4 + 8x^2 + 8xy + 2y^2) = x^{12}F(x, y)$.

Now, $F(0, y) = (y^2 + 2)y^2$ and we use Hensel's lemma to lift the factors $y^2 + 2$ and y^2. After lifting and mapping the factors back to the original x and y, we obtain

$$\begin{aligned} g &= -4x^6 - 8x^5y + 2x^3 + y^2, \\ h &= x^5 + 4x^4 + 4x^2y + y^2. \end{aligned}$$

Note that $g = (y^2 + 2x^3) - 8x^5y - 4x^6$ and $h = (y + 2x^2)^2 + x^5$ are equal in the low degree terms to the factors appearing in f.

We can now compute $p = (y - \bar{\gamma}_1)(y - \bar{\gamma}_2)(y - \bar{\gamma}_4)(y - \bar{\gamma}_5)(y - \bar{\gamma}_6) = ((y^2 + 2x^3) - 8x^5y - 4x^6)y(8x^5y - x^5 + 12x^4 - 2x^3 - 4x^2y + y^2 - 1)$.

To separate all the Puiseux segments, we can use this method iteratively. In each step we separate the segment with smallest initial exponent from the rest. Now consider blocks inside a segment which have the same initial exponents but whose initial terms are not conjugate. In this case we can also use Hensel's lemma to split the blocks after applying the above transformation, hence we can still proceed in the same way.

To be able to separate all blocks, it remains to consider the separation of blocks that have the same initial rational term (and therefore the same initial exponent). Suppose that f_1 is a factor of f containing some Puiseux blocks of f such that they all have the same initial terms $\eta = a_1x^{m_1} + \cdots + a_lx^{m_l}$, $a_i \in k, m_i \in \mathbb{Z}_{\geq 0}$, $1 \leq i \leq l$. (There can be fewer terms than in the rational part of the expansions.) In this case, we first apply the transformation $y = y_1 + \eta$, and compute $f_2(x, y_1) = f_1(x, y_1 + \eta)$. Then f_2 will contain the same expansions as f_1 but without the initial terms η. We can now proceed as before to separate the blocks. After computing the factors corresponding to each block, we replace y_1 by $y - \eta$, to get the factor we were looking for.

Algorithm 7.5.2 summarizes these ideas.

The ideas from (de Jong and Pfister, 2000, Theorem 5.1.20) can in some cases also be used for our purpose. However, the cited theorem is not as general as we require, and the details on how to initiate the algorithm are not given.

Algorithm 7.5.2 Block splitting

Input: $f \in k[x,y]$ irreducible polynomial, monic of y–degree n; $d \in \mathbb{Z}_{\geq 0}$.

Output: $f_0, f_1, \ldots, f_r$ such that the expansions of each f_i are the same as the i-th Puiseux block of f up to order d in x.

1: compute $g_0, h_0 \in k[y]$ such that $g_0 h_0 = f(0,y)$, $g_0 = y^l$ for some $l \in \mathbb{Z}_{\geq 0}$ and $\langle g_0, h_0 \rangle = k[y]$
2: $(f_0, g) = \text{Hensel}(f, g_0, h_0, d)$, where f_0 is the lifting of h_0 and g is the lifting of g_0, up to order d in x
3: $\{g_1, \ldots, g_s\} = \text{SegmentSplitting}(g, d)$, the factors corresponding to the different Puiseux segments of g
4: **for all** g_i, $i = 1, \ldots, s$ **do**
5: $\quad \eta_i :=$ the common rational part of all expansions in g_i
6: $\quad \tilde{g}_i = g_i(x, y + \eta_i)$
7: $\quad \{\tilde{g}_{i,1}, \ldots, \tilde{g}_{i,r_i}\} = \text{BlockSplitting}(\tilde{g}_i, d)$
8: $\quad g_{i,j}(x,y) = \tilde{g}_{i,j}(x, y - \eta_i)$, $j = 1, \ldots, r_i$
9: **end for**
10: $\{f_1, \ldots, f_r\} = \cup_{i=1}^{s} \{g_{i,1}, \ldots, g_{i,r_i}\}$
11: **return** $\{f_0, f_1, \ldots, f_r\}$.

Our final goal is to separate all factors corresponding to different groups of conjugate expansions. In this case, we do not know of any algorithm to do it without working in algebraic extensions. We compute the conjugate Puiseux expansions $\bar{\gamma}_1, \ldots, \bar{\gamma}_s$ up to the desired degree and then compute the product $(y - \bar{\gamma}_1) \cdots (y - \bar{\gamma}_s)$. This last step is only needed when a Puiseux block contains more than one conjugacy class of expansions.

We combine all the contents of this section in a general splitting algorithm.

7.6 Local integral basis

To compute all the elements of the integral basis, we first show how to compute a local integral basis at the origin, that is, an integral basis for the local ring $A_{\langle x,y \rangle}$. We can ignore the Puiseux expansions of f that do not vanish at the origin, since these expansions are units in the local ring. Hence, we assume $f \in k[[x]][y]$, with all the expansions of f vanishing at the origin. By Lemma 7.1.10, for each d, $0 \leq d \leq n-1$, where $n = \deg(f)$, we look for a polynomial p of y–degree d with maximum valuation at f. (The case $d = n-1$ was in fact already analyzed in Section 7.3.) Let Γ be the set of Puiseux, expansions of f. We have seen that if we allow for a more general $\tilde{p} \in \mathcal{P}_x[y]$, whose Puiseux expansions are $N = \{\eta_1, \ldots, \eta_d\}$, we can assume $N \subset \Gamma$.

We could therefore proceed as before. For each subset $\mathcal{A} \subseteq \{1, \ldots, n\}$ of d elements, we define

$$\text{Int}_{\mathcal{A}} = \min_{j \notin \mathcal{A}} \left(\sum_{i \in A} v(\gamma_i - \gamma_j) \right)$$

Algorithm 7.5.3 Splitting

Input: $f \in k[x,y]$ irreducible polynomial, monic of y–degree n; $e \in \mathbb{Z}_{\geq 0}$.

Output: $L = \{f_0, f_1, \ldots, f_r\}$ such that the expansions of each f_i are the same as the i-th conjugacy class of Puiseux expansions of f up to order e in x.

