Gert-Martin Greuel, Gerhard Pfister

A SINGULAR Introduction to Commutative Algebra

Mathematics – Monograph (English)

with contributions by
Olaf Bachmann, Christoph Lossen and Hans Schönemann

Second, Extended Edition

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

To Ursula, Ursina, Joscha, Bastian, Wanja, Grischa
G.–M. G.

To Marlis, Alexander, Jeannette
G. P.

Preface to the Second Edition

The first edition of this book was published 5 years ago. When we have been asked to prepare another edition, we decided not only to correct typographical errors, update the references, and improve some of the proofs but also to add new material, some appearing in printed form for the first time.

The major changes in this edition are the following:

(1) A new section about non–commutative Gröbner basis is added to chapter one, written mainly by Viktor Levandovskyy.
(2) Two new sections about characteristic sets and triangular sets together with the corresponding decomposition–algorithm are added to chapter four.
(3) There is a new appendix about polynomial factorization containing univariate factorization over $\mathbb{F}_p$ and $\mathbb{Q}$ and algebraic extensions, as well as multivariate factorization over these fields and over the algebraic closure of $\mathbb{Q}$.
(4) The system SINGULAR has improved quite a lot. A new CD is included, containing the version 3-0-3 with all examples of the book and several new SINGULAR–libraries.
(5) The appendix concerning SINGULAR is rewritten corresponding to the version 3-0-3. In particular, more examples on how to write libraries and about the communication with other systems are given.

We should like to thank many readers for helpful comments and finding typographical errors in the first edition. We thank the Singular Team for the support in producing the new CD. Special thanks to Anne Frühbis–Krüger, Santiago Laplagne, Thomas Markwig, Hans Schönemann, Oliver Wienand, for proof–reading, Viktor Levandovskyy for providing the chapter on non–commutative Gröbner bases and Petra Bäsell for typing the manuscript.

Kaiserslautern, July, 2007

Gert–Martin Greuel
Gerhard Pfister

Preface to the First Edition

In theory there is no difference
between theory and practice.
In practice there is.

Yogi Berra

A SINGULAR Introduction to Commutative Algebra offers a rigorous introduction to commutative algebra and, at the same time, provides algorithms and computational practice. In this book, we do not separate the theoretical and the computational part. Coincidentally, as new concepts are introduced, it is consequently shown, by means of concrete examples and general procedures, how these concepts are handled by a computer. We believe that this combination of theory and practice will provide not only a fast way to enter a rather abstract field but also a better understanding of the theory, showing concurrently how the theory can be applied.

We exemplify the computational part by using the computer algebra system SINGULAR, a system for polynomial computations, which was developed in order to support mathematical research in commutative algebra, algebraic geometry and singularity theory. As the restriction to a specific system is necessary for such an exposition, the book should be useful also for users of other systems (such as *Macaulay2* and *CoCoA*) with similar goals. Indeed, once the algorithms and the method of their application in one system is known, it is usually not difficult to transfer them to another system.

The choice of the topics in this book is largely motivated by what we believe is most useful for studying commutative algebra with a view toward algebraic geometry and singularity theory. The development of commutative algebra, although a mathematical discipline in its own right, has been greatly influenced by problems in algebraic geometry and, conversely, contributed significantly to the solution of geometric problems. The relationship between both disciplines can be characterized by saying that algebra provides rigour while geometry provides intuition.

In this connection, we place computer algebra on top of rigour, but we should like to stress its limited value if it is used without intuition.

During the past thirty years, in commutative algebra, as in many parts of mathematics, there has been a change of interest from a most general theo-

retical setting towards a more concrete and algorithmic understanding. One of the reasons for this was that new algorithms, together with the development of fast computers, allowed non–trivial computations, which had been intractable before. Another reason is the growing belief that algorithms can contribute to a better understanding of a problem. The human idea of "understanding", obviously, depends on the historical, cultural and technical status of the society and, nowadays, understanding in mathematics requires more and more algorithmic treatment and computational mastering. We hope that this book will contribute to a better understanding of commutative algebra and its applications in this sense.

The algorithms in this book are almost all based on Gröbner bases or standard bases. The theory of Gröbner bases is by far the most important tool for computations in commutative algebra and algebraic geometry. Gröbner bases were introduced originally by Buchberger as a basis for algorithms to test the solvability of a system of polynomial computations, to count the number of solutions (with multiplicities) if this number is finite and, more algebraically, to compute in the quotient ring modulo the given polynomials. Since then, Gröbner bases have played an important role for any symbolic computations involving polynomial data, not only in mathematics. We present, right at the beginning, the theory of Gröbner bases and, more generally, standard bases, in a somewhat new flavour.

Synopsis of the Contents of this Book

From the beginning, our aim is to be able to compute effectively in a polynomial ring as well as in the localization of a polynomial ring at a maximal ideal. Geometrically, this means that we want to compute globally with (affine or projective) algebraic varieties and locally with its singularities. In other words, we develop the theory and tools to study the solutions of a system of polynomial equations, either globally or in a neighbourhood of a given point.

The first two chapters introduce the basic theories of rings, ideals, modules and standard bases. They do not require more than a course in linear algebra, together with some training, to follow and do rigorous proofs. The main emphasis is on ideals and modules over polynomial rings. In the examples, we use a few facts from algebra, mainly from field theory, and mainly to illustrate how to use SINGULAR to compute over these fields.

In order to treat Gröbner bases, we need, in addition to the ring structure, a total ordering on the set of monomials. We do not require, as is the case in usual treatments of Gröbner bases, that this ordering be a well–ordering. Indeed, non–well–orderings give rise to local rings, and are necessary for a computational treatment of local commutative algebra. Therefore, we introduce, at an early stage, the general notion of localization. Having this, we introduce the notion of a (weak) normal form in an axiomatic way. The standard basis algorithm, as we present it, is the same for any monomial ordering,

only the normal form algorithm differs for well–orderings, called global orderings in this book, and for non–global orderings, called local, respectively mixed, orderings.

A standard basis of an ideal or a module is nothing but a special set of generators (the leading monomials generate the leading ideal), which allows the computation of many invariants of the ideal or module just from its leading monomials. We follow the tradition and call a standard basis for a global ordering a Gröbner basis. The algorithm for computing Gröbner bases is Buchberger's celebrated algorithm. It was modified by Mora to compute standard bases for local orderings, and generalized by the authors to arbitrary (mixed) orderings. Mixed orderings are necessary to generalize algorithms (which use an extra variable to be eliminated later) from polynomial rings to local rings. As the general standard basis algorithm already requires slightly more abstraction than Buchberger's original algorithm, we present it first in the framework of ideals. The generalization to modules is then a matter of translation after the reader has become familiar with modules. Chapter 2 also contains some less elementary concepts such as tensor products, syzygies and resolutions. We use syzygies to give a proof of Buchberger's criterion and, at the same time, the main step for a constructive proof of Hilbert's syzygy theorem for the (localization of the) polynomial ring. These first two chapters finish with a collection of methods on how to use standard bases for various computations with ideals and modules, so–called "Gröbner basics".

The next four chapters treat some more involved but central concepts of commutative algebra. We follow the same method as in the first two chapters, by consequently showing how to use computers to compute more complicated algebraic structures as well. Naturally, the presentation is a little more condensed, and the verification of several facts of a rather elementary nature are left to the reader as an exercise.

Chapter 3 treats integral closure, dimension theory and Noether normalization. Noether normalization is a cornerstone in the theory of affine algebras, theoretically as well as computationally. It relates affine algebras, in a controlled manner, to polynomial algebras. We apply the Noether normalization to develop the dimension theory for affine algebras, to prove the Hilbert Nullstellensatz and E. Noether's theorem that the normalization of an affine ring (that is, the integral closure in its total ring of fractions) is a finite extension. For all this, we provide algorithms and concrete examples on how to compute them. A highlight of this chapter is the algorithm to compute the non–normal locus and the normalization of an affine ring. This algorithm is based on a criterion due to Grauert and Remmert, which had escaped the computer algebra community for many years, and was rediscovered by T. de Jong. The chapter ends with an extra section containing some of the larger procedures, written in the SINGULAR programming language.

Chapter 4 is devoted to primary decomposition and related topics such as the equidimensional part and the radical of an ideal. We start with the

usual, short and elegant but not constructive proof, of primary decomposition of an ideal. Then we present the constructive approach due to Gianni, Trager and Zacharias. This algorithm returns the primary ideals and the associated primes of an ideal in the polynomial ring over a field of characteristic 0, but also works well if the characteristic is sufficiently large, depending on the given ideal. The algorithm, as implemented in SINGULAR is often surprisingly fast. As in Chapter 3, we present the main procedures in an extra section.

In contrast to the relatively simple existence proof for primary decomposition, it is extremely difficult to actually decompose even quite simple ideals, by hand. The reason becomes clear when we consider the constructive proofs which are all quite involved, and which use many non–obvious results from commutative algebra, field theory and Gröbner bases. Indeed, primary decomposition is an important example, where we learn much more from the constructive proof than from the abstract one.

In Chapter 5 we introduce the Hilbert function and the Hilbert polynomial of graded modules together with its application to dimension theory. The Hilbert polynomial, respectively its local counterpart, the Hilbert–Samuel polynomial, contains important information about a homogeneous ideal in a polynomial ring, respectively an arbitrary ideal, in a local ring. The most important one, besides the dimension, is the degree in the homogeneous case, respectively the multiplicity in the local case. We prove that the Hilbert (–Samuel) polynomial of an ideal and of its leading ideal coincide, with respect to a degree ordering, which is the basis for the computation of these functions. The chapter finishes with a proof of the Jacobian criterion for affine K–algebras and its application to the computation of the singular locus, which uses the equidimensional decomposition of the previous chapter; other algorithms, not using any decomposition, are given in the exercises to Chapter 7.

Standard bases were, independent of Buchberger, introduced by Hironaka in connection with resolution of singularities and by Grauert in connection with deformation of singularities, both for ideals in power series rings. We introduce completions and formal power series in Chapter 6. We prove the classical Weierstraß preparation and division theorems and Grauert's generalization of the division theorem to ideals, in formal power series rings. Besides this, the main result here is that standard bases of ideals in power series rings can be computed if the ideal is generated by polynomials. This is the basis for computations in local analytic geometry and singularity theory.

The last chapter, Chapter 7, gives a short introduction to homological algebra. The main purpose is to study various aspects of depth and flatness. Both notions play an important role in modern commutative algebra and algebraic geometry. Indeed, flatness is the algebraic reason for what the ancient geometers called "principle of conservation of numbers", as it guarantees that certain invariants behave continuously in families of modules, respectively varieties. After studying and showing how to compute Tor–modules, we use Fit-

ting ideals to show that the flat locus of a finitely presented module is open. Moreover, we present an algorithm to compute the non–flat locus and, even further, a flattening stratification of a finitely presented module. We study, in some detail, the relation between flatness and standard bases, which is somewhat subtle for mixed monomial orderings. In particular, we use flatness to show that, for any monomial ordering, the ideal and the leading ideal have the same dimension.

In the final sections of this chapter we use the Koszul complex to study the relation between the depth and the projective dimension of a module. In particular, we prove the Auslander–Buchsbaum formula and Serre's characterization of regular local rings. These can be used to effectively test the Cohen–Macaulay property and the regularity of a local K–algebra.

The book ends with two appendices, one on the geometric background and the second one on an overview on the main functionality of the system SINGULAR.

The geometric background introduces the geometric language, to illustrate some of the algebraic constructions introduced in the previous chapters. One of the objects is to explain, in the affine as well as in the projective setting, the geometric meaning of elimination as a method to compute the (closure of the) image of a morphism. Moreover, we explain the geometric meaning of the degree and the multiplicity defined in the chapter on the Hilbert Polynomial (Chapter 5), and prove some of its geometric properties. This appendix ends with a view towards singularity theory, just touching on Milnor and Tjurina numbers, Arnold's classification of singularities, and deformation theory. All this, together with other concepts of singularity theory, such as Puiseux series of plane curve singularities and monodromy of isolated hypersurface singularities, and many more, which are not treated in this book, can be found in the accompanying libraries of SINGULAR.

The second appendix gives a condensed overview of the programming language of SINGULAR, data types, functions and control structure of the system, as well as of the procedures appearing in the libraries distributed with the system. Moreover, we show by three examples (Maple, Mathematica, MuPAD), how SINGULAR can communicate with other systems.

How to Use the Text

The present book is based on a series of lectures held by the authors over the past ten years. We tried several combinations in courses of two, respectively four, hours per week in a semester (12 – 14 weeks). There are at least four aspects on how to use the text for a lecture:

(A) Focus on computational aspects of standard bases, and syzygies.

A possible selection for a two–hour lecture is to treat Chapters 1 and 2 completely (possibly omitting 2.6, 2.7). In a four–hour course one can treat, additionally, 3.1 – 3.5 together with either 4.1 – 4.3 or 4.1 and 5.1 – 5.3.

(B) Focus on applications of methods based on standard basis, respectively syzygies, for treating more advanced problems such as primary decomposition, Hilbert functions, or flatness (regarding the standard basis, respectively syzygy, computations as "black boxes").

In this context a two–hour lecture could cover Sections 1.1 – 1.4 (only treating global orderings), 1.6 (omitting the algorithms), 1.8, 2.1, Chapter 3 and Section 4.1. A four–hour lecture could treat, in addition, the case of local orderings, Section 1.5, and selected parts of Chapters 5 and 7.

(C) Focus on the theory of commutative algebra, using SINGULAR as a tool for examples and experiments.

Here a two–hour course could be based on Sections 1.1, 1.3, 1.4, 2.1, 2.2, 2.4, 2.7, 3.1 – 3.5 and 4.1. For a four–hour lecture one could choose, additionally, Chapter 5 and Sections 7.1 – 7.4.

(D) Focus on geometric aspects, using SINGULAR as a tool for examples.

In this context a two–hour lecture could be based on Appendix A.1, A.2 and A.4, together with the needed concepts and statements of Chapters 1 and 3. For a four–hour lecture one is free to choose additional parts of the appendix (again together with the necessary background from Chapters 1 – 7).

Of course, the book may also serve as a basis for seminars and, last but not least, as a reference book for computational commutative algebra and algebraic geometry.

Working with SINGULAR

The original motivation for the authors to develop a computer algebra system in the mid eighties, was the need to compute invariants of ideals and modules in local rings, such as Milnor numbers, Tjurina numbers, and dimensions of modules of differentials. The question was whether the exactness of the Poincaré complex of a complete intersection curve singularity is equivalent to the curve being quasihomogeneous. This question was answered by an early version of SINGULAR: it is not [190]. In the sequel, the development of SINGULAR was always influenced by mathematical problems, for instance, the famous Zariski conjecture, saying that the constancy of the Milnor number in a family implies constant multiplicity [111]. This conjecture is still unsolved.

Enclosed in the book one finds a CD with folders `EXAMPLES`, `LIBRARIES`, `MAC`, `MANUAL`, `UNIX` and `WINDOWS`. The folder `EXAMPLES` contains all SINGULAR Examples of the book, the procedures and the links to Mathematica, Maple and MuPAD. The other folders contain the SINGULAR binaries for the respective platforms, the manual, a tutorial and the SINGULAR libraries. SINGULAR can be installed following the instructions in the `INSTALL_<platform>.html` (or `INSTALL_<platform>.txt`) file of the respective folder. We also should like to refer to the SINGULAR homepage

http://www.singular.uni-kl.de

which always offers the possibility to download the newest version of SINGULAR, provides support for SINGULAR users and a discussion forum. Moreover, one finds there a lot of useful information around SINGULAR, for instance, more advanced examples and applications than provided in this book.

Comments and Corrections

We should like to encourage comments, suggestions and corrections to the book. Please send them to either of us:

Gert–Martin Greuel greuel@mathematik.uni-kl.de
Gerhard Pfister pfister@mathematik.uni-kl.de

We also encourage the readers to check the web site for *A SINGULAR Introduction to Commutative Algebra*,

http://www.singular.uni-kl.de/Singular-book.html

This site will contain lists of corrections, respectively of solutions for selected exercises.

Acknowledgements

As is customary for textbooks, we use and reproduce results from commutative algebra, usually without any specific attribution and reference. However, we should like to mention that we have learned commutative algebra mainly from the books of Zariski–Samuel [238], Nagata [183], Atiyah–Macdonald [6], Matsumura [159] and from Eisenbud's recent book [66]. The geometric background and motivation, present at all times while writing this book, were laid by our teachers Egbert Brieskorn and Herbert Kurke. The reader will easily recognize that our book owes a lot to the admirable work of the above–mentioned mathematicians, which we gratefully acknowledge.

There remains only the pleasant duty of thanking the many people who have contributed in one way or another to the preparation of this work. First of all, we should like to mention Christoph Lossen, who not only substantially improved the presentation but also contributed to the theory as well as to proofs, examples and exercises.

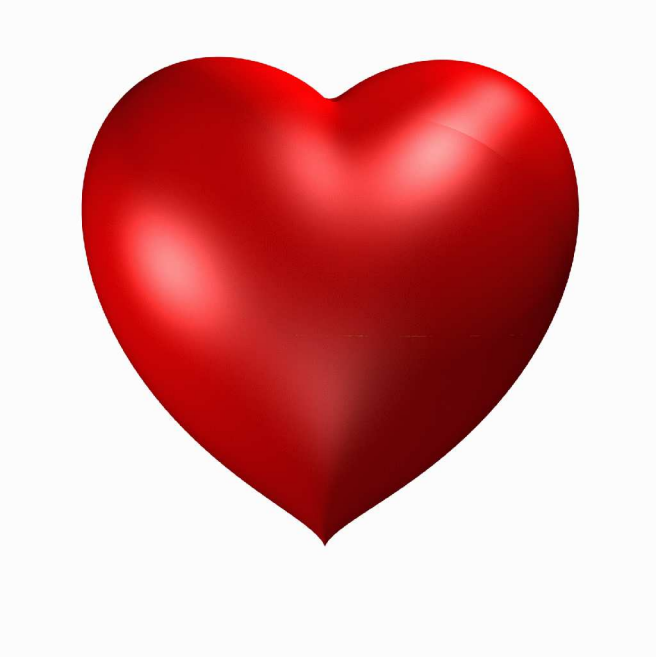
The book could not have been written without the system SINGULAR, which has been developed over a period of about fifteen years by Hans Schönemann and the authors, with considerable contributions by Olaf Bachmann. We feel that it is just fair to mention these two as co–authors of the book, acknowledging, in this way, their contribution as the principal creators of the SINGULAR system.[1]

[1] *"Software is hard. It's harder than anything else I've ever had to do."* (Donald E. Knuth)

Further main contributors to SINGULAR include: W. Decker, A. Frühbis-Krüger, H. Grassmann, T. Keilen, K. Krüger, V. Levandovskyy, C. Lossen, M. Messollen, W. Neumann, W. Pohl, J. Schmidt, M. Schulze, T. Siebert, R. Stobbe, M. Wenk, E. Westenberger and T. Wichmann, together with many authors of SINGULAR libraries mentioned in the headers of the corresponding library.

Proofreading was done by many of the above contributors and, moreover, by Y. Drozd, T. de Jong, D. Popescu, and our students M. Brickenstein, K. Dehmann, M. Kunte, H. Markwig and M. Olbermann. Last but not least, Pauline Bitsch did the LaTeX–typesetting of many versions of our manuscript and most of the pictures were prepared by Thomas Keilen.

We wish to express our heartfelt[2] thanks to all these contributors.



The book is dedicated to our families, especially to our wives Ursula and Marlis, whose encouragement and constant support have been invaluable.

Kaiserslautern, March, 2002

Gert–Martin Greuel
Gerhard Pfister

[2] The heart is displayed by using the programme `surf`, see SINGULAR Example A.1.1.

Contents

1. Rings, Ideals and Standard Bases

1.1 Rings, Polynomials and Ring Maps

The concept of a ring is probably the most basic one in commutative and non–commutative algebra. Best known are the ring of integers $\mathbb{Z}$ and the polynomial ring $K[x]$ in one variable x over a field K.

We shall now introduce the general concept of a ring with special emphasis on polynomial rings.

Definition 1.1.1.

(1) A *ring* is a set A together with an addition $+ : A \times A \to A$, $(a, b) \mapsto a+b$, and a multiplication $\cdot : A \times A \to A$, $(a, b) \mapsto a \cdot b = ab$, satisfying
   a) A, together with the addition, is an abelian group; the neutral element being denoted by 0 and the inverse of $a \in A$ by $-a$;
   b) the multiplication on A is associative, that is, $(ab)c = a(bc)$ and the distributive law holds, that is, $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$, for all $a, b, c \in A$.

(2) A is called *commutative* if $ab = ba$ for $a, b \in A$ and has an *identity* if there exists an element in A, denoted by 1, such that $1 \cdot a = a \cdot 1$ for all $a \in A$.

In this book, except for chapter 1.9, a *ring always means a commutative ring with identity*. Because of (1) a ring cannot be empty but it may consist only of one element 0, this being the case if and only if $1 = 0$.

Definition 1.1.2.

(1) A subset of a ring A is called a *subring* if it contains 1 and is closed under the ring operations induced from A.

(2) $u \in A$ is called a *unit* if there exists a $u' \in A$ such that $uu' = 1$. The set of units is denoted by A^*; it is a group under multiplication.

(3) A ring is a *field* if $1 \neq 0$ and any non–zero element is a unit, that is $A^* = A - \{0\}$.

(4) Let A be a ring, $a \in A$, then $\langle a \rangle := \{af \mid f \in A\}$.

Any field is a ring, such as $\mathbb{Q}$ (the rational numbers), or $\mathbb{R}$ (the real numbers), or $\mathbb{C}$ (the complex numbers), or $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (the finite field with p elements

where p is a prime number, cf. Exercise 1.1.3) but $\mathbb{Z}$ (the integers) is a ring which is not a field.

$\mathbb{Z}$ is a subring of $\mathbb{Q}$, we have $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. $\mathbb{N} \subset \mathbb{Z}$ denotes the set of nonnegative integers.

Definition 1.1.3. Let A be a ring.

(1) A *monomial* in n variables (or indeterminates) $x_1, \ldots, x_n$ is a power product

$$x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, \qquad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n .$$

The set of monomials in n variables is denoted by

$$\mathrm{Mon}(x_1, \ldots, x_n) = \mathrm{Mon}_n := \{x^\alpha \mid \alpha \in \mathbb{N}^n\} .$$

Note that $\mathrm{Mon}(x_1, \ldots, x_n)$ is a semigroup under multiplication, with neutral element $1 = x_1^0 \cdot \ldots \cdot x_n^0$.
We write $x^\alpha \mid x^\beta$ if x^α *divides* x^β, which means that $\alpha_i \leq \beta_i$ for all i and, hence, $x^\beta = x^\gamma x^\alpha$ for $\gamma = \beta - \alpha \in \mathbb{N}^n$.

(2) A *term* is a monomial times a coefficient (an element of A),

$$ax^\alpha = ax_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, \quad a \in A .$$

(3) A *polynomial over* A is a finite A–linear combination of monomials, that is, a finite sum of terms,

$$f = \sum_\alpha a_\alpha x^\alpha = \sum_{\alpha \in \mathbb{N}^n}^{\text{finite}} a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} ,$$

with $a_\alpha \in A$. For $\alpha \in \mathbb{N}^n$, let $|\alpha| := \alpha_1 + \cdots + \alpha_n$.
The integer $\deg(f) := \max\{|\alpha| \mid a_\alpha \neq 0\}$ is called the *degree* of f if $f \neq 0$; we set $\deg(f) = -1$ for f the zero polynomial.

(4) The *polynomial ring* $A[x] = A[x_1, \ldots, x_n]$ in n variables over A is the set of all polynomials together with the usual addition and multiplication:

$$\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha := \sum_\alpha (a_\alpha + b_\alpha) x^\alpha,$$

$$\left(\sum_\alpha a_\alpha x^\alpha\right) \cdot \left(\sum_\beta b_\beta x^\beta\right) := \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right) x^\gamma .$$

$A[x_1, \ldots, x_n]$ is a commutative ring with identity $1 = x_1^0 \cdot \ldots \cdot x_n^0$ which we identify with the identity element $1 \in A$. Elements of $A \subset A[x]$ are called *constant polynomials*, they are characterized by having degree ≤ 0. A is called the *ground ring* of $A[x]$, respectively the *ground field*, if A is a field.

Note that any monomial is a term (with coefficient 1) but, for example, 0 is a term but not a monomial. For us the most important case is the polynomial ring $K[x] = K[x_1, \ldots, x_n]$ over a field K. By Exercise 1.3.1 only the non–zero constants are units of $K[x]$, that is, $K[x]^* = K^* = K \setminus \{0\}$.

If K is an infinite field, we can identify polynomials $f \in K[x_1, \ldots, x_n]$ with their associated *polynomial function*

$$\tilde{f} : K^n \longrightarrow K, \quad (p_1, \ldots, p_n) \longmapsto f(p_1, \ldots, p_n)\,,$$

but for finite fields $\tilde{f}$ may be zero for a non–zero f (cf. Exercise 1.1.4).

Any polynomial in $n-1$ variables can be considered as a polynomial in n variables (where the n–th variable does not appear) with the usual ring operations on polynomials in n variables. Hence, $A[x_1, \ldots, x_{n-1}] \subset A[x_1, \ldots, x_n]$ is a subring and it follows directly from the definition of polynomials that

$$A[x_1, \ldots, x_n] = (A[x_1, \ldots, x_{n-1}])[x_n]\,.$$

Hence, we can write $f \in A[x_1, \ldots, x_n]$ in a unique way, either as

$$f = \sum_{\alpha \in \mathbb{N}^n}^{\text{finite}} a_\alpha x^\alpha,\ a_\alpha \in A$$

or as

$$f = \sum_{\nu \in \mathbb{N}}^{\text{finite}} f_\nu x_n^\nu\,, \quad f_\nu \in A[x_1, \ldots, x_{n-1}]\,.$$

The first representation of f is called *distributive* while the second is called *recursive*.

Remark 1.1.4. Both representations play an important role in computer algebra. The practical performance of an implemented algorithm may depend drastically on the internal representation of polynomials (in the computer). Usually the distributive representation is chosen for algorithms related to Gröbner basis computations while the recursive representation is preferred for algorithms related to factorization of polynomials.

Definition 1.1.5. A *morphism* or *homomorphism* of rings is a map $\varphi : A \to B$ satisfying $\varphi(a + a') = \varphi(a) + \varphi(a')$, $\varphi(aa') = \varphi(a)\varphi(a')$, for all $a, a' \in A$, and $\varphi(1) = 1$. We call a morphism of rings also a *ring map*, and B is called an *A–algebra*.[1]

We have $\varphi(a) = \varphi(a \cdot 1) = \varphi(a) \cdot 1$. If φ is fixed, we also write $a \cdot b$ instead of $\varphi(a) \cdot b$ for $a \in A$ and $b \in B$.

[1] See also Example 2.1.2 and Definition 2.1.3.

Lemma 1.1.6. *Let $A[x_1, \dots x_n]$ be a polynomial ring, $\psi : A \to B$ a ring map, C a B–algebra, and $f_1, \dots, f_n \in C$. Then there exists a unique ring map*

$$\varphi : A[x_1, \dots, x_n] \longrightarrow C$$

satisfying $\varphi(x_i) = f_i$ for $i = 1, \dots, n$ and $\varphi(a) = \psi(a) \cdot 1 \in C$ for $a \in A$.

Proof. Given any $f = \sum_\alpha a_\alpha x^\alpha \in A[x]$, then a ring map φ with $\varphi(x_i) = f_i$, and $\varphi(a) = \psi(a)$ for $a \in A$ must satisfy (by Definition 1.1.5)

$$\varphi(f) = \sum_\alpha \psi(a_\alpha)\varphi(x_1)^{\alpha_1} \cdot \ldots \cdot \varphi(x_n)^{\alpha_n} .$$

Hence, φ is uniquely determined. Moreover, defining $\varphi(f)$ for $f \in A[x]$ by the above formula, it is easy to see that φ becomes a homomorphism, which proves existence. □

We shall apply this lemma mainly to the case where C is the polynomial ring $B[y_1, \dots, y_m]$.

In SINGULAR one can define polynomial rings over the following fields:

(1) the field of rational numbers $\mathbb{Q}$,
(2) finite fields $\mathbb{F}_p$, p a prime number ≤ 32003,
(3) finite fields $\mathrm{GF}(p^n)$ with p^n elements, p a prime, $p^n \leq 2^{15}$,
(4) transcendental extensions of $\mathbb{Q}$ or $\mathbb{F}_p$,
(5) simple algebraic extensions of $\mathbb{Q}$ or $\mathbb{F}_p$,
(6) simple precision real floating point numbers,
(7) arbitrary prescribed real floating point numbers,
(8) arbitrary prescribed complex floating point numbers.

For the definitions of rings over fields of type (3) and (5) we use the fact that for a polynomial ring $K[x]$ in one variable x over a field and $f \in K[x] \setminus \{0\}$ the quotient ring $K[x]/\langle f \rangle$ is a field if and only if f is *irreducible*, that is, f cannot be written as a product of two polynomials of lower degree (cf. Exercise 1.1.5). If f is irreducible and monic, then it is called the *minimal polynomial* of the field extension $K \subset K[x]/\langle f \rangle$ (cf. Example 1.1.8).

Remark 1.1.7. Indeed, the computation over the above fields (1) – (5) is exact, only limited by the internal memory of the computer. Strictly speaking, floating point numbers, as in (6) – (8), do not represent the field of real (or complex) numbers. Because of rounding errors, the product of two non–zero elements or the difference between two unequal elements may be zero (the latter case is the more serious one since the individual elements may be very big). Of course, in many cases one can trust the result, but we should like to emphasize that this remains the responsibility of the user, even if one computes with very high precision.

In SINGULAR, field elements have the type *number* but notice that one *can define and use numbers only in a polynomial ring with at least one variable* and a specified monomial ordering. For example, if one wishes to compute with arbitrarily big integers or with exact arithmetic in $\mathbb{Q}$, this can be done as follows:

SINGULAR Example 1.1.8 (computation in fields).
In the examples below we have used the degree reverse lexicographical ordering `dp` but we could have used any other monomial ordering (cf. Section 1.2). Actually, this makes no difference as long as we do simple manipulations with polynomials. However, more complicated operations on ideals such as the `std` or `groebner` command return results which depend very much on the chosen ordering.

(1) Computation in the field of *rational numbers*:

```
ring A = 0,x,dp;
number n = 12345/6789;
n^5;                    //common divisors are cancelled
//-> 1179910858126071875/59350279669807543
```

Note: Typing just `123456789^5;` will result in integer overflow since `123456789` is considered as an integer (machine integer of limited size) and not as an element in the field of rational numbers; however, also correct would be `number(123456789)^5;`.

(2) Computation in *finite fields*:

```
ring A1 = 32003,x,dp;   //finite field Z/32003
number(123456789)^5;
//-> 8705

ring A2 = (2^3,a),x,dp; //finite (Galois) field GF(8)
                        //with 8 elements
number n = a+a2;        //a is a generator of the group
                        //GF(8)-{0}
n^5;
//-> a6
minpoly;                //minimal polynomial of GF(8)
//-> 1*a^3+1*a^1+1*a^0

ring A3 = (2,a),x,dp;   //infinite field Z/2(a) of
                        //characteristic 2
minpoly = a20+a3+1;     //define a minimal polynomial
                        //a^20+a^3+1
                        //now the ground field is
                        //GF(2^20)=Z/2[a]/<a^20+a^3+1>,
number n = a+a2;        //a finite field
```

```
                          //with 2^20 elements
n^5;                      //a is a generator of the group
                          //GF(2^20)-{0}
//-> (a10+a9+a6+a5)
```

Note: For computation in finite fields $\mathbb{Z}/p\mathbb{Z}$, $p \leq 32003$, respectively $GF(p^n)$, $p^n \leq 2^{15}$, one should use rings as `A1` respectively `A2` since for these fields SINGULAR uses look–up tables, which is quite fast. For other finite fields a *minimal polynomial* as in `A3` must be specified. A good choice are the *Conway polynomials* (cf. [126]). SINGULAR does not, however, check the irreducibility of the chosen minimal polynomial. This can be done as in the following example.

```
ring tst = 2,a,dp;
factorize(a20+a2+1,1);
//-> _[1]=a3+a+1   //not irreducible! We have two factors
//-> _[2]=a7+a5+a4+a3+1
factorize(a20+a3+1,1);   //irreducible
//-> _[1]=a20+a3+1
```

To obtain the multiplicities of the factors, use `factorize(a20+a2+1);`.

(3) Computation with *real* and *complex floating point numbers*, 30 digits precision:

```
ring R1 = (real,30),x,dp;
number n = 123456789.0;
n^5;             //compute with a precision of 30 digits
//-> 0.286797186029971810723376143809e+41
```

Note: n^5 is a number whose integral part has 41 digits (indicated by `e+41`). However, only 30 digits are computed.

```
ring R2 = (complex,30,I),x,dp;//I denotes imaginary unit
number n = 123456789.0+0.0001*I;
n^5;            //complex number with 30 digits precision
//-> (0.286797186029971810723374262133e+41
     +I*116152861399129622075046746710)
```

(4) Computation with rational numbers and *parameters*, that is, in $\mathbb{Q}(a,b,c)$, the quotient field of $\mathbb{Q}[a,b,c]$:

```
ring R3 = (0,a,b,c),x,dp;
number n = 12345a+12345/(78bc);
n^2;
//->(103021740900a2b2c2+2641583100abc+16933225)/(676b2c2)
n/9c;
//-> (320970abc+4115)/(234bc2)
```

We shall now show how to define the polynomial ring in n variables $x_1, \ldots, x_n$ over the above mentioned fields K. We can do this for any n, but we have to specify an integer n first. The same remark applies if we work with transcendental extensions of degree m; we usually call the elements $t_1, \ldots, t_m$ of a transcendental basis (free) *parameters*. If g is any non–zero polynomial in the parameters $t_1, \ldots, t_m$, then g and $1/g$ are numbers in the corresponding ring.

For further examples see the SINGULAR Manual [116].

SINGULAR Example 1.1.9 (computation in polynomial rings).

Let us create *polynomial rings* over different fields. By typing the name of the *ring* we obtain all relevant information about the ring.

```
ring A = 0,(x,y,z),dp;
poly f = x3+y2+z2;           //same as x^3+y^2+z^2
f*f-f;
//-> x6+2x3y2+2x3z2+y4+2y2z2+z4-x3-y2-z2
```

SINGULAR understands short (e.g., `2x2+y3`) and long (e.g., `2*x^2+y^3`) input. By default the short output is displayed in rings without parameters and with one–letter variables, whilst the long output is used, for example, for indexed variables. The command `short=0;` forces all output to be displayed in the long format.

Computations in polynomial rings over other fields follow the same pattern. Try `ring R=32003,x(1..3),dp;` (finite ground field), respectively `ring R=(0,a,b,c),(x,y,z,w),dp;` (ground field with parameters), and type `R;` to obtain information about the ring. The command `setring` allows switching from one ring to another, for example, `setring A4;` makes `A4` the basering.

We use Lemma 1.1.6 to define ring maps in SINGULAR. Indeed, one has three possibilities, `fetch, imap` and `map`, to define ring maps by giving the name of the preimage ring and a list of polynomials $f_1, \ldots, f_n$ (as many as there are variables in the preimage ring) in the current basering. The commands `fetch`, respectively `imap`, map an object directly from the preimage ring to the basering whereas `fetch` maps the first variable to the first, the second to the second and so on (hence, is convenient for renaming the variables), while `imap` maps a variable to the variable with the same name (or to 0 if it does not exist), hence is convenient for inclusion of sub–rings or for changing the monomial ordering.

Note: All maps go from a predefined ring to the basering.

SINGULAR Example 1.1.10 (methods for creating ring maps).

map: preimage ring $\longrightarrow$ basering

(1) General definition of a *map*:

```
ring A = 0,(a,b,c),dp;
poly f = a+b+ab+c3;

ring B = 0,(x,y,z),dp;
map F  = A, x+y,x-y,z;//map F from ring A (to basering B)
                      //sending a -> x+y, b -> x-y, c -> z
poly g = F(f);        //apply F
g;
//-> z3+x2-y2+2x
```

(2) Special maps (`imap, fetch`):

```
ring A1 = 0,(x,y,c,b,a,z),dp;
imap(A,f);            //imap preserves names of variables
//-> c3+ba+b+a
fetch(A,f);           //fetch preserves order of variables
//-> c3+xy+x+y
```

Exercises

1.1.1. The set of units A^* of a ring A is a group under multiplication.

1.1.2. The *direct sum of rings* $A \oplus B$, together with component–wise addition and multiplication is again a ring.

1.1.3. Prove that, for $n \in \mathbb{Z}$, the following are equivalent:

(1) $\mathbb{Z}/\langle n\rangle$ is a field.
(2) $\mathbb{Z}/\langle n\rangle$ is an integral domain.
(3) n is a prime number.

1.1.4. Let K be a field and $f \in K[x_1, \ldots, x_n]$. Then f determines a *polynomial function* $\widetilde{f} : K^n \to K$, $(p_1, \ldots, p_n) \mapsto f(p_1, \ldots, p_n)$.

(1) If K is infinite then f is uniquely determined by $\tilde{f}$.
(2) Show by an example that this is not necessarily true for K finite.
(3) Let K be a finite field with q elements. Show that each polynomial $f \in K[x_1, \ldots, x_n]$ of degree at most $q-1$ in each variable is already determined by the polynomial function $\widetilde{f} : K^n \to K$.

1.1.5. Let $f \in K[x]$ be a non–constant polynomial in one variable over the field K. f is called *irreducible* if $f \notin K$ and if it is not the product of two polynomials of strictly smaller degree. Prove that the following are equivalent:

(1) $K[x]/\langle f\rangle$ is a field.
(2) $K[x]/\langle f\rangle$ is an integral domain.
(3) f is irreducible.

1.1.6. An irreducible polynomial $f = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$, K a field, is called *separable*, if f has only simple roots in $\overline{K}$, the algebraic closure of K.

An algebraic field extension $K \subset L$ is called *separable* if any element $a \in L$ is separable over K, that is, the minimal polynomial of a over K is separable.

(1) Show that $f \neq 0$ is separable if and only if f and its formal derivative $Df := na_n x^{n-1} + \cdots + a_1$ have no common factor of degree ≥ 1.
(2) A finite separable field extension $K \subset L$ is generated by a *primitive element*, that is, there exists an irreducible $f \in K[x]$ such that $L \cong K[x]/\langle f\rangle$.
(3) K is called a *perfect field* if every irreducible polynomial $f \in K[x]$ is separable. Show that finite fields, algebraically closed fields and fields of characteristic 0 are perfect.

1.1.7. Which of the fields in SINGULAR, (1) – (5), are perfect, which not?

1.1.8. Compute `(10!)^5` with the help of SINGULAR.

1.1.9. Declare in SINGULAR a polynomial ring in the variables `x(1)`, `x(2)`, `x(3)`, `x(4)` over the finite field with eight elements

1.1.10. Declare in SINGULAR the ring $A = \mathbb{Q}(a,b,c)[x,y,z,w]$ and compute f^2/c^2 for $f = (ax^3 + by^2 + cz^2)(ac - bc)$.

1.1.11. Declare in SINGULAR the rings $A = \mathbb{Q}[a,b,c]$ and $B = \mathbb{Q}[a]$. In A define the polynomial $f = a + b + ab + c^3$. Try in B the commands `imap(A,f)` and `fetch(A,f)`.

1.1.12. Declare in SINGULAR the ring $\mathbb{Q}(i)[u,v,w]$, $i^2 = -1$, and compute $\big((i + i^2 + 1)(uvw)\big)^3$.

1.1.13. Write a SINGULAR procedure, depending on two integers p, d, with p a prime, which returns all polynomials in $\mathbb{F}_p[x]$ of degree d such that the corresponding polynomial function vanishes. Use the procedure to display all $f \in (\mathbb{Z}/5\mathbb{Z})[x]$ of degree ≤ 6 such that $\tilde{f} = 0$.

1.2 Monomial Orderings

The presentation of a polynomial as a linear combination of monomials is unique only up to an order of the summands, due to the commutativity of the addition. We can make this order unique by choosing a total ordering on the set of monomials. For further applications it is necessary, however, that the ordering is compatible with the semigroup structure on Mon_n.

Definition 1.2.1. A *monomial ordering* or *semigroup ordering* is a total (or linear) ordering $>$ on the set of monomials $\mathrm{Mon}_n = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ in n variables satisfying

$$x^\alpha > x^\beta \implies x^\gamma x^\alpha > x^\gamma x^\beta$$

for all $\alpha, \beta, \gamma \in \mathbb{N}^n$. We say also $>$ is a *monomial ordering on* $A[x_1, \ldots, x_n]$, A any ring, meaning that $>$ is a monomial ordering on Mon_n.

We identify Mon_n with $\mathbb{N}^n$, and then a monomial ordering is a total ordering on $\mathbb{N}^n$, which is compatible with the semigroup structure on $\mathbb{N}^n$ given by addition. A typical, and important, example is provided by the lexicographical ordering on $\mathbb{N}^n$: $x^\alpha > x^\beta$ if and only if the first non–zero entry of $\alpha - \beta$ is positive. We shall see different monomial orderings later.

Monomial orderings provide an extra structure on the set of monomials and, hence, also on the polynomial ring. Although they have been used in several places to prove difficult mathematical theorems they are hardly part of classical commutative algebra. Monomial orderings, however, can be quite powerful tools in theoretical investigations (cf. [98]) but, in addition, they are indispensable in many serious and deeper polynomial computations.

From a practical point of view, a monomial ordering $>$ allows us to write a polynomial $f \in K[x]$ in a unique ordered way as

$$f = a_\alpha x^\alpha + a_\beta x^\beta + \cdots + a_\gamma x^\gamma \,,$$

with $x^\alpha > x^\beta > \cdots > x^\gamma$, where no coefficient is zero (a sparse representation of f). Moreover, this allows the representation of a polynomial in a computer as an ordered list of coefficients, making equality tests very simple and fast (assuming this is the case for the ground field). Additionally, this order does not change if we multiply f with a monomial. For highly sophisticated presentations of monomials and polynomials in a computer see [10]. There are many more and deeper properties of monomial orderings and, moreover, different orderings have different further properties.

Definition 1.2.2. Let $>$ be a fixed monomial ordering. Write $f \in K[x]$, $f \neq 0$, in a unique way as a sum of non–zero terms

$$f = a_\alpha x^\alpha + a_\beta x^\beta + \cdots + a_\gamma x^\gamma, \quad x^\alpha > x^\beta > \cdots > x^\gamma \,,$$

and $a_\alpha, a_\beta, \ldots, a_\gamma \in K$. We define:

(1) $\mathrm{LM}(f) :=$ `leadmonom(f)`$:= x^\alpha$, the *leading monomial* of f,
(2) $\mathrm{LE}(f) :=$ `leadexp(f)`$:= \alpha$, the *leading exponent* of f,
(3) $\mathrm{LT}(f) :=$ `lead(f)`$:= a_\alpha x^\alpha$, the *leading term* or *head* of f,
(4) $\mathrm{LC}(f) :=$ `leadcoef(f)`$:= a_\alpha$, the *leading coefficient* of f
(5) $\mathrm{tail}(f) := f -$ `lead(f)`$= a_\beta x^\beta + \cdots + a_\gamma x^\gamma$, the *tail* of f.

Let us consider an example with the lexicographical ordering. In SINGULAR every polynomial belongs to a ring which has to be defined first. We define the ring $A = \mathbb{Q}[x, y, z]$ together with the lexicographical ordering.

A is the name of the ring, *0* the characteristic of the ground field $\mathbb{Q}$, x, y, z are the names of the variables and `lp` defines the lexicographical ordering with $x > y > z$, see Example 1.2.8.

SINGULAR Example 1.2.3 (leading data).

```
ring A = 0,(x,y,z),lp;
poly f = y4z3+2x2y2z2+3x5+4z4+5y2;
f;                          //display f in a lex-ordered way
//-> 3x5+2x2y2z2+y4z3+5y2+4z4
leadmonom(f);               //leading monomial
//-> x5
leadexp(f);                 //leading exponent
//-> 5,0,0
lead(f);                    //leading term
//-> 3x5
leadcoef(f);                //leading coefficient
//-> 3
f - lead(f);                //tail
//-> 2x2y2z2+y4z3+5y2+4z4
```

The most important distinction is between global and local orderings.

Definition 1.2.4. Let $>$ be a monomial ordering on $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$.

(1) $>$ is called a *global ordering* if $x^\alpha > 1$ for all $\alpha \neq (0, \ldots, 0)$,
(2) $>$ is called a *local ordering* if $x^\alpha < 1$ for all $\alpha \neq (0, \ldots, 0)$,
(3) $>$ is called a *mixed ordering* if it is neither global nor local.

Of course, if we turn the ordering around by setting $x^\alpha >' x^\beta$ if $x^\beta > x^\alpha$, then $>'$ is global if and only if $>$ is local. However, local and global (and mixed) orderings have quite different properties. Here are the most important characterizations of a global ordering.

Lemma 1.2.5. *Let $>$ be a monomial ordering, then the following conditions are equivalent:*

(1) $>$ is a well–ordering.
(2) $x_i > 1$ for $i = 1, \ldots, n$.
(3) $x^\alpha > 1$ for all $\alpha \neq (0, \ldots, 0)$, that is, $>$ is global.
(4) $\alpha \geq_{nat} \beta$ and $\alpha \neq \beta$ implies $x^\alpha > x^\beta$.

The last condition means that $>$ is a refinement of the natural partial ordering on $\mathbb{N}^n$ defined by

$$(\alpha_1, \ldots, \alpha_n) \geq_{\text{nat}} (\beta_1, \ldots, \beta_n) \ :\Longleftrightarrow\ \alpha_i \geq \beta_i \text{ for all } i\,.$$

Proof. (1) $\Rightarrow$ (2): if $x_i < 1$ for some i, then $x_i^p < x_i^{p-1} < 1$, yielding a set of monomials without smallest element (recall that a well–ordering is a total ordering on a set such that each non–empty subset has a smallest element).

(2) $\Rightarrow$ (3): write $x^\alpha = x^{\alpha'} x_j$ for some j and use induction. For (3) $\Rightarrow$ (4) let $(\alpha_1, \ldots, \alpha_n) \geq_{\mathrm{nat}} (\beta_1, \ldots, \beta_n)$ and $\alpha \neq \beta$. Then $\gamma := \alpha - \beta \in \mathbb{N}^n \setminus \{0\}$, hence $x^\gamma > 1$ and, therefore, $x^\alpha = x^\beta x^\gamma > x^\beta$.

(4) $\Rightarrow$ (1): Let M be a non–empty set of monomials. By Dickson's Lemma (Lemma 1.2.6) there is a finite subset $B \subset M$ such that for each $x^\alpha \in M$ there is an $x^\beta \in B$ with $\beta \leq_{\mathrm{nat}} \alpha$. By assumption, $x^\beta < x^\alpha$ or $x^\beta = x^\alpha$, that is, B contains a smallest element of M with respect to $>$. □

Lemma 1.2.6 (Dickson, 1913). *Let $M \subset \mathbb{N}^n$ be any subset. Then there is a* finite *set $B \subset M$ satisfying*

$$\forall\, \alpha \in M\ \exists\, \beta \in B \text{ such that } \beta \leq_{nat} \alpha\,.$$

B is sometimes called a Dickson basis *of M.*

Proof. We write $\geq$ instead of $\geq_{\mathrm{nat}}$ and use induction on n. For $n = 1$ we can take the minimum of M as the only element of B.

For $n > 1$ and $i \in \mathbb{N}$ define

$$M_i = \{\alpha' = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^{n-1} \mid (\alpha', i) \in M\}$$

and, by induction, M_i has a Dickson basis B_i.

Again, by induction hypothesis, $\bigcup_{i\in\mathbb{N}} B_i$ has a Dickson basis B'. B' is finite, hence $B' \subset B_1 \cup \cdots \cup B_s$ for some s.

We claim that

$$B := \{(\beta', i) \in \mathbb{N}^n \mid 0 \leq i \leq s,\ \beta' \in B_i\}$$

is a Dickson basis of M.

To see this, let $(\alpha', \alpha_n) \in M$. Then $\alpha' \in M_{\alpha_n}$ and, since B_{α_n} is a Dickson basis of M_{α_n}, there is a $\beta' \in B_{\alpha_n}$ with $\beta' \leq \alpha'$. If $\alpha_n \leq s$, then $(\beta', \alpha_n) \in B$ and $(\beta', \alpha_n) \leq (\alpha', \alpha_n)$. If $\alpha_n > s$, we can find a $\gamma' \in B'$ and an $i \leq s$ such that $\gamma' \leq \beta'$ and $(\gamma', i) \in B_i$. Then $(\gamma', i) \in B$ and $(\gamma', i) \leq (\alpha', \alpha_n)$. □

Remark 1.2.7. If A is an $n \times n$ integer matrix with only non–negative entries and determinant $\neq 0$, and if $>$ is a monomial ordering, we can define a *matrix ordering* $>_{(A,>)}$ by setting

$$x^\alpha >_{(A,>)} x^\beta \ :\Longleftrightarrow\ x^{A\alpha} > x^{A\beta}$$

where α and β are considered as column vectors. By Exercise 1.2.6 (2), $>_{(A,>)}$ is again a monomial ordering. We can even use matrices $A \in \mathrm{GL}(n, \mathbb{R})$ with real entries to obtain a monomial ordering by setting

$$x^\alpha >_A x^\beta \ :\Longleftrightarrow\ A\alpha > A\beta\,,$$

where $>$ on the right–hand side is the lexicographical ordering on $\mathbb{R}^n$.

Robbiano proved in [196], that every monomial ordering arises in this way from the lexicographical ordering on $\mathbb{R}^n$. However, we do not need this fact (cf. Exercise 1.2.9).

Important examples of monomial orderings are:

Example 1.2.8 (monomial orderings).
In the following examples we fix an enumeration $x_1, \ldots, x_n$ of the variables, any other enumeration leads to a different ordering.

(1) Global Orderings

(i) *Lexicographical ordering* $>_{lp}$ (also denoted by lex):

$$x^\alpha >_{lp} x^\beta \iff \exists\, 1 \le i \le n : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i\,.$$

(ii) *Degree reverse lexicographical ordering* $>_{dp}$ (denoted by degrevlex):

$$\begin{aligned} x^\alpha >_{dp} x^\beta \iff & \deg x^\alpha > \deg x^\beta \\ & \text{or } \big(\deg x^\alpha = \deg x^\beta \text{ and } \exists\, 1 \le i \le n : \\ & \qquad \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1},\ \alpha_i < \beta_i\big)\,, \end{aligned}$$

where $\deg x^\alpha = \alpha_1 + \cdots + \alpha_n$.

(iii) *Degree lexicographical ordering* $>_{Dp}$ (also denoted by deglex):

$$\begin{aligned} x^\alpha >_{Dp} x^\beta \iff & \deg x^\alpha > \deg x^\beta \\ & \text{or } \big(\deg x^\alpha = \deg x^\beta \text{ and } \exists\, 1 \le i \le n : \\ & \qquad \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1},\ \alpha_i > \beta_i\big). \end{aligned}$$

In all three cases $x_1, \ldots, x_n > 1$. For example, we have $x_1^3 >_{lp} x_1^2x_2^2$ but $x_1^2x_2^2 >_{dp,Dp} x_1^3$. An example where `dp` and `Dp` differ: $x_1^2x_2x_3^2 >_{Dp} x_1x_2^3x_3$ but $x_1x_2^3x_3 >_{dp} x_1^2x_2x_3^2$.

Given a vector $w = (w_1, \ldots, w_n)$ of integers, we define the *weighted degree* of x^α by

$$\text{w–deg}(x^\alpha) := \langle w, \alpha\rangle := w_1\alpha_1 + \cdots + w_n\alpha_n\,,$$

that is, the variable x_i has degree w_i. For a polynomial $f = \sum_\alpha a_\alpha x^\alpha$, we define the weighted degree,

$$\text{w–deg}(f) := \max\big\{\text{w–deg}(x^\alpha) \;\big|\; a_\alpha \neq 0\big\}\,.$$

Using the weighted degree in (ii), respectively (iii), with all $w_i > 0$, instead of the usual degree, we obtain the *weighted reverse lexicographical ordering*, `wp`$(w_1, \ldots, w_n)$, respectively the *weighted lexicographical ordering*, `Wp`$(w_1, \ldots, w_n)$.

(2) Local Orderings

(i) *Negative lexicographical ordering* $>_{ls}$:

$$x^\alpha >_{ls} x^\beta \iff \exists\, 1 \le i \le n, \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i\,.$$

(ii) *Negative degree reverse lexicographical ordering* $>_{ds}$:

$$\begin{aligned} x^\alpha >_{ds} x^\beta \iff & \deg x^\alpha < \deg x^\beta, \text{ where } \deg x^\alpha = \alpha_1 + \cdots + \alpha_n, \\ & \text{or } \big(\deg x^\alpha = \deg x^\beta \text{ and } \exists\, 1 \le i \le n : \\ & \qquad \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1},\, \alpha_i < \beta_i\big). \end{aligned}$$

(iii) *Negative degree lexicographical ordering* $>_{Ds}$:

$$\begin{aligned} x^\alpha >_{Ds} x^\beta \iff & \deg x^\alpha < \deg x^\beta, \\ & \text{or } \big(\deg x^\alpha = \deg x^\beta \text{ and } \exists\, 1 \le i \le n : \\ & \qquad \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1},\, \alpha_i > \beta_i\big). \end{aligned}$$

Similarly, as above, we can define weighted versions $\mathtt{ws}(w_1, \ldots, w_n)$ and $\mathtt{Ws}(w_1, \ldots, w_n)$ of the two last local orderings.

(3) Product or Block Orderings

Now consider $>_1$, a monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$, and $>_2$, a monomial ordering on $\mathrm{Mon}(y_1, \ldots, y_m)$. Then the *product ordering* or *block ordering* $>$, also denoted by $(>_1, >_2)$ on $\mathrm{Mon}(x_1, \ldots, x_n, y_1, \ldots, y_m)$, is defined as

$$\begin{aligned} x^\alpha y^\beta > x^{\alpha'} y^{\beta'} \iff & x^\alpha >_1 x^{\alpha'} \\ & \text{or } \big(x^\alpha = x^{\alpha'} \text{ and } y^\beta >_2 y^{\beta'}\big). \end{aligned}$$

If $>_1$ is a global ordering then the product ordering has the property that monomials which contain an x_i are always larger than monomials containing no x_i. If the special orderings $>_1$ on $\mathrm{Mon}(x_1, \ldots, x_n)$ and $>_2$ on $\mathrm{Mon}(y_1, \ldots, y_m)$ are irrelevant, for a product ordering on $\mathrm{Mon}(x_1, \ldots, x_n, y_1, \ldots, y_m)$ we write just $x \gg y$.
If $>_1$ and $>_2$ are global (respectively local), then the product ordering is global (respectively local) but the product ordering is mixed if one of the orderings $>_1$ and $>_2$ is global and the other local. This is how mixed orderings arise in a natural way.

Definition 1.2.9. A monomial ordering $>$ on $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ is called a *weighted degree ordering* if there exists a vector $w = (w_1, \ldots, w_n)$ of non–zero integers such that

$$\text{w–deg}(x^\alpha) > \text{w–deg}(x^\beta) \implies x^\alpha > x^\beta\,.$$

It is called a *global* (respectively *local*) *degree ordering* if the above holds for $w_i = 1$ (respectively $w_i = -1$) for all i.

Remark 1.2.10. Consider a matrix ordering defined by $A \in \mathrm{GL}(n, \mathbb{R})$. Since the columns of A are lexicographically greater than the 0–vector if and only if the variables are greater than 1, it follows that a matrix ordering $>_A$ is a well–ordering if and only if the first non–zero entry in each column of A is positive. It is a (weighted) degree ordering if and only if all entries in the first row of A are non–zero.

Of course, different matrices can define the same ordering. For examples of matrices defining the above orderings see the SINGULAR Manual.

Although we can represent any monomial ordering $>$ as a matrix ordering $>_A$ for some $A \in \mathrm{GL}(n, \mathbb{R})$, it turns out to be useful to represent $>$ just by one weight vector. This is, in general, not possible on the set of all monomials (cf. Exercise 1.2.10) but it is possible, as we shall see, for finite subsets.

For this purpose, we introduce the set of differences

$$D := \{\alpha - \beta \mid x^\alpha > x^\beta\} \subset \mathbb{Z}^n$$

associated to a monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$. D has the following properties,

- $0 \notin D$,
- $\gamma_1, \gamma_2 \in D \Longrightarrow \gamma_1 + \gamma_2 \in D$.

The last property follows from the fact that $>$ is a semigroup ordering. Namely, if $\gamma_1 = \alpha_1 - \beta_1,\ \gamma_2 = \alpha_2 - \beta_2 \in D$, then $x^{\alpha_1} > x^{\beta_1}$ implies that $x^{\alpha_1+\alpha_2} > x^{\beta_1+\alpha_2}$, and $x^{\alpha_2} > x^{\beta_2}$ implies that $x^{\beta_1+\alpha_2} > x^{\beta_1+\beta_2}$, therefore $x^{\alpha_1+\alpha_2} > x^{\beta_1+\beta_2}$ and $\gamma_1 + \gamma_2 = (\alpha_1 + \alpha_2) - (\beta_1 + \beta_2) \in D$.

It follows that $\sum_{i=1}^k n_i\gamma_i \in D$ for $n_i \in \mathbb{N} \setminus \{0\}$ and $\gamma_i \in D$, and, hence, $\sum_{i=1}^k r_i\gamma_i \neq 0$ for any finite linear combination of elements of D with $r_i \in \mathbb{Q}_{>0}$. In particular, no convex combination $\sum_{i=1}^k r_i\gamma_i$, $r_i \in \mathbb{Q}_{\geq 0}$, $\sum_{i=1}^k r_i = 1$, yields 0, that is, 0 is not contained in the convex hull of D. This fact will be used in the following lemma.

Lemma 1.2.11. *Let $>$ be a monomial ordering and $M \subset \mathrm{Mon}(x_1, \ldots, x_n)$ a finite set. Then there exists some $w = (w_1, \ldots, w_n) \in \mathbb{Z}^n$ such that $x^\alpha > x^\beta$ if and only if $\langle w, \alpha\rangle > \langle w, \beta\rangle$ for all $x^\alpha, x^\beta \in M$. Moreover, w can be chosen such that $w_i > 0$ for $x_i > 1$ and $w_i < 0$ if $x_i < 1$.*

The integer vector w is called a *weight–vector* and we say that w induces $>$ on M.

Proof. Since $\langle w, \alpha\rangle > \langle w, \beta\rangle$ if and only if $\langle w, \alpha - \beta\rangle > 0$, we have to find $w \in \mathbb{Z}^n$ such that $\langle w, \gamma\rangle > 0$ for all

$$\gamma \in D_M := \{\alpha - \beta \in D \mid x^\alpha, x^\beta \in M,\ x^\alpha > x^\beta\}\,.$$

This means that D_M should be in the positive half–space defined by the linear form $\langle w, -\rangle$ on $\mathbb{Q}^n$. Since 0 is not contained in the convex hull of D_M and

since D_M is finite, we can, indeed, find such a linear form (see, for example, [221], Theorem 2.10).

To see the last statement, include 1 and x_i, $i = 1, \ldots, n$, into M. Then $w_i > 0$ if $x_i > 1$ and $w_i < 0$ if $x_i < 1$. □

Example 1.2.12. A weight vector for the lexicographical ordering `lp` can be determined as follows. For $M \subset \mathrm{Mon}_n$ finite, consider an n–dimensional cube spanned by the coordinate axes containing M. Choose an integer v larger than the side length of this cube. Then $w = (v^{n-1}, v^{n-2}, \ldots, v, 1)$ induces `lp` on M.

We shall now define in SINGULAR the same ring $\mathbb{Q}[x, y, z]$ with different orderings, which are considered as different rings in SINGULAR. Then we map a given polynomial f to the different rings using `imap` and display f as a sum of terms in decreasing order, the method by which f is represented in the given ring.

SINGULAR Example 1.2.13 (monomial orderings).
Global orderings are denoted with a `p` at the end, referring to "polynomial ring" while local orderings end with an `s`, referring to "series ring". Note that SINGULAR stores and outputs a polynomial in an ordered way, in decreasing order.

(1) Global orderings:

```
ring A1 = 0,(x,y,z),lp;      //lexicographical
poly f = x3yz + y5 + z4 + x3 + xy2; f;
//-> x3yz+x3+xy2+y5+z4

ring A2 = 0,(x,y,z),dp;     //degree reverse lexicographical
poly f = imap(A1,f); f;
//-> y5+x3yz+z4+x3+xy2

ring A3 = 0,(x,y,z),Dp;     //degree lexicographical
poly f = imap(A1,f); f;
//-> x3yz+y5+z4+x3+xy2

ring A4 = 0,(x,y,z),Wp(5,3,2);//weighted degree
                               //lexicographical
poly f = imap(A1,f); f;
//-> x3yz+x3+y5+xy2+z4
```

(2) Local orderings:

```
ring A5 = 0,(x,y,z),ls;      //negative lexicographical
poly f = imap(A1,f); f;
//-> z4+y5+xy2+x3+x3yz
```

```
ring A6 = 0,(x,y,z),ds;      //negative degree reverse
                             //lexicographical
poly f = imap(A1,f); f;
//-> x3+xy2+z4+y5+x3yz

ring A7 = 0,(x,y,z),Ws(5,3,2);//negative weighted degree
                              //lexicographical
poly f = imap(A1,f); f;
//-> z4+xy2+x3+y5+x3yz
```

(3) Product and matrix orderings:

```
ring A8 = 0,(x,y,z),(dp(1),ds(2)); //mixed product ordering
poly f = imap(A1,f); f;
//-> x3+x3yz+xy2+z4+y5

intmat A[3][3] = -1, -1, -1, 0, 0, 1, 0, 1, 0;
print(A);
//->     -1    -1    -1
//->      0     0     1
//->      0     1     0
```

Now define your own matrix ordering using A:

```
ring A9 = 0,(x,y,z),M(A); //a local ordering
poly f = imap(A1,f); f;
//-> xy2+x3+z4+x3yz+y5
```

Exercises

1.2.1. Show that `lp`, `dp`, `Dp`, `wp(w(1..m))`, `Wp(w(1..n))`, respectively `ls`, `ds`, `Ds`, `ws(w(1..m))`, `Ws(w(1..n))`, as defined in Example 1.2.8 are indeed global, respectively local, monomial orderings.

1.2.2. Determine the names of the orderings given by the following matrices:

$$\begin{pmatrix}1&1\\0&-1\end{pmatrix},\quad \begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \begin{pmatrix}-1&-1\\0&-1\end{pmatrix},\quad \begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad \begin{pmatrix}1&2\\0&-1\end{pmatrix},\quad \begin{pmatrix}1&1&0&0\\0&-1&0&0\\0&0&-1&-1\\0&0&0&-1\end{pmatrix}.$$

1.2.3. Order the polynomial $x^4+z^5+x^3z+yz^4+x^2y^2$ with respect to the orderings `dp,Dp,lp,ds,Ds,ls,wp(5,3,4),ws(5,5,4)`.

1.2.4. Compute the leading term and the leading coefficient

$$f = 4xy^2z + 4z^2 - 5x^3 + 7xy^2 - 7y^4$$

with respect to the orderings `lp` on $\mathbb{Q}[x,y,z]$, `lp` on $\mathbb{Q}(x)[z,y]$, `lp` on $\mathbb{Q}[z,y,x]$, `Dp` on $(\mathbb{Z}/2\mathbb{Z})[z,y,x]$, `ls` on $\mathbb{Q}[x,y,z]$, `wp(w(1..3))` on $(\mathbb{Z}/2\mathbb{Z})[x,y,z]$, where `wp(w(1..3))` is given by w–deg$(x^\alpha y^\beta z^\gamma) := 3\alpha + 2\beta + \gamma$.

1.2.5. Determine matrices defining the orderings `dp`, `Dp`, `lp`, `ds`, `Ds`, `ls`, `wp(5,3,4)`, `ws(5,5,4)`.

1.2.6. Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$.

(1) Let $w=(w_1,\ldots,w_n)\in\mathbb{R}^n$ be arbitrary. Show that

$$x^\alpha >_w x^\beta :\Longleftrightarrow \langle w,\alpha\rangle > \langle w,\beta\rangle \text{ or } \langle w,\alpha\rangle = \langle w,\beta\rangle \text{ and } x^\alpha > x^\beta$$

defines a monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$.

Note that the ordering $>_w$ is a (weighted) degree ordering. It is a global ordering if $w_i>0$ for all i and a local ordering if $w_i<0$ for all i.

(2) Let A be an $n\times n$ integer matrix with non–negative entries, which is invertible over $\mathbb{Q}$. Show that

$$x^\alpha >_{(A,>)} x^\beta \Leftrightarrow x^{A\alpha} > x^{A\beta}$$

defines a monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$.

1.2.7. (1) Prove the claim made in Example 1.2.12.

(2) Consider a matrix ordering $>_A$ for some matrix $A\in\mathrm{GL}(n,\mathbb{Q})$ and $M\subset \mathrm{Mon}_n$ a finite set. Use (1) and the fact that $x^\alpha >_A x^\beta$ if and only if $A\alpha >_{\mathrm{lex}} A\beta$ to determine a weight vector which induces $>_A$ on M.

1.2.8. (1) Determine weight vectors w which induce `dp`, respectively `ds`, on $M=\{x^iy^jz^k \mid 1\le i,j,k\le 5\}$.

(2) Check your result, using SINGULAR, in the following way: create a polynomial f, being the sum of all monomials of degree ≤ 5 in the rings with ordering `dp`, respectively `ds`, and convert f to a string. Then do the same in the rings with ordering `wp(w)`, respectively `ws(-w)`, (`(a(w),lp)`, respectively `(a(-w),lp)`), and compare the respective strings.

1.2.9. Show that any monomial ordering $>$ can be defined as $>_A$ by a matrix $A\in\mathrm{GL}(n,\mathbb{R})$.

(Hint: You may proceed as follows: first show that a semigroup ordering on $(\mathbb{Z}^n_{\ge 0},+)$ extends in a unique way to a group ordering on $(\mathbb{Q}^n,+)$. Then show that, for any $\mathbb{Q}$–subvector space $V\subset\mathbb{Q}^n$ of dimension r, the set

$$V_0 := \left\{ z\in\mathbb{R}^n \;\middle|\; \begin{array}{c} \forall\,\varepsilon>0\ \exists\ z_+(\varepsilon), z_-(\varepsilon)\in U_\varepsilon(z)\cap V \\ \text{such that } z_+(\varepsilon)>0, z_-(\varepsilon)<0 \end{array} \right\}$$

is an $\mathbb{R}$–subvector space in $\mathbb{R}^n$ of dimension $r-1$. Use this to construct, successively, the rows of A.)