1: Compute $\{g_0, g_1, \ldots, g_s\} = \text{BlockSplitting}(f, e)$
2: $L = \{g_0\}$
3: **for** $i = 1, \ldots, s$ **do**
4: Compute $\Gamma = \{\gamma_1, \ldots, \gamma_l\}$, the singular part of the expansions of g_i.
5: $l =$ number of conjugacy classes in Γ
6: **if** $l > 1$ **then**
7: **for** $j = 1, \ldots, l$ **do**
8: Compute $\Gamma_j = \{\gamma_{j,1}, \ldots, \gamma_{j,s_j}\}$, the expansions of the j-th conjugacy class of Γ, up to order e in x
9: $h_j = (y - \gamma_{j,1}) \cdots (y - \gamma_{j,s_j})$
10: **end for**
11: $L = L \cup \{h_1, \ldots, h_k\}$
12: **else**
13: $L = L \cup \{g_i\}$
14: **end if**
15: **end for**
16: **return** L.

and take $\mathcal{A}$ for which $\text{Int}_{\mathcal{A}}$ is maximum. Then, $\tilde{p} = \prod_{i \notin \mathcal{A}} (y - \gamma_i)$ and $v_f(\tilde{p}) = \text{Int}_{\mathcal{A}}$. We define $o(\Gamma, d) = v_f(\tilde{p})$, the maximal valuation at f for all elements of $\mathcal{P}_x[y]$ of y–degree d. From $\tilde{p}$, we construct $p \in k[x,y]$ such that $v_f(\tilde{p}) = v_f(p)$ in a similar way as we did in Algorithm 7.3.1.

However, computing the maximum in this way can be quite time-consuming, as the number of subsets can be large. To do this more efficiently, we group the expansions in conjugacy classes.

Extending the previous definitions, for any subset Δ of expansions of f of s elements, and any $c \in \mathbb{Z}_{\geq 0}$, $0 \leq c < s$, we set $f_\Delta = \prod_{\delta \in \Delta} (y - \delta)$ and define

$$o(\Delta, c) = \max_{N \subseteq \Delta} v_{f_\Delta} \left(\prod_{\eta \in N} (y - \eta) \right),$$

where the maximum is taken over all subsets $N \subseteq \Delta$ of c elements, and assume that for $\tilde{p}_\Delta(c) \in \mathcal{P}_x[y]$ the maximum is attained.

Recall that for a given $N \subseteq \Delta$, we have the formula

$$v_{f_\Delta} \left(\prod_{\eta \in N} (y - \eta) \right) = \min_{\delta \in \Delta \setminus N} \left(\sum_{\eta \in N} v(\delta - \eta) \right).$$

We explain first the case where all the expansions of f at the origin are conjugate.

7.6.1 One conjugacy class of expansions

Let $\Gamma = \{\gamma_1, \ldots, \gamma_s\}$ be the expansions of f at the origin, corresponding all to the same conjugacy class.

To compute $o(\Gamma, c)$, we do not apply the above formulas but we compute a polynomial $p \in k[x, y]$ of y–degree c such that $v_f(p) = o(\Gamma, c)$, truncating the expansions in the conjugacy class. The algorithm to compute the factor is a generalization of Algorithm 7.3.1 and is given in Algorithm 7.6.1. As in the case of Algorithm 7.3.1, it gives the best possible truncation in the sense that if $p = \text{TruncatedFactorGeneral}(\Gamma, c)$, then for any $\gamma \in \Gamma$, $v_\gamma(p)$ is maximal over all polynomials in $k[x, y]$ of y–degree c. This implies that $v_f(p) = o(\Gamma, c)$.

Hence we can compute $o(\Gamma, c)$ by the formula

$$o(\Gamma, c) = \sum_{\eta \in N} v(\gamma - \eta),$$

where $N = \{\eta_1, \ldots \eta_c\}$ is the set of expansions appearing in p. (For any expansion $\gamma \in \Gamma$ the result of the sum is the same, because conjugating the above expression does not modify N.)

Algorithm 7.6.1 Truncated Factor General

Input: $\{\bar{\gamma}_i = a_1^i x^{t_1} + \cdots + a_k^i x^{t_k}, 1 \leq i \leq d\}$, the singular parts of a conjugacy class Γ of Puiseux expansions of f, $c \in \mathbb{N}$, $c < d$.

Output: $p \in k[x, y]$ of y–degree c such that $v_f(p) = v_f(\tilde{p})$, with $\tilde{p}$ the element of $\mathcal{P}_x[y]$ of degree c with maximal valuation at f.

1: Set $\eta_1, \ldots, \eta_r$ the different expansions in the set $\{\overline{\gamma_1}^{t_{k-1}}, \ldots, \overline{\gamma_d}^{t_{k-1}}\}$
2: $u = \lfloor c/r \rfloor$, $c' = c - ur$
3: $g_1 = \text{TruncatedFactorGeneral}(\{\eta_1, \ldots, \eta_r\}, c')$
4: **if** $u > 0$ **then**
5: $\quad g = (y - \overline{\gamma_1}^{t_{k-1}}) \cdots (y - \overline{\gamma_d}^{t_{k-1}})$
6: $\quad$ **return** $p = g^u g_1$.
7: **else**
8: $\quad$ **return** $p = g_1$.
9: **end if**

7.6.2 The general case

The main result for constructing p in the general case is given in the following theorem, which generalizes the results in (van Hoeij, 1994).

Theorem 7.6.1. *Let $f \in k[x, y]$ and $\tilde{p} \in \mathcal{P}_x[y]$ of y–degree d with maximal valuation at f. Then there exists $p \in k[x, y]$ of y–degree d such that $v_f(\tilde{p}) = v_f(p)$ and such that the Puiseux expansions of p are all truncations of expansions of f.*

Proof. In (van Hoeij, 1994) it is proved that there exists $q \in k[x, y]$ of y–degree d such that $v_f(\tilde{p}) = v_f(q)$. To construct p we truncate the expansions appearing in

q, removing all the terms that do not coincide with the initial parts of Puiseux expansions of f. By doing this, the valuation does not decrease, $v_f(p) = v_f(q) = v_f(\tilde{p})$, and $p \in k[x, y]$. □

Based on this result, instead of starting with $\tilde{p}$ and then building p from it in such a way that the valuation at f does not decrease, we can directly build a polynomial p of maximal valuation among all polynomials coming from truncating expansions of f.