1.2.10. Let $w_1,\ldots,w_n\in\mathbb{R}$ be linearly independent over $\mathbb{Q}$ and define $>$ by setting $x^\alpha<x^\beta$ if $\sum_{i=1}^n w_i\alpha_i < \sum_{i=1}^n w_i\beta_i$. Prove that $>$ is a monomial ordering. Show that there is no matrix $A\in\mathrm{GL}(n,\mathbb{Q})$ defining this ordering.

1.3 Ideals and Quotient Rings

Ideals are in the centre of commutative algebra and algebraic geometry. Here we introduce only the basic notions related to them.

Let A be a ring, as always, commutative and with 1.

Definition 1.3.1. A subset $I \subset A$ is called an *ideal* if it is an additive subgroup which is closed under scalar multiplication, that is,

$$\begin{aligned} f, g \in I &\implies f + g \in I \\ f \in I, a \in A &\implies af \in I. \end{aligned}$$

Definition 1.3.2.

(1) Let $I \subset A$ be an ideal. A family $(f_\lambda)_{\lambda\in\Lambda}$, Λ any index set, and $f_\lambda \in I$, is called a *system of generators* of I if every element $f \in I$ can be expressed as a finite linear combination $f = \sum_\lambda a_\lambda f_\lambda$ for suitable $a_\lambda \in A$. We then write

$$I = \langle f_\lambda \mid \lambda \in \Lambda\rangle_A = \langle f_\lambda \mid \lambda \in \Lambda\rangle = \sum_{\lambda\in\Lambda} f_\lambda A$$

or, if $\Lambda = \{1, \ldots, k\}$,

$$I = \langle f_1, \ldots, f_k\rangle_A = \langle f_1, \ldots, f_k\rangle .$$

(2) I is called *finitely generated* if it has a finite system of generators; it is called *principal* if it can be generated by one element.
(3) If $(I_\lambda)_{\lambda\in\Lambda}$ is a family of ideals, then $\sum_{\lambda\in\Lambda} I_\lambda$ denotes the ideal generated by $\bigcup_{\lambda\in\Lambda} I_\lambda$.
(4) If I_1, I_2 are ideals, then $I_1 I_2$ (or $I_1 \cdot I_2$) denotes the ideal generated by the set $\{ab \mid a \in I_1,\, b \in I_2\}$.

Note that the union of ideals is, in general, not an ideal (but the intersection is). We have

$$\sum_{\lambda\in\Lambda} I_\lambda = \left\{ \sum_{\lambda\in\Lambda} a_\lambda \;\middle|\; a_\lambda \in I_\lambda,\ a_\lambda = 0 \text{ for almost all } \lambda \right\} .$$

Because the empty sum is defined to be 0, the 0–ideal is generated by the empty set (but also by 0). The expression $f = \sum_\lambda a_\lambda f_\lambda$ as a linear combination of the generators is, in general, by no means unique. For example, if $I = \langle f_1, f_2\rangle$ then we have the *trivial relation* $f_1 f_2 - f_2 f_1 = 0$, hence $a_1 f_1 = a_2 f_2$ with $a_1 = f_2$, $a_2 = f_1$. Usually there are also further relations, which lead to the notion of the module of syzygies (cf. Chapter 2).

Ideals occur in connection with ring maps. If $\varphi : A \to B$ is a ring homomorphism and $J \subset B$ an ideal, then the *preimage*

$$\varphi^{-1}(J) = \{a \in A \mid \varphi(a) \in J\}$$

is an ideal. In particular,

$$\operatorname{Ker}\varphi = \{a \in A \mid \varphi(a) = 0\}$$

is an ideal in A. On the other hand, the *image*

$$\varphi(I) = \{\varphi(a) \mid a \in I\}$$

of an ideal $I \subset A$ is, in general, not an ideal. In particular, $\operatorname{Im}\varphi = \varphi(A) \subset B$ is not, generally, an ideal (for example, consider $\mathbb{Z} \subset \mathbb{Q}$, then no non–zero ideal in $\mathbb{Z}$ is an ideal in $\mathbb{Q}$). All these statements are very easy to check.

φ is called *injective* if $\operatorname{Ker}\varphi = 0$, and *surjective* if $\operatorname{Im}\varphi = B$. A *bijective*, that is injective and surjective, morphism is called an *isomorphism*, an isomorphism from A to A an *automorphism*.

SINGULAR contains the built–in command `preimage` which can be used to compute the kernel of a ring map.

If a ring map $\varphi : K[x_1, \ldots, x_k] \to K[y_1, \ldots, y_m]$ is given by $f_1, \ldots, f_k$, that is, $\varphi(x_i) = f_i$, then φ is surjective if and only if $y_1, \ldots, y_m$ are contained in the subring $\operatorname{Im}\varphi = K[f_1, \ldots, f_m]$ of $K[y_1, \ldots, y_m]$. This fact is used in SINGULAR to check surjectivity.

We shall explain the algorithms for checking injectivity, surjectivity, bijectivity of a ring map in Chapter 2. Here we just apply the corresponding procedures from `algebra.lib`.

SINGULAR Example 1.3.3 (properties of ring maps).
(1) Checking injectivity:

```
ring S = 0,(a,b,c),lp;
ring R = 0,(x,y,z),dp;
ideal i = x, y, x2-y3;
map phi = S,i;     //a map from S to R, a->x, b->y, c->x2-y3
LIB "algebra.lib"; //load algebra.lib
```

By default, SINGULAR displays the names and paths of those libraries which are used by `algebra.lib` and which are also loaded. We suppress this message.

We test injectivity using the procedure `is_injective`, then we compute the kernel by using the procedure `alg_kernel` (which displays the kernel, an object of the preimage ring, as a string).

```
is_injective(phi,S);
//-> 0                          // phi is not injective
```

```
ideal j = x, x+y, z-x2+y3;
map psi = S,j;                  // another map from S to R
is_injective(psi,S);
//-> 1                          // psi is injective

alg_kernel(phi,S);
//-> b^3-a^2+c                  // <b^3-a^2+c> = Ker(phi)
alg_kernel(psi,S);
//-> 0
```

(2) Computing the *preimage*:

Using the `preimage` command, we must first go back to S, since the preimage is an ideal in the preimage ring.

```
ideal Z;                    //the zero ideal in R
setring S;
preimage(R,phi,Z);          //computes kernel of phi in S
//-> _[1]=a2-b3-c           //kernel of phi = preimage of Z
```

(3) Checking *surjectivity* and *bijectivity*.

```
setring R;
is_surjective(psi,S);
//-> 1
is_bijective(psi,S);        //faster than is_injective,
                            //is_surjective
//-> 1
```

Definition 1.3.4. A ring A is called *Noetherian* if every ideal in A is finitely generated.

It is a fundamental fact that the polynomial ring $A[x_1, \ldots, x_n]$ over a Noetherian ring A is again Noetherian; this is the content of the Hilbert basis theorem. Since a field is obviously a Noetherian ring, the polynomial ring over a field is Noetherian. It follows that the kernel of a ring map between Noetherian rings is finitely generated. An important point of the SINGULAR Example 1.3.3 is that we can explicitly compute a finite set of generators for the kernel of a map between polynomial rings.

Theorem 1.3.5 (Hilbert basis theorem). *If A is a Noetherian ring then the polynomial ring $A[x_1, \ldots, x_n]$ is Noetherian.*

For the proof of the Hilbert basis theorem we use

Proposition 1.3.6. *The following properties of a ring A are equivalent:*

(1) A is Noetherian.
(2) Every ascending chain of ideals

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset I_k \subset \ldots$$

becomes stationary (that is, there exists some j_0 such that $I_j = I_{j_0}$ for all $j \geq j_0$).
(3) Every non–empty set of ideals in A has a maximal element (with regard to inclusion).

Condition (2) is called the *ascending chain condition* and (3) the *maximality condition*. We leave the proof of this proposition as Exercise 1.3.9.

Proof of Theorem 1.3.5. We need to show the theorem only for $n = 1$, the general case follows by induction.

We argue by contradiction. Let us assume that there exists an ideal $I \subset A[x]$ which is not finitely generated. Choose polynomials

$$f_1 \in I, \quad f_2 \in I \setminus \langle f_1 \rangle, \quad \ldots, \quad f_{k+1} \in I \setminus \langle f_1, \ldots, f_k \rangle, \quad \ldots$$

of minimal possible degree. If $d_i = \deg(f_i)$,

$$f_i = a_i x^{d_i} + \text{ lower terms in } x\,,$$

then $d_1 \leq d_2 \leq \ldots$ and $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \ldots$ is an ascending chain of ideals in A. By assumption it is stationary, that is, $\langle a_1, \ldots, a_k \rangle = \langle a_1, \ldots, a_{k+1} \rangle$ for some k, hence, $a_{k+1} = \sum_{i=1}^{k} b_i a_i$ for suitable $b_i \in A$. Consider the polynomial

$$g = f_{k+1} - \sum_{i=1}^{k} b_i x^{d_{k+1}-d_i} f_i = a_{k+1} x^{d_{k+1}} - \sum_{i=1}^{k} b_i a_i x^{d_{k+1}} + \text{ lower terms}\,.$$

Since $f_{k+1} \in I \setminus \langle f_1, \ldots, f_k \rangle$, it follows that $g \in I \setminus \langle f_1, \ldots, f_k \rangle$ is a polynomial of degree smaller than d_{k+1}, a contradiction to the choice of f_{k+1}. □

Definition 1.3.7. Let I be any ideal in the ring A. We define the *quotient ring* or *factor ring* A/I as follows.

(1) A/I is the set of co–sets $\{[a] := a + I \mid a \in A\}$[2] with addition and multiplication defined via representatives:

$$[a] + [b] := [a + b],$$
$$[a] \cdot [b] := [a \cdot b].$$

[2] $a + I := \{a + f \mid f \in I\}$.

It is easy to see that the definitions are independent of the chosen representatives and that $(A/I, +, \cdot)$ is, indeed, a ring. Moreover, A/I is not the zero ring if and only if $1 \notin I$.

(2) The *residue map* or *quotient map* is defined by

$$\pi : A \longrightarrow A/I\,, \quad a \longmapsto [a]\,.$$

π is a surjective ring homomorphism with kernel I.

The following lemma is left as an easy exercise.

Lemma 1.3.8. *The map $J \mapsto \pi(J)$ induces a bijection*

$$\{\textit{ideals in } A \textit{ containing } I\} \longrightarrow \{\textit{ideals in } A/I\}$$

with $J' \mapsto \pi^{-1}(J')$ being the inverse map.

Definition 1.3.9.

(1) An element $a \in A$ is called a *zerodivisor* if there exists an element $b \in A \setminus \{0\}$ satisfying $ab = 0$; otherwise a is a *non–zerodivisor*.
(2) A is called an *integral domain* if $A \neq 0$ and if A has no zerodivisors except 0.
(3) A is a *principal ideal ring* if every ideal in A is principal; if A is, moreover, an integral domain it is called a *principal ideal domain*.

Polynomial rings over a field are integral domains (Exercise 1.3.1 (4)). This is, however, not generally true for quotient rings $K[x_1, \ldots, x_n]/I$. For example, if $I = \langle f \cdot g \rangle$ with $f, g \in K[x_1, \ldots, x_n]$ polynomials of positive degree, then $[f]$ and $[g]$ are zerodivisors in $K[x_1, \ldots, x_n]/I$ and not zero.

A ring A, which is isomorphic to a factor ring $K[x_1, \ldots, x_n]/I$, is called an *affine ring* over K.

Definition 1.3.10. Let $I \subset A$ be an ideal.

(1) I is a *prime ideal* if $I \neq A$ and if for each $a, b \in A : ab \in I \Rightarrow a \in I$ or $b \in I$.
(2) I is a *maximal ideal* if $I \neq A$ and if it is maximal with respect to inclusion (that is, for any ideal $I' \subsetneq A$ and $I \subset I'$ implies $I = I'$).
(3) The set of prime ideals is denoted by $\mathrm{Spec}(A)$ and the set of maximal ideals by $\mathrm{Max}(A)$.

The set of prime ideals $\mathrm{Spec}(A)$ of a ring A is made a topological space by endowing it with the so–called Zariski topology, creating, thus, a bridge between algebra and topology. We refer to the Appendix, in particular A.3, for a short introduction. In many cases in the text we use $\mathrm{Spec}(A)$ just as a set. But, from time to time, when we think we should relax and enjoy geometry, then we consider the affine space $\mathrm{Spec}(A)$ instead of the ring A and the variety $V(I) \subset \mathrm{Spec}(A)$ instead of the ideal I. Most of the examples deal with affine rings over a field K.

Lemma 1.3.11.

(1) $I \subset A$ is a prime ideal if and only if A/I is an integral domain.
(2) $I \subset A$ is a maximal ideal if and only if A/I is a field.
(3) Every maximal ideal is prime.

Proof. Let $I \subsetneq A$. For $a, b \in A$ we have $ab \in I \iff [ab] = [a] \cdot [b] = 0$ in A/I, which implies (1). By Lemma 1.3.8, A/I has only the trivial ideals 0 and A/I, if and only if I and A are the only ideals of A which contain I, which implies (2). Finally, (3) follows from (2) and (1), since a field is an integral domain. □

If $\varphi : A \to B$ is a ring map and $I \subset B$ is a prime ideal, then $\varphi^{-1}(I)$ is a prime ideal (an easy check). However, the preimage of a maximal ideal need not be maximal. (Consider $\mathbb{Z} \subset \mathbb{Q}$, then 0 is a maximal ideal in $\mathbb{Q}$ but not in $\mathbb{Z}$.)

Lemma 1.3.12. *Let A be a ring.*

(1) Let $P, I, J \subset A$ be ideals with P prime. Then $I \not\subset P$, $IJ \subset P$ implies $J \subset P$.
(2) Let $I_1, \ldots, I_n$, $P \subset A$ be ideals with P prime and $\bigcap_{i=1}^n I_i \subset P$ (respectively $\bigcap_i I_i = P$), then $P \supset I_i$ (respectively $P = I_i$) for some i.
*(3) (*Prime avoidance*) Let $P_1, \ldots, P_n$, $I \subset A$ be ideals with P_i prime and $I \subset \bigcup_{i=1}^n P_i$, then $I \subset P_i$ for some i.*

Proof. For (1) let $J = \langle f_1, \ldots, f_n \rangle$ and $x \in I$ such that $x \notin P$. By assumption, we have $xf_i \in P$ for all i. Now P is prime and, therefore, $f_i \in P$ for all i. This implies that $J \subset P$.

To prove (2) assume that $\bigcap I_i \subset P$. Then $\prod I_i \subset P$ and, therefore, using (1), $I_k \subset P$ for some k. If, additionally, $\bigcap I_i = P$, then $P = I_k$.

To prove (3) we use induction on n. The case $n = 1$ is trivial. Assume (3) is true for $n-1$ prime ideals. If $I \subset \bigcup_{j \neq i} P_j$ for some i, then $I \subset P_k$ for some k.

We may assume now that $I \not\subset \bigcup_{j \neq i} P_j$ for all $i = 1, \ldots, n$ and choose $x_1, \ldots, x_n \in I$ such that $x_i \notin \bigcup_{j \neq i} P_j$. This implies especially that $x_i \in P_i$ because $x_i \in I \subset \bigcup P_j$.

Now consider the element $x_1 + x_2 \cdot \ldots \cdot x_n \in I$. Since $I \subset \bigcup P_j$, there exists a k such that $x_1 + x_2 \cdot \ldots \cdot x_n \in P_k$. If $k = 1$ then, since $x_1 \in P_1$, we obtain $x_2 \cdot \ldots \cdot x_n \in P_1$. This implies that $x_\ell \in P_1$ for some $\ell > 1$ which is a contradiction to the choice of $x_\ell \notin \bigcup_{j \neq \ell} P_j$. If $k > 1$ then, since $x_2 \cdot \ldots \cdot x_n \in P_k$, we obtain $x_1 \in P_k$ which is again a contradiction to the choice of $x_1 \notin \bigcup_{j \neq 1} P_j$. □

Many of the concepts introduced so far in this section can be treated effectively using SINGULAR. We define a quotient ring and test equality and the zerodivisor property in the quotient ring.

SINGULAR Example 1.3.13 (computation in quotient rings).
(1) Define a *quotient ring*:

```
ring R = 32003,(x,y,z),dp;
ideal I = x2+y2-z5, z-x-y2;
qring Q = groebner(I);   //defines the quotient ring Q = R/I
Q;
//-> //   characteristic : 32003
//-> //   number of vars : 3
//-> //        block   1 : ordering dp
//-> //                  : names    x y z
//-> //        block   2 : ordering C
//-> // quotient ring from ideal
//-> _[1]=y2+x-z
//-> _[2]=z5-x2+x-z
```

(2) *Equality test* in quotient rings:
Equality test in quotient rings is difficult. The test `f==g` checks only formal equality of polynomials, it does not work correctly in quotient rings. Instead, we have to compute a normal form of the difference `f - g`. Why and how this works, will be explained in Section 1.6 on standard bases.

```
poly f = z2+y2;
poly g = z2+2x-2z-3z5+3x2+6y2;
reduce(f-g,std(0));  //normal form, result is 0 iff f=g in Q
//-> 0
```

The same can be tested without going to the quotient ring.

```
setring R;
poly f = z2+y2;   poly g = z2+2x-2z-3z5+3x2+6y2;
reduce(f-g,groebner(I)); //result is 0 iff f-g is in I
//-> 0
```

(3) *Zerodivisor test* in quotient rings:

```
setring Q;
ideal q = quotient(0,f);//this defines q = <0>:<f>
q = reduce(q,std(0));   //normal form of ideal q in Q
size(q);                //the number of non-zero generators
//-> 0                  //hence, f is a non-zerodivisor in Q
```

Testing primality of a principal ideal $\langle f \rangle$ in a polynomial ring is easily achieved by using `factorize(f);`. For an arbitrary ideal this is much more involved. One can use `primdecGTZ` or `primdecSY` from `primdec.lib`, as will be explained in Chapter 4.

(4) Computing the *inverse* in quotient rings:

If $I \subset K[x] = K[x_1, \ldots, x_n]$ is a maximal ideal, then the quotient ring $K[x]/I$ is a field. To be able to compute effectively in the field $K[x]/I$ we need, in addition to the ring operations, the inverse of a non–zero element. The following example shows that we can effectively compute in all fields of finite type over a prime field.

If the polynomial f is invertible, then the command `lift(f,1)[1,1]` gives the inverse (`lift` checks whether $1 \in \langle f \rangle$ and then expresses 1 as a multiple of f):

```
ring R=(0,x),(y,z),dp;
ideal I=-z5+y2+(x2),-y2+z+(-x);
I=std(I);
qring Q=I;
```

We shall now compute the inverse of z in $Q = R/I$.

```
poly p=lift(z,1)[1,1];
p;
//->1/(x2-x)*z4-1/(x2-x)
```

We make a test for p being the inverse of z.

```
reduce(p*z,std(0));
//->1
```

The ideal I is a maximal ideal if and only if R/I is a field. We shall now prove that, in our example, I is a maximal ideal.

```
ring R1=(0,x),(z,y),lp;
ideal I=imap(R,I);
I=std(I);
I;
//-> I[1]=y10+(5x)*y8+(10x2)*y6+(10x3)*y4+(5x4-1)*y2+(x5-x2)
//-> I[2]=z-y2+(-x)
```

Since $\mathbb{Q}(x)[z,y]/\langle z - y^2 - x \rangle \cong \mathbb{Q}(x)[y]$, we see that

$$R/I \cong \mathbb{Q}(x)[y]/\langle y^{10} + 5xy^8 + 10x^2y^6 + 10x^3y^4 + (5x^4 - 1)y^2 + x^5 - x^2 \rangle \,.$$

```
factorize(I[1]);
//-> [1]:
//->     _[1]=1
//->     _[2]=y10+(5x)*y8+(10x2)*y6+(10x3)*y4+(5x4-1)*y2
//->             +(x5-x2)
//-> [2]:
//->     1,1
```

The polynomial is irreducible and, therefore, R/I is a field and I a maximal ideal.

Definition 1.3.14. Let A be a ring and $I, J \subset A$ ideals.

(1) The *ideal quotient* of I by J is defined as

$$I : J := \left\{ a \in A \,\middle|\, aJ \subset I \right\}.$$

The *saturation of I with respect to J* is

$$I : J^{\infty} = \left\{ a \in A \,\middle|\, \exists\, n \text{ such that } aJ^n \subset I \right\}.$$

(2) The *radical* of I, denoted by $\sqrt{I}$ or $\operatorname{rad}(I)$ is the ideal

$$\sqrt{I} = \left\{ a \in A \,\middle|\, \exists\, d \in \mathbb{N} \text{ such that } a^d \in I \right\},$$

which is an ideal containing I. I is called *reduced* or a *radical ideal* if $I = \sqrt{I}$.

(3) $a \in A$ is called *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$; the minimal n is called *index of nilpotency*. The set of nilpotent elements of A is equal to $\sqrt{\langle 0 \rangle}$ and called the *nilradical* of A.

(4) The ring A itself is called *reduced* if it has no nilpotent elements except 0, that is, if $\sqrt{\langle 0 \rangle} = \langle 0 \rangle$. For any ring, the quotient ring

$$A_{\text{red}} = A/\sqrt{\langle 0 \rangle}$$

is called the *reduction* of A or the *reduced ring associated to A*.

The ideal quotient $I : J$ is an ideal in A which is very useful. In SINGULAR the command `quotient(I,J);` computes generators of this ideal. In particular,

$$\langle 0 \rangle : J = \operatorname{Ann}_A(J)$$

is the *annihilator* of J and, hence, $\langle 0 \rangle : \langle f \rangle = \langle 0 \rangle$ if and only if f is a non–zerodivisor of A.

It is clear that A_{red} is reduced and that $A = A_{\text{red}}$ if and only if A is reduced. Any integral domain is reduced.

Computing the radical is already quite involved (cf. Chapter 4). The radical membership problem is, however, much easier (cf. Section 1.8.6).

SINGULAR Example 1.3.15 (computing with radicals).

(1) Compute the radical of an ideal:

```
ring R = 0,(x,y,z),dp;
poly p = z4+2z2+1;
LIB "primdec.lib";         //loads library for radical
```

```
radical(p);                 //squarefree part of p
//-> _[1]=z2+1

ideal I = xyz, x2, y4+y5;  //a more complicated ideal
radical(I);
//-> _[1]=x
//-> _[2]=y2+y              //we see that I is not reduced
```

(2) Compute the *index of nilpotency* in a quotient ring:
Since y^2+y is contained in the radical of I, some power of y^2+y must be contained in I. We compute the minimal power k so that $(y^2+y)^k$ is contained in I by using the normal form as in Example 1.3.13. This is the same as saying that y^2+y is nilpotent in the quotient ring R/I and then k is the index of nilpotency of y^2+y in R/I.

```
ideal Is = groebner(I);
int k;
while (reduce((y2+y)^k,Is) != 0 ) {k++;}
k;
//-> 4          //minimal power (index of nilpotency) is 4
```

Exercises

1.3.1. Let A be a ring and $f = \sum_{|\alpha|\geq 0} a_\alpha x^\alpha \in A[x_1,\ldots,x_n]$. Prove the following statements:

(1) f is nilpotent if and only if a_α is nilpotent for all α.
(Hint: choose a monomial ordering and argue by induction on the number of summands.)
In particular: $A[x_1,\ldots,x_n]$ is reduced if and only if A is reduced.

(2) f is a unit in $A[x_1,\ldots,x_n]$ if and only if $a_{0,\ldots,0}$ is a unit in A and a_α are nilpotent for $\alpha \neq 0$.
(Hint: Remember the geometric series for $1/(1-g)$ and use (1).)
In particular: $(A[x_1,\ldots,x_n])^* = A^*$ if and only if A is reduced.

(3) f is a zerodivisor in $A[x_1,\ldots,x_n]$ if and only if there exists some $a \neq 0$ in A such that $af = 0$. Give two proofs: one by induction on n, the other by using a monomial ordering.
(Hint: choose a monomial ordering and $g \in A[x_1,\ldots,x_n]$ with minimal number of terms so that $f \cdot g = 0$, consider the biggest term and conclude that g must be a monomial.)

(4) $A[x_1,\ldots,x_n]$ is an integral domain if and only if $\deg(fg) = \deg(f) + \deg(g)$ for all $f, g \in A[x_1,\ldots,x_n]$.
In particular: $A[x_1,\ldots,x_n]$ is an integral domain if and only if A is an integral domain.

1.3.2. Let $\varphi : A \to B$ be a ring homomorphism, I an ideal in A and J an ideal in B. Show that:

(1) $\varphi^{-1}(J) \subset I$ is an ideal.
(2) $\varphi(I)$ is a subring of B, not necessarily with 1, but, in general, not an ideal.
(3) If φ is surjective then $\varphi(I)$ is an ideal in B.

1.3.3. Prove the following statements:

(1) $\mathbb{Z}$ and the polynomial ring $K[x]$ in one variable over a field are principal ideal domains [use division with remainder].
(2) Let A be any ring, then $A[x_1, \ldots, x_n]$, $n > 1$, is not a principal ideal domain.

1.3.4. Let A be a ring. A non–unit $f \in A$ is called *irreducible* if $f = f_1 f_2$, $f_1, f_2 \in A$, implies that f_1 or f_2 is a unit. f is called a *prime element* if $\langle f \rangle$ is a prime ideal. Prove Exercise 1.1.5 with $K[x]$ replaced by any principal ideal domain A. Moreover, prove that the conditions (1) – (3) of Exercise 1.1.5 are equivalent to

(4) The ideal $\langle f \rangle$ is a prime ideal.
(5) The ideal $\langle f \rangle$ is a maximal ideal.

1.3.5. Let R be a principal ideal domain. Use Exercise 1.3.4 to prove that every non–unit $f \in R$ can be written in a unique way as a product of finitely many prime elements. Unique means here modulo permutation and multiplication with a unit.

1.3.6. The quotient ring of a principal ideal ring is a principal ideal ring. Show, by an example, that the quotient ring of an integral domain (respectively a reduced ring) need not be an integral domain.

1.3.7. (1) If A, B are principal ideal rings, then, also $A \oplus B$.
(2) $A \oplus B$ is never an integral domain, unless A or B are trivial.
(3) How many ideals has $K \oplus F$ if K and F are fields?

1.3.8. Prove the following statements:

(1) Let $n > 1$, then $\mathbb{Z}/n\mathbb{Z}$ is reduced if and only if n is a product of pairwise different primes.
(2) Let K be a field, and let $f \in K[x_1, \ldots, x_n]$ be a polynomial of degree ≥ 1. Then $K[x_1, \ldots, x_n]/\langle f \rangle$ is reduced (respectively an integral domain) if and only if f is a product of pairwise different irreducible polynomials (respectively irreducible).

1.3.9. Prove Proposition 1.3.6.

1.3.10. Prove Lemma 1.3.8.

1.3.11. Let A be a Noetherian ring, and let $I \subset A$ be an ideal. Prove that A/I is Noetherian.

1.3.12. Let A be a Noetherian ring, and let $\varphi : A \to A$ be a surjective ring homomorphism. Prove that φ is injective.

1.3.13. (*Chinese remainder theorem*) Let A be a ring, and let $I_1, \ldots, I_s$ be ideals in A. Assume that $\bigcap_{j=1}^{s} I_j = \langle 0 \rangle$ and $I_j + I_k = A$ for $j \neq k$. Prove that the canonical map

$$A \longrightarrow \bigoplus_{j=1}^{s} A/I_j\,, \quad a \longmapsto (a + I_1, \ldots, a + I_s)\,,$$

is an isomorphism of rings[3]

1.3.14. Let K be a field and A a K–algebra. Then A is called an *Artinian K–algebra* if $\dim_K(A) < \infty$. Prove the following statements:

(1) An Artinian K–algebra is Noetherian.
(2) A is an Artinian K–algebra if and only if each descending chain of ideals

$$I_1 \supset I_2 \supset I_3 \supset \ldots \supset I_k \supset \ldots$$

becomes stationary (that is, there exists some j_0 such that $I_j = I_{j_0}$ for all $j \geq j_0$). [4]

1.3.15. Show that $\mathbb{Q}[x]/\langle x^2+1\rangle$ is a field and compute in this field the quotient $(x^3+x^2+x)/(x^3+x^2+1)$, first by hand and then by using SINGULAR as in Example 1.3.13. Alternatively use the method of Example 1.1.8 (in characteristic 0), defining a `minpoly`.

1.3.16. Let $f = x^3+y^3+z^3+3xyz$, and let I be the ideal in $\mathbb{Q}[x,y,z]$, respectively $\mathbb{F}_3[x,y,z]$, generated by f and its partial derivatives. Moreover, let $R := \mathbb{Q}[x,y,z]/I$ and $S := \mathbb{F}_3[x,y,z]/I$.

(1) Is xyz a zerodivisor in R, respectively in S?
(2) Compute the index of nilpotency of $x+y+z$ in R, respectively S.

(Hint: type `?diff;` or `?jacob;` to see how to create the ideal I.)

1.4 Local Rings and Localization

Localization of a ring means enlarging the ring by allowing denominators, similar to the passage from $\mathbb{Z}$ to $\mathbb{Q}$. The name, however, comes from the geometric interpretation. For example, localizing $K[x_1, \ldots, x_n]$ at $\langle x_1, \ldots, x_n \rangle$

[3] If $A = \mathbb{Z}$ the theorem can be reformulated as follows: Let $a_1, \ldots, a_s \in \mathbb{Z}$ such that $\gcd(a_i, a_j) = 1$ for $i \neq j$ and $a = \prod_{i=1}^{s} a_i$. Then for given $x_1, \ldots, x_s \in \mathbb{Z}$ the congruences $x \equiv x_i \mod a_i, 1 \leq i \leq s$ have a solution which is uniquely determined modulo a. The procedure `chineseRem` of the library `crypto.lib` computes this solution.

[4] This is the usual way to define an *Artinian ring*.

means considering rational functions f/g where f and g are polynomials with $g(0) \neq 0$. Of course, any polynomial $f = f/1$ is of this form but, as g may have zeros arbitrary close to 0, f/g is defined only locally, in an arbitrary small neighbourhood of 0 (cf. Appendix A.8).

Definition 1.4.1. A ring A is called *local* if it has exactly one maximal ideal $\mathfrak{m}$. $A/\mathfrak{m}$ is called the *residue field* of A. Rings with finitely many maximal ideals are called *semi–local*. We denote local rings also by $(A, \mathfrak{m})$ or $(A, \mathfrak{m}, K)$ where $K = A/\mathfrak{m}$.

Fields are local rings. A polynomial ring $K[x_1, \ldots, x_n]$ with $n \geq 1$ over a field K is, however, never local. To see this, consider for any $(a_1, \ldots, a_n) \in K^n$ the ideal $\mathfrak{m}_a := \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Since $\varphi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$, $\varphi(x_i) := x_i - a_i$, is an isomorphism sending $\mathfrak{m}_0 = \langle x_1, \ldots, x_n \rangle$ to $\mathfrak{m}_a$, it follows that $K[x_1, \ldots, x_n]/\mathfrak{m}_a \cong K$ is a field, hence $\mathfrak{m}_a$ is a maximal ideal. Since K has at least two elements, K^n has at least two different points and, hence, $K[x_1, \ldots, x_n]$ has at least as many maximal ideals as K^n points (those of type $\mathfrak{m}_a$). If K is algebraically closed, then the ideals $\mathfrak{m}_a$, $a \in K^n$ are all maximal ideals of $K[x_1, \ldots, x_n]$ (this is one form of Hilbert's Nullstellensatz).

A typical local ring is the formal power series ring $K[[x_1, \ldots, x_n]]$ with maximal ideal $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$, that is, all power series without constant term. That this ring is local follows easily from Lemma 1.4.3. We shall treat power series rings in Chapter 6. Other examples are localizations of polynomial rings at prime ideals, cf. Example 1.4.6.

Theorem 1.4.2. *Every ring $A \neq 0$ contains at least one maximal ideal. If $I \subsetneq A$ is an ideal, then there exists a maximal ideal $\mathfrak{m} \subset A$ such that $I \subset \mathfrak{m}$.*

Proof. The first statement follows from the second with $I = 0$. If I is not maximal there exists an $f_1 \in A$ such that $I \subsetneq I_1 := \langle I, f_1 \rangle \subsetneq A$. If I_1 is not maximal there is an f_2 such that $I_1 \subsetneq I_2 = \langle I_1, f_2 \rangle \subsetneq A$. Continuing in this manner, we obtain a sequence of strictly increasing ideals $I \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$ which must become stationary, say $I_m = I_n$ for $m \geq n$ if A is Noetherian by Proposition 1.3.6. Thus, I_n is maximal and contains I. In general, if A is not Noetherian, $\bigcup_{n \geq 1} I_n$ is an ideal containing I, and the result follows from Zorn's lemma.[5] □

Lemma 1.4.3. *Let A be a ring.*

(1) A is a local ring if and only if the set of non–units is an ideal (which is then the maximal ideal).
(2) Let $\mathfrak{m} \subset A$ be a maximal ideal such that every element of the form $1 + a$, $a \in \mathfrak{m}$ is a unit. Then A is local.

[5] Zorn's Lemma says: let $\mathcal{S}$ be a non–empty system of sets such that for each chain $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ in $\mathcal{S}$, the union of the chain elements belong to $\mathcal{S}$. Then any element of $\mathcal{S}$ is contained in a maximal element (w.r.t. inclusion) of $\mathcal{S}$. This "lemma" is actually an axiom, equivalent to the axiom of choice.