Moreover, the choice and truncation of a given number of expansions in a conjugacy class can be done independently of the choice and truncation of expansions in other classes, as we see in the next lemma.

Lemma 7.6.2. *Let $f \in k[x, y]$ and v the maximal valuation at f among all polynomials in $k[x, y]$ of y–degree d. Let $\Gamma_1, \ldots, \Gamma_r$ be the conjugacy classes of expansions of f. There exist $q_1, \ldots, q_r \in k[x, y]$ such that $p = q_1 \cdots q_r$ has y–degree d, $v_f(p) = v$ and q_i has maximal valuation at $f_i = \prod_{\gamma \in \Gamma_i}(y - \gamma)$, $1 \leq i \leq r$, among all the polynomials of the same y–degree as q_i.*

Proof. For a given $d \in \mathbb{N}$, let $\tilde{p} \in \mathcal{P}_x[y]$ and $p \in k[x, y]$ be as in Theorem 7.6.1. That is $v_f(p) = v_f(\tilde{p})$ and p is obtained from $\tilde{p}$ by truncating its Puiseux expansions. If different choices of expansions in Γ give the maximal valuation, for each possibility we define $w = (c_1, \ldots, c_r)$, c_i the number of expansions in Γ_i and take $\tilde{p}$ with largest w under the lexicographical ordering.

Let N be the expansions appearing in $\tilde{p}$ and for a given j $(1 \leq j \leq r)$ let $N_j = N \cap \Gamma_j$. Let $\tilde{p}_j = \prod_{\eta \in N_j}(y - \eta)$ and p_j the minimum truncation of the expansions in $\tilde{p}_j$ to get an element in $k[x, y]$.

We first show that $p = p_1 \cdots p_r$ (that is, the truncation in each class can be done independently from the truncation in other classes). If $N_1 \neq \emptyset$, take $\eta_1 \in N_1$. We want to prove that the truncation of η_1 to build p (which we note $t(\eta_1)$) is the same as the truncation of η_1 to build p_1 (which we note $t_1(\eta_1)$).

If not, this means that there exists η_2 in some N_i, $i > 1$, such that $t(\eta_1)$ and $t(\eta_2)$ are conjugate elements in the extension $k[x] \hookrightarrow \mathcal{P}_x$ and such that no expansion in N_1 is truncated to $t(\eta_2)$. (Note that since p is over the ground field, all the conjugates of $t(\eta_1)$ must also be expansions of p.)

Let $G = G(k[x] \hookrightarrow \mathcal{P}_x)$ be the Galois group of the extension, and let $g \in G$ be such that $g(t(\eta_1)) = t(\eta_2)$. Then $g(\eta_1) \in \Gamma_1$ but is not in N_1. But then, to build $\tilde{p}$, we could have taken $g(\eta_1)$ instead of η_2 and $v_f(\tilde{p})$ would remain equal (if for $t(\eta_1)$ the best continuation is η_1, then for $g(t(\eta_1))$ the best continuation must be $g(\eta_1)$). This contradicts the fact that, because of the lexicographical ordering used, we were taking the largest possible number of expansions in Γ_1.

Therefore, all the conjugates of $t(\eta_1)$ come from truncating expansions in N_1. Now, proceeding inductively, we prove that the truncation of any expansion can be done inside each conjugacy class Γ_i, independently of the expansions chosen in other conjugacy classes. □

The lemma says that we can compute the optimal p restricting to products of polynomials q_i which only depend on the number of expansions chosen in each conjugacy class, and therefore we only have to decide optimally how many expansions to choose in each conjugacy class. We explain this in more detail.

We now explain how to build the element of the integral basis.

Let $\Gamma_1, \ldots, \Gamma_r$ be the different conjugacy classes of expansions of f and n_i be the number of expansions in the i-th conjugacy class, $1 \leq i \leq r$. For $0 \leq c < n_i$, we define $p_i(c) = \text{TruncatedFactorGeneral}(\Gamma_i, c)$ and $p_i(n_i) = f_i$ developed up to degree e in x (which can be done by Algorithm 7.5.3). We call $N_i(c)$ the Puiseux expansions appearing in $p_i(c)$.

Next, we consider the set of tuples $T_d = \{(c_1, \ldots, c_r), c_i \in \mathbb{Z}_{\geq 0}, 0 \leq c_i \leq n_i, c_1 + \cdots + c_r = d\}$. For $w = (c_1, \ldots, c_r) \in T_d$, the polynomial of maximal valuation at f containing c_i expansions in the i-th conjugacy class is $p_w = p_1(c_1) \cdots p_r(c_r)$. The valuation of p_w at f can be computed by the formula

$$v_f(p_w) = \min_{1 \leq i \leq r} \left\{ o(\Gamma_i, c_i) + \sum_{j \neq i} v_{\gamma_{(i,1)}}(p_j(c_j)) \right\}.$$

We look for the vector $w = (c_1, \ldots, c_r)$ for which $v_f(p_w)$ is maximal, and for such w we set $p_d := p_w$. The numerator of the element of degree d in the integral basis is p_d and the denominator is $x^{\lfloor v_f(p_d) \rfloor}$.

Algorithm 7.6.2 Integral element

Input: $(\Gamma_1, f_{\Gamma_1}), \ldots, (\Gamma_r, f_{\Gamma_r})$, the singular parts of some conjugacy classes of expansions of f and their corresponding factors developed up to x–degree e; $d \in \mathbb{Z}_{\geq 0}$ ($0 \leq c \leq \deg_y(g)$, where $g = f_{\Gamma_1} \cdots f_{\Gamma_r}$).

Output: $p \in k[x, y]$ of y–degree d of maximal valuation at $g = f_{\Gamma_1} \cdots f_{\Gamma_r}$; $o \in \mathbb{Q}_{\geq 0}$, the valuation of p at g.

1: $m_i = \#\Gamma_i$ for $1 \leq i \leq r$
2: $T = \{(c_1, \ldots, c_r) : c_i \in \mathbb{Z}_{\geq 0}, 0 \leq c_i \leq m_i \text{ for } 1 \leq i \leq r; c_1 + \cdots + c_r = d\}$
3: **for** $w = (c_1, \ldots, c_r) \in T$ **do**
4: **if** $0 \leq c_i < m_i$ **then**
5: $p_i(c_i) = \text{TruncatedFactorGeneral}(\Gamma_i, c_i)$
6: **else**
7: $p_i(c_i) = f_{\Gamma_i}$
8: **end if**
9: $p_w = p_1(c_1) \cdots p_r(c_r)$
10: $v_g(p_w) = \min_{1 \leq i \leq r} \left\{ o(\Gamma_i, c_i) + \sum_{j \neq i} v_{\gamma_i}(p_j(c_j)) \right\}$, where γ_i is any expansion of Γ_i.
11: **end for**
12: $p = p_w$ for w such that $v_g(p_w)$ is maximal
13: **return** $(p, v_g(p))$.

7.6.3 The optimization problem

To apply the algorithm described above, we must run over all the elements of T_d and compute the corresponding valuations. This can still be slow when T_d is large.

In this section, we explain how to find the optimal $(c_1, \ldots, c_r) \in T_d$ in an efficient way. Instead of considering tuples of r elements, we will always consider tuples of 2 elements and proceed iteratively.

For each Puiseux block Π_i, $1 \leq i \leq a$, we define

$$L_i = \{(\Gamma_{(i,1)}, f_{\Gamma_{(i,1)}}), \ldots, (\Gamma_{(i,r_i)}, f_{\Gamma_{(i,r_i)}})\},$$

where $\Gamma_{(i,j)}$ is the set of singular parts of the j-th conjugacy classes of the i-th block and $f_{\Gamma_{(i,j)}}$ is the corresponding factor of f developed up to x–degree e.

For a list L of this kind, we define $f_L = \prod_{(\Gamma, f_\Gamma) \in L} f_\Gamma$ and we show how to compute $p_L(c)$, the polynomial in $k[x, y]$ of y–degree c of maximal valuation at f_L, $0 \leq c \leq m$, where m is the degree of f_L. For a Puiseux series γ, the notation $\gamma \in L$ will mean that there exists $(\Gamma, f_\Gamma) \in L$ such that $\gamma \in \Gamma$.

We group the lists in new lists $\Lambda_1, \ldots, \Lambda_u$ such that all the expansions in the same list Λ_i have the same initial term (or conjugate initial terms). We order them in increasing order by the initial exponent. (The order among groups with the same initial exponent is not important.) Since $v(\gamma_i)$ is the same for any $\gamma_i \in \Lambda_i$, we define $v(i) = v(\gamma_i)$. The key property is that if $1 \leq i < j \leq u$, then $v(\gamma_i - \gamma_j) = v(i)$ for any $\gamma_i \in \Lambda_i$ and $\gamma_j \in \Lambda_j$.

Let m_i be the number of expansions in Λ_i, $1 \leq i \leq u$. We define $\Theta_i = \Lambda_i + \cdots + \Lambda_u$ and we want to compute inductively $p_{\Theta_i}(c)$, for $0 \leq c \leq m_i + \cdots + m_u$.

We start by computing $p_{\Theta_u}(c) = p_{\Lambda_u}(c)$ for $0 \leq c \leq m_u$. For any $1 \leq i \leq u$ and $1 \leq c \leq m_u$ we can compute $p_{\Lambda_i}(c)$ using Algorithm 7.6.2, or applying this new algorithm recursively as we will see below. Next, we proceed recursively to compute $\{p_{\Theta_i}(c)\}_{0 \leq c \leq m_i + \cdots + m_u}$ from $\{p_{\Theta i+1}(c)\}_{0 \leq c \leq m_{i+1} + \cdots + m_u}$, for $1 \leq i < u$.

The property mentioned above implies that $v(\gamma_i - \gamma_{i+1}) = v(i)$ for any $\gamma_i \in \Lambda_i$ and $\gamma_{i+1} \in \Theta_{i+1}$.

Hence for any set N_1 of c_1 expansions of Λ_i and any set N_2 of c_2 expansions of Θ_{i+1}, if $q_1 = \prod_{\eta \in N_1}(y - \eta)$, $q_2 = \prod_{\eta \in N_2}(y - \eta)$ and $q = q_1 q_2$, then

$$v_{\gamma_i}(q_2) = c_2 v(i)$$

Since $v_{f_{\Lambda_i}}(q_1)$ is the minimum of $v_{\gamma_i}(q_1)$ for $\gamma_i \in \Lambda_i$, we obtain that

$$\min_{\gamma \in \Lambda_i} v_\gamma(q) = v_{f_{\Lambda_i}}(q_1) + c_2 v(i).$$

Similarly,

$$\min_{\gamma \in \Theta_{i+1}} v_\gamma(q) = c_1 v(i) + v_{f_{\Theta_{i+1}}}(q_2).$$

We conclude that

$$v_{f_{\Theta_i}}(q) = \min\{v_{f_{\Lambda_i}}(q_1) + c_2 v(i), c_1 v(i) + v_{f_{\Theta_{i+1}}}(q_2)\}.$$

This allows us to compute inductively

$$o(\Theta_i, c) = \max_{c_1+c_2=c} v_{f_{\Theta_i}}(p_{\Lambda_i}(c_1) p_{\Theta_{i+1}}(c_2))$$

and define $p_{\Theta_i}(c)$ as the polynomial for which the maximum is obtained.

The numerator of the element of degree d in the integral basis is

$$p_d = p_{\Theta_1}(d)$$

and the denominator is $x^{\lfloor v_f(p_d) \rfloor}$.

For computing the best polynomials in each block, we can use this strategy recursively. We summarize the method in Algorithm 7.6.3.

Algorithm 7.6.3 Local Integral Basis

Input: $L = \{L_1, \ldots, L_r\}$, where $L_i = \{(\Gamma_{(i,1)}, f_{\Gamma_{(i,1)}}), \ldots, (\Gamma_{(i,u_i)}, f_{\Gamma_{(i,u_i)}})\}$, the singular parts of the conjugacy classes of some Puiseux blocks of f and their corresponding factors developed up to x–degree e.