Proof. (1) is obvious. To see (2) let $u \in A \setminus \mathfrak{m}$. Since $\mathfrak{m}$ is maximal $\langle \mathfrak{m}, u\rangle = A$ and, hence, $1 = uv + a$ for some $v \in A$, $a \in \mathfrak{m}$. By assumption $uv = 1 - a$ is a unit. Hence, u is a unit and $\mathfrak{m}$ is the set of non–units. The claim follows from (1). □

Localization generalizes the construction of the quotient field: if A is an integral domain, then the set

$$\mathrm{Quot}(A) := Q(A) := \left\{ \frac{a}{b} \;\middle|\; a, b \in A,\ b \neq 0 \right\},$$

together with the operations

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

is a field, the *quotient field* or *field of fractions* of A. Here a/b denotes the class of (a, b) under the equivalence relation

$$(a, b) \sim (a', b') \ :\Longleftrightarrow\ ab' = a'b\,.$$

The map $A \to Q(A)$, $a \mapsto a/1$ is an injective ring homomorphism and we identify A with its image. Since $a/b = 0$ if and only if $a = 0$, every element $a/b \neq 0$ has an inverse b/a and, therefore, $Q(A)$ is a field.

The denominators in $Q(A)$ are the elements of the set $S = A \setminus \{0\}$ and S satisfies
(1) $1 \in S$,
(2) $a \in S,\ b \in S \implies ab \in S$.

This notion can be generalized as follows.

Definition 1.4.4. Let A be a ring.

(1) A subset $S \subset A$ is called *multiplicative* or *multiplicatively closed* if conditions (1) and (2) above hold.
(2) Let $S \subset A$ be multiplicatively closed. We define the *localization* or the *ring of fractions* $S^{-1}A$ of A with respect to S as follows:

$$S^{-1}A := \left\{ \frac{a}{b} \;\middle|\; a \in A,\ b \in S \right\}$$

where a/b denotes the equivalence class of $(a, b) \in A \times S$ with respect to the following equivalence relation:

$$(a, b) \sim (a', b') :\Longleftrightarrow \exists\ s \in S \text{ such that } s(ab' - a'b) = 0\,.$$

Moreover, on $S^{-1}A$ we define an addition and multiplication by the same formulas as for the quotient field above.

The following proposition is left as an exercise.

Proposition 1.4.5.

(1) The operations $+$ and $\cdot$ on $S^{-1}A$ are well–defined (independent of the chosen representatives) and make $S^{-1}A$ a ring (commutative and with $1 = 1/1$).
(2) The map $j : A \to S^{-1}A$, $a \mapsto a/1$ is a ring homomorphism satisfying
  a) $j(s)$ is a unit in $S^{-1}A$ if $s \in S$,
  b) $j(a) = 0$ if and only if $as = 0$ for some $s \in S$,
  c) j is injective if and only if S consists of non–zerodivisors,
  d) j is bijective if and only if S consists of units.
(3) $S^{-1}A = 0$ if and only if $0 \in S$.
(4) If $S_1 \subset S_2$ are multiplicatively closed in A and consist of non–zerodivisors, then $S_1^{-1}A \subset S_2^{-1}A$.
(5) Every ideal in $S^{-1}A$ is generated by the image of an ideal in A under the map j. Moreover, the prime ideals in $S^{-1}A$ are in one–to–one correspondence with the prime ideals in A which do not meet S.

Examples 1.4.6.

(1) $A \setminus P$ is multiplicatively closed for any prime ideal $P \subset A$. The localization of A with respect to $A \setminus P$ is denoted by A_P and

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

is called the *localization* of A *at the prime ideal* P.
The set

$$PA_P = \left\{ \frac{a}{b} \;\middle|\; a \in P,\ b \notin P \right\}$$

is clearly an ideal in A_P. Any element $a/b \in A_P \setminus PA_P$ satisfies $a \notin P$, hence, $b/a \in A_P$ and, therefore, a/b is a unit.
This shows that A_P is a local ring with maximal ideal PA_P by Lemma 1.4.3. In particular, if $\mathfrak{m} \subset A$ is a maximal ideal then $A_{\mathfrak{m}}$ is local with maximal ideal $\mathfrak{m}A_{\mathfrak{m}}$.
(2) For any $f \in A$, the set $S := \{f^n \mid n \geq 0\}$ is multiplicatively closed (with $f^0 = 1$). We use the special notation

$$A_f := S^{-1}A = \left\{ \frac{a}{f^n} \;\middle|\; a \in A, n \geq 0 \right\},$$

not to be confused with $A_{\langle f \rangle}$, if $\langle f \rangle \subset A$ is a prime ideal.
(3) The set S of all non–zerodivisors of A is multiplicatively closed. For this S, $S^{-1}A =: Q(A) =: \mathrm{Quot}(A)$ is called the *total ring of fractions* or the *total quotient ring* of A. If A is an integral domain, this is just the quotient field of A.

Two special but important cases are the following: if $K[x_1,\dots,x_n]$ is the polynomial ring over a field, then the quotient field is denoted by $K(x_1,\dots,x_n)$,

$$K(x_1,\dots,x_n) := Q(K[x_1,\dots,x_n])\,,$$

which is also called the *function field* in n variables; the x_i are then also called *parameters*. For computing with parameters cf. SINGULAR-Example 1.1.8.

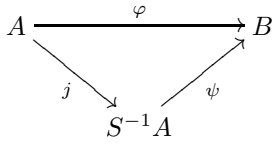
The localization of $K[x] = K[x_1,\dots,x_n]$ with respect to the maximal ideal $\langle x\rangle = \langle x_1,\dots,x_n\rangle$ is

$$K[x]_{\langle x\rangle} = \left\{ \frac{f}{g} \;\middle|\; f,g \in K[x],\ g(0)\neq 0 \right\}.$$

It is an important fact that we can compute in this ring without explicit denominators, just by defining a suitable monomial ordering on $K[x]$ (cf. Section 1.5). More generally, we can compute in $K[x]_{\mathfrak{m}_a}$, $\mathfrak{m}_a = \langle x_1-a_1,\dots x_n-a_n\rangle$, for any $a=(a_1,\dots,a_n)\in K^n$, by translating our polynomial data to $K[x]_{\langle x\rangle}$ via the ring map $x_i \mapsto x_i + a_i$.

Proposition 1.4.7. *Let $\varphi : A \to B$ be a ring homomorphism, $S \subset A$ multiplicatively closed, and $j : A \to S^{-1}A$ the canonical ring homomorphism $a \mapsto a/1$.*

(1) Assume
(i) $\varphi(s)$ is a unit in B for all $s \in S$.
Then there exists a unique ring homomorphism $\psi : S^{-1}A \to B$ such that the following diagram commutes:



(2) Assume moreover
(ii) $\varphi(a) = 0$ implies $sa = 0$ for some $s \in S$,
(iii) every element of B is of the form $\varphi(a)\varphi(s)^{-1}$.
Then ψ is an isomorphism.

Property (1) is called the *universal property of localization*.

Proof. (1) Since $\varphi(a) = \psi(a/1)$ for $a \in A$, we obtain, for any $a/s \in S^{-1}A$, that $\psi(a/s) = \psi(a/1)\cdot\psi(1/s) = \psi(a/1)\psi(s/1)^{-1} = \varphi(a)\varphi(s)^{-1}$. In particular, ψ is unique if it exists. Now define $\psi(a/s) := \varphi(a)\varphi(s)^{-1}$ and check that ψ is well–defined and a ring homomorphism.
(2) (ii) implies that ψ is injective and (iii) that ψ is surjective. □

Lemma 1.4.8. *Let $S \subset A$ be multiplicatively closed and $j : A \to S^{-1}A$ the canonical ring homomorphism $a \mapsto a/1$.*

(1) If $J \subset S^{-1}A$ is an ideal and $I = j^{-1}(J)$ then $IS^{-1}A = J$. In particular, if $f_1, \ldots, f_k$ generate I over A then $f_1, \ldots, f_k$ generate J over $S^{-1}A$.
(2) If A is Noetherian, then $S^{-1}A$ is Noetherian.

Proof. (1) If $f/s \in J$ then $f/1 = s \cdot f/s \in J$, hence $f \in I = j^{-1}(J)$ and, therefore, $f/s = f \cdot 1/s \in IS^{-1}A$. The other inclusion is clear. Statement (2) follows directly from (1). □

To define the local ring $K[x]_{\langle x\rangle} = K[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$ in SINGULAR, we have to choose a local ordering such as `ds, Ds, ls` or a weighted local ordering. This is explained in detail in the next section. We shall now show the difference between local and global rings by some examples. Note that objects defined in the local ring $K[x]_{\langle x\rangle}$ contain geometric information (usually only) about a Zariski neighbourhood of $0 \in K^n$ (cf. A.2, page 454), while objects in $K[x]$ contain geometric information which is valid in the whole affine space K^n.

Consider the ideal $I = \langle y(x-1), z(x-1)\rangle \subset \mathbb{Q}[x, y, z]$ and consider the common zero–set of all elements of I,

$$\begin{aligned} V(I) &= \{(x, y, z) \in \mathbb{C}^3 \mid f(x, y, z) = 0 \ \ \forall\, f \in I\} \\ &= \{(x, y, z) \in \mathbb{C}^3 \mid y(x-1) = z(x-1) = 0\}\,. \end{aligned}$$

The real picture of $V(I)$ is displayed in Figure 1.1.

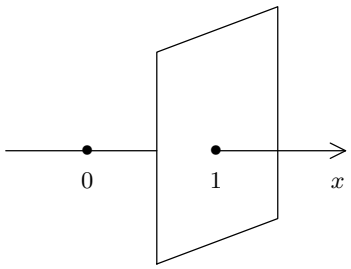


Fig. 1.1. The real zero–set of $\langle y(x-1), z(x-1)\rangle$

Although we treat dimension theory later, it should be intuitively clear from the picture that the (local) dimension of $V(I)$ is 1 at the point $(0, 0, 0)$ and 2 at the point $(1, 0, 0)$.

We compute the global dimension of $V(I)$ (which is the maximum of the dimensions at each point) and then the dimension of $V(I)$ in the points $(0, 0, 0)$ and $(1, 0, 0)$. As we shall see in Section 3.3, we always have to compute a standard basis of the ideal with respect to the given ordering first and then apply the command `dim`.

SINGULAR Example 1.4.9 (global versus local rings).

(1) Compute the dimension of $V(I)$, that is, compute $\dim(I)$, the Krull dimension of S/I, $S = \mathbb{Q}[x, y, z]$ (cf. Chapter 3, Section 3.3).

```
ring S = 0,(x,y,z),dp;
ideal I = y*(x-1), z*(x-1);
ideal J = std(I);   //compute a standard basis J of I in S
J;                  //J = <z(x-1),y(x-1)>
//-> J[1]=xz-z
//-> J[2]=xy-y
dim(J);             //the (global) dimension of V(I) is 2
//-> 2

reduce(y,J);        //y is not in I
                    //(result is 0 iff y is in I)
//-> y
```

(2) Compute the dimension of $V(I)$ at $0 = (0, 0, 0)$, that is, compute $\dim(I)$, the Krull dimension of R/IR, $R = \mathbb{Q}[x, y, z]_{\langle x,y,z\rangle}$.

```
ring R = 0,(x,y,z),ds;
ideal I = fetch(S,I);//fetch I from S to basering
ideal J = std(I);    //compute a standard basis J of I in R
J;
//-> J[1]=y          //J = <y,z> since x-1 is a unit in R
//-> J[2]=z
dim(J);
//-> 1               //(local) dimension of V(I) at 0 is 1
reduce(y,J);
//-> 0               //now y is in IR = JR
```

(3) Compute the dimension of $V(I)$ at $(1, 0, 0)$, that is, compute $\dim(I_1)$, the Krull dimension of R/I_1R in $R = \mathbb{Q}[x, y, z]_{\langle x,y,z\rangle}$ where I_1 is the translation of I to $(1, 0, 0)$.

```
map trans = S, x+1,y,z;  //replace x by x+1 and leave
                         //y,z fixed, i.e., translate
                         //(0,0,0) to (1,0,0)
ideal I1 = trans(I);
I1;
//-> I1[1]=xy
//-> I1[2]=xz
dim(std(I1));            //dimension of V(I) at (1,0,0) is 2
//-> 2
```

(4) Compute the (global) dimension of $V(I)$ after translation.

```
setring S;                //go back to global ring S
map trans = S, x+1,y,z;
ideal I1 = trans(I);      //translate I, as in (3)
I1;
//-> I1[1]=xy
//-> I1[2]=xz
dim(std(I1));             //(global) dimension of translated
//-> 2                    //variety has not changed

kill S,R;
```

The above computation illustrates what is intuitively clear from the picture in Figure 1.1: the dimension of the local rings varies. Dimension theory is treated in detail in Chapter 3, Section 3.3. For this example, it is enough to have an intuitive feeling for the dimension as it is visualized in the real picture of $V(I)$.

Exercises

1.4.1. Prove Proposition 1.4.5.

1.4.2. Let A be a ring, $I \subset A$ an ideal and $f \in A$.
Prove that $IA_f \cap A$ is the saturation of I with respect to f, that is, equal to $I : \langle f \rangle^\infty = \{g \in A \mid \exists\, n \text{ such that } gf^n \in I\}$.

1.4.3. Let $(A, \mathfrak{m})$ be a local K–algebra, K a field, and $I \subset A$ an ideal such that $\dim_K(A/I) < \infty$. Show that $\mathfrak{m}^n \subset I$ for some n.

1.4.4. Let A be a ring and $J(A)$ the intersection of all maximal ideals of A, which is called the *Jacobson radical* of A. Prove that for all $x \in J(A)$, $1 + x$ is a unit in A.

1.4.5. Let S and T be two multiplicatively closed sets in the ring A. Show that ST is multiplicatively closed and that $(ST)^{-1}(A)$ and $T^{-1}(S^{-1}A)$ are isomorphic, if T denotes also the image of T in $S^{-1}A$.

In particular, if $S \subset T$ then $T^{-1}A \cong T^{-1}(S^{-1}A)$. Hence, for $Q \subset P$ two prime ideals we obtain $A_Q \cong (A_P)_{QA_P}$.

1.4.6. Let $S \subset A$ be the set of non–zerodivisors. Show the following statements about the total ring of fractions $\mathrm{Quot}(A) = S^{-1}A$:

(1) S is the biggest multiplicatively closed subset of A such that $A \to S^{-1}A$ is injective.
(2) Each element of $\mathrm{Quot}(A)$ is either a unit or a zerodivisor.
(3) A ring A, such that each non–unit is a zerodivisor, is equal to its total ring of fractions, that is, $A \to \mathrm{Quot}(A)$ is bijective.

1.4.7. (1) Consider the two rings

$$A = \mathbb{C}[x,y]/\langle x^2 - y^3\rangle \text{ and } B = \mathbb{C}[x,y]/\langle xy\rangle$$

and the multiplicative sets:
- S the set of non–zerodivisors of A, respectively of B, and
- $T := A \setminus \langle x,y\rangle_A$, respectively $T := B \setminus \langle x,y\rangle_B$.

Determine the localizations of A and B with respect to T and S.

(2) Are any two of the six rings A, B, $S^{-1}A$, $S^{-1}B$, $T^{-1}A$, $T^{-1}B$ isomorphic?

1.4.8. Let A be a ring and $B = A/(P_1 \cap \cdots \cap P_r)$ with $P_i \subset A$ prime ideals. Show that the rings $\mathrm{Quot}(B)$ and $\bigoplus_{i=1}^{r} \mathrm{Quot}(A/P_i)$ are isomorphic. In particular, $\mathrm{Quot}(B)$ is a direct sum of fields.

(Hint: use Exercise 1.3.13.)

1.4.9. Let A be a *unique factorization domain* (that is, A is a domain and every non–unit of A can be written as a product of irreducible elements such that the factors are uniquely determined up to multiplication with units) and $S \subset A$ multiplicatively closed. Show that $S^{-1}A$ is a unique factorization domain.

(Hint: enlarge, if necessary, S to a multiplicative system $\widetilde{S}$ such that
(1) $\widetilde{S}^{-1}A = S^{-1}A$ and
(2) if $s \in \widetilde{S}$ and $s = s_1 s_2$ then $s_1, s_2 \in \widetilde{S}$.)

1.4.10. Let A be an integral domain. Then, for any prime ideal $P \subset A$, we consider the localization A_P as a subring of the quotient field $\mathrm{Quot}(A)$ and, hence, we can consider their intersection. Show that

$$A = \bigcap_{P \in \mathrm{Spec}\, A} A_P = \bigcap_{\mathfrak{m} \in \mathrm{Max}\, A} A_{\mathfrak{m}}\,.$$

1.4.11. Let $I = I_1 I_2 I_3 \subset Q[x,y,z]$ be the product of the ideals $I_1 = \langle z - x^2\rangle$, $I_2 = \langle y,z\rangle$ and $I_3 = \langle x\rangle$. Compute, as in SINGULAR Example 1.4.9, the dimension of $V(I)$ at the points $(0,0,0)$, $(0,0,1)$, $(1,0,0)$ and $(1,1,1)$. Draw a real picture of $V(I)$ and interpret your results geometrically.

1.5 Rings Associated to Monomial Orderings

In this section we show that non–global monomial orderings lead to new rings which are localizations of the polynomial ring. This fact has far–reaching computational consequences. For example, choosing a local ordering, we can, basically, do the same calculations in the localization of a polynomial ring as with a global ordering in the polynomial ring itself. In particular, we can effectively compute in $K[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_k\rangle}$ for $k \leq n$ (by Lemma 1.5.2 (3) and Example 1.5.3).

Let $>$ be a monomial ordering on the set of monomials $\mathrm{Mon}(x_1,\dots,x_n) = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$, and $K[x] = K[x_1,\dots,x_n]$ the polynomial ring in n variables over a field K. Then the leading monomial function LM has the following properties for polynomials $f, g \in K[x] \setminus \{0\}$:

(1) $\mathrm{LM}(gf) = \mathrm{LM}(g)\,\mathrm{LM}(f)$.
(2) $\mathrm{LM}(g+f) \leq \max\{\mathrm{LM}(g), \mathrm{LM}(f)\}$ with equality if and only if the leading terms of f and g do not cancel.

In particular, it follows that

$$S_> := \{u \in K[x] \setminus \{0\} \mid \mathrm{LM}(u) = 1\}$$

is a multiplicatively closed set.

Definition 1.5.1. For any monomial ordering $>$ on $\mathrm{Mon}(x_1,\dots,x_n)$, we define

$$K[x]_> := S_>^{-1}K[x] = \left\{ \frac{f}{u} \;\middle|\; f, u \in K[x],\ \mathrm{LM}(u) = 1 \right\},$$

the localization of $K[x]$ with respect to $S_>$ and call $K[x]_>$ the *ring associated to* $K[x]$ *and* $>$.

Note that $S_> = K^*$ if and only if $>$ is global and $S_> = K[x] \setminus \langle x_1,\dots,x_n\rangle$ if and only if $>$ is local.

Lemma 1.5.2. *Let K be a field, $K[x] = K[x_1,\dots,x_n]$, and let $>$ be a monomial ordering on* $\mathrm{Mon}(x_1,\dots,x_n)$. *Then*

(1) $K[x] \subset K[x]_> \subset K[x]_{\langle x\rangle}$.
(2) The set of units in $K[x]_>$ *is given by*

$$(K[x]_>)^* = \left\{ \frac{v}{u} \;\middle|\; u, v \in K[x],\ \mathrm{LM}(v) = \mathrm{LM}(u) = 1 \right\},$$

and satisfies $(K[x]_>)^* \cap K[x] = S_>$.
(3) $K[x] = K[x]_>$ *if and only if* $>$ *is a global ordering and* $K[x]_> = K[x]_{\langle x\rangle}$ *if and only if* $>$ *is a local ordering.*
(4) $K[x]_>$ *is a Noetherian ring.*
(5) $K[x]_>$ *is factorial.*

We shall see later (Corollary 7.4.6) that the inclusions of Lemma 1.5.2 (1) are flat ring morphisms.

Proof. (1) The first inclusion is clear by Proposition 1.4.5 (2), the second follows from Proposition 1.4.5 (4) since $\mathrm{LM}(u) = 1$ implies $u \notin \langle x\rangle$.
(2) If f/u is a unit in $K[x]_>$, there is a h/v such that $(f/u)\cdot(h/v) = 1$. Hence, $fh = uv$ and $\mathrm{LM}(f)\,\mathrm{LM}(h) = 1$, which implies $\mathrm{LM}(f) = 1$.

(3) By Proposition 1.4.5 (2), $K[x] = K[x]_>$ if and only if $S_>$ consists of units of $K[x]$, that is if and only if $S_> \subset K^*$, which is equivalent to $>$ being global. The second equality follows since $K[x] \setminus \langle x \rangle$ consists of units in $K[x]_>$ if and only if every polynomial with non–zero constant term belongs to $S_>$ which is equivalent to $>$ being local.
(4) Follows from Lemma 1.4.8.
(5) Since $K[x]$ is factorial, this follows from Exercise 1.4.9. □

Examples 1.5.3. We describe some familiar and some less familiar rings, associated to a polynomial ring and a monomial ordering.

(1) Let $K[x,y] = K[x_1,\ldots,x_n,y_1,\ldots,y_m]$ and consider the product ordering $> = (>_1,>_2)$ on $\mathrm{Mon}(x_1,\ldots,x_n,y_1,\ldots,y_m)$, where $>_1$ is global on $\mathrm{Mon}(x_1,\ldots,x_n)$ and $>_2$ is local on $\mathrm{Mon}(y_1,\ldots,y_m)$. Then

$$x^\alpha y^\gamma > 1 > y^\beta \text{ for all } \alpha,\beta \neq 0, \text{ all } \gamma$$

and hence $S_> = K^* + \langle y \rangle \cdot K[y]$. It follows that

$$K[x,y]_> = (K[y]_{\langle y \rangle})[x]\,,$$

which equals $K[y]_{\langle y \rangle} \otimes_K K[x]$ (cf. Section 2.7 for the tensor product).

(2) Now let $>_1$ be local and $>_2$ global, $> = (>_1,>_2)$, then

$$x^\alpha y^\gamma < 1 < y^\beta \text{ for all } \alpha,\beta \neq 0, \text{ all } \gamma$$

and hence $S_> = K^* + \langle x \rangle K[x,y]$. We obtain strict inclusions

$$(K[x]_{\langle x \rangle})[y] \subsetneq K[x,y]_> \subsetneq K[x,y]_{\langle x \rangle}\,,$$

since $1/(1+xy)$ is in the second but not in the first and $1/y$ is in the third but not in the second ring.

(3) If $>_1$ is global, $>_2$ arbitrary and $> = (>_1,>_2)$ then $S_>$ consists of elements $u \in K[y]$ satisfying $\mathrm{LM}_{>_2}(u) = 1$. Hence,

$$K[x,y]_> = (K[y]_{>_2})[x]$$

(cf. Exercise 2.7.12). This ordering has the following *elimination property* for $x_1,\ldots,x_n$:

$$f \in K[x,y],\ \mathrm{LM}(f) \in K[y] \Rightarrow f \in K[y]\,.$$

(4) Let $>$ be a local ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$ and $K(y)$ the quotient field of $K[y] = K[y_1,\ldots,y_m]$. It is not difficult to see that

$$K(y)[x]_> = K[x,y]_{\langle x \rangle}$$

(Exercise 1.5.6). Hence, we can effectively compute in the localization $K[x_1,\ldots,x_n]_P$, where P is a prime ideal generated by a subset of the variables.

Definition 1.5.4. A monomial ordering $>$ on $K[x_1,\dots,x_n]$ having the elimination property for $x_1,\dots,x_s$ (cf. Example 1.5.3 (3)) is called an *elimination ordering* for $x_1,\dots,x_s$.

An elimination ordering need not be a product ordering but must satisfy $x_i > 1$ for $i = 1,\dots,s$ (since, if $x_i < 1$ then $\mathrm{LM}(1+x_i) = 1$ but $1+x_i \notin K[x_{s+1},\dots,x_n]$), that is, an elimination ordering for $x_1,\dots,x_s$ must be global on $\mathrm{Mon}(x_1,\dots,x_s)$. Since the lexicographical ordering is the product of the degree orderings on $\mathrm{Mon}(x_i)$ for $i = 1,\dots,n$, it is an elimination ordering for $x_1,\dots,x_j$, for $j = 1,\dots,n$. (Cf. Section 1.8.2 for applications of elimination orderings.)

We now extend the leading data to $K[x]_>$.

Definition 1.5.5. Let $>$ be any monomial ordering:

(1) For $f \in K[x]_>$ choose $u \in K[x]$ such that $\mathrm{LT}(u) = 1$ and $uf \in K[x]$. We define

$$\begin{aligned}\mathrm{LM}(f) &:= \mathrm{LM}(uf),\\ \mathrm{LC}(f) &:= \mathrm{LC}(uf),\\ \mathrm{LT}(f) &:= \mathrm{LT}(uf),\\ \mathrm{LE}(f) &:= \mathrm{LE}(uf),\end{aligned}$$

and $\mathrm{tail}(f) = f - \mathrm{LT}(f)$.

(2) For any subset $G \subset K[x]_>$ define the ideal

$$L_>(G) := L(G) := \langle \mathrm{LM}(g) \mid g \in G \setminus \{0\} \rangle_{K[x]}.$$

$L(G) \subset K[x]$ is called the *leading ideal* of G.

Remark 1.5.6.

(1) The definitions in 1.5.5 (1) are independent of the choice of u.
(2) Since $K[x]_> \subset K[x]_{\langle x\rangle} \subset K[[x]]$, where $K[[x]]$ denotes the formal power series ring (cf. Section 6.1), we may consider $f \in K[x]_>$ as a formal power series. It follows easily that $\mathrm{LM}(f)$, respectively $\mathrm{LT}(f)$, corresponds to a unique monomial, respectively term, in the power series expansion of f. Hence $\mathrm{tail}(f)$ is the power series of f with the leading term deleted.
(3) Note that if I is an ideal, then $L(I)$ is the ideal generated by all leading monomials of all elements of I and not only by the leading monomials of a given set of generators of I.

Example 1.5.7.

(1) Consider $\mathbb{Q}[x]$ with a local ordering (in one variable all local, respectively global, orderings coincide). For $f = 3x/(1+x) + x$ we have $\mathrm{LM}(f) = x$, $\mathrm{LC}(f) = 4$, $\mathrm{LT}(f) = 4x$, $\mathrm{LE}(f) = 1$ and $\mathrm{tail}(f) = -3x^2/(1+x)$.

(2) Let $G = \{f, g\}$ with $f = xy^2 + xy$, $g = x^2y + x^2 - y \in \mathbb{Q}[x, y]$ and monomial ordering `dp`. If $I = \langle f, g\rangle$ then $L(G) \subsetneq L(I)$, since $L(G) = \langle xy^2, x^2y\rangle$, but $xf - yg = y^2$. Thus, $y^2 \in L(I)$, but $y^2 \notin L(G)$.

Ring maps between rings associated to a monomial ordering are almost as easy as ring maps between polynomial rings.

Lemma 1.5.8. *Let $\psi : K \to L$ be a morphism of fields and $>_1$, $>_2$, monomial orderings on $\mathrm{Mon}(x_1, \ldots, x_n)$ and on $\mathrm{Mon}(y_1, \ldots, y_m)$. Let $f_1, \ldots, f_n \in L[y_1, \ldots, y_m]_{>_2}$ and assume that, for all $h \in S_{>_1}$, $h(f_1, \ldots, f_n) \in S_{>_2}$. Then there exists a unique ring map*

$$\varphi : K[x_1, \ldots, x_n]_{>_1} \to L[y_1, \ldots, y_m]_{>_2}$$

satisfying $\varphi(x_i) = f_i$ for $i = 1, \ldots, n$, and $\varphi(a) = \psi(a)$ for $a \in K$.

Proof. By Lemma 1.1.6, there is a unique ring map $\widetilde{\varphi} : K[x] \to L[y]_{>_2}$ with $\widetilde{\varphi}(x_i) = f_i$ and $\widetilde{\varphi}(a) = \psi(a)$, $a \in K$. The assumption says that $\widetilde{\varphi}(u)$ is a unit in $L[y]_{>_2}$ for each $u \in S_{>_1}$. Hence, the result follows from the universal property of localization (Proposition 1.4.7). □

In particular, if $>_1$ is global, there is no condition on the f_i and any elements $f_1, \ldots, f_n \in K[y_1, \ldots, y_m]_>$ define a unique map

$$K[x_1, \ldots, x_n] \longrightarrow K[y_1, \ldots, y_m]_>, \quad x_i \longmapsto f_i\,,$$

for any monomial ordering $>$ on $\mathrm{Mon}(y_1, \ldots, y_m)$.

Remark 1.5.9. With the notations of Lemma 1.5.8, the condition "$h \in S_{>_1}$ implies $h(f_1, \ldots, f_n) \in S_{>_2}$" cannot be replaced by "$1 >_2 \mathrm{LM}(f_i)$ for those i where $1 >_1 x_i$". Consider the following example: let $>_1$, respectively $>_2$, be defined on $K[x, y]$ by the matrix $\left(\begin{smallmatrix} -2 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, respectively $\left(\begin{smallmatrix} -1 & 2 \\ 1 & 0 \end{smallmatrix}\right)$. Then $x <_1 y$ and $x <_2 y$ but $xy + 1 \in S_{<_1}$ and $xy + 1 \notin S_{>_2}$.

SINGULAR Example 1.5.10 (realization of rings).
We show how to create the rings of Examples 1.5.3. Note that SINGULAR sorts the monomials with respect to the monomial ordering, the greatest being first. Hence, the position of 1 in the output shows which monomials are greater, respectively smaller, than 1.

```
int n,m=2,3;
ring A1 = 0,(x(1..n),y(1..m)),(dp(n),ds(m));
poly f  = x(1)*x(2)^2+1+y(1)^10+x(1)*y(2)^5+y(3);
f;
//-> x(1)*x(2)^2+x(1)*y(2)^5+1+y(3)+y(1)^10

1>y(1)^10;  //the monomial 1 is greater than y(1)^10
```

```
//-> 1

ring A2 = 0,(x(1..n),y(1..m)),(ds(n),dp(m));
fetch(A1,f);
//-> y(1)^10+y(3)+1+x(1)*y(2)^5+x(1)*x(2)^2

x(1)*y(2)^5<1;
//-> 1

ring A3 = 0,(x(1..n),y(1..m)),(dp(n),ds(2),dp(m-2));
fetch(A1,f);
//-> x(1)*x(2)^2+x(1)*y(2)^5+y(3)+1+y(1)^10
```

Exercises

1.5.1. Prove Remark 1.5.6.

1.5.2. Give one possible realization of the following rings within SINGULAR:

(1) $\mathbb{Q}[x,y,z]$,
(2) $\mathbb{F}_5[x,y,z]$,
(3) $\mathbb{Q}[x,y,z]/\langle x^5+y^3+z^2\rangle$,
(4) $\mathbb{Q}(i)[x,y]$, $i^2=-1$,
(5) $\mathbb{F}_{27}[x_1,\ldots,x_{10}]_{\langle x_1,\ldots,x_{10}\rangle}$,
(6) $\mathbb{F}_{32003}[x,y,z]_{\langle x,y,z\rangle}/\langle x^5+y^3+z^2, xy\rangle$,
(7) $\mathbb{Q}(t)[x,y,z]$,
(8) $\big(\mathbb{Q}[t]/(t^3+t^2+1)\big)[x,y,z]_{\langle x,y,z\rangle}$,
(9) $(\mathbb{Q}[t]_{\langle t\rangle})[x,y,z]$,
(10) $\mathbb{F}_2(a,b,c)[x,y,z]_{\langle x,y,z\rangle}$.

(Hint: see the SINGULAR Manual for how to define a quotient ring modulo some ideal.)

1.5.3. What are the units in the rings of Exercise 1.5.2?

1.5.4. Write a SINGULAR procedure, having as input a polynomial f and returning 1 if f is a unit in the basering and 0 otherwise.

(Hint: type `?procedures;`.)

Test the procedure by creating, for each ring of Exercise 1.5.2, two polynomials, one a unit, the other not.

1.5.5. Write a SINGULAR procedure, having as input a polynomial f and an integer n, which returns the power series expansion of the inverse of f up to terms of degree n if f is a unit in the basering and 0 if f is not a unit.

(Hint: remember the geometric series.)

1.5.6. (1) Let $>$ be a local ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$. Show that $K[x_1,\ldots,x_n,y_1,\ldots,y_m]_{\langle x_1,\ldots,x_n\rangle} = K(y_1,\ldots,y_m)[x_1,\ldots,x_n]_>$.
(2) Implement the ring $\mathbb{Q}[x,y,z]_{\langle x,y\rangle}$ inside SINGULAR.

1.6 Normal Forms and Standard Bases

In this section we define standard bases, respectively Gröbner bases, of an ideal $I \subset K[x]_>$ as a set of polynomials of I such that their leading monomials generate the leading ideal $L(I)$. The next section gives an algorithm to compute standard bases. For global orderings this is Buchberger's algorithm, which is a generalization of the Gaussian elimination algorithm and the Euclidean algorithm. For local orderings it is Mora's tangent cone algorithm, which itself is a variant of Buchberger's algorithm. The general case is a variation of Mora's algorithm, which is due to the authors and implemented in SINGULAR since 1990.