Output: $\{(p_0, o_0), \ldots, (p_m, o_m)\}$ such that $p_i \in k[x, y]$ $(0 \leq i \leq m)$ has y–degree i and maximal valuation at $g = f_{\Gamma_{(1,1)}} \cdots f_{\Gamma_{(r,u_r)}}$; $o_i \in \mathbb{Q}_{\geq 0}$, $o_i = v_g(p_i)$, where $m = \deg_y(g)$.

if $r = 1$ **then**
  return $\{\text{IntegralElement}(L_1, c)\}_{0 \leq c \leq m}$.
else
  $f_{L_i} = \prod_{j=1}^{u_i} f_{\Gamma_{(i,j)}}$, for $1 \leq i \leq r$
  Group the lists $L_1, \ldots, L_r$ in lists $\Lambda_1, \ldots, \Lambda_u$ such that all the expansions in the same list Λ_i have the same or conjugate initial terms (without considering the common rational part of all expansions, if any), ordered by the initial exponent in increasing order
  $f_{\Lambda_i} = \prod_{L_j \in \Lambda_i} f_{L_j}$ and $m_i = \deg(f_{\Lambda_i})$, for $1 \leq i \leq u$
  $\Theta_u = \Lambda_u$, $f_{\Theta_u} = f_{\Lambda_u}$
  $\{(p_{\Theta_u}(c), o(\Theta_u, c))\}_{0 \leq c \leq m_u} = \text{LocalIntegralBasis}(\Theta_u)$
  for $i = u - 1, \ldots, 1$ **do**
    $\Theta_i = \Lambda_i + \Theta_{i+1}$, $f_{\Theta_i} = f_{\Lambda_i} f_{\Theta_{i+1}}$
    $\{(p_{\Lambda_i}(c), o(\Lambda_i, c))\}_{0 \leq c \leq m_i} = \text{LocalIntegralBasis}(\Lambda_i)$
    for $c = 0, \ldots, m_i + \cdots + m_r$ **do**
      $o(\Theta_i, c) = \max_{c_1+c_2=c} v_{f_{\Theta_i}}(p_{\Lambda_i}(c_1) p_{\Theta_{i+1}}(c_2))$
      $p_{\Theta_i}(c) =$ the polynomial for which the maximum is obtained
    end for
  end for
  return $\{(p_{\Theta_1}(c), o(\Theta_1, c))\}_{0 \leq c \leq m}$.
end if

We apply this algorithm to Example 7.1.13.

Example 7.6.3. Let $f = (y^3 - x^7)(y^2 - x^3) + y^6 \in \mathbb{Q}[x, y]$. As we have seen in Example 7.1.13, the maximum integrality exponent is $e = 7$.

We take $\Gamma_1 = \{\gamma_1, \gamma_2, \gamma_3\}$ and $\Gamma_2 = \{\gamma_3, \gamma_4\}$ from 7.1.13. Computing the development of $(y - \gamma_1)(y - \gamma_2)(y - \gamma_3)$ up to degree 7 we get $f_1 = y^3$. Similarly, the development of $(y-\gamma_4)(y-\gamma_5)$ up to order 7, is $f_2 = y^2+x^3y+2x^6y-x^3-x^6$ (we omit the details of this computations which can be done using Hensel's lemma).

The input for Algorithm 7.6.3 is $L = \{L_1, L_2\} = \{\{(\Gamma_1, f_1)\}, \{(\Gamma_2, f_2)\}\}$.

We have $\Lambda_1 = L_1$, $\Lambda_2 = L_2$ and $u = 2$. Also $f_{\Lambda_1} = f_1$, $f_{\Lambda_2} = f_2$, $m_1 = 3$ and $m_2 = 2$.

Hence $\Theta_2 = \Lambda_2$, $f_{\Theta_2} = f_{\Lambda_2}$ and the local integral basis corresponding to Θ_2 is

$$\{(1, 0), (y, 1), (f_2, \infty)\}.$$

For $i = 1$, $\Theta_1 = L$ and $f_{\Theta_1} = f_1 f_2$. The local integral basis corresponding to Λ_1 is

$$\{(1, 0), (y, 2), (y^2, 4), (f_1, \infty)\}.$$

Now we have to choose the best combinations for each $c = 0, \ldots, m$. For example, for $c = 3$, we try the pairs $(c_1, c_2) \in \{(1, 2), (2, 1), (3, 0)\}$ and find that the best choice is $(c_1, c_2) = (1, 2)$, for which $v_{f_{\vartheta_1}}(p_{\Lambda_1(2)} p_{\Theta_2}(0)) = v_{f_{\vartheta_1}}(y f_2) = 16/3$.

Applying the formulas for all c, $0 \leq c \leq 5$, we get the output

$$\{(1, 0), (y, 1), (f_2, 3), (yf_2, 16/3), (y^2 f_2, 23/3), (f_1 f_2, \infty)\}.$$

The first five elements define the integral basis $\left\langle 1, \frac{y}{x}, \frac{f_2}{x^3}, \frac{f_2 y}{x^5}, \frac{f_2 y^2}{x^7} \right\rangle_{k[x]}$.

7.7 Integral bases algorithm

We are now ready to give the complete algorithm for computing integral bases.

7.7.1 One singularity at the origin

When f has only one singularity at the origin, for computing the (global) integral basis we have to multiply the numerators of the local integral basis at the origin by the factor corresponding to the expansions that do not vanish at the origin. As noted in the sketch of the algorithm (Section 7.2), for the terms of degree smaller than the degree of that factor, the integrality exponent will be 0.

Combining the results of the previous sections we obtain Algorithm 7.7.1 for computing the integral basis, for the case of an isolated singularity at the origin.

Algorithm 7.7.1 Integral basis

Input: $f \in k[x,y]$ irreducible polynomial, monic of y–degree n, with an isolated singularity at the origin.

Output: $b_0, \ldots, b_{n-1}$, an integral basis of $k[x,y]/\langle f \rangle$.

1: Compute $\Gamma = \{\bar{\gamma}_1, \ldots, \bar{\gamma}_s\}$, the singular part of the Puiseux expansions $\{\gamma_1, \ldots, \gamma_s\}$ of f that vanish at $y = 0$

2: Compute the maximal integrality exponent $e = E(f)$ as indicated in Section 7.1.4

3: $\{h, f_1, \ldots, f_r\} = \text{Splitting}(f, e)$, where f_i, $1 \leq i \leq r$, are the factors corresponding to the conjugacy classes of expansions of f that vanish at the origin and h is the factor of the expansions that vanishes outside, both developed up to degree e

4: Set $L = \{L_1, \ldots, L_s\}$, where $L_i = \{(\Gamma_{(i,1)}, f_{\Gamma_{(i,1)}}), \ldots, (\Gamma_{(i,u_i)}, f_{\Gamma_{(i,u_i)}})\}$, the singular parts of the conjugacy classes of the i-th Puiseux block of f and their corresponding factors developed up to x–degree e

5: $m = n - \deg(h)$

6: $\{(p_0, o_0), \ldots, (p_m, o_m)\} = \text{LocalIntegralBasis}(L)$

7: **for** $i = 0, \ldots, \deg(h) - 1$ **do**

8: $\quad b_i = y^i$

9: **end for**

10: **for** $i = 0, \ldots, m - 1$ **do**

11: $\quad b_{\deg(h)+i} = h \cdot p_i / x^{\lfloor o(i) \rfloor}$

12: **end for**

13: **return** $\{b_0, \ldots, b_{n-1}\}$.