The leading ideal $L(I)$ contains a lot of information about the ideal I, which often can be computed purely combinatorially from $L(I)$, because the leading ideal is *generated by monomials*. Standard bases have turned out to be the fundamental tool for computations with ideals and modules. The idea of standard bases is already contained in the work of Gordan [93]. Later, monomial orderings were used by Macaulay [157] and Gröbner [117] to study Hilbert functions of graded ideals, and, more generally, to find bases of zero–dimensional factor rings. The notion of a standard basis was introduced later, independently, by Hironaka [123], Grauert [98] (for special local orderings) and Buchberger [32] (for global orderings).

In the following, special emphasis is made to axiomatically characterize normal forms, respectively weak normal forms, which play an important role in the standard basis algorithm. They generalize division with remainder to the case of ideals, respectively finite sets of polynomials.

In the case of a global ordering, for any polynomial f and any ideal I, there is a unique normal form $\mathrm{NF}(f \mid I)$ of f with respect to I, such that no monomial of $\mathrm{NF}(f \mid I)$ is in the leading ideal $L(I)$. This can be used to decide, for instance, whether f is in the ideal I (if the normal form is 0).

In the general case, the above property turns out to be too strong. Hence, the requirements for a normal form have to be weakened. For instance, for the decision whether a polynomial is in an ideal or not, only the leading term of a normal form $\mathrm{NF}(f \mid I)$ is important. Thus, for this purpose, it is enough to require that $\mathrm{NF}(f \mid I)$ is either 0 or has a leading term, which is not in $L(I)$. After weakening the requirements, there is no more uniqueness statement for the normal form.

Our intention is to keep the definition of a normal form as general as possible. Moreover, our presentation separates the normal form algorithm from a general standard basis algorithm and shows that different versions of standard basis algorithms are due to different normal forms.

The axiomatic definition of a normal form as presented in this section has been introduced in [111, 112], although its properties have already commonly been used before. It seems to be the minimal requirement in order to carry through standard basis theory in the present context.

Let $>$ be a fixed monomial ordering and let, in this section,

$$R = K[x_1, \ldots, x_n]_>$$

be the localization of $K[x] = K[x_1, \ldots, x_n]$ with respect to $>$. Recall that $R = S_>^{-1}K[x]$ with $S_> = \{u \in K[x] \setminus \{0\} \mid \mathrm{LM}(u) = 1\}$, and that $R = K[x]$ if $>$ is global and $R = K[x]_{\langle x \rangle}$ if $>$ is local. In any case, R may be considered as a subring of the ring $K[[x]]$ of formal power series (cf. Section 6.1).

Definition 1.6.1. Let $I \subset R$ be an ideal.

(1) A finite set $G \subset R$ is called a *standard basis* of I if

$$G \subset I, \text{ and } L(I) = L(G)\,.$$

That is, G is a standard basis, if the leading monomials of the elements of G generate the leading ideal of I, or, in other words, if for any $f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $\mathrm{LM}(g) \mid \mathrm{LM}(f)$.

(2) If $>$ is global, a standard basis is also called a *Gröbner basis*.

(3) If we just say that G is a standard basis, we mean that G is a standard basis of the ideal $\langle G \rangle_R$ generated by G.

Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$. Then each non–zero ideal $I \subset K[x]_>$ has a standard basis. To see this, choose a finite set of generators $m_1, \ldots, m_s$ of $L(I) \subset K[x]$, which exists, since $K[x]$ is Noetherian (Theorem 1.3.5). By definition of the leading ideal, these generators are leading monomials of suitable elements $g_1, \ldots, g_s \in I$. By construction, the set $\{g_1, \ldots, g_s\}$ is a standard basis for I.

Definition 1.6.2. Let $G \subset R$ be any subset.

(1) G is called *interreduced* if $0 \notin G$ and if $\mathrm{LM}(g) \nmid \mathrm{LM}(f)$ for any two elements $f \neq g$ in G. An interreduced standard basis is also called *minimal*.

(2) $f \in R$ is called *(completely) reduced with respect to* G if no monomial of the power series expansion of f is contained in $L(G)$.

(3) G is called *(completely) reduced* if G is interreduced and if, for any $g \in G$, $\mathrm{LC}(g) = 1$ and $\mathrm{tail}(g)$ is completely reduced with respect to G.

Remark 1.6.3.

(1) If $>$ is a global ordering, then any finite set G can be transformed into an interreduced set: for any $g \in G$ such that there exists an $f \in G \setminus \{g\}$ with $\mathrm{LM}(f) \mid \mathrm{LM}(g)$ replace g by $g - mf$, where m is a term with $\mathrm{LT}(g) = m\,\mathrm{LT}(f)$. The result is called the *(inter)reduction* of G; it generates the same ideal as G.

(2) Every standard basis G can be transformed into an interreduced one by just deleting elements of G: delete zeros and then, successively, any g such that $\mathrm{LM}(g)$ is divisible by $\mathrm{LM}(f)$ for some $f \in G \setminus \{g\}$. The result is again a standard basis. Thus, G is interreduced if and only if G is minimal (that is, we cannot delete any element of G without violating the property of being a standard basis).
(3) Let $G \subset R$ be an interreduced set and $g \in G$. If $\mathrm{tail}(g)$ is not reduced with respect to G, the power series expansion of $\mathrm{tail}(g)$ has a monomial which is either divisible by $L(g)$ or by $L(f)$ for some $f \in G \setminus \{g\}$. If $>$ is global, then no monomial of $\mathrm{tail}(g)$ is divisible by $L(g)$ since $>$ refines the natural partial ordering on $\mathbb{N}^n$, that is, $\mathrm{tail}(g)$ is reduced with respect to $\{g\}$. For local or mixed orderings, however, it is possible to reduce $\mathrm{tail}(g)$ with g and we actually have to do this.
(4) It follows that a Gröbner basis $G \subset K[x]$, which consists of monic polynomials, is (completely) reduced if for any $f \neq g \in G$, $\mathrm{LM}(g)$ does not divide any monomial of f.

We shall see later that reduced Gröbner bases can always be computed[6] (cf. the remark after Algorithm 1.6.10), and are unique (Exercise 1.6.1), but reduced standard bases are, in general, not computable (in a finite number of steps).

The following two definitions are crucial for our treatment of standard bases.

Definition 1.6.4. Let $\mathcal{G}$ denote the set of all finite lists $G \subset R$.

$$\mathrm{NF} : R \times \mathcal{G} \to R,\ (f, G) \mapsto \mathrm{NF}(f \mid G)\,,$$

is called a *normal form* on R if, for all $G \in \mathcal{G}$,

(0) $\mathrm{NF}(0 \mid G) = 0\,,$

and, for all $f \in R$ and $G \in \mathcal{G}$,

(1) $\mathrm{NF}(f \mid G) \neq 0 \implies \mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G)$.
(2) If $G = \{g_1, \ldots, g_s\}$, then $f - \mathrm{NF}(f|G)$ (or, by abuse of notation, f) has a *standard representation* with respect to $\mathrm{NF}(- \mid G)$, that is,

$$f - \mathrm{NF}(f \mid G) = \sum_{i=1}^{s} a_i g_i,\ \ a_i \in R\,,\ \ s \geq 0\,,$$

satisfying $\mathrm{LM}(\Sigma_{i=1}^{s} a_i g_i) \geq \mathrm{LM}(a_i g_i)$ for all i such that $a_i g_i \neq 0$.
NF is called a *reduced normal form*, if, moreover, $\mathrm{NF}(f \mid G)$ is reduced with respect to G.

[6] The SINGULAR command `std` can be forced to compute reduced Gröbner bases G (up to normalization) using `option(redSB)`. To normalize G, one may use the SINGULAR command `simplify(G,1)`.

Definition 1.6.5.

(1) A map $\mathrm{NF} : R \times \mathcal{G} \to R$, as in Definition 1.6.4, is called a *weak normal form* on R if it satisfies (0),(1) of 1.6.4 and, instead of (2),

(2') for all $f \in R$ and $G \in \mathcal{G}$ there exists a unit $u \in R^*$ such that uf has a standard representation with respect to $\mathrm{NF}(- \mid G)$.

(2) A weak normal form NF is called *polynomial* if, whenever $f \in K[x]$ and $G \subset K[x]$, there exists a unit $u \in R^* \cap K[x]$ such that uf has a standard representation with $a_i \in K[x]$.

Remark 1.6.6.

(1) The notion of weak normal forms is only interesting for non–global orderings since for global orderings we have $R = K[x]$ and, hence, $R^* = K^*$. Even in general, if a weak normal form NF exists, then, theoretically, there exists also a normal form $\widetilde{\mathrm{NF}}$

$$(f, G) \longmapsto \frac{1}{u}\,\mathrm{NF}(f \mid G) =: \widetilde{\mathrm{NF}}(f \mid G)$$

for an appropriate choice of $u \in R^*$ (depending on f and G). However, we are really interested in polynomial normal forms, and for non–global orderings $1/u$ is, in general, not a polynomial but a power series.
Note that $R^* \cap K[x] = S_>$.

(2) Consider $f = y$, $g = (y - x)(1 - y)$, and $G = \{g\}$ in $R = K[x, y]_{\langle x,y\rangle}$ with local ordering `ls`. Assume $h := \mathrm{NF}(f \mid G) \in K[x, y]$ is a polynomial normal form of f with respect to G. Since $f \notin \langle G\rangle_R = \langle y - x\rangle_R$, we have $h \neq 0$, hence, $\mathrm{LM}(h) \notin L(G) = \langle y\rangle$. Moreover $h - y = h - f \in \langle y - x\rangle_R$, which implies $\mathrm{LM}(h) < 1$. Therefore, we obtain $h = xh'$ for some h' (because of the chosen ordering `ls`). However, $y - xh' \notin \langle (y - x)(1 - y)\rangle_{K[x,y]}$ (substitute $(0, 1)$ for (x, y)) and, therefore no polynomial normal form of (f, G) exists. On the other hand, setting $u = (1 - y)$ and $h = x(1 - y)$ then $uy - h = (y - x)(1 - y)$ and, hence, h is a polynomial weak normal form.

(3) For applications (weak) normal forms are most useful if G is a standard basis of $\langle G\rangle_R$. We shall demonstrate this with a first application in Lemma 1.6.7.

(4) $f = \sum_i a_i g_i$ being a standard representation means that no cancellation of leading terms $> \mathrm{LM}(f)$ between the $a_i g_i$ can occur and that $\mathrm{LM}(f) = \mathrm{LM}(a_i g_i)$ for at least one i.

(5) We do not distinguish strictly between lists and (ordered) sets. Since, in the definition of normal form, we allow repetitions of elements in G we need lists, that is, sequences of elements, instead of sets. We assume a given set G to be ordered (somehow) when we apply $\mathrm{NF}(- \mid G)$.

(6) The existence of a normal form resp. a polynomial weak normal form with respect to $G \subset K[x]$ which we prove in Algorithm 1.6.10 resp. Algorithm 1.7.6 says:
For any $f \in R$ there exist polynomials $u, a_1, \ldots, a_s \in K[\underline{x}]$ such that

$$uf = \sum_{i=1}^{s} a_i g_i + h, \ \mathrm{LM}(u) = 1,$$

satisfying:
(1) If $h \neq 0$ then $\mathrm{LM}(h)$ is not divisible by $\mathrm{LM}(g_i)$, $i = 1, \ldots, s$,
(2) $\mathrm{LM}(\sum_{i=1}^{s} a_i g_i) \geq \mathrm{LM}(a_i g_i)$ for all i with $a_i g_i \neq 0$ (and hence equality holds for at least one i).
Moreover, if $>$ is global then the unit u can be chosen as 1.

Thus the existence of a (weak) normal form is a *division theorem* where f (resp. uf) is divided by $G = \{g_1, \ldots, g_s\}$ with main part $\sum_{i=1}^{s} a_i g_i$ and *remainder* $h = \mathrm{NF}(f|G)$.
The SINGULAR command *reduce* or *NF* resp. *division* returns the remainder h resp. h together with the a_i and the unit u.

Lemma 1.6.7. *Let $I \subset R$ be an ideal, $G \subset I$ a standard basis of I and $\mathrm{NF}(- \mid G)$ a weak normal form on R with respect to G.*

(1) For any $f \in R$ we have $f \in I$ if and only if $\mathrm{NF}(f \mid G) = 0$.
(2) If $J \subset R$ is an ideal with $I \subset J$, then $L(I) = L(J)$ implies $I = J$.
(3) $I = \langle G \rangle_R$, that is, the standard basis G generates I as R–ideal.
(4) If $\mathrm{NF}(- \mid G)$ is a reduced normal form, then it is unique.[7]

Proof. (1) If $\mathrm{NF}(f \mid G) = 0$ then $uf \in I$ and, hence, $f \in I$. If $\mathrm{NF}(f \mid G) \neq 0$, then $\mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G) = L(I)$, hence $\mathrm{NF}(f \mid G) \notin I$, which implies $f \notin I$, since $\langle G \rangle_R \subset I$. To prove (2), let $f \in J$ and assume that $\mathrm{NF}(f \mid G) \neq 0$. Then $\mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G) = L(I) = L(J)$, contradicting $\mathrm{NF}(f \mid G) \in J$. Hence, $f \in I$ by (1).

(3) follows from (2), since $L(I) = L(G) \subset L(\langle G \rangle_R) \subset L(I)$, in particular, G is also a standard basis of $\langle G \rangle_R$. Finally, to prove (4), let $f \in R$ and assume that h, h' are two reduced normal forms of f with respect to G. Then no monomial of the power series expansion of h or h' is divisible by any monomial of $L(G)$ and, moreover, $h - h' = (f - h') - (f - h) \in \langle G \rangle_R = I$. If $h - h' \neq 0$, then $\mathrm{LM}(h - h') \in L(I) = L(G)$, a contradiction, since $\mathrm{LM}(h - h')$ is a monomial of either h or h'. □

Remark 1.6.8. The above properties are well–known for Gröbner bases with $R = K[x]$. For local or mixed orderings it is quite important to work rigorously with R instead of $K[x]$. We give an example showing that none of the

[7] In the case of a global ordering, we shall see below that such a reduced normal form exists. Then we also write $\mathrm{NF}(- \mid I)$ for $\mathrm{NF}(- \mid G)$, G any standard basis of I, and call it the *normal form with respect to I*.

above properties (1)–(3) holds for $K[x]$, if they make sense, that is, if the input data are polynomial.

Let $f_1 := x^{10} - x^9y^2$, $f_2 := y^8 - x^2y^7$, $f_3 := x^{10}y^7$, and consider the (local) ordering `ds` on $K[x,y]$. Then $R = K[x,y]_{\langle x,y\rangle}$, $(1-xy)f_3 = y^7f_1 + x^9yf_2$, and we set

$$I := \langle f_1, f_2\rangle_R = \langle f_1, f_2, f_3\rangle_R\,,\quad I' := \langle f_1, f_2\rangle_{K[x,y]}\,,\quad J' := \langle f_1, f_2, f_3\rangle_{K[x,y]},$$

and $G := \{f_1, f_2\}$. Then G is a reduced standard basis of I (since we must multiply f_1 at least with y^8 and f_2 with x^{10} to produce new monomials, but $L(G) \supset \langle x,y\rangle^{17}$). If $\mathrm{NF}(-\mid G)$ is any weak normal form on R, then $\mathrm{NF}(f_3 \mid G) = 0$, since $f_3 \in I$. Hence, we have in this case

(1) $\mathrm{NF}(f_3 \mid G) = 0$, but $f_3 \notin I'$,
(2) $I' \subset J'$, $L(I') = L(J')$, but $I' \neq J'$,
(3) $G \subset J'$, but $\langle G\rangle_{K[x]} \neq J'$.

Note that J' is even $\langle x,y\rangle$–primary (for a definition cf. Chapter 4).

We concentrate first on well–orderings, Gröbner bases and *Buchberger's algorithm*. To describe Buchberger's normal form algorithm, we need the notion of an s–polynomial, due to Buchberger.

Definition 1.6.9. Let $f, g \in R \setminus \{0\}$ with $\mathrm{LM}(f) = x^\alpha$ and $\mathrm{LM}(g) = x^\beta$, respectively. Set

$$\gamma := \mathrm{lcm}(\alpha,\beta) := \big(\max(\alpha_1,\beta_1), \ldots, \max(\alpha_n,\beta_n)\big)$$

and let $\mathrm{lcm}(x^\alpha, x^\beta) := x^\gamma$ be the *least common multiple* of x^α and x^β. We define the *s–polynomial* (*spoly*, for short) of f and g to be

$$\mathrm{spoly}(f,g) := x^{\gamma-\alpha}f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot x^{\gamma-\beta}g\,.$$

If $\mathrm{LM}(g)$ divides $\mathrm{LM}(f)$, say $\mathrm{LM}(g) = x^\beta$, $\mathrm{LM}(f) = x^\alpha$, then the s–polynomial is particularly simple,

$$\mathrm{spoly}(f,g) = f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot x^{\alpha-\beta}g\,,$$

and $\mathrm{LM}\big(\mathrm{spoly}(f,g)\big) < \mathrm{LM}(f)$.

For the normal form algorithm, the s–polynomial will only be used in the second form, while for the standard basis algorithm we need it in the general form above. In order to be able to use the same expression in both algorithms, we prefer the above definition of the s–polynomial and not the symmetric form $\mathrm{LC}(g)x^{\gamma-\alpha}f - \mathrm{LC}(f)x^{\gamma-\beta}g$. Both are, of course, equivalent, since we work over a field K. However, in connection with pseudo standard bases (Exercise 2.3.6) we have to use the symmetric form.

Algorithm 1.6.10 (NFBuchberger($f \mid G$)).
Assume that $>$ is a global monomial ordering.

Input: $f \in K[x]$, $G \in \mathcal{G}$

Output: $h \in K[x]$, a normal form of f with respect to G.

- $h := f$;
- while ($h \neq 0$ and $G_h := \{g \in G \mid \mathrm{LM}(g) \text{ divides } \mathrm{LM}(h)\} \neq \emptyset$)
  choose any $g \in G_h$;
  $h := \mathrm{spoly}(h, g)$;
- return h;

Note that each specific choice of "any" can give a different normal form function.

Proof. The algorithm terminates, since in the i–th step of the while loop we create (setting $h_0 := f$) an s–polynomial

$$h_i = h_{i-1} - m_i g_i, \quad \mathrm{LM}(h_{i-1}) > \mathrm{LM}(h_i)\,,$$

where m_i is a term such that $\mathrm{LT}(m_i g_i) = \mathrm{LT}(h_{i-1})$, and $g_i \in G$ (allowing repetitions).

Since $>$ is a well–ordering, $\{\mathrm{LM}(h_i)\}$ has a minimum, which is reached at some step m. We obtain

$$\begin{aligned} h_1 &= f - m_1 g_1 \\ h_2 &= h_1 - m_2 g_2 = f - m_1 g_1 - m_2 g_2 \\ &\vdots \\ h_m &= f - \sum_{i=1}^{m} m_i g_i, \end{aligned}$$

satisfying $\mathrm{LM}(f) = \mathrm{LM}(m_1 g_1) > \mathrm{LM}(m_i g_i) > \mathrm{LM}(h_m)$. This shows that $h := h_m$ is a normal form with respect to G.

Moreover, if $h \neq 0$, then $G_h = \emptyset$ and, hence, $\mathrm{LM}(h) \notin L(G)$ if $h \neq 0$. This proves correctness, independent of the specific choice of "any" in the while loop. □

It is easy to extend NFBuchberger to a reduced normal form. Either we do tail–reduction during NFBuchberger, that is, we set

$$\begin{aligned} &h := \mathrm{spoly}(h, g); \\ &h := \mathrm{LT}(h) + \mathrm{NFBuchberger}(\mathrm{tail}\big(h) \mid G\big); \end{aligned}$$

in the while loop, or do tail–reduction after applying NFBuchberger, as in Algorithm 1.6.11. Indeed, the argument holds for any normal form with respect to a global ordering.

Algorithm 1.6.11 (redNFBuchberger$(f \mid G)$**).**
Assume that $>$ is a global monomial ordering.

Input: $f \in K[x]$, $G \in \mathcal{G}$
Output: $h \in K[x]$, a reduced normal form of f with respect to G

- $h := 0,\ g := f$;
- while $(g \neq 0)$
  $g :=$ NFBuchberger $(g \mid G)$;
  if $(g \neq 0)$
    $h := h + \mathrm{LT}(g)$;
    $g := \mathrm{tail}(g)$;
- return $h/\mathrm{LC}(h)$;

Since $\mathrm{tail}(g)$ has strictly smaller leading term than g, the algorithm terminates, since $>$ is a well–ordering. Correctness follows from the correctness of NFBuchberger.

Example 1.6.12. Let $>$ be the ordering `dp` on $\mathrm{Mon}(x, y, z)$,

$$f = x^3 + y^2 + 2z^2 + x + y + 1\,, \quad G = \{x, y\}\,.$$

NFBuchberger proceeds as follows:

$\mathrm{LM}(f) = x^3,\ G_f = \{x\}$,
$h_1 = \mathrm{spoly}(f, x) = y^2 + 2z^2 + x + y + 1$,
$\mathrm{LM}(h_1) = y^2,\ G_{h_1} = \{y\}$,
$h_2 = \mathrm{spoly}(h_1, y) = 2z^2 + x + y + 1,\ G_{h_2} = \emptyset$.

Hence, NFBuchberger$(f \mid G) = 2z^2 + x + y + 1$. For the reduced normal form in Algorithm 1.6.11 we obtain:

$g_0 =$ NFBuchberger$(f \mid G) = 2z^2 + x + y + 1$, $\mathrm{LT}(g_0) = 2z^2$,
$h_1 = 2z^2,\ g_1 = \mathrm{tail}(g_0) = x + y + 1$,
$g_2 =$ NFBuchberger$(g_1 \mid G) = 1,\ \mathrm{LT}(g_2) = 1$,
$h_2 = 2z^2 + 1,\ g_3 = \mathrm{tail}(g_2) = 0$.

Hence, redNFBuchberger$(f \mid G) = z^2 + 1/2$.

SINGULAR Example 1.6.13 (normal form).
Note that $\mathrm{NF}(f \mid G)$ may depend on the sorting of the elements of G. The function `reduce` computes a normal form.

```
ring A  = 0,(x,y,z),dp;  //a global ordering
poly f  = x2yz+xy2z+y2z+z3+xy;
poly f1 = xy+y2-1;
poly f2 = xy;
ideal G = f1,f2;
```

```
ideal S = std(G);        //a standard basis of <G>
S;
//-> S[1]=xy
//-> S[2]=y2-1

reduce(f,G);
//** G is no standardbasis
//-> y2z+z3              //NF w.r.t. a non-standard basis

G=f2,f1;
reduce(f,G);
//** G is no standardbasis
//-> y2z+z3-y2+xz+1      //NF for a different numbering in G

reduce(f,S,1);           //NFBuchberger
//-> z3+xy+z

reduce(f,S);             //redNFBuchberger
//-> z3+z
```

Remark 1.6.14. There exists also the notion of a *standard basis over a ring*. Namely, let R be Noetherian and $R[x] = R[x_1, \ldots, x_n]$. The leading data of $f \in R[x_1, \ldots, x_n] \setminus \{0\}$ with respect to a monomial ordering $>$ on $\mathrm{Mon}(x_1, \ldots, x_n)$ are defined as in Definition 1.2.2. If $I \subset R[x]$ is an ideal and $G \subset I$ a finite set, then G is a *standard basis* of I if

$$\langle \mathrm{LT}(f) \mid f \in I \rangle = \langle \mathrm{LT}(g) \mid g \in G \rangle .$$

Note that we used leading terms and not leading monomials (which is, of course, equivalent if R is a field). The normal form algorithm over rings is more complicated than over fields. For example, if $>$ is a global ordering, the algorithm NFBuchberger has to be modified to

$h := f$;
while ($h \neq 0$ and $G_h = \{g_1, \ldots, g_s\} \neq \emptyset$ and $\mathrm{LT}(h) \in \langle \mathrm{LT}(g) \mid g \in G_h \rangle$)
  choose $c_i \in R \setminus \{0\}$ and monomials m_i with $m_i \,\mathrm{LM}(g_i) = \mathrm{LM}(h)$ such that
    $\mathrm{LT}(h) = c_1 m_1 \,\mathrm{LT}(g_1) + \cdots + c_s m_s \,\mathrm{LT}(g_s)$;
  $h := h - \sum_{i=1}^{s} c_i m_i g_i$;
return h;

The determination of the c_i requires the solving of linear equations over R and not just a divisibility test for monomials as for s–polynomials. With this normal form, standard bases can be computed as in the next section. For details see [1], [90], [129].

In practice, however, this notion is not frequently used so far and there seems to be no publicly available system having this implemented. A weaker concept are the *comprehensive Gröbner bases* of Weispfenning [232], which

are Gröbner bases depending on parameters and which specialize to a Gröbner basis for all possible fixed values of the parameters.

For a simple criterion, when the *specialization of a standard basis* is again a standard basis, see Exercises 2.3.7, 2.3.8, where we introduce *pseudo standard bases*.

Exercises

Let $>$ be any monomial ordering and $R = K[x_1, \ldots, x_n]_>$.

1.6.1. Let $I \subset R$ be an ideal. Show that if I has a reduced standard basis, then it is unique.

1.6.2. Let $>$ be a local or mixed ordering. Prove that Algorithm 1.6.11 computes, theoretically, (possibly in infinitely many steps) for $f \in R$ and $G \subset R$ a reduced normal form. Hence, it can be used to compute, for local degree orderings, a normal form which is completely reduced up to a finite, but arbitrarily high order.

1.6.3. Show by an example, with f and G consisting of polynomials and $>$ not global, that a completely reduced normal form of f with respect to G does not exist in R. (Note that Exercise 1.6.2 only says that it exists as formal power series.)

1.6.4. Apply NFBuchberger to $(f, G, >)$ without using Singular:

(1) $f = 1$, $G = \{x - 1\}$ and ordering `lp`, respectively `ls`.
(2) $f = x^4 + y^4 + z^4 + xyz$, $G = \{\partial f/\partial x, \partial f/\partial y, \partial f/\partial z\}$ and ordering `dp`.

1.6.5. Give a direct argument that the set G in Exercise 1.6.4 (2) is a standard basis with respect to `dp`.

1.6.6. Write a Singular procedure, having two polynomials f, g as input and returning spoly(f, g) as output.

1.6.7. Write your own Singular procedure, having a polynomial f and an ideal I as input and NFBuchberger $(f \mid I)$ as output by always choosing the first element from G_h. (Note that an ideal is given by a list of polynomials.)

1.6.8. Implement, as Singular procedures, the two ways described in the text to compute a reduced normal form. (The first method is a good exercise in recursive programming.)

Check your procedures with the Singular Example 1.6.13.

1.6.9. Let $R = K[t_1, \ldots, t_n]$, K a field. Write a Singular procedure which computes the normal form NFBuchberger over the ring R, as explained in Remark 1.6.14.

(Hint: use the Singular command `lift`.)

1.7 The Standard Basis Algorithm

Let $>$ be a fixed monomial ordering and let, in this section,

$$R = K[x_1, \ldots, x_n]_>$$

be the localization of $K[x]$, $x = (x_1, \ldots, x_n)$, with respect to $>$. Recall that $R = S_>^{-1}K[x]$ with $S_> = \{u \in K[x] \setminus \{0\} \mid \mathrm{LM}(u) = 1\}$, and that $R = K[x]$ if $>$ is global and $R = K[x]_{\langle x\rangle}$ if $>$ is local. In any case, R may be considered as a subring of the ring $K[[x]]$ of formal power series.

The idea of many standard basis algorithms may be formalized as follows:

Algorithm 1.7.1 (STANDARD(G,NF)).
Let $>$ be any monomial ordering, and $R := K[x_1, \ldots, x_n]_>$.

Input: $G \in \mathcal{G}$, NF an algorithm returning a weak normal form.
Output: $S \in \mathcal{G}$ such that S is a standard basis of $I = \langle G\rangle_R \subset R$

- $S := G$;
- $P := \{(f, g) \mid f, g \in S, f \neq g\}$, the pair–set;
- while $(P \neq \emptyset)$
  - choose $(f, g) \in P$;
  - $P := P \setminus \{(f, g)\}$;
  - $h := \mathrm{NF}\big(\mathrm{spoly}(f, g) \mid S\big)$;
  - if $(h \neq 0)$
    - $P := P \cup \{(h, f) \mid f \in S\}$;
    - $S := S \cup \{h\}$;
- return S;

To see termination of STANDARD, note that if $h \neq 0$ then $\mathrm{LM}(h) \notin L(S)$ by property (i) of NF. Hence, we obtain a strictly increasing sequence of monomial ideals $L(S)$ of $K[x]$, which becomes stationary as $K[x]$ is Noetherian. That is, after finitely many steps, we always have $\mathrm{NF}\big(\mathrm{spoly}(f, g) \mid S\big) = 0$ for $(f, g) \in P$, and, again after finitely many steps, the pair-set P will become empty. Correctness follows from applying Buchberger's fundamental standard basis criterion below.

Remark 1.7.2. If NF is a reduced normal form and if G is reduced, then S, as returned by STANDARD(G,NF), is a reduced standard basis if we delete elements whose leading monomials are divisible by a leading monomial of another element in S. If G is not reduced, we may apply a reduced normal form afterwards to $(f, S \setminus \{f\})$ for all $f \in S$ in order to obtain a reduced standard basis.

Theorem 1.7.3 (Buchberger's criterion). *Let $I \subset R$ be an ideal and $G = \{g_1, \ldots, g_s\} \subset I$. Let $\mathrm{NF}(- \mid G)$ be a weak normal form on R with respect to G. Then the following are equivalent:* [8]

[8] Usually, the implication (4) $\Rightarrow$ (1) is called Buchberger's criterion. But with our concept of (weak) normal forms, we need, indeed, the implication (5) $\Rightarrow$ (1) to prove the correctness of the standard basis algorithm.

(1) G is a standard basis of I.
(2) $\mathrm{NF}(f \mid G) = 0$ *for all* $f \in I$.
(3) Each $f \in I$ *has a standard representation with respect to* $\mathrm{NF}(- \mid G)$.
(4) G generates I and $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) = 0$ *for* $i, j = 1, \ldots, s$.
(5) G generates I and $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G_{ij}\big) = 0$ *for a suitable subset* $G_{ij} \subset G$ *and* $i, j = 1, \ldots, s$.

Proof. The implication (1) $\Rightarrow$ (2) follows from Lemma 1.6.7, (2) $\Rightarrow$ (3) is trivial. To see (3) $\Rightarrow$ (4), note that $h := \mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) \in I$ and, hence, either $h = 0$ or $\mathrm{LM}(h) \in L(G)$ by (3), a contradiction to property (i) of NF. The fact that G generates I follows immediately from (3). (4) $\Rightarrow$ (5) is trivial.

Finally, the implication (5) $\Rightarrow$ (1) is the important Buchberger criterion which allows the checking and construction of standard bases in finitely many steps. Our proof uses syzygies and is, therefore, postponed to the next chapter. □

Example 1.7.4. Let $>$ be the ordering `dp` on $\mathrm{Mon}(x, y)$, NF=NFBUCHBERGER and $G = \{x^2 + y, xy + x\}$. Then we obtain as initialization

$S = \{x^2 + y, xy + x\}$
$P = \{(x^2 + y, xy + x)\}$.

The while–loop gives, in the first turn,

$P = \emptyset$
$h = \mathrm{NF}(-x^2 + y^2 \mid S) = y^2 + y$
$P = \{(y^2 + y, x^2 + y),\ (y^2 + y, xy + x)\}$
$S = \{x^2 + y, xy + x, y^2 + y\}$.

In the second turn

$P = \{(y^2 + y, xy + x)\}$
$h = \mathrm{NF}(-x^2 y + y^3 \mid S) = 0$.

In the third turn

$P = \emptyset$
$h = \mathrm{NF}(0 \mid S) = 0$.

The algorithm terminates and $S = \{x^2 + y, xy + x, y^2 + y\}$ is a standard basis.

We present now a general normal form algorithm, which works for any monomial ordering. The basic idea is due to Mora [176], but our algorithm is more general, with a different notion of ecart. It has been implemented in SINGULAR since 1990, the first publication appeared in [97], [111].

Before turning to the details, let us first analyze Buchberger's algorithm in the case of a non–global ordering. We may assume that in $K[x, y]$ we have $x_1, \ldots, x_n < 1$, $y_1, \ldots, y_m > 1$ $(m \geq 0)$.

Look at the sequence $m_i = c_i x^{\alpha_i} y^{\beta_i}$, $i \geq 1$, of terms constructed in the algorithm NFBUCHBERGER. If $\deg_x(m_i)$ is bounded, then, since $>$ induces a well–ordering on $K[y]$, the algorithm stops after finitely many steps.

On the other hand, if the degree of m_i in x is unbounded, then, for each fixed factor x^{α_i}, there can only be finitely many cofactors y^{β_j} and, hence, $\sum_{i \geq 1} m_i$ converges in the $\langle x \rangle$–adic topology (cf. Definition 6.1.6), that is,

$\sum_{i\geq 1} m_i \in K[y][[x]]$. If $G = \{g_1, \ldots, g_s\}$ we may gather the factors m_j of any g_i, obtaining thus in NFBuchberger an expression

$$h = f - \sum_{i=1}^{s} a_i g_i\,, \quad h, a_i \in K[y][[x]]\,,$$

which holds in $K[y][[x]]$. However, this process does not stop.