7.7.2 The general algorithm

To compute an integral basis in the general setting, we apply the results from Section 5.6 to put together the local results.

In the presence of several singularities, Algorithm 7.7.1 computes the local contribution to the normalization at the origin (see Definition 5.6.2). The reason is that the proof given in (van Hoeij, 1994, Section 2.4) of Lemma 7.1.9 is still valid when there are other singularities outside the line $x = 0$. (If there are other singularities at the line $x = 0$, we can always apply a linear coordinate change so that all the singularities have a different x-coordinate.) Therefore, Algorithm 7.7.1 will compute an integral extension of A such that its localization at the origin generates the normalization of the local ring, as required in Proposition 5.6.1.

For computing the local contributions at singularities outside the origin, we first apply a translation to move the singularity to the origin, compute the local contribution at the origin, and apply the inverse translation to the output.

Remark 7.7.1. Note that our local algorithm can handle groups of conjugate singularities simultaneously, in a similar way as in (van Hoeij, 1994, Section 4). If $I \subset k[x, y]$ is an associated prime of the singular locus, corresponding to a group of conjugate singularities, we apply a linear coordinate change if necessary, so that no two of these singularities have the same y-coordinate. Then we can find polynomials $q_1, q_2 \in K[x]$ such that $I = \langle q_1(x), y - q_2(x)\rangle$. We take α a root of $q_1(x)$ and traslate the singularity $(\alpha, q_2(\alpha))$ to the origin. We compute the local integral basis at the origin and apply the inverse traslation to the output. The common denominator of the resulting generators will be a power of $x - \alpha$. We replace $(x - \alpha)$ by $q_1(x)$ in the denominators and we eliminate α from the numerators by considering α as a new variable and reducing each numerator by the numerators of smaller degree, using an elimination order $\alpha \gg y \gg x$.

Finally, we put all the local results together applying Algorithm 5.6.2. (Note that the integral basis consists of $k[x]$-module generators, which are also A-module generators.)

Once we compute generators of the normalization, we can compute the (global) integral basis applying the results in Section 6.2.

In the next section we analyze the performance of this approach.

7.8 Timings

We present some timings which compare the implementation of our algorithm in Singular with that of van Hoeij's algorithm in Maple. We compute the integral basis for $A = \mathbb{Q}[x, y]/\langle f\rangle$ with the specified polynomials f. All computations were done on a compute server running a 1.60GHz Dual AMD Opteron 242 with 8GB ram. For the cases when f has only one singular point, it is given as part of the input to both algorithms. That is, no computation or decomposition of

the singular locus is done. When the singular locus has more than one point, the timings involve decomposing the singular locus, computing the local contributions, and combining them. We remark that for obtaining the integral basis, singularities at infinity of the curve $\{f = 0\}$ do not matter.

7.8.1 A_k-singularity

The plane curves with defining equation $f(x, y) = y^2 + x^{k+1} + y^d$, $k \geq 1$, $d \geq 3$ have exactly one singularity at the origin, which is of type A_k.

k	d	Singular	Maple
5	10	0	0
5	100	0	2.4
5	500	14	262
50	60	0	2.6
50	100	0	7
50	500	16	385
90	100	0	12
90	500	13	509
400	500	16	1689

7.8.2 D_k-singularity

The plane curves with defining equation $f(x, y) = x(x^{k-1} + y^2) + y^d$, $k \geq 2$, $d \geq 3$ have exactly one D_k-singularity at the origin:

k	d	Singular	Maple
5	10	0	0
5	100	2	2.6
5	500	51	206
50	60	1	14
50	100	2	45
50	500	49	2114
90	100	2	142
90	500	50	5918
400	500	50	> 6000

7.8.3 Ordinary multiple points

We consider random curves of degree d with an ordinary k-fold point at the origin. The defining polynomials were generated by the function `polyDK` from the Singular library `integralbasis` (Böhm et al., 2011b) (using the random seed 1231).

k	d	SINGULAR	MAPLE
5	10	0	0
15	20	0	3
15	30	1	1095
20	25	0	13
20	30	1	352

7.8.4 Curves with many A_k singularities

The curves defined by the equation

$$f = \left(x^{k+1} + y^{k+1} + z^{k+1}\right)^2 - 4\left(x^{k+1}y^{k+1} + y^{k+1}z^{k+1} + z^{k+1}x^{k+1}\right)$$

with $z = 2x - y + 1$ (to have all singularities of the projective curve in the affine chart) were constructed in (Hirano, 1992) by Hirano, and have $3\,(k+1)$ singularities of type A_k.

n	SINGULAR	MAPLE
6	2	11
8	18	109
10	240	4756

The curves

$$f = x^{2n} + y^{2n} + z^{2n} + 2(x^n z^n - x^n y^n + y^n z^n)$$

with $z = x - 2y + 1$ given by Cogolludo in (Cogolludo, 1999) have $3n$ singularities of type A_{n-1} if n is odd.

n	SINGULAR	MAPLE
5	1	3
7	2	37
9	27	478
11	53	> 6000

7.8.5 More general singularities

We now consider some examples of curves which have singularities of type other than ADE or ordinary multiple points:

(1) $f = -x^{15} + 21x^{14} - 8x^{13}y + 6x^{13} + 16x^{12}y - 20x^{11}y^2 + x^{12} - 8x^{11}y + 36x^{10}y^2 - 24x^9y^3 - 4x^9y^2 + 16x^8y^3 - 26x^7y^4 + 6x^6y^4 - 8x^5y^5 - 4x^3y^6 + y^8$: one singularity at the origin with multiplicity $m = 8$ and delta invariant $\delta = 42$, a node, and a set of 6 conjugate nodes. [Pfister]

(2) $f = (y^4 + 2x^3y^2 + x^6 + x^5y)^3 + x^{11}y^{11}$: one singularity at the origin with $m = 12$ and $\delta = 133$. [Pfister]

(3) $f = (y^5 + y^4x^7 + 2x^8)(y^3 + 7x^4)(y^7 + 2x^{12})(y^{11} + 2x^{18}) + y^{30}$: one singularity at the origin with $m = 26$ and $\delta = 523$.

(4) $f = (y^{15} + 2x^{38})(y^{19} + 7x^{52}) + y^{36}$: one singularity at the origin with $m = 34$ and $\delta = 1440$.

(5) $f = (y^{15} + 2x^{38})(y^{19} + 7x^{52}) + y^{100}$: higher degree, but same type of singularity.

(6) $f = y^{40} + xy^{13} + x^4y^5 + x^5 + 2x^4 + x^3$: one double point with $\delta = 2$ and one triple point with $\delta = 19$ (see van Hoeij, 1994, Section 6.1).

(7) $f = y^{200} + xy^{13} + x^4y^5 + x^5 + 2x^4 + x^3$: higher degree, but same type of singularity.

(8) $f = (y^{35} + y^{34}x^7 + 2x^{38})(y^{33} + 7x^{44})(y^{37} + 2x^{52}) + y^{110}$: one singularity at the origin with $m = 105$ and $\delta = 6528$.

Although some of the examples have only one singularity at the origin, we apply the local and the global algorithm in all cases. That is, in the columns labeled *Origin*, we compute the timings for the local contribution to the integral basis at the origin, which does not involve the decomposition of the singular locus. In the columns labeled *Global*, we decompose the singular locus, compute the local contributions, and combine them.

	Origin		Global			
No.	SINGULAR	MAPLE	SINGULAR	SINGULAR*	MAPLE	y–degree
1	0	0	0	5	1	8
2	36	2	37	37	2	12
3	2	6	> 6000	41	16	30
4	1	10	1	> 6000	12	36
5	0	47	1	> 6000	115	100
6	1	0	1	1	1	40
7	9	12	35	10	50	200
8	154	5708	> 6000	> 6000	> 6000	110

For column SINGULAR* we use modular techniques for computing the decomposition of the singular locus. In this table, the computations in Singular that did not finish are all due to the computation of the decomposition of the singular locus (although we know that these examples have only one singularity at the origin).

We note that in most cases our proposed algorithm is much faster than the algorithm implemented in MAPLE. Only in the last table, there is one example in which SINGULAR is significantly slower than MAPLE. For this example, the singular part of the Puiseux expansions involve high degree algebraic extensions, which is at the moment, not optimally implemented in SINGULAR. We expect this to me improved in the future, which will improve our timings in those cases.

Bibliography

M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

J. Böhm, W. Decker, S. Laplagne, G. Pfister, A. Steenpass, and S. Steidel. Parallel algorithms for normalization. arXiv:1110.4299v1 [math.AC], 2011a.

J. Böhm, W. Decker, S. Laplagne, and F. Seelisch. `integralbasis.lib`. A SINGULAR library for computing integral bases in algebraic function fields, 2011b.

J. Böhm, W. Decker, S. Laplagne, and F. Seelisch. `paraplanecurves.lib`. A SINGULAR library for parametrization of rational plane curves, 2011c.

J. Böhm, W. Decker, S. Laplagne, and F. Seelisch. Computing integral bases via localization and Hensel lifting. Preprint, 2012a.

J. Böhm, W. Decker, S. Laplagne, and F. Seelisch. Local to global algorithms for the Gorenstein adjoint ideal of a curve. Preprint, 2012b.

J. Böhm, W. Decker, S. Laplagne, and F. Seelisch. Parametrization of rational curves. Preprint, 2012c.

W. Bosma, J. J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997.

J. P. Brennan and W. V. Vasconcelos. On the structure of closed ideals. *Math. Scand.*, 88(1):3–16, 2001.

E. Brieskorn and H. Knorrer. *Plane Algebraic Curves*. Birkhauser Verlag, 1986.

W. Bruns and R. Koch. Computing the integral closure of an affine semigroup. *Univ. Iagel. Acta Math.*, (39):59–70, 2001.

B. Buchberger. An algorithmic criterion for the solvability of algebraic system of equations. *Aequaotiones Math*, (4):374–383, 1970.

B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bull.*, 10(3):19–29, 1976.

M. Caboara, P. Conti, and C. Traverso. Yet another algorithm for ideal decomposition. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, (12):39–54, 1997.

J. I. Cogolludo. Fundamental group for some cuspidal curves. *Bull. London Math. Soc.*, 31:136–142, 1999.

H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. ISBN 3-540-55640-0.

D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms*. Springer, 1996.

T. de Jong. An algorithm for computing the integral closure. *J. Symbolic Comput.*, 26(3):273–277, 1998.

T. de Jong and G. Pfister. *Local analytic geometry*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 2000. ISBN 3-528-03137-9. Basic theory and applications.

W. Decker, T. de Jong, G.-M. Greuel, and G. Pfister. The normalization: a new algorithm, implementation and comparisons. In *Computational methods for representations of groups and algebras (Essen, 1997)*, volume 173 of *Progr. Math.*, pages 177–185. Birkhäuser, Basel, 1999a.

W. Decker, S. Laplagne, G. Pfister, and H. Schönemann. `primdec.lib`. A SINGULAR library for computing primary decomposition and radical of ideals, 2006.

W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3-1-3 — A computer algebra system for polynomial computations. 2011. http://www.singular.uni-kl.de.

Wolfram Decker, Gert-Martin Greuel, and Gerhard Pfister. Primary decomposition: algorithms and comparisons. In *Algorithmic algebra and number theory (Heidelberg, 1997)*, pages 187–220. Springer, Berlin, 1999b.

A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, (33):73–94, 1991.

J. P. G. L. Dirichlet. *Vorlesungen über Zahlentheorie*. Herausgegeben und mit Zusätzen versehen von R. Dedekind. Vierte, umgearbeitete und vermehrte Auflage. Chelsea Publishing Co., New York, 1968.

T. W. Dubé. The structure of polynomial ideals and grobner bases. *SIAM J. Comput.*, (19):750–773, 1990.

D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. ISBN 0-387-94269-6. With a view toward algebraic geometry.