The standard example is in one variable x, with $x < 1$, $f := x$ and $G := \{g = x - x^2\}$. Using NFBuchberger we obtain

$$x - \left(\sum_{i=0}^{\infty} x^i\right)(x - x^2) = 0$$

in $K[[x]]$, which is true, since $\sum_{i=0}^{\infty} x^i = 1/(1-x)$ in $K[[x]]$. However, the algorithm constructs a power series $\sum_{i=0}^{\infty} x^i$ having infinitely many terms and not the finite expression $1/(1-x)$.

In order to avoid infinite power series, we have to allow a wider class of elements for the reduction in order to create a standard expression of the form

$$uf = \sum_{i=1}^{s} a_i g_i + \mathrm{NF}(f \mid G)\,,$$

where u is a unit in R, and u, a_i and $\mathrm{NF}(f \mid G)$ are polynomials in the case when the input data f and $G = \{g_1, \ldots, g_s\}$ are polynomials. In the previous example we arrive at an expression

$$(1-x)x = x - x^2$$

instead of $x = (\sum_{i=0}^{\infty} x^i)(x - x^2)$.

Definition 1.7.5. For $f \in K[x] \setminus \{0\}$ we define the *ecart* of f as

$$\mathrm{ecart}(f) := \deg f - \deg \mathrm{LM}(f)\,.$$

Note that, for a homogeneous polynomial f, we have $\mathrm{ecart}(f) = 0$.

If $w = (w_1, \ldots, w_n)$ is any tuple of positive real numbers, we can define the *weighted ecart* by $\mathrm{ecart}_w(f) := \text{w–deg}(f) - \text{w–deg}\big(\mathrm{LM}(f)\big)$. In the following normal form algorithm NFMora, we may always take ecart_w instead of ecart, the algorithm works as well. It was noted in [94] that, for certain examples, the algorithm can become much faster for a good choice of w.

Another description of $\mathrm{ecart}(f)$ turns out to be quite useful. Let f^h denote the homogenization of f with respect to a new variable t (such that all monomials of f are of the same degree, cf. Exercise 1.7.4). Define on $\mathrm{Mon}(t, x_1, \ldots, x_n)$ an ordering $>_h$ by $t^p x^\alpha >_h t^q x^\beta$ if $p + |\alpha| > q + |\beta|$ or if $p + |\alpha| = q + |\beta|$ and $x^\alpha > x^\beta$. Equivalently, $>_h$ is given by the matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}$$

where A is a matrix defining the ordering on $K[x]$. This defines a well–ordering on $\mathrm{Mon}(t,x)$.

For $f \in K[x]$ we have

$$\mathrm{LM}_{>_h}(f^h) = t^{\mathrm{ecart}(f)}\,\mathrm{LM}_>(f)\,,$$

in particular, $\mathrm{ecart}(f) = \deg_t \mathrm{LM}_{>_h}(f^h)$.

Algorithm 1.7.6 (NFMora($f \mid G$)).
Let $>$ be any monomial ordering.

Input: $f \in K[x]$, G a finite list in $K[x]$
Output: $h \in K[x]$ a polynomial weak normal form of f with respect to G.

- $h := f$;
- $T := G$;
- while($h \neq 0$ and $T_h := \{g \in T \mid \mathrm{LM}(g) \mid \mathrm{LM}(h)\} \neq \emptyset$)
  choose $g \in T_h$ with $\mathrm{ecart}(g)$ minimal;
  if $(\mathrm{ecart}(g) > \mathrm{ecart}(h))$
  $T := T \cup \{h\}$;
  $h := \mathrm{spoly}(h, g)$;
- return h;

Example 1.7.7. Let $>$ be the ordering `ds` on $\mathrm{Mon}(x,y,z)$, $f = x^2+y^2+z^3+x^4+y^5$, $G = \{x, y\}$. Then NFMora $(f \mid G) = z^3+x^4+y^5$.

If the input is homogeneous, then the ecart is always 0 and NFMora is equal to NFBuchberger. If $>$ is a well–ordering, then $\mathrm{LM}(g) \mid \mathrm{LM}(h)$ implies that $\mathrm{LM}(g) \leq \mathrm{LM}(h)$, hence, even if h is added to T during the algorithm, it cannot be used in further reductions. Thus, NFMora is the same as NFBuchberger, but with a special selection strategy for the elements from G.

Proof of Algorithm 1.7.6. Termination is most easily seen by using homogenization: start with $h := f^h$ and $T := G^h = \{g^h \mid g \in G\}$. The while loop looks as follows (see Exercise 1.7.9):

- while ($h \neq 0$ and $T_h := \{g \in T \mid \mathrm{LM}(g)$ divides $t^\alpha\,\mathrm{LM}(h)$ for some $\alpha\} \neq \emptyset$)
  choose $g \in T_h$ with $\alpha \geq 0$ minimal;
  if $(\alpha > 0)$
  $T := T \cup \{h\}$;
  $h := \mathrm{spoly}(t^\alpha h, g)$;
  $h := (h|_{t=1})^h$;
- return $h|_{t=1}$;

Since R is Noetherian, there exists some positive integer N such that $L(T_\nu)$ becomes stable for $\nu \geq N$, where T_ν denotes the set T after the ν–th turn of the while loop. The next h, therefore, satisfies $\mathrm{LM}(h) \in L(T_N) = L(T)$, whence, $\mathrm{LM}(g)$ divides $\mathrm{LM}(h)$ for some $g \in T$ and $\alpha = 0$. That is, T_ν itself becomes stable for $\nu \geq N$ and the algorithm continues with fixed T. Then it terminates, since $>$ is a well–ordering on $K[t, x]$.

To see correctness, consider the ν–th turn in the while loop of Algorithm 1.7.6. There we create (with $h_0 := f$) $h_\nu := \mathrm{spoly}(h_{\nu-1}, g'_\nu)$ for some $g'_\nu \in T_{\nu-1}$ such that $\mathrm{LM}(g'_\nu) \mid \mathrm{LM}(h_{\nu-1})$. Hence, there exists some term $m_\nu \in K[x]$, $\mathrm{LT}(m_\nu g'_\nu) = \mathrm{LT}(h_{\nu-1})$, such that

$$h_\nu = h_{\nu-1} - m_\nu g'_\nu\,, \quad \mathrm{LM}(h_{\nu-1}) = \mathrm{LM}(m_\nu g'_\nu) > \mathrm{LM}(h_\nu)\,,$$

Now for g'_ν we have two possibilities:

(1) $g'_\nu = g_i \in G = \{g_1, \ldots, g_s\}$ for some i, or
(2) $g'_\nu \in T \setminus G \subset \{h_0, h_1, \ldots, h_{\nu-2}\}$.

Suppose, by induction, that in the first $\nu - 1$ steps ($\nu \geq 1$) we have constructed standard representations

$$u_j f = \sum_{i=1}^{s} a_i^{(j)} g_i + h_j, \quad u_j \in S_>, \quad a_i^{(j)} \in K[x]\,,$$

$0 \leq j \leq \nu - 1$, starting with $u_0 := 1$, $a_i^{(0)} := 0$.

Consider this standard representation for $j = \nu - 1$. In case (1), we replace $h_{\nu-1}$ on the right–hand side by $h_\nu + m_\nu g_i$, hence, obtaining

$$u_\nu f = \sum_{i=1}^{s} a_i^{(\nu)} g_i + h_\nu$$

with $u_\nu := u_{\nu-1}$ and some $a_i^{(\nu)} \in K[x]$.

In case (2), we have to substitute $h_{\nu-1}$ by

$$h_\nu + m_\nu h_j = h_\nu - m_\nu \left(\sum_{i=1}^{s} a_i^{(j)} g_i - u_j f \right)$$

with $j < \nu - 1$. Hence, we obtain an expression

$$(u_{\nu-1} - m_\nu u_j) f = \sum_{i=1}^{s} a_i^{(\nu)} g_i + h_\nu\,, \quad a_i^{(\nu)} \in K[x]\,.$$

Since $\mathrm{LM}(m_\nu) \cdot \mathrm{LM}(h_j) = \mathrm{LM}(m_\nu h_j) = \mathrm{LM}(h_{\nu-1}) < \mathrm{LM}(h_j)$, we obtain that $\mathrm{LM}(m_\nu) < 1$ and, hence, $u_\nu = u_{\nu-1} - m_\nu u_j \in S_>$. □

It is clear that, with a little extra storage, the algorithm does also return $u \in S_>$. Moreover, with quite a bit of bookkeeping one obtains the a_i.

Now, the standard basis algorithm for arbitrary monomial orderings formally looks as follows:

Algorithm 1.7.8 (StandardBasis(G)).
Let $>$ be any monomial ordering, $R = K[x]_>$.

Input: $G = \{g_1, \ldots, g_s\} \subset K[x]$
Output: $S = \{h_1, \ldots, h_t\} \subset K[x]$ such that S is a standard basis of the ideal $\langle G \rangle_R \subset R$.

- $S :=$ Standard(G,NFMora);
- return S;

The following corollary shows that the property of being a standard basis depends only on the ordering of finitely many monomials. This property is used in our study of flatness and standard bases (Section 7.5).

Corollary 1.7.9 (finite determinacy of standard bases). *Let $I \subset K[x]$ be an ideal and $G \subset K[x]$ be a standard basis of I with respect to an arbitrary monomial ordering $>$. Then there exists a finite set $F \subset \mathrm{Mon}(x)$ with the following properties:*

Let $>_1$ be any monomial ordering on $\mathrm{Mon}(x)$ coinciding with $>$ on F, then

(1) $\mathrm{LM}_>(g) = \mathrm{LM}_{>_1}(g)$ for all $g \in G$,
(2) G is a standard basis of I with respect to $>_1$.

Proof. We apply Theorem 1.7.3 with NF = NFMora.

Let $G = \{g_1, \ldots, g_s\}$, and let F be the set of all monomials occurring in all polynomials during the reduction process of $\mathrm{spoly}(g_i, g_j)$ to 0 in NFMora. Then $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) = 0$ also with respect to $>_1$, and the result follows, using Theorem 1.7.3 (4). □

SINGULAR Example 1.7.10 (standard bases).
The same generators for an ideal give different standard bases with respect to different orderings:

```
ring A  = 0,(x,y),dp;   //global ordering: degrevlex
ideal I = x10+x9y2,y8-x2y7;
ideal J = std(I);
J;
//-> J[1]=x2y7-y8   J[2]=x9y2+x10   J[3]=x12y+xy11
//-> J[4]=x13-xy12  J[5]=y14+xy12   J[6]=xy13+y12

ring A1 = 0,(x,y),lp;   //global ordering: lex
ideal I = fetch(A,I);
```

```
ideal J = std(I);
J;
//-> J[1]=y15-y12 J[2]=xy12+y14 J[3]=x2y7-y8 J[4]=x10+x9y2

ring B  = 0,(x,y),ds;   //local ordering: local degrevlex
ideal I = fetch(A,I);
ideal J = std(I);
J;
//-> J[1]=y8-x2y7   J[2]=x10+x9y2

ring B1 = 0,(x,y),ls;   //local ordering: negative lex
ideal I = fetch(A,I);
ideal J = std(I);
J;
//-> J[1]=y8-x2y7    J[2]=x9y2+x10    J[3]=x13

intmat O[3][3]=1,1,1,0,-1,-1,0,0,-1;
ring  C = 0,(t,x,y),M(O);     //global ordering: matrix O
ideal I = homog(imap(A,I),t); //gives a standard basis for
                              //local degrevlex
ideal J = std(I);             //cf. Exercise 1.7.5
      J = subst(J,t,1);
J;
//-> J[1]=-x2y7+y8    J[2]=x9y2+x10    J[3]=x12y7+x9y10
                              //already J[1],J[2] is a
                              //standard basis
```

We finish this section with the so–called highest corner, a notion which is computationally extremely useful for 0–dimensional ideals in local rings. Moreover, the highest corner is tightly connected with the determinacy of an isolated hypersurface singularity (cf. A.9).

Definition 1.7.11. Let $>$ be a monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$ and let $I \subset K[x_1,\ldots,x_n]_>$ be an ideal. A monomial $m \in \mathrm{Mon}(x_1,\ldots,x_n)$ is called the *highest corner* of I (with respect to $>$), denoted by $\mathrm{HC}(I)$, if

(1) $m \notin L(I)$;
(2) $m' \in \mathrm{Mon}(x_1,\ldots,x_n)$, $m' < m \implies m' \in L(I)$.

Note that for a global ordering the highest corner is 1 if I is a proper ideal (and does not exist if $1 \in I$). Since, by definition $\mathrm{HC}(I) = \mathrm{HC}\big(L(I)\big)$, it can be computed combinatorially from a standard basis of I.

SINGULAR has a built–in function `highcorner` which returns, for a given set of generators $f_1,\ldots,f_k$ of I, the highest corner of the ideal $\langle \mathrm{LM}(f_1),\ldots,\mathrm{LM}(f_k)\rangle$, respectively 0, if the highest corner does not exist.

SINGULAR Example 1.7.12 (highest corner).

```
ring A = 0,(x,y),ds;
ideal I = y4+x5,x3y3;
highcorner(I);
//-> // ** I is not a standard basis
//-> 0                //no highest corner for <y4,x3y3>

std(I);
//-> _[1]=y4+x5   _[2]=x3y3   _[3]=x8
highcorner(std(I));
//-> x7y2
```

The highest corner of I is x^7y^2, as can be seen from Figure 1.2.

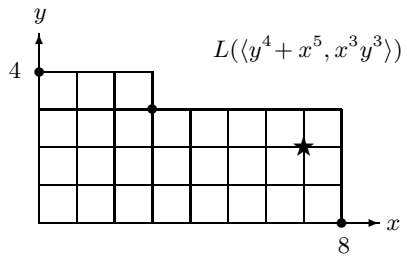


Fig. 1.2. $L(\langle y^4+x^5, x^3y^3\rangle)$ is generated by the monomials y^4, x^3y^3, x^8 (marked by a •). The highest corner is x^7y^2 (marked by a ★).

Lemma 1.7.13. *Let $>$ be a monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$ and $I \subset K[x_1,\ldots,x_n]_>$ be an ideal. Let m be a monomial such that $m' < m$ implies $m' \in L(I)$. Let $f \in K[x_1,\ldots,x_n]$ such that $\mathrm{LM}(f) < m$. Then $f \in I$.*

Proof. Let $r =$ NFMora $(f \mid G)$, G a standard basis for I. If $r \neq 0$, then $\mathrm{LM}(r) < \mathrm{LM}(f) < m$ and, therefore, $\mathrm{LM}(r) \in I$ which is a contradiction to the properties of the normal form. □

Lemma 1.7.14. *Let $>$ be a monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$ and denote by $z_1,\ldots,z_r$ the variables < 1 from $\{x_1,\ldots,x_n\}$ and by $y_1,\ldots,y_s$ the variables > 1 $(0 \leq r,s, r+s=n)$. Assume that the restriction of $>$ to $\mathrm{Mon}(z_1,\ldots,z_r)$ is a weighted degree ordering. The following are equivalent for an ideal $I \subset K[x_1,\ldots,x_n]_>$:*

(1) $\mathrm{HC}(I)$ *exists,*
(2) $\langle z_1,\ldots,z_r\rangle^N \subset L(I)$ *for some* $N \geq 0$,
(3) $\langle z_1,\ldots,z_r\rangle^M \subset I$ *for some* $M \geq 0$.

Moreover, $\mathrm{HC}(I) \in \mathrm{Mon}(z_1,\ldots,z_r)$ *if it exists.*

Proof. To see that (1) implies (2), let $m := \mathrm{HC}(I)$. If $m = 1$, then $1 \notin I$ and $z_1, \ldots, z_r \in L(I)$ by definition of the highest corner. If $m \neq 1$ and if we write $m = x_i m'$ for some monomial m' then $x_i < 1$ (otherwise, $m' < m$, which would imply $m' \in L(I)$, hence, $m \in L(I)$, a contradiction), and it follows that $m \in \mathrm{Mon}(z_1, \ldots, z_r)$. Since $>$ is a weighted degree ordering on $\mathrm{Mon}(z_1, \ldots, z_r)$, the definition of the highest corner implies (2).

Conversely, if $\langle z_1, \ldots, z_r \rangle^N \subset L(I)$ then there are only finitely many monomials in $\mathrm{Mon}(z_1, \ldots, z_r)$ which are not in $L(I)$. This finite set has a minimum m. If $m' = z^\alpha y^\beta < m$ then $z^\alpha < m$ which implies $z^\alpha \in L(I)$ and, hence, $m' \in L(I)$.

The implication (3) $\Rightarrow$ (2) being trivial, it remains only to show that (2) implies (3). Let $M \geq N$. Since $z_i^M \in L(I)$, we have $z_i^M + h_i \in I$ for some h_i with $\mathrm{LM}(h_i) = z^\alpha y^\beta < z_i^M$, in particular, $z^\alpha < z_i^M$. Let $m := \mathrm{HC}(I)$, which exists by the equivalence of (2) and (1) proven before, and enlarge M, if necessary, such that $z_i^M \leq m$. Then $z^\alpha < m$ implies $z^\alpha \in L(I)$ and, hence, $\mathrm{LM}(h_i) \in L(I)$. Now we apply Lemma 1.7.13 and obtain $h_i \in I$. Therefore, $z_i^M \in I$ for $i = 1, \ldots, r$, and (3) follows. □

Remark 1.7.15. As a direct consequence, for a local weighted degree ordering, we have

$$\begin{aligned} \mathrm{HC}(I) \text{ exists } &\iff \dim_K(K[x_1, \ldots, x_n]_>/I) < \infty \\ &\iff \dim_K\big(K[x_1, \ldots, x_n]/L(I)\big) < \infty\,. \end{aligned}$$

Indeed, we show in Section 7.5 that, for any monomial ordering,

$$\dim_K(K[x_1, \ldots, x_n]_>/I) = \dim_K\big(K[x_1, \ldots, x_n]/L(I)\big)\,.$$

(see also Corollary 5.3.14).

Remark 1.7.16. The implications (2) $\Leftrightarrow$ (3) $\Rightarrow$ (1) in Lemma 1.7.14 hold without any assumption on the ordering $>$. This is a consequence of Lemma 1.2.11.

The implication (1) $\Rightarrow$ (2) is wrong in general: let $>$ be the negative lexicographical ordering `ls` and $I = \langle xy, x^2 \rangle$, then $\mathrm{HC}(I) = x$.

Lemma 1.7.17. *Let $>$ be a weighted degree ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$. Moreover, let $f_1, \ldots, f_k$ be a set of generators of the ideal $I \subset K[x_1, \ldots, x_n]_>$ such that $J := \langle \mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_k) \rangle$ has a highest corner $m := \mathrm{HC}(J)$, and let $f \in K[x_1, \ldots, x_n]_>$. Then the following holds:*

(1) $\mathrm{HC}(I)$ *exists, and, moreover,* $\mathrm{HC}(I) \geq \mathrm{HC}(J)$ *and* $\mathrm{HC}(I) = \mathrm{HC}(J)$ *if $f_1, \ldots, f_k$ is a standard basis of I.*
(2) If $\mathrm{LM}(f) < \mathrm{HC}(J)$ *then $f \in I$.*
(3) For a fixed monomial $m' < \mathrm{HC}(J)$ *set* $M = \{i \mid \mathrm{LM}(f_i) \leq m'\}$ *and define*

$$\hat{f}_i := \begin{cases} f_i, & \text{if } i \in M \\ f_i + a_i \cdot m', & \text{if } i \notin M \end{cases}$$

where $a_i \in K$ is arbitrary. Then $I = \langle \hat{f}_1, \ldots, \hat{f}_k \rangle$.

Proof. (1) Since $J \subset L(I)$ and $J = L(I)$ if $f_1, \ldots, f_k$ is a standard basis, the claim follows from Lemma 1.7.14.

(2) $\mathrm{LM}(f) < m$ implies $\mathrm{LM}(f) \in L(J) \subset L(I)$. The assertion is a consequence of Lemma 1.7.13.

(3) Since $m' < m$, $m' \in I$ by (2) and, therefore, $I = \langle \hat{f}_1, \ldots, \hat{f}_k, m' \rangle$. We have to show $m' \in \widehat{I} = \langle \hat{f}_1, \ldots, \hat{f}_k \rangle$. Since $\mathrm{LM}(f_i) = \mathrm{LM}(\hat{f}_i)$ for all i, we can apply (2) to $\widehat{I}$ instead of I with the same J and m and, therefore, $m' \in \widehat{I}$. □

The lemma shows that we can delete from f_i all terms $a \cdot m'$, $a \in K$, with $m' < \min\{m, \mathrm{LM}(f_i)\}$, still keeping a set of generators of I. This is used in SINGULAR during standard basis computations in local orderings to keep the polynomials sparse and to have *early termination* if, in the reduction process, the leading monomial becomes smaller than the highest corner.

Exercises

1.7.1. Prove the *Product Criterion*: let $f, g \in K[x_1, \ldots, x_n]$ be polynomials such that $\mathrm{lcm}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big) = \mathrm{LM}(f) \cdot \mathrm{LM}(g)$, then

$$\mathrm{NF}\big(\mathrm{spoly}(f,g) \mid \{f,g\}\big) = 0\,.$$

(Hint: It is sufficient to prove the statement for NF = NFMora. Assume that $\mathrm{LC}(f) = \mathrm{LC}(g) = 1$ and claim that $\mathrm{spoly}(f,g) = -\mathrm{tail}(g)f + \mathrm{tail}(f)g$. Moreover, assume that, after some steps in NFMora, $u \cdot \mathrm{spoly}(f,g)$ (u a unit) is reduced to $hf + kg$. If $\mathrm{LT}(hf) + \mathrm{LT}(kg) = 0$ then $\mathrm{LT}(h) = m \cdot \mathrm{LM}(g)$ and $\mathrm{LT}(k) = -m\,\mathrm{LM}(f)$ for a suitable term m, and $(u - m)\,\mathrm{spoly}(f,g)$ is reduced to $\mathrm{tail}(h)f + \mathrm{tail}(k)g$. If $\mathrm{LT}(hf) + \mathrm{LT}(kg) \neq 0$ then assume $\mathrm{LM}(hf + kg) = \mathrm{LM}(hf)$, and $hf + kg$ reduces to $\mathrm{tail}(h)f + kg$.)

1.7.2. Let $I := \langle x^3y^2 + x^4, x^2y^3 + y^4 \rangle \subset K[x,y]$ (resp. $I := \langle x^3 + y^2, y^4 + x \rangle$). Compute (without using SINGULAR) a standard basis of I with respect to the degree lexicographical ordering (respectively lexicographical ordering).

1.7.3. Which of the following orderings are elimination orderings: `lp`, `ls`, `(lp(n),ls(m))`, `(ls(n),lp(m))`, `(a(1,...,1,0,...0),dp)`?

Compute a standard basis of the ideal $\langle x - t^2, y - t^3, z - t^4 \rangle$ for all those orderings.

1.7.4. For an arbitrary polynomial $g \in K[x_1, \ldots, x_n]$ of degree d, let

$$g^h(x_0, x_1, \ldots, x_n) := x_0^d g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in K[x_0, \ldots, x_n]$$

be the *homogenization* of g (with respect to x_0). For an ideal $I \subset K[x_1, \ldots, x_n]$ let $I^h := \langle f^h \mid f \in I \rangle \subset K[x_0, \ldots, x_n]$.

Let $>$ be a global degree ordering, and let $\{f_1, \ldots, f_m\}$ be a Gröbner basis of I. Prove that

$$I^h = \langle f_1^h, \ldots, f_m^h \rangle .$$

1.7.5. For $w = (w_1, \ldots, w_n) \in \mathbb{Z}^n$, $w_i \neq 0$ for $i = 1, \ldots, n$, and a polynomial $g \in K[x_1, \ldots, x_n]$ with w–deg$(g) = d$, let

$$g^h(x_0, x_1, \ldots, x_n) := x_0^d g\left(\frac{x_1}{x_0^{w_1}}, \ldots, \frac{x_n}{x_0^{w_n}}\right) \in K[x_0, \ldots, x_n]$$

be the *(weighted) homogenization* of g (with respect to x_0). For an ideal $I \subset K[x_1, \ldots, x_n]$ let $I^h := \langle f^h \mid f \in I \rangle \subset K[x_0, \ldots, x_n]$.

Let $>$ be a weighted degree ordering with weight vector w, and let $\{f_1, \ldots, f_m\}$ be a Gröbner basis of I. Prove that

$$I^h K[x,t]_{>_h} = \langle f_1^h, \ldots, f_m^h \rangle K[x,t]_{>_h} ,$$

where $>_h$ denotes the monomial ordering on Mon$(x_0, \ldots, x_n)$ defined by the matrix

$$\begin{pmatrix} 1 & w_1 & \ldots & w_m \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}$$

with $A \in \mathrm{GL}(n, \mathbb{R})$ a matrix defining $>$ on Mon$(x_1, \ldots, x_n)$.

1.7.6. Let $A \in \mathrm{GL}(n, \mathbb{Q})$ be a matrix defining, on Mon$(x_1, \ldots, x_n)$, the ordering $>$ and let $I = \langle f_1, \ldots, f_m \rangle \subset K[x_1, \ldots, x_n]$ be an ideal. Consider the ordering $>_h$ on Mon$(t, x_1, \ldots, x_n)$ defined by the matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}$$

(cf. the remark after Definition 1.7.5) and let $\{G_1, \ldots, G_s\}$ be a homogeneous standard basis of $\langle f_1^h, \ldots, f_m^h \rangle$, f_i^h, the homogenization of f_i with respect to t. Prove that $\{G_1|_{t=1}, \ldots, G_s|_{t=1}\}$ is a standard basis for I.

1.7.7. Let $I = \langle f_1, \ldots, f_m \rangle \subset K[x_1, \ldots, x_n]$ be an ideal, and consider on Mon$(t, x_1, \ldots, x_n)$ the ordering `dp` (respectively `Dp`). Let $\{G_1, \ldots, G_s\}$ be a standard basis of $\langle f_1^h, \ldots, f_m^h \rangle$, f_i^h, the homogenization of f_i with respect to t. Prove that $\{G_1|_{t=1}, \ldots, G_s|_{t=1}\}$ is a standard basis for I with respect to the ordering `ls` on Mon$(x_n, x_{n-1}, \ldots, x_1)$ (respectively `Ds` on Mon$(x_1, \ldots, x_n)$).

1.7.8. Let $I = \langle f_1, \ldots, f_m \rangle \subset K[x_1, \ldots, x_n]$ be an ideal, and consider on Mon$(x_1, \ldots, x_n, t)$ the ordering `dp`. Let $\{G_1, \ldots, G_s\}$ be a standard basis of $\langle f_1^h, \ldots, f_m^h \rangle$, f_i^h the homogenization of f_i with respect to t. Prove that $\{G_1|_{t=1}, \ldots, G_s|_{t=1}\}$ is a standard basis for I with respect to the ordering `dp` on Mon$(x_1, \ldots, x_n)$.

1.7.9. Prove that the while loops in Algorithm 1.7.6 and at the beginning of its proof give the same result.

1.7.10. Check (by hand) whether the following polynomials f are contained in the respective ideals I:

(1) $f = xy^3 - z^2 + y^5 - z^3,\ I = \langle -x^3 + y, x^2y - z\rangle$ in $\mathbb{Q}[x,y,z]$,
(2) $f = x^3z - 2y^2,\ I = \langle yz - y, xy + 2z^2, y - z\rangle$ in $\mathbb{Q}[x,y,z]$,
(3) f and I as in (2) but in $\mathbb{Q}[x,y,z]_{\langle x,y,z\rangle}$.

1.7.11. Verify your computation in 1.7.10 by using SINGULAR.

1.7.12. Compute a standard basis of

(1) $\langle x^3, x^2y - y^3\rangle$ with respect to `ls` and `lp`.
(2) $\langle x^3 + xy, x^2y - y^3\rangle$ with respect to `ds` and `dp`.

1.7.13. Determine all solutions in $\mathbb{C}^2$ of the system of polynomial equations

$$xy - x - 2y + 2 = 0\,, \quad x^2 + xy - 2x = 0\,.$$

(Hint: compute first a lexicographical Gröbner basis of the two polynomials.)

1.7.14. Use SINGULAR to determine all points in $\mathbb{C}^3$ lying on the variety V given by:

(1) $V = V(xz - y, xy + 2z^2, y - z)$,
(2) $V = V(x^2 + y^2 + z^2 - 1, y^2 - z, x^2 + y^2)$.

1.7.15. Consider $f(x,y) := x^2 - y^3 - \frac{3}{2}y^2$.

(1) Compute all critical points of f (that is, points where $\partial f/\partial x$ and $\partial f/\partial y$ vanish).
(2) Which of the critical points are local minima, maxima, saddle points?
(3) Do the same for $g(x,y) = f(x,y)\cdot(y-1)$.

1.7.16. Let K be a field, let $\mathfrak{m} \subset K[x_1,\ldots,x_n]$ be a maximal ideal, and let $L := K[x_1,\ldots,x_n]/\mathfrak{m}$. Moreover, let $I = \langle f_1,\ldots,f_m\rangle \subset L[y_1,\ldots,y_s]$ be an ideal, and let $J := \langle F_1,\ldots,F_m\rangle \subset K[x_1,\ldots,x_n,y_1,\ldots,y_s]$ be generated by representatives F_i of the f_i, $i = 1,\ldots,m$.

Finally, let $\{H_1,\ldots,H_t\}$ be a standard basis of J with respect to a block ordering $>= (>_1, >_2)$ on $\mathrm{Mon}(y_1,\ldots,y_s,x_1,\ldots,x_n)$ with $>_1, >_2$ global.

(1) Prove that $\{H_1 \bmod \mathfrak{m},\ldots,H_t \bmod \mathfrak{m}\}$ is a standard basis of I with respect to $>_1$.
(2) Write a SINGULAR procedure to compute a minimal standard basis in $L[y_1,\ldots,y_s]$ (where K is one of the base fields of SINGULAR) such that the leading coefficients are 1.

1.7.17. Let $I \subset K[x_1,\ldots,x_n]$ be an ideal and $>$ a monomial ordering. Then there exists a weight vector $w = (w_1,\ldots,w_n) \in \mathbb{Z}^n$, with $w_i > 0$ if $x_i > 1$ and $w_i < 0$ if $x_i < 1$, such that the weighted degree lexicographical ordering defined by w and the given ordering $>$ yield the same leading ideal $L(I)$.

(Hint: use Lemma 1.2.11.)

1.7.18. (1) Let $I \subset K[x_1,\dots,x_n]_>$ be an ideal, and let $>$ denote the negative lexicographical ordering `ls`. Moreover, let x^α, $\alpha = (\alpha_1,\dots,\alpha_n)$ denote the highest corner of I. Show that, for $i = 1,\dots,n$,

$$\alpha_i = \max\{p \mid x_1^{\alpha_1} \cdot \ldots \cdot x_{i-1}^{\alpha_{i-1}} x_i^p \notin L(I)\}\,.$$

(2) Compute the highest corner of $I = \langle x^2+x^2y, y^3+xy^3, z^3-xz^2\rangle$ with respect to the orderings `ls` and `ds`.
(This can be done by hand; you may check your results by using the SINGULAR function `highcorner`.)

1.7.19. Let K be a field, x one variable and $>$ the well–ordering on $K[x]$.

(1) Prove that the standard basis algorithm is the Euclidean algorithm.
(2) Use SINGULAR to compute for $f = (x^3+5)^2(x-2)(x^2+x+2)^4$ and $g = (x^3+5)(x^2-3)(x^2+x+2)$ the $\gcd(f,g)$. Try `std(ideal(f,g))` and `gcd(f,g)`.

1.7.20. Let K be a field, $x = (x_1,\dots,x_n)$ and $>$ the lexicographical ordering on $K[x]$.

(1) Prove that the standard basis algorithm is the Gaussian elimination algorithm if it is applied to linear polynomials.
(2) Use SINGULAR to solve the following linear system of equations:

$$\begin{aligned} 22x + 77y + z &= 3 \\ x + y + z &= 77 \\ x - y - z &= -11\,. \end{aligned}$$

With `option(redSB)` the complete reduction of the standard basis can be forced. Try both possibilities.

1.7.21. Prove that the equivalence of (2) and (3) in Lemma 1.7.14 holds for any monomial ordering.

1.7.22. Let $>$ be an arbitrary monomial ordering on $\mathrm{Mon}(x_1,\dots,x_n)$, and let $I \subset K[x]$ be an ideal. Let $G \subset K[x]$ be a standard basis of I with respect to $>$. Assume, moreover that $\dim_K(K[x]/L(I)) < \infty$. Prove that there exists a standard basis $G' \supset G$ such that REDNFBUCHBERGER$(- \mid G')$ terminates.
(Hint: Denote by $z = (z_1,\dots,z_r)$ the variables < 1. Use Exercise 1.7.21 to choose M such that $\langle z\rangle^M \subset I$. Enlarge G by adding all monomials in z of degree M.)

1.7.23. Let $>$ be an arbitrary monomial ordering on $\mathrm{Mon}(x_1,\dots,x_n)$, and let $I \subset K[x]_>$ be an ideal. Denote by $z = (z_1,\dots,z_r)$ the variables < 1, and assume that $\langle z\rangle^m \subset I$ for some positive integer m. Prove that the canonical injection $K[x]/(I \cap K[x]) \hookrightarrow K[x]_>/I$ is an isomorphism.

1.7.24. Use Remark 1.6.14 and Exercise 1.6.9 for writing a SINGULAR procedure which computes standard bases over a polynomial ring $K[t_1,\dots,t_s]$, K a field.

1.8 Operations on Ideals and Their Computation

The methods developed so far already allow some interesting applications to basic ideal operations.