D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, (110):207–235, 1992.

D. J. Ford. The construction of maximal orders over a Dedekind domain. *J. Symbolic Comput.*, 4(1):69–75, 1987.

P. Gianni and B. Trager. Integral closure of Noetherian rings. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 212–216 (electronic), New York, 1997. ACM.

P. Gianni, B. Trager, and G. Zacharias. Bases and primary decomposition of ideals. *J. Symbolic Computation*, (6):149–167, 1988.

M. Giusti. Some effective problems in polynomial ideal theory. *EUROSAM 84, Lecture Notes in Computer Science*, (174):159–171, 1984.

H. Grauert and R. Remmert. *Analytische Stellenalgebren.* Springer-Verlag, Berlin, 1971. Unter Mitarbeit von O. Riemenschneider, Die Grundlehren der mathematischen Wissenschaften, Band 176.

D. R. Grayson and M. E. Stillman. Macaulay2 1.2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/, 2009.

G.-M. Greuel and G. Pfister. *A Singular introduction to commutative algebra.* Springer, Berlin, extended edition, 2008. ISBN 978-3-540-73541-0. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX).

G.-M. Greuel, S. Laplagne, and G. Pfister. `normal.lib`. A SINGULAR library for computing the normalization of affine rings, 2009.

Gert-Martin Greuel, Santiago Laplagne, and Frank Seelisch. Normalization of rings. *J. Symbolic Comput.*, 45(9):887–901, 2010.

J. Heintz. Definability and fast quantifier elimination over algebraically closed fields. *Theor. Comp. Science*, (24):239–278, 1983.

F. Hess. Computing Riemann–Roch spaces in algebraic function fields and related topics. *Journal of Symbolic Computation*, 33:425–445, 2002.

A. Hirano. Construction of plane curves with cusps. *Saitama Math. J*, 10:21–24, 1992.

T. Hirsch. `reesclos.lib`. A SINGULAR library for computing the integral closure of ideals, 2001.

M.-D. Huang and D. Ieradi. Efficient algorithms for the Riemann–Roch problem and for addition in the Jacobian of a curve. *Journal of Symbolic Computation*, 18:519–539, 1994.

G. Kemper. The calculation of radical ideals in positive characteristic. *J. Symbolic Computation*, (34):229–238, 2002.

T. Krick and A. Logar. Membership problem, representation problem and the computation of the radical for one-dimensional ideals. *Progress in Mathematics*, (94):203–216, 1991a.

T. Krick and A. Logar. An algorithm for the computation of the radical of an ideal in the ring of polynomials. *AAECC9, Springer LNCS*, (539):195–205, 1991b.

T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic nullstellensatz. *Duke Math J.*, (109):521–598, 2001.

S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002. ISBN 0-387-95385-X.

S. Laplagne. An algorithm for the computation of the radical of an ideal. In *ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 191–195, New York, NY, USA, 2006a. ACM Press.

S. Laplagne. Computation of the minimal associated primes. In Wolfram Decker, Mike Dewar, Erich Kaltofen, and Stephen Watt, editors, *Challenges in Symbolic Computation Software*, number 06271 in Dagstuhl Seminar Proceedings. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany, 2006b.

E. Lasker. Zur Theorie der moduln und Ideale. *Math. Ann.*, 60(1):20–116, 1905.

D. A. Leonard and R. Pellikaan. Integral closures and weight functions over finite fields. *Finite Fields Appl.*, 9(4):479–504, 2003.

R. Matsumoto. Computing the radical of an ideal in positive characteristic. *J. Symbolic Computation*, (32):263–271, 2001.

M. Mňuk. An algebraic approach to computing adjoint curves. *J. Symbolic Comput.*, 23(2-3):229–240, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

E. Noether. Idealtheorie in Ringbereichen. *Math. Ann.*, 83(1-2):24–66, 1921.

M. Reid. *Undergraduate commutative algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1995. ISBN 0-521-45255-4.

A. Seidenberg. Construction of the integral closure of a finite integral domain. *Rend. Sem. Mat. Fis. Milano*, 40:100–120, 1970.

A. Seidenberg. Constructions in algebra. *Trans. Amer. Math. Soc.*, (197):273–313, 1974.

A. Seidenberg. Construction of the integral closure of a finite integral domain. II. *Proc. Amer. Math. Soc.*, 52:368–372, 1975.

Anurag K. Singh and Irena Swanson. An algorithm for computing the integral closure. *Algebra Number Theory*, 3(5):587–595, 2009.

H.J.S. Smith. On systems of linear indeterminate equations and congruences. *Philosophical Transactions of the Royal Society of London*, pages 293–326, 1861.

G. Stolzenberg. Constructive normalization of an algebraic variety. *Bull. Amer. Math. Soc.*, 74:595–599, 1968.

I. Swanson and C. Huneke. *Integral closure of ideals, rings, and modules*, volume 336 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006. ISBN 0-521-68860-4.

C. Traverso. A study on algebraic algorithms: the normalization. *Rend. Sem. Mat. Univ. Politec. Torino*, (Special Issue):111–130 (1987), 1986. Conference on algebraic varieties of small dimension (Turin, 1985).

B. L. van der Waerden. *Modern Algebra. Vol. I.* Frederick Ungar Publishing Co., New York, N. Y., 1949. Translated from the second revised German edition by Fred Blum, With revisions and additions by the author.

M. van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *J. Symbolic Comput.*, 18(4):353–363, 1994.

M. van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *J. Symbolic Comput.*, 23(2-3):209–227, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

W. V. Vasconcelos. Computing the integral closure of an affine domain. *Proc. Amer. Math. Soc.*, 113(3):633–638, 1991.

W. V. Vasconcelos. *Computational methods in commutative algebra and algebraic geometry*, volume 2 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. ISBN 3-540-60520-7. With chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman.

W. V. Vasconcelos. Divisorial extensions and the computation of integral closures. *J. Symbolic Comput.*, 30(5):595–604, 2000.

W. V. Vasconcelos. *Integral closure. Rees algebras, multiplicities, algorithms.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005. ISBN 3-540-25540-0.

R. J. Walker. *Algebraic Curves*. Princeton Mathematical Series, vol. 13. Princeton University Press, Princeton, N. J., 1950.