In general, we assume we have given a finite set of ideals, each is given by a finite set of polynomial generators. We want to either affirmatively answer a specific question about the ideals or to compute a specific operation on these ideals, that is, compute a finite set of generators for the result of the operation.

1.8.1 Ideal Membership

Let $K[x] = K[x_1, \ldots, x_n]$ be the polynomial ring over a field K, $>_0$ an arbitrary monomial ordering and $R = K[x]_{>_0}$ the ring associated to $K[x]$ and $>_0$. Recall that $K[x] \subset R \subset K[x]_{\langle x \rangle}$, and that $R = K[x]_{\langle x \rangle}$ if and only if $>_0$ is local (cf. Section 1.5).

Let NF denote a weak normal form and redNF a reduced normal form (cf. Section 1.6). We do not need any further assumptions about NF, respectively redNF, however, we may think of NFBuchberger (1.6.10), respectively redNFBuchberger (1.6.11), if $>_0$ is global, and NFMora (1.7.6) in the general case. These are also the normal forms implemented in Singular.

Problem: Given $f, f_1, \ldots, f_k \in K[x]$, and let $I = \langle f_1, \ldots, f_k \rangle_R$. We wish to decide whether $f \in I$, or not.

Solution: We choose any monomial ordering $>$ such that $K[x]_> = R$ and compute a standard basis $G = \{g_1, \ldots, g_s\}$ of I with respect to $>$. If NF is any weak normal form, then $f \in I$ if and only if $\mathrm{NF}(f \mid G) = 0$. Correctness follows from Lemma 1.6.7. □

Since the result is independent of the chosen NF, we should use, for reasons of efficiency, a non–reduced normal form. If $>_0$ is global, we usually choose `dp` and, if $>_0$ is local, then `ls` or `ds` are preferred.

SINGULAR Example 1.8.1 (ideal membership).
(1) Check inclusion of a polynomial in an ideal

```
ring A  = 0,(x,y),dp;
ideal I = x10+x9y2,y8-x2y7;
ideal J = std(I);
poly f  = x2y7+y14;
reduce(f,J,1);      //3rd parameter 1 avoids tail reduction
//-> -xy12+x2y7      //f is not in I
     f  = xy13+y12;
reduce(f,J,1);
//-> 0              //f is in I
```

(2) Check inclusion and equality of ideals.

```
ideal K = f,x2y7+y14;
reduce(K,J,1);      //normal form for each generator of K

//-> _[1]=0  _[2]=-xy12+x2y7   //K is not in I

K=f,y14+xy12;
size(reduce(K,J,1));          //result is 0 iff K is in I

//-> 0
```

Now assume that $f \in I = \langle f_1, \ldots, f_k \rangle_R$. Then there exist $u \in K[x] \cap R^*$, $a_1, \ldots, a_k \in K[x]$ such that

$$uf = a_1 f_1 + \cdots + a_k f_k. \qquad (*)$$

If $\{f_1, \ldots, f_k\}$ is a standard basis of I, then, in principle, the normal form algorithm NFMora provides u and the a_i. However, it is also possible to express f as a linear combination of arbitrary given generators $f_1, \ldots, f_k$, by using the `lift` or `division` command. How this can be done is explained in Chapter 2, Section 2.8.1.

If the ordering is global, then we can choose $u = 1$ in the above expression (*). This is illustrated in the following example.

SINGULAR Example 1.8.2 (linear combination of ideal members). We exemplify the Singular commands `lift` and `division`:

```
ring A  = 0,(x,y),dp;
ideal I = x10+x9y2,y8-x2y7;
poly f  = xy13+y12;
matrix M=lift(I,f);        //f=M[1,1]*I[1]+...+M[r,1]*I[r]
M;
//-> M[1,1]=y7
//-> M[2,1]=x7y2+x8+x5y3+x6y+x3y4+x4y2+xy5+x2y3+y4
```

Hence, f can be expressed as a linear combination of $I[1]$ and $I[2]$ using M:

```
f-M[1,1]*I[1]-M[2,1]*I[2]; //test
//-> 0
```

In a local ring we can, in general, only express uf as a polynomial linear combination of the generators of I if $f \in I$:

```
ring R = 0,(x,y,z),ds;
poly f = yx2+yx;
ideal I = x-x2,y+x;
```

```
list L = division(f,I);            //division with remainder
L;
//-> [1]:                 [2]:                [3]:
//->    _[1,1]=y-y2          _[1]=0              _[1,1]=1+y
//->    _[2,1]=2xy

matrix(f)*L[3] - matrix(I)*L[1] - matrix(L[2]);   //test
//-> _[1,1]=0
```

Hence $(1+y)f = (x-x^2)(y-y^2) + (y+x)(2xy)$, the remainder being 0.

1.8.2 Intersection with Subrings (Elimination of variables)

This is one of the most important applications of Gröbner bases. The problem may be formulated as follows (we restrict ourselves for the moment to the case of the polynomial ring):

Problem: Given $f_1, \ldots, f_k \in K[x] = K[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_k \rangle_{K[x]}$, we should like to find generators of the ideal

$$I' = I \cap K[x_{s+1}, \ldots, x_n], \quad s < n\,.$$

Elements of the ideal I' are said to be obtained from $f_1, \ldots, f_k$ *by eliminating* $x_1, \ldots, x_s$.

In order to treat this problem, we need a global elimination ordering for $x_1, \ldots, x_s$. We can use the lexicographical ordering `lp` which is an elimination ordering (Definition 1.5.4) for each s, but `lp` is, in almost all cases, the most expensive choice. A good choice is, usually, `(dp(s),dp(n-s))`, the product ordering of two degrevlex orderings. But there is another way to construct an elimination ordering which is often quite fast.

Let $>$ be an arbitrary ordering and let $a_1, \ldots, a_s$ be positive integers. Define $>_a$ by

$$\begin{aligned} x^\alpha >_a x^\beta :\Longleftrightarrow\ & a_1\alpha_1 + \cdots + a_s\alpha_s > a_1\beta_1 + \cdots + a_s\beta_s \\ & \text{or } \ a_1\alpha_1 + \cdots + a_s\alpha_s = a_1\beta_1 + \cdots + a_s\beta_s \ \text{ and } \ x^\alpha > x^\beta\,. \end{aligned}$$

Then $>_a$ is an elimination ordering and $a = (a_1, \ldots, a_s)$ is called an *extra weight vector*.

If $>$ is an arbitrary elimination ordering for $x_1, \ldots, x_s$, then

$$K[x_1, \ldots, x_n]_> = (K[x_{s+1}, \ldots, x_n]_{>'})[x_1, \ldots, x_s]\,,$$

since the units in $K[x]_>$ do not involve $x_1, \ldots, x_s$ (we denote, by $>'$, the ordering on $\mathrm{Mon}(x_{s+1}, \ldots, x_n)$ induced by $>$). Hence, $f \in K[x_{s+1}, \ldots, x_n]_{>'}$ for any $f \in K[x_1, \ldots, x_n]_>$ such that $\mathrm{LM}(f) \in K[x_{s+1}, \ldots, x_n]$.

The following lemma is the basis for solving the elimination problem.

Lemma 1.8.3. *Let $>$ be an elimination ordering for $x_1, \ldots, x_s$ on the set of monomials* $\mathrm{Mon}(x_1, \ldots, x_n)$*, and let $I \subset K[x_1, \ldots, x_n]_>$ be an ideal. If $S = \{g_1, \ldots, g_k\}$ is a standard basis of I, then*

$$S' := \{g \in S \mid \mathrm{LM}(g) \in K[x_{s+1}, \ldots, x_n]\}$$

is a standard basis of $I' := I \cap K[x_{s+1}, \ldots, x_n]_{>'}$. In particular, S' generates the ideal I'.

Proof. Given $f \in I' \subset I$ there exists $g_i \in S$ such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f)$, since S is a standard basis of I. Since $f \in K[x_{s+1}, \ldots, x_n]_>$, we have $\mathrm{LM}(f) \in K[x_{s+1}, \ldots, x_n]$ and, hence, $g_i \in S'$ by the above remark. Finally, since $S' \subset I'$, S' is a standard basis of I'. □

The general elimination problem can be posed, for any ring associated to a monomial ordering, as follows. Recall that the ordering on the variable to be eliminated must be global.

Problem: Given polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, let $I := \langle f_1, \ldots, f_k \rangle_R$ with $R := (K[x_{s+1}, \ldots, x_n]_>)[x_1, \ldots, x_s]$ for some monomial ordering $>$ on $\mathrm{Mon}(x_{s+1}, \ldots, x_n)$. Find generators for the ideal $I' := I \cap K[x_{s+1}, \ldots, x_n]_>$.

Solution: Choose an elimination ordering for $x_1, \ldots, x_s$ on $\mathrm{Mon}(x_1, \ldots, x_n)$, which induces the given ordering $>$ on $\mathrm{Mon}(x_{s+1}, \ldots, x_n)$, and compute a standard basis $S = \{g_1, \ldots, g_k\}$ of I. By Lemma 1.8.3, those g_i, for which $\mathrm{LM}(g_i)$ does not involve $x_1, \ldots, x_s$, generate I' (even more, they are a standard basis of I').

A good choice of an ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$ may be `(dp(s),>)`, but instead of $>$ we may choose any ordering $>'$ on $\mathrm{Mon}(x_{s+1}, \ldots, x_n)$ such that $K[x_{s+1}, \ldots, x_n]_{>'} = K[x_{s+1}, \ldots, x_n]_>$. For any global ordering $>$ on $\mathrm{Mon}(x_{s+1}, \ldots, x_n)$, we have, thus, a solution to the elimination problem in the polynomial ring, as stated at the beginning of this section. □

SINGULAR Example 1.8.4 (elimination of variables).

```
ring A =0,(t,x,y,z),dp;
ideal I=t2+x2+y2+z2,t2+2x2-xy-z2,t+y3-z3;

eliminate(I,t);
//-> _[1]=x2-xy-y2-2z2       _[2]=y6-2y3z3+z6+2x2-xy-z2
```

Alternatively choose a product ordering:

```
ring A1=0,(t,x,y,z),(dp(1),dp(3));
ideal I=imap(A,I);
ideal J=std(I);
J;
//-> J[1]=x2-xy-y2-2z2    J[2]=y6-2y3z3+z6+2x2-xy-z2
//-> J[3]=t+y3-z3
```

We can also choose the *extra weight vector* $a = (1, 0, 0, 0)$ to obtain an elimination ordering:

```
ring A2=0,(t,x,y,z),(a(1),dp);
ideal I=imap(A,I);
ideal J=std(I);
J;
//-> J[1]=x2-xy-y2-2z2    J[2]=y6-2y3z3+z6+2x2-xy-z2
//-> J[3]=t+y3-z3
```

By Lemma 1.8.3, the elements of `J` which do not involve t (here `J[1]` and `J[2]`), are a standard basis of $I \cap K[x, y, z]$.

1.8.3 Zariski Closure of the Image

Here we study the geometric counterpart of elimination. The reader who is not familiar with the geometrical background should read Section A.1 first. In this section we assume K to be algebraically closed.

Suppose $\varphi : K[x] = K[x_1, \ldots, x_n] \to K[t] = K[t_1, \ldots, t_m]$ is a ring map given by $f_1, \ldots, f_n \in K[t]$ such that $\varphi(x_i) = f_i$. Let $I = \langle g_1, \ldots, g_k \rangle \subset K[t]$ and $J = \langle h_1, \ldots, h_l \rangle \subset K[x]$ be ideals such that $\varphi(J) \subset I$. Then φ induces a ring map $\bar{\varphi} : K[x]/J \to K[t]/I$ and, hence, we obtain a commutative diagram of morphism of affine schemes (cf. Section A.1)

$$\begin{array}{ccc} X := V(I) & \xrightarrow{f=\bar{\varphi}^{\#}} & V(J) =: Y \\ \downarrow & & \downarrow \\ \mathbb{A}^m & \xrightarrow{\varphi^{\#}} & \mathbb{A}^n . \end{array}$$

We cannot compute the image $f(X)$, since it is, in general, not closed. However, we can compute the (Zariski) closure $\overline{f(X)}$.

Problem: The problem is to find polynomials $p_1, \ldots, p_r \in K[x]$ such that

$$\overline{f(X)} = V(p_1, \ldots, p_r) \subset \mathbb{A}^n .$$

Solution: Define the ideal

$$N = \langle g_1(t), \ldots, g_k(t), x_1 - f_1(t), \ldots, x_n - f_n(t) \rangle_{K[t,x]}$$

and eliminate $t_1, \ldots, t_m$ from N, that is, compute generators $p_1, \ldots, p_r \in K[x]$ of $N \cap K[x]$. Then $V(p_1, \ldots, p_r) = \overline{f(X)}$.

Hence, we can proceed as in Section 1.8.2. We choose a global ordering which is an elimination ordering for $t_1, \ldots, t_m$ on $\mathrm{Mon}(t_1, \ldots, t_m, x_1, \ldots, x_n)$, compute a Gröbner basis G of N and select those elements $p_1, \ldots, p_r$ from G which do not depend on t. Correctness follows from Lemma A.3.10. □

Since K is algebraically closed (with $f = (f_1, \ldots, f_n) : K^m \to K^n$), Lemma A.2.18 implies

$$\overline{f(X)} = \overline{\{x \in K^n \mid \exists\, t \in K^m \text{ such that } f(t) = x\}}\,.$$

The following example shows that the question whether $f(X)$ is closed or not may depend on the field.

Example 1.8.5. Consider the ring map $\varphi : K[x] \to K[x,y]/\langle x^2+y^2-1\rangle$ given by $\varphi(x) := x$, and the induced morphism

$$\begin{array}{ccc} X := V(\langle x^2+y^2-1\rangle) & \xrightarrow{f=\bar{\varphi}^{\#}} & V(\langle 0\rangle) \\ \big\downarrow & & \big\| \\ \mathbb{A}^2 & \xrightarrow{\varphi^{\#}} & \mathbb{A}^1\,. \end{array}$$

It is easy to see that, if K is algebraically closed, then f is surjective, and hence, $f(X)$ is closed. However, if $K = \mathbb{R}$, then $f(X)$ is a segment but the Zariski closure of the segment is the whole line.

Now we treat the problem of computing the closure of the image of a map between spectra of local rings. More generally, let $>_1$, respectively $>_2$, be monomial orderings on $\mathrm{Mon}(x_1, \ldots, x_n)$, respectively $\mathrm{Mon}(t_1, \ldots, t_m)$, and let $\varphi : K[x]_{>_1} \to K[t]_{>_2}$ be a ring map defined by $\varphi(x_i) = f_i(t) \in K[t]$ (cf. Lemma 1.5.8).

Let $I \subset K[t]$ and $J \subset K[x]$ be ideals as above, satisfying $\varphi(J) \subset I$, and

$$\bar{\varphi} : K[x]_{>_1}/J \to K[t]_{>_2}/I$$

the induced map.

Problem: We want to compute equations for $\overline{f(X)} \subset Y$ for the map

$$f = \bar{\varphi}^{\#} : X = \mathrm{Spec}(K[t]_{>_2}/I) \longrightarrow Y = \mathrm{Spec}(K[x]_{>_1}/J)\,.$$

We claim that the following algorithm solves the problem:

Solution: Choose any ordering $>$ on $\mathrm{Mon}(t_1, \ldots, t_m, x_1, \ldots, x_n)$ which is an elimination ordering for $t_1, \ldots, t_m$ and satisfies $K[x]_{>'} \subset K[x]_{>_1}$ where $>'$ is the ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$ induced by $>$.[9] Compute a standard basis G of the ideal

$$N := \langle I,\, J,\, x_1 - f_1(t), \ldots, x_n - f_n(t)\rangle$$

as above with respect to this ordering. Select those elements $p_1, \ldots, p_r$ from G which do not depend on t. Then $\overline{f(X)} = V(\langle p_1, \ldots, p_r\rangle_{K[x]_{>_1}})$. □

[9] We could choose, for example, $>$ to be $\big(\mathtt{dp}(m), \mathtt{dp}(n)\big)$ or $>$ to be $\big(\mathtt{dp}(m), >_1\big)$.

The only problem in seeing correctness results from the fact that we only assume $K[x]_{>'} \subset K[x]_{>_1}$ but no other relation between $>$ and $>_1, >_2$.

The graph construction from Appendix A.2, applied to the localized rings, shows that $\overline{f(X)}$ is the zero–set of the ideal

$$N \cdot (K[t]_{>_2} \otimes_K K[x]_{>_1}) \cap K[x]_{>_1} .$$

Now the above algorithm computes polynomial generators of the intersection $(N \cdot K[t,x]_>) \cap K[x]_{>'}$. We have $K[t,x]_> = K[t] \otimes K[x]_{>'}$, $K[x]_{>'} \subset K[x]_{>_1}$ and an inclusion of rings

$$K[t,x] \subset R_1 := K[t,x]_> \subset R_2 := K[t]_{>_2} \otimes K[x]_{>_1} \subset R_3 := K[t,x]_{(>_2,>_1)} ,$$

where $(>_2, >_1)$ is the product ordering on $\mathrm{Mon}(t_1, \ldots, t_m, x_1, \ldots, x_n)$.

Moreover, by Lemma 1.4.8 (1), we have $(N \cdot R_3) \cap K[t,x] = N$, hence, $(N \cdot R_i) \cap K[t,x] = N$ for $i = 1, 2$ and, therefore,

$$(N \cdot R_1) \cap K[x] = N \cap K[x] = (N \cdot R_2) \cap K[x] .$$

Again, by Lemma 1.4.8 (1), $(N \cdot R_2) \cap K[x]_{>_1} = (N \cdot R_2 \cap K[x]) \cdot K[x]_{>_1}$ and $(N \cdot R_1) \cap K[x]_{>'} = (N \cdot R_1 \cap K[x]) \cdot K[x]_{>'}$. Altogether, we have

$$\begin{aligned} (N \cdot R_2) \cap K[x]_{>_1} &= \big((N \cdot R_1) \cap K[x]\big) \cdot K[x]_{>_1} \\ &= \big((N \cdot R_1) \cap K[x]_{>'}\big) \cdot K[x]_{>_1}, \end{aligned}$$

where the left–hand side defines $\overline{f(X)}$ and generators for the right–hand side are computed. □

Thus, we have many choices for orderings on $\mathrm{Mon}(x_1, \ldots, x_n)$ for computing $\overline{f(X)} \subset Y$. In particular, we can always choose a global ordering.

SINGULAR Example 1.8.6 (Zariski closure of the image).
Compute an implicit equation for the surface defined parametrically by the map $f : \mathbb{A}^2 \to \mathbb{A}^3$, $(u,v) \mapsto (uv, uv^2, u^2)$.

```
ring A =0,(u,v,x,y,z),dp;
ideal I=x-uv,y-uv2,z-u2;
ideal J=eliminate(I,uv);
J;
//-> J[1]=x4-y2z           //defines the closure of f(X)
```

Note that the image does not contain the y–axis, however, the closure of the image contains the y–axis. This surface is called the *Whitney umbrella*.

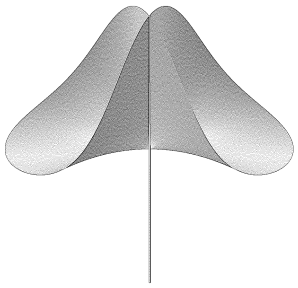


Fig. 1.3. Whitney Umbrella

1.8.4 Solvability of Polynomial Equations

Problem: Given $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, we want to assure whether the system of polynomial equations

$$f_1(x) = \cdots = f_k(x) = 0$$

has a solution in $\overline{K}^n$, where $\overline{K}$ is the algebraic closure of K.

Let $I = \langle f_1, \ldots, f_k \rangle_{K[x]}$, then the question is whether the algebraic set $V(I) \subset \overline{K}^n$ is empty or not.

Solution: By Hilbert's Nullstellensatz, $V(I) = \emptyset$ if and only if $1 \in I$. We compute a Gröbner basis G of I with respect to any global ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$ and normalize it (that is, divide every $g \in G$ by $\mathrm{LC}(g)$). Since $1 \in I$ if and only if $1 \in L(I)$, we have $V(I) = \emptyset$ if and only if 1 is an element of a normalized Gröbner basis of I. Of course, we can avoid normalizing, which is expensive in rings with parameters. Since $1 \in I$ if and only if G contains a non–zero constant polynomial, we have only to look for an element of degree 0 in G. □

1.8.5 Solving Polynomial Equations

A fundamental task with countless applications is to solve a system of polynomial equations, $f_1(x) = 0, \ldots, f_k(x) = 0$, $f_i \in K[x] = K[x_1, \ldots, x_n]$. However, what is actually meant by "solving" very much depends on the context. For instance, it could mean to determine one (respectively some, respectively all) points of the solution set $V(f_1, \ldots, f_k)$, either considered as a subset of K^n or of $\overline{K}^n$, where $\overline{K}$ is the algebraic closure of K (for notations cf. Section A.1).

Here, we consider only the case where the ideal $I = \langle f_1, \ldots, f_k \rangle_{K[x]}$ is 0–dimensional, that is, where $f_1 = \cdots = f_k = 0$ has only finitely many solutions in $\overline{K}^n$.

From an algebraic point of view, a primary decomposition $I = \bigcap_{i=1}^{r} Q_i$ of I with $P_i = \sqrt{Q_i} \subset K[x_1, \ldots, x_n]$ a maximal ideal, could be considered as a solution (cf. Chapter 4). At least, it provides a decomposition $V(I) = V(P_1) \cup \cdots \cup V(P_r)$ and if $p = (p_1, \ldots, p_n) \in K^n$ is a solution, then $P_j = \langle x_1 - p_1, \ldots, x_n - p_n \rangle$ for some j and we can, indeed, recover the coordinates of p from a primary decomposition of I. Moreover, for solutions $p \in \overline{K}^n$ which are not in K^n the primary decomposition provides irreducible polynomials defining a field extension $\widetilde{K}$ of K such that p has coordinates in $\widetilde{K}$ (cf. Chapter 4).

Besides the fact that primary decomposition is very expensive, the answer would be unsatisfactory from a practical point of view. Indeed, if $K = \mathbb{R}$ or $\mathbb{C}$, most people would probably interpret solving as finding approximate numerical coordinates of one (respectively some, respectively all) point(s) of $V(I)$. And this means that, at some point, we need a numerical root finder.

Numerical solving of equations (even transcendental or (partial) differential equations) is a highly developed discipline in mathematics which is very successful in applications to real life problems. However, there are inherent problems which often make it difficult, or even impossible, either to find a solution or to ensure that a detected solution is (approximately) correct. Particular problems are, for example, to find *all* solutions or to guarantee stability and convergence of algorithms in the presence of singularities. In this context symbolic methods can be useful in preparing the system by finding another set of generators for I (hence, having the same solutions) which is better suited for numerical computations.

Here we describe only how lexicographical Gröbner bases can be used to reduce the problem of multivariate solving to univariate solving.

Problem: Given $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, $K = \mathbb{R}$ or $\mathbb{C}$, which we assume to have only finitely many solutions $p_1, \ldots, p_r \in \mathbb{C}^n$. We wish to find coordinates of all p_i in decimal format up to a given number of digits. We are also interested in locating multiple solutions.

Solution: Compute a lexicographical Gröbner basis $G = \{g_1, \ldots, g_s\}$ of I for $x_1 > x_2 > \cdots > x_n$. Then we have (cf. Exercise 1.8.6) $s \geq n$ and, after renumbering G, there are elements $g_1, \ldots, g_n \in G$ such that

$$\begin{aligned}
g_1 &= g_1(x_n), && \mathrm{LM}(g_1) = x_n^{n_n},\\
g_2 &= g_2(x_{n-1}, x_n), && \mathrm{LM}(g_2) = x_{n-1}^{n_{n-1}},\\
&\vdots\\
g_n &= g_n(x_1, \ldots, x_n), && \mathrm{LM}(g_n) = x_1^{n_1}.
\end{aligned}$$

Now use any numerical univariate solver (for example Laguerre's method) to find all complex solutions of $g_1(x_n) = 0$ up to the required number of digits. Substitute these in g_2 and for each substitution solve g_2 in x_{n-1}, as before. Continue in this way up to g_n. Thus, we computed all coordinates of all solutions of $g_1 = \cdots = g_n = 0$. Finally, we have to discard those solutions for which one of the remaining polynomials $g_{n+1}, \ldots, g_s$ does not vanish. □

We should like to mention that this is not the best possible method. In particular, the last step, that is, discarding non–solutions, may lead to numerical problems. A better method is to use *triangular sets*, either in the spirit of Lazard [148] or Möller [170] (cf. [102] for experimental results and a comparison to resultant based methods). Triangular sets are implemented in the SINGULAR library `triang.lib`.

SINGULAR Example 1.8.7 (solving equations).

```
ring  A=0,(x,y,z),lp;
ideal I=x2+y+z-1,
        x+y2+z-1,
        x+y+z2-1;
ideal J=groebner(I);    //the lexicographical Groebner basis
J;
//-> J[1]=z6-4z4+4z3-z2       J[2]=2yz2+z4-z2
//-> J[3]=y2-y-z2+z           J[4]=x+y+z2-1
```

We use the multivariate solver based on triangular sets, due to Möller and Hillebrand [170], [123], and the univariate Laguerre–solver.

```
LIB"solve.lib";
list s1=solve(I,6);
//-> // name of new current ring: AC
s1;
//-> [1]:          [2]:     [3]:           [4]:     [5]:
//->    [1]:          [1]:     [1]:           [1]:     [1]:
//->        0.414214     0        -2.414214      1        0
//->    [2]:          [2]:     [2]:           [2]:     [2]:
//->        0.414214     0        -2.414214      0        1
//->    [3]:          [3]:     [3]:           [3]:     [3]:
//->        0.414214     1        -2.414214      0        0
```

If we want to compute the zeros with multiplicities then we use 1 as a third parameter for the `solve` command:

```
setring A;
list s2=solve(I,6,1);
s2;
//-> [1]:                       [2]:
//->     [1]:                       [1]:
//->         [1]:                       [1]:
//->             [1]:                       [1]:
//->                 -2.414214                  0
//->             [2]:                       [2]:
//->                 -2.414214                  1
//->             [3]:                       [3]:
```

```
//->                  -2.414214                    0
//->          [2]:                        [2]:
//->              [1]:                        [1]:
//->                  0.414214                    1
//->              [2]:                        [2]:
//->                  0.414214                    0
//->              [3]:                        [3]:
//->                  0.414214                    0
//->      [2]:                            [3]:
//->          1                               [1]:
//->                                              0
//->                                          [2]:
//->                                              0
//->                                          [3]:
//->                                              1
//->                                  [2]:
//->                                      2
```

The output has to be interpreted as follows: there are two zeros of multiplicity 1 and three zeros ((0, 1, 0), (1, 0, 0), (0, 0, 1)) of multiplicity 2.

Note that a possible way to check whether a system of polynomial equations $f_1 = \cdots = f_k = 0$ has finitely many solutions in $\overline{K}$, is to compute a Gröbner basis G of $I = \langle f_1, \ldots, f_k \rangle$ with respect to any ordering (usually `dp` is the fastest). Then $V(I)$ is finite if and only if `dim(G)`$=0$ or, equivalently, `lead(G)` contains $x_i^{n_i}$ for $i = 1, \ldots, n$ and some n_i (and then the number of solutions is $\leq n_1 \cdot \ldots \cdot n_n$). The number of solutions, counting multiplicities, in $\overline{K}^n$ is equal to `vdim(G)`$= \dim_K K[x]/I$ (cf. Exercises 1.8.6 to 1.8.8).

1.8.6 Radical Membership

Problem: Let $f_1, \ldots, f_k \in K[x]_>$, $>$ a monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$ and $I = \langle f_1, \ldots, f_k \rangle_{K[x]_>}$. Given some $f \in K[x]_>$ we want to decide whether $f \in \sqrt{I}$. The following lemma, which is sometimes called *Rabinowich's trick*, is the basis for solving this problem. [10]

Lemma 1.8.8. *Let A be a ring, $I \subset A$ an ideal and $f \in A$. Then*

$$f \in \sqrt{I} \iff 1 \in \tilde{I} := \langle I, 1 - tf \rangle_{A[t]}$$

where t is an additional new variable.

Proof. If $f^m \in I$ then $t^m f^m \in \tilde{I}$ and, hence,

$$1 = t^m f^m + (1 - t^m f^m) = t^m f^m + (1 - tf)(1 + tf + \cdots + t^{m-1} f^{m-1}) \in \tilde{I}\,.$$

[10] We can even compute the full radical $\sqrt{I}$ as is shown in Section 4.5, but this is a much harder computation.

Conversely, let $1 \in \tilde{I}$. Without loss of generality, we may assume that f is not nilpotent since, otherwise, f is clearly in $\sqrt{I}$.

By assumption, there are $f_1, \ldots, f_k \in I$ and $a_i(t) = \sum_{j=0}^{d_i} a_{ij} t^j \in A[t]$, $i = 0, \ldots, k$ such that

$$1 = \sum_{i=1}^{k} a_i(t) f_i + a_0(t)(1 - tf)\,.$$

Since f is not nilpotent we can replace t by $1/f$ and obtain

$$1 = \sum_i a_i \left(\frac{1}{f}\right) f_i = \sum_{i,j} a_{ij} f^{-j} f_i$$

in the localization A_f, see Section 1.4. Multiplying with f^m, for m sufficiently large, we obtain $f^m = \sum_{i,j}(a_{ij} f^{m-j}) f_i \in I$ (even in A, not only in A_f). □

Solution: By Lemma 1.8.8, we have $f \in \sqrt{I}$ if and only if

$$1 \in J := \langle f_1, \ldots, f_k, 1 - tf \rangle (K[x]_>)[t]\,,$$

where t is a new variable.

To solve the problem, we choose on $\mathrm{Mon}(t, x_1, \ldots, x_n)$ an elimination ordering for t inducing $>'$ on $\mathrm{Mon}(x_1, \ldots, x_n)$ such that $K[x]_{>'} = K[x]_>$ (for example, take `(lp(1),>)`) and compute a standard basis G of J. Then $f \in \sqrt{I}$ if and only if G contains an element g with $\mathrm{LM}(g) = 1$. □

SINGULAR Example 1.8.9 (radical membership).

```
ring A =0,(x,y,z),dp;
ideal I=x5,xy3,y7,z3+xyz;
poly f =x+y+z;

ring B =0,(t,x,y,z),dp; //need t for radical test
ideal I=imap(A,I);
poly f =imap(A,f);
I=I,1-t*f;
std(I);
//-> _[1]=1             //f is in the radical

LIB"primdec.lib";   //just to see, we compute the radical
setring A;
radical(I);
//-> _[1]=z   _[2]=y     _[3]=x
```

1.8.7 Intersection of Ideals

Problem: Given $f_1, \ldots, f_k, h_1, \ldots, h_r \in K[x]$ and $>$ a monomial ordering. Let $I_1 = \langle f_1, \ldots, f_k \rangle K[x]_>$ and $I_2 = \langle h_1, \ldots, h_r \rangle K[x]_>$. We wish to find generators for $I_1 \cap I_2$.

Consider the ideal $J := \langle tf_1, \ldots, tf_k, (1-t)h_1, \ldots, (1-t)h_r \rangle (K[x]_>)[t]$.

Lemma 1.8.10. *With the above notations,* $I_1 \cap I_2 = J \cap K[x]_>$.

Proof. Let $f \in J \cap K[x]_>$, then

$$f(x) = t \cdot \sum_{i=1}^{k} a_i(t,x) f_i(x) + (1-t) \sum_{j=1}^{r} b_j(t,x) h_j(x) \,.$$

Since the polynomial f is independent of t, we have $f = \sum_{i=1}^{k} a_i(1,x) f_i \in I_1$ and $f = \sum_{j=1}^{r} b_j(0,x) h_j \in I_2$, hence $f \in I_1 \cap I_2$. Conversely, if $f \in I_1 \cap I_2$, then $f = tf + (1-t)f \in J \cap K[x]_>$. □

Solution: We choose an elimination ordering for t on $\mathrm{Mon}(t, x_1, \ldots, x_n)$ inducing $>'$ on $\mathrm{Mon}(x_1, \ldots, x_n)$ such that $K[x]_{>'} = K[x]_>$ (for example, take `(lp(1),>)`). Then we compute a standard basis of J and get generators for $J \cap K[x]_>$ as in Section 1.8.2 □

A different solution, using syzygies, is described in Chapter 2, Section 2.8.3.

SINGULAR Example 1.8.11 (intersection of ideals).

```
ring A=0,(x,y,z),dp;
ideal I1=x,y;
ideal I2=y2,z;
intersect(I1,I2);        //the built-in SINGULAR command
//-> _[1]=y2    _[2]=yz    _[3]=xz

ring B=0,(t,x,y,z),dp;   //the way described above
ideal I1=imap(A,I1);
ideal I2=imap(A,I2);
ideal J=t*I1+(1-t)*I2;
eliminate(J,t);
//-> _[1]=yz  _[2]=xz   _[3]=y2
```

1.8.8 Quotient of Ideals

Problem: Let I_1 and $I_2 \subset K[x]_>$ be as in Section 1.8.7. We want to compute

$$I_1 : I_2 = \{ g \in K[x]_> \mid gI_2 \subset I_1 \} \,.$$

Since, obviously, $I_1 : \langle h_1, \ldots, h_r \rangle = \bigcap_{i=1}^{r} (I_1 : \langle h_i \rangle)$, we can compute $I_1 : \langle h_i \rangle$ for each i and then apply SINGULAR Example 1.8.11. The next lemma shows a way to compute $I_1 : \langle h_i \rangle$.

Lemma 1.8.12. *Let $I \subset K[x]_>$ be an ideal, and let $h \in K[x]_>$, $h \neq 0$. Moreover, let $I \cap \langle h\rangle = \langle g_1 \cdot h, \ldots, g_s \cdot h\rangle$. Then $I : \langle h\rangle = \langle g_1, \ldots, g_s\rangle_{K[x]_>}$.*

Proof. Any set of generators of $I \cap \langle h\rangle$ is of the form $\{g_1 h, \ldots, g_s h\}$. Therefore, $h\langle g_1, \ldots, g_s\rangle \subset I$, hence $\langle g_1, \ldots, g_s\rangle \subset I : \langle h\rangle$. Conversely, if $g \in I : \langle h\rangle$, then $hg \in I \cap \langle h\rangle$ and $hg = h \cdot \sum_i a_i g_i$ for some a_i. Since $K[x]_>$ has no zero-divisors and $h \neq 0$, we have $g = \sum_i a_i g_i$ which proves the claim. □

Solution 1: We can compute $I_1 : I_2$ by computing, for $i = 1, \ldots, r$, $I_1 \cap \langle h_i\rangle$ according to Section 1.8.7, divide the generators by h_i getting $I_1 : \langle h_i\rangle$ and compute the intersection $\bigcap_i (I_1 : \langle h_i\rangle)$, according to Section 1.8.7. □

Instead of computing $\bigcap_i (I_1 : \langle h_i\rangle)$, we can define

$$h := h_1 + t_1 h_2 + \cdots + t_{r-1} h_r \in K[t_1, \ldots, t_{r-1}, x_1, \ldots, x_n]$$

and obtain

$$I_1 : I_2 = \Big(I_1(K[x]_>)[t] : \langle h\rangle\Big) \cap K[x]_> .$$

This holds, since $g(x) \in I_1 : \langle h\rangle$ if and only if

$$g(x)\big(h_1(x) + t_1 h_2(x) + \cdots + t_{r-1} h_r(x)\big) = \sum_{i=1}^{k} a_i(x,t) f_i(x)$$

for some $a_i \in (K[x]_>)[t]$, which is equivalent to $g(x) h_j(x) \in \langle f_1, \ldots, f_k\rangle_{K[x]_>}$ for all j (set $t_i := 0$ for all i, and then $t_j := 1$ and $t_i = 0$ for $i \neq j$).

Solution 2: Define h as above. We can compute $I_1 : \langle h\rangle$ by Lemma 1.8.12 and then $I_1 : I_2$ by eliminating $t_1, \ldots, t_{r-1}$ from $I_1 : \langle h\rangle$ according to Section 1.8.2.

The same procedure works with $h := h_1 + t h_2 + t^2 h_3 + \cdots + t^{r-1} h_r \in (K[x]_>)[t]$ with just one new variable t (Exercise 1.8.2). □

SINGULAR Example 1.8.13 (quotient of ideals).

```
ring A=0,(x,y,z),dp;
ideal I1=x,y;
ideal I2=y2,z;
quotient(I1,I2);        //the built-in SINGULAR command
//-> _[1]=y    _[2]=x
```

Now let us proceed as described in Lemma 1.8.12:

```
ideal J1=intersect(I1,ideal(I2[1]));
ideal J2=intersect(I1,ideal(I2[2]));
J1;
//-> J1[1]=y2
```

`J1/I2[1]=1` implies `I1:I2[1]=A`.

```
J2;
//-> J2[1]=yz   J2[2]=xz
```

`J2/I2[2]=<x,y>` implies `I1:I2[2]=<x,y>` and all together we obtain `I1:I2=<x,y>`:

```
ideal K1=J1[1]/I2[1];
ideal K2=J2[1]/I2[2],J2[2]/I2[2];
intersect(K1,K2);
//-> _[1]=y   _[2]=x
```

1.8.9 Saturation

Let $I_1, I_2 \subset K[x]_>$ be as in Section 1.8.7. We consider the quotient of I_1 by powers of I_2

$$I_1 = I_1 : I_2^0 \subset I_1 : I_2^1 \subset I_1 : I_2^2 \subset I_1 : I_2^3 \subset \ldots \subset K[x]_> .$$

Since $K[x]_>$ is Noetherian, there exists an s such that $I_1 : I_2^s = I_1 : I_2^{s+i}$ for all $i \geq 0$. Such an s satisfies

$$I_1 : I_2^\infty := \bigcup_{i \geq 0} I_1 : I_2^i = I_1 : I_2^s ,$$

and $I_1 : I_2^s$ is called the *saturation of* I_1 *with respect to* I_2.

The minimal such s is called the *saturation exponent*. If I_1 is radical, then the saturation exponent is 1.

Problem: Given ideals $I_1, I_2 \subset K[x]_>$, we want to compute generators for $I_1 : I_2^\infty$ and the saturation exponent.

Solution: Set $I^{(0)} = I_1$ and compute successively $I^{(j+1)} = I^{(j)} : I_2$, $j \geq 0$, by any of the methods of Section 1.8.8. In each step check whether $I^{(j+1)} \subset I^{(j)}$, by using Section 1.8.1. If s is the first j when this happens, then $I^{(s)} = I_1 : I_2^\infty$ and s is the saturation exponent. □

Correctness follows from $I^{(j)} = I_1 : I_2^j$, which is a consequence of Lemma 1.8.14 (1). The above method is usually much faster than computing $I_1 : I_2^j$, since I_2^j can become quite large.

To provide a geometric interpretation of ideal–quotient and saturation, we state the following:

Lemma 1.8.14. *Let A be a ring and I_1, I_2, I_3 ideals in A.*

(1) a) $(I_1 \cap I_2) : I_3 = (I_1 : I_3) \cap (I_2 : I_3)$, *in particular*
$I_1 : I_3 = (I_1 \cap I_2) : I_3$ *if* $I_3 \subset I_2$,
b) $(I_1 : I_2) : I_3 = I_1 : (I_2 \cdot I_3)$.
(2) If I_1 is prime and $I_2 \not\subset I_1$, then $I_1 : I_2^j = I_1$ for $j \geq 1$.
(3) If $I_1 = \bigcap_{i=1}^r J_i$ with J_i prime, then $I_1 : I_2^\infty = I_1 : I_2 = \bigcap_{I_2 \not\subset J_i} J_i$.

Proof. (1) is an easy exercise.

(2) $I_1 \subset I_1 : I_2^j$ is clear. Let $gI_2^j \in I_1$. Since $I_2 \not\subset I_1$ and I_1 is radical, $I_2^j \not\subset I_1$ and we can find an $h \in I_2^j$ such that $h \notin I_1$ and $gh \in I_1$. Since I_1 is prime, we have $g \in I_1$.

(3) follows from (1) and (2) since $I_2^s \not\subset J_i$ if and only if $I_2 \not\subset J_i$:

$$\left(\bigcap_{j=1}^{r} J_i\right) : I_2^s = \left(\bigcap_{I_2^s \not\subset J_i} (J_i : I_2^s)\right) \cap \left(\bigcap_{I_2^s \subset J_i} J_i : I_2^s\right) = \bigcap_{I_2^s \not\subset J_i} J_i \,. \qquad \square$$

We shall see in Chapter 3 that in a Noetherian ring each radical ideal I_1 has a prime decomposition $I_1 = \bigcap_{i=1}^{r} J_i$ with J_i prime. For the *geometric interpretation of* the *ideal quotient* and the *saturation*, we use the notations of Appendix A.2, respectively A.3. We have

$$V(I_1) = \bigcup_{i=1}^{r} V(J_i) \,.$$

Moreover, we have $I_2 \subset J_i$ if and only if $V(J_i)$ is a closed subscheme of $V(I_2)$. Hence, the variety defined by $I_1 : I_2$ is

$$V(I_1 : I_2) = \bigcup_{V(J_i) \not\subset V(I_2)} V(J_i) \,.$$

In other words, if I_1 is a radical ideal, then $V(I_1 : I_2)$ is the Zariski closure of $V(I_1) \setminus V(I_2)$.

Note that $V(\langle 0 \rangle : I) = \operatorname{supp}(I) := \{P \in \operatorname{Spec}(A) \mid P \supset \operatorname{Ann}_A(I)\}$, due to Lemma 2.1.41 below. More generally, for finitely generated ideals I_1, I_2,

$$V(I_1 : I_2) = \operatorname{supp}\big((I_2 + I_1)/I_1\big) \subset \operatorname{Spec}(A/I_1) \,.$$

Here is another example, where we do not know a priori whether we are dealing with a radical ideal or not: given an ideal $I \subset K[x_1, \ldots, x_n]$ and some point $a = (a_1, \ldots, a_n) \in V(I)$ such that $V' := V(I) \setminus \{a\} \subset \mathbb{A}^n$ is Zariski closed. We wish to know equations for V', that is, some ideal I' such that $V' = V(I')$. At the moment, we only know that there exist such ideal I' and an ideal $J \subset K[x]$ satisfying $I = I' \cap J$ and $V(J) = \{a\}$, but we neither know I' nor J. Now, since $V(J) = \{a\}$, some power of the maximal ideal $\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is contained in J (see Lemma A.2.3). Now, since $I' \not\subset \mathfrak{m}_a$, it is not difficult to show that $I' : \mathfrak{m}_a = I'$, using the existence of a primary decomposition (Theorem 4.1.4) and Exercise 4.1.3. Hence, again using Exercise 4.1.3, we can conclude that $I : \mathfrak{m}_a^\infty = I' : \mathfrak{m}_a^\infty = I'$, that is,

$$V(I) \setminus \{a\} = V(I : \mathfrak{m}_a^\infty) \,.$$

In general, however, a geometric interpretation of $I_1 : I_2$ is more difficult and requires a careful study of the primary decompositions of I_1 and I_2. $I_1 : I_2$,

or even $I_1 : I_2^\infty$, may not kill a whole component of $V(I_1)$, it may just reduce part of the structure. For example, if $I_1 = \langle xy^2, y^3 \rangle$, $I_2 = \langle x, y \rangle$, then

$$I_1 : I_2 = I_1 : I_2^\infty = \langle xy^2, y^3 \rangle : \langle x, y \rangle = \langle y^2 \rangle \,,$$

hence, $V(I_1 : I_2)$ is set-theoretically the same as $V(I_1)$ (namely, the x–axis), just with a slightly reduced structure (indicated in Figure 1.4 by the small arrow pointing in y–direction).

Fig. 1.4. Symbolic pictures of $V(\langle xy^2, y^3 \rangle)$ and $V(\langle xy^2, y^3 \rangle : \langle x, y \rangle)$.

Saturation is an important tool in computational projective geometry, cf. Appendix A.5, in particular, Lemma A.5.2 and the subsequent discussion.

SINGULAR Example 1.8.15 (saturation).

```
ring A  =0,(x,y,z),dp;
ideal I1=x5z3,xyz,yz4;
ideal I2=z;
LIB"elim.lib";
sat(I1,I2);                       //the SINGULAR procedure
//-> [1]:                         //the result
//->    _[1]=y
//->    _[2]=x5
//-> [2]:
//->    4                          //the saturation exponent

ideal J=quotient(I1,I2);          //the way described above
int k;
while(size(reduce(J,std(I1)))!=0)
{
   k++;
   I1=J;
   J=quotient(I1,I2);
}
J;
//-> J[1]=y   J[2]=x5
k;
//-> 4             //we needed to take the quotient 4 times
```

1.8.10 Kernel of a Ring Map

Let $\varphi : R_1 := (K[x]_{>_1})/I \to (K[y]_{>_2})/J =: R_2$ be a ring map defined by polynomials $\varphi(x_i) = f_i \in K[y] = K[y_1, \ldots, y_m]$ for $i = 1, \ldots, n$ (and assume that the monomial orderings satisfy $1 >_2 \mathrm{LM}(f_i)$ if $1 >_1 x_i$, cf. Lemma 1.5.8).

Define $J_0 := J \cap K[y]$, and $I_0 := I \cap K[x]$. Then φ is induced by

$$\tilde{\varphi} : K[x]/I_0 \to K[y]/J_0\,, \quad x_i \mapsto f_i\,,$$

and we have a commutative diagram

$$\begin{array}{ccc} K[x]/I_0 & \xrightarrow{\tilde{\varphi}} & K[y]/J_0 \\ \big\downarrow & & \big\downarrow \\ R_1 & \xrightarrow{\varphi} & R_2\,. \end{array}$$

Problem: Let I, J and φ be as above. Compute generators for $\mathrm{Ker}(\varphi)$.

Solution: Assume that $J_0 = \langle g_1, \ldots, g_s\rangle_{K[y]}$ and $I_0 = \langle h_1, \ldots, h_t\rangle_{K[x]}$.[11] Set $H := \langle h_1, \ldots, h_t, g_1, \ldots, g_s, x_1 - f_1, \ldots, x_n - f_n\rangle \subset K[x, y]$, and compute $H' := H \cap K[x]$ by eliminating $y_1, \ldots, y_m$ from H (cf. Section 1.8.2). Then H' generates $\mathrm{Ker}(\varphi)$ by the following lemma. □

Lemma 1.8.16. *With the above notations,* $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\tilde{\varphi})R_1$ *and*

$$\mathrm{Ker}(\tilde{\varphi}) = \big(I_0 + \langle g_1, \ldots, g_s, x_1 - f_1, \ldots, x_n - f_n\rangle_{K[x,y]} \cap K[x]\big) \ \mathit{mod}\ I_0\,.$$

In particular, if $>_1$ *is global, then* $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\tilde{\varphi})$.

Proof. Obviously $\mathrm{Ker}(\tilde{\varphi})R_1 \subset \mathrm{Ker}(\varphi)$. On the other hand, let $h \in \mathrm{Ker}(\varphi)$, where $h = (h_1/h_2) + I$ for some $h_1 \in K[x]$, $h_2 \in S_{>_1}$, then $h_1 + I_0 \in \mathrm{Ker}(\tilde{\varphi})$. We conclude that $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\tilde{\varphi})R_1$.

Now let $h \in K[x]$ satisfy $\tilde{\varphi}(h + I_0) = 0$, in other words, there exist polynomials $a_1, \ldots, a_s \in K[y]$ such that

$$h(f_1, \ldots, f_n) + \sum_{j=1}^{s} a_j g_j = 0\,.$$

Applying Taylor's formula to the polynomial $h(x)$, we obtain

[11] Let $>$ be any monomial ordering on $K[x]$, let $f_1, \ldots, f_m \in K[x]$, and let I be the ideal generated by $f_1, \ldots, f_m$ in $K[x]_>$. Then, for global orderings we have $\langle f_1, \ldots, f_m\rangle_{K[x]} = I_0$ but, if $>$ is non–global, the inclusion $\langle f_1, \ldots, f_m\rangle_{K[x]} \subset I_0 := I \cap K[x]$ may be strict. To compute I_0 in this case, one may proceed as follows: compute a primary decomposition $Q_1 \cap \ldots \cap Q_s$ of $\langle f_1, \ldots, f_m\rangle_{K[x]}$ (see Chapter 4). Assume that $Q_i K[x]_> \subsetneq K[x]_>$ iff $1 \le i \le t$. Then $I_0 = Q_1 \cap \ldots \cap Q_t$.

$$h(x) = h(f_1, \ldots, f_n) + \sum_{i=1}^{n} \frac{\partial h}{\partial x_i}(f_1, \ldots, f_n) \cdot \big(x_i - f_i\big) + \ldots .$$

This implies that, for suitable $b_i \in K[x, y]$,

$$h(x) + \sum_{i=1}^{n} b_i(x, y) \cdot \big(x_i - f_i(y)\big) + \sum_{j=1}^{s} a_j(y) g_j(y) = 0 .$$

This implies that $h \in \langle g_1, \ldots, g_s, x_1 - f_1(y), \ldots, x_n - f_n(y)\rangle_{K[x,y]} \cap K[x]$.

Conversely, let $h \in I_0 + \langle g_1, \ldots, g_s, x_1 - f_1(y), \ldots, x_n - f_n(y)\rangle_{K[x,y]} \cap K[x]$,

$$h = h_1 + \sum_{i=1}^{s} a_i g_i + \sum_{i=1}^{n} b_i (x_i - f_i), \quad h_1 \in I_0 .$$

Substituting x_i by f_i we obtain

$$h(f_1, \ldots, f_n) = h_1(f_1, \ldots, f_n) + \sum_{i=1}^{s} a_i(f_1, \ldots, f_n, y) g_i .$$

But $h_1(f_1, \ldots, f_n) \in J_0$ and $g_1, \ldots, g_s \in J_0$, hence, $h(f_1, \ldots, f_n) \in J_0$, which proves the claim. □

Remark 1.8.17. Given a ring map $\tilde{\varphi} : A \to B$, and $J \subset B$ an ideal, then $\tilde{\varphi}$ induces a ring map $\varphi : A \to B/J$ and $\mathrm{Ker}(\varphi) = \tilde{\varphi}^{-1}(J)$. Hence, the same method for computing the kernel can be used to compute preimages of ideals. Since $\mathrm{Ker}(\varphi) = \varphi^{-1}(0)$, to compute kernels or preimages is equivalent. SINGULAR has the built–in command `preimage`.

SINGULAR Example 1.8.18 (kernel of a ring map).

```
ring A=0,(x,y,z),dp;
ring B=0,(a,b),dp;
map phi=A,a2,ab,b2;
ideal zero;               //compute the preimage of 0
setring A;
preimage(B,phi,zero);     //the built-in SINGULAR command
//-> _[1]=y2-xz

ring C=0,(x,y,z,a,b), dp; //the method described above
ideal H=x-a2, y-ab, z-b2;
eliminate(H,ab);
//-> _[1]=y2-xz
```

1.8.11 Algebraic Dependence and Subalgebra Membership

Recall that a sequence of polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ is called *algebraically dependent* if there exists a polynomial $g \in K[y_1, \ldots, y_k] \setminus \{0\}$ satisfying $g(f_1, \ldots, f_k) = 0$. This is equivalent to $\mathrm{Ker}(\varphi) \neq 0$, where $\varphi : K[y_1, \ldots, y_k] \to K[x_1, \ldots, x_n]$ is defined by $\varphi(y_i) = f_i$. $\mathrm{Ker}(\varphi)$ can be computed according to Section 1.8.10, and any $g \in \mathrm{Ker}(\varphi) \setminus \{0\}$ defines an algebraic relation between the $f_1, \ldots, f_k$. In particular, $f_1, \ldots, f_k$ are algebraically independent if and only if $\mathrm{Ker}(\varphi) = 0$ and this problem was solved in Section 1.8.10.

Related, but slightly different is the subalgebra–membership problem.

Problem: Given $f \in K[x_1, \ldots, x_n]$, we may ask whether f is an element of the subalgebra $K[f_1, \ldots, f_k] \subset K[x_1, \ldots, x_n] = K[x]$.

Solution 1: Define $\psi : K[y_0, \ldots, y_k] \to K[x]$, $y_0 \mapsto f$, $y_i \mapsto f_i$, compute $\mathrm{Ker}(\psi)$ according to Section 1.8.10 and check whether $\mathrm{Ker}(\psi)$ contains an element of the form $y_0 - g(y_1, \ldots, y_k)$. That is, we define an elimination ordering for $x_1, \ldots, x_n$ on $\mathrm{Mon}(x_1, \ldots, x_n, y_0, \ldots, y_k)$ with y_0 greater than $y_1, \ldots, y_k$ (for example, `(dp(n), dp(1), dp(k))`) and compute a standard basis G of $\langle y_0 - f, y_1 - f_1, \ldots y_k - f_k \rangle$. Then G contains an element with leading monomial y_0 if and only if $f \in K[f_1, \ldots, f_k]$. □

Solution 2: Compute a standard basis of $\langle y_1 - f_1, \ldots, y_k - f_k \rangle$ for an elimination ordering for $x_1, \ldots, x_n$ on $\mathrm{Mon}(x_1, \ldots, x_n, y_1, \ldots, y_k)$ and check whether the normal form of f with respect to this standard basis does not involve any x_i. This is the case if and only if $f \in K[f_1, \ldots, f_k]$ and the normal form expresses f as a polynomial in $f_1, \ldots, f_k$. □

We omit the proofs for these statements (cf. Exercise 1.8.10).

Note that $f \in K[f_1, \ldots, f_k]$ implies a relation $h(f, f_1, \ldots, f_k) = 0$ with $h(y_0, y_1, \ldots, y_k) = y_0 - g(y_1, \ldots, y_n)$, hence $f, f_1, \ldots, f_k$ are algebraically dependent (the converse does not need to be true).

Note further that the map $\varphi : K[y_1, \ldots, y_k] \to K[x_1, \ldots, x_n]$, $y_i \to f_i(x)$ is surjective if and only if $x_i \in K[f_1, \ldots, f_k]$ for all i. Hence, Solution 1 or Solution 2 can be used to check whether a given ring map is surjective.

SINGULAR Example 1.8.19 (algebraic dependence).

```
ring A=0,(x,y),dp;
poly f=x4-y4;
poly f1=x2+y2;
poly f2=x2-y2;
LIB"algebra.lib";
algDependent(ideal(f,f1,f2))[1];//a SINGULAR procedure
//-> 1

ring B=0,(u,v,w),dp;           //the method described above
```

```
setring A;
ideal zero;
map phi=B,f,f1,f2;
setring B;
preimage(A,phi,zero);          //the kernel of phi
//-> _[1]=vw-u                 //f=f1*f2 and hence f,f1,f2
                               //are algebraically dependent
```

SINGULAR Example 1.8.20 (subalgebra membership).

```
ring A=0,(x,y),dp;
poly f,f1,f2=x4-y4,x2+y2,x2-y2;
LIB"algebra.lib";
inSubring(f,ideal(f1,f2));//a SINGULAR procedure
//-> [1]:
//->      1               //means f is contained in K[f1,f2]
//-> [2]:
//->      y(1)*y(2)-y(0)  //means f1*f2-f=0
```

Another SINGULAR procedure which also tests subalgebra membership is `algebra_containment`.

Now let us proceed as explained in the text:

```
ring B = 0,(x,y,u,v,w),(dp(2),dp(1),dp(2)); //solution 1
ideal H=u-imap(A,f),v-imap(A,f1),w-imap(A,f2);
std(H);
//-> _[1]=u-vw    _[2]=2y2-v+w   _[3]=x2-y2-w
```

Since u appears as a leading monomial, $f \in K[f_1, f_2]$. Moreover, the existence of $u - vw$ in H implies $f = f_1 f_2$.

```
ring C=0,(x,y,v,w),(dp(2),dp(2));  //solution 2
ideal H=v-imap(A,f1), w-imap(A,f2);
poly f=imap(A,f);
reduce(f,std(H));
//-> vw                          //again we find f=f1*f2
```

Exercises

1.8.1. Let I_1, I_2 be two ideals in $K[x]_>$ with $I_2 = \langle h_1, \ldots, h_r \rangle$, $h_i \in K[x]$. Define $h := h_1 + th_2 + t^2 h_3 + \cdots + t^{r-1} h_r \in K[x, t]$. Prove that

$$I_1 : I_2 = (I_1 : h) \cap K[x]_> .$$

1.8.2. Let $I := \langle x^2 + 2y^2 - 3,\ x^2 + xy + y^2 - 3 \rangle \subset \mathbb{Q}[x, y]$. Compute the intersections $I \cap \mathbb{Q}[x]$ and $I \cap \mathbb{Q}[y]$.

1.8.3. Let $\varphi : \mathbb{Q}^2 \to \mathbb{Q}^4$ be the map defined by $(s,t) \mapsto (s^4, s^3t, st^3, t^4)$. Compute the Zariski closure of the image, $\overline{\varphi(\mathbb{Q}^2)}$, and decide whether $\varphi(\mathbb{Q}^2)$ coincides with its closure or not.

1.8.4. Compute all complex solutions of the system

$$x^2 + 2y^2 - 2 = 0$$
$$x^2 + xy + y^2 - 2 = 0\,.$$

1.8.5. Check whether the polynomial x^2+5x is in the radical of the ideal $I = \langle x^2+y^3, y^7+x^3y^5\rangle_{K[x,y]}$, respectively of the ideal $IK[x,y]_{\langle x,y\rangle}$.

1.8.6. Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$, let $I \subset K[x]_>$ be an ideal, and let G be a standard basis of I with respect to $>$. Show that the following are equivalent:

(1) $\dim_K(K[x]_>/I) < \infty$,
(2) for each $i = 1,\ldots,n$ there exists an $n_i \geq 0$ such that $x_i^{n_i}$ is a leading monomial of an element of G.

(Hint: Use Exercise 1.7.22)

1.8.7. Let $K[x]$ be the polynomial ring in one variable, and let $f \in K[x]$ decompose into linear factors, $f = (x-a_1)^{n_1} \cdot \ldots \cdot (x-a_r)^{n_r}$ for pairwise different $a_i \in K$. Show that $SK[x]/\langle f\rangle \cong K[x]/\langle x-a_1\rangle^{n_1} \oplus \cdots \oplus K[x]/\langle x-a_r\rangle^{n_r}$ and conclude that $\dim_K K[x]/\langle f\rangle = n_1 + \cdots + n_r$.

1.8.8. Let $I = \langle f_1,\ldots,f_k\rangle \subset K[x_1,\ldots,x_n]$ be an ideal. Use a lexicographical Gröbner basis of I to show that $\dim_K(K[x]/I) < \infty$ if and only if the system of equations $f_1 = \ldots = f_k = 0$ has only finitely many solutions in $\overline{K}^n$, where $\overline{K}$ denotes the algebraic closure of K.

(Hint: use induction on n, the previous exercises and Appendix A.)

1.8.9. Prove statement (1) of Lemma 1.8.14.

1.8.10. Prove that Solutions 1 and 2 to the subalgebra–membership problem in Section 1.8.11 are correct.

1.8.11. Use SINGULAR to check whether the line defined by $x+y=3$ (respectively $x+y=500$) and the circle defined by $x^2+y^2=2$ intersect.

1.8.12. Compute the kernel of the ring map $\mathbb{Q}[x,y,z] \to \mathbb{Q}[t]/\langle t^{12}\rangle$ defined by $x \mapsto t^5$, $y \mapsto t^7+t^8$, $z \mapsto t^{11}$.

1.8.13. Show that the ring $\mathbb{Q}[s^4, s^3t, st^3, t^4]$ is isomorphic to

$$\mathbb{Q}[x_1,x_2,x_3,x_4]/I$$

with $I = \langle x_2x_3 - x_1x_4, x_3^3 - x_2x_4^2, x_2^3 - x_1^2x_3, x_1x_3^2 - x_2^2x_4\rangle$.

1.8.14. Create a homogeneous polynomial p of degree 3 in three variables with random coefficients and use the `lift` command to express p as a linear combination of the partial derivatives of p.

1.9 Non–Commutative G–Algebras

SINGULAR contains a kernel extension (sometimes called PLURAL), providing Gröbner bases algorithms and implementations of Gröbner bases for ideals and modules in non–commutative G-algebras and, more generally, GR–algebras with respect to global monomial orderings. In this section we give a short introduction to the basic definitions and some of the non–commutative features of SINGULAR. For simplicity we restrict ourselves mainly to ideals, the case of modules being an immediate generalization.

In non–commutative algebras we have three kinds of ideals, namely left, right and two–sided ideals[12]. Given a finite set $F = \{f_1, \ldots, f_k\}$ from an algebra A, we denote by ${}_A\langle F\rangle = \{\sum_{i=1}^k a_i f_i | a_i \in A\}$ the left ideal, by $\langle F\rangle_A = \{\sum_{i=1}^k f_i a_i | a_i \in A\}$ the right ideal and by ${}_A\langle F\rangle_A = \{\sum_{i,j} a_i f_j b_i | a_i, b_i \in A\}$ a two–sided ideal[13], generated by F. The same notation will be used for monoid ideals in the commutative monoid $\mathbb{N}^n$.

Let $T_n = K\langle x_1, \ldots, x_n\rangle$ be the free associative K–algebra, generated by $\{x_1, \ldots, x_n\}$ over K. A K–basis of T consists of *words* $x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \ldots x_{i_m}^{\alpha_m}$, where $1 \leq i_1, i_2, \ldots, i_m \leq n$ with $m \geq 0$ and $\alpha_i \geq 0$. The elements of the form $x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \ldots x_{i_m}^{\alpha_m}$, with ordered indices $1 \leq i_1 < i_2 < \ldots < i_m \leq n$, are often called *standard words* and form a subset of the set of all words. The subvector space of T_n generated by the standard words is called vectorspace of *standard polynomials*.

Every finitely presented associative K–algebra A is isomorphic to T_n/I for some n and some two–sided ideal $I \subset T_n$. If I is given by a finite set of two–sided generators $I_1, \ldots, I_k$[14] we say that A is generated by $\{x_1, \ldots, x_n\}$ subject to the relations $\{I_1, \ldots, I_k\}$. We use the notation $A = K\langle x_1, \ldots, x_n \mid I_1 = 0, \ldots, I_k = 0\rangle$.

A K–algebra A is said to have a *Poincaré–Birkhoff–Witt* (shortly, *PBW*) *basis*, if the set of standard words $\{x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \mid \alpha_k \geq 0\}$ is a K-basis of A. It is clear, that the commutative polynomial ring $K[x_1, \ldots, x_n]$ has a PBW basis and that the free associative K–algebra $K\langle x_1, \ldots, x_n\rangle$ does not have one. However, many important non–commutative algebras have a PBW basis.

Definition 1.9.1. Let $c_{ij} \in K \setminus \{0\}$ and $d_{ij} \in T_n$, $1 \leq i < j \leq n$, be standard polynomials. Consider the algebra

$$A = K\langle x_1, \ldots, x_n \mid x_j x_i = c_{ij} \cdot x_i x_j + d_{ij},\ 1 \leq i < j \leq n\rangle.$$

[12] $I \subset A$ is called a *left–sided* (resp. *right–sided* resp. *two–sided*) *ideal* if I is a subset which is closed under addition and under multiplication by elements from A from the left (resp. from the right, resp. from both sides).

[13] Here is a difference to the commutative case. In the sum different terms $a_i, f_j b_i$ with the same f_j are necessary.

[14] This means that I is the set of linear combinations of the form $\sum_{i,j} a_i I_j b_i$ with $a_i, b_i \in T_n$.

A is called a *G–algebra*, if the following two conditions hold:

(1) there exists a monomial well–ordering $<$ on $\mathbb{N}^n$ such that[15]

$$\forall i < j \quad \mathrm{LM}(d_{ij}) < x_i x_j.$$

(2) For all $1 \leq i < j < k \leq n$, the polynomial

$$c_{ik}c_{jk} \cdot d_{ij}x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik}x_j + d_{jk}x_i - c_{ij}c_{ik} \cdot x_i d_{jk}$$

reduces to 0 with respect to the relations of A.

The matrices (c_{ij}) and (d_{ij}) are called *structural matrices*.

G–algebras, first introduced under this name by J. Apel in [3], were studied in [178]. They are also called *algebras of solvable type* [132], [135], [154] and *PBW algebras* [38].

Proposition 1.9.2. *Let A be a G–algebra. Then*

(1) A has a PBW basis $\{x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n} \mid \alpha_i \geq 0\}$,
(2) A is left and right Noetherian,
(3) A is an integral domain.

The proof of this proposition and a list of further important properties of G–algebras can be found e.g. in [152],[153].

Examples of G–algebras include:

- Weyl algebras [51] and their various generalizations [154],
- quasi–commutative polynomial rings (for example, the quantum plane $yx = q \cdot xy$ and the anti–commutative rings with relations $x_j x_i = -x_i x_j$),
- universal enveloping algebras of finite dimensional Lie algebras [60],
- some iterated Ore extensions [132],
- many quantum groups [38] and nonstandard quantum deformations,
- many important operator algebras [44], [154], et cetera,

(cf. the SINGULAR libraries `ncalg.lib, nctools.lib` and `qmatrix.lib`).

In the following example we set up several algebras with SINGULAR. According to Definition 1.9.1, we have to define two (strictly upper triangular) $n \times n$ matrices c and d. The initialization command `ncalgebra(C,D)`, executed in a commutative ring, turns the ring into a non–commutative G–algebra or returns an error message. An error message is returned, if the condition $\mathrm{LM}(d_{ij}) < x_i x_j$, for all $1 \leq i < j \leq n$, is not satisfied by the ordering in the given commutative ring.

[15] The notion of leading monomial, $\mathrm{LM}(f)$, for a standard polynomial f is defined as in the commutative case (cf. Definition 1.9.5).

SINGULAR Example 1.9.3 (enveloping algebra). Consider the universal enveloping algebra $U(\mathfrak{sl}_2)$ over the field K of characteristic 0. It is defined as $K\langle e, f, h \mid fe = ef - h,\ he = eh + 2e,\ hf = fh - 2f\rangle$. Thus, $c_{12} = c_{13} = c_{23} = 1$ and $d_{12} = -h$, $d_{13} = 2e$, $d_{23} = -2f$. The explicit definition of $U(\mathfrak{sl}_2)$ in SINGULAR is as follows:

```
ring r = 0,(e,f,h),dp;
matrix C[3][3];
C[1,2] = 1; C[1,3] = 1; C[2,3] = 1;
matrix D[3][3];
D[1,2] = -h;
D[1,3] = 2e;
D[2,3] = -2f;
ncalgebra(C,D);
```

Since the nonzero entries of the matrix C are all equal, we can execute `ncalgebra(1,D);` and obtain the same result.

Examining the properties of the ring `r`, we see that in addition to the data usually displayed for commutative polynomial rings, the non–commutative relations between variables are also displayed.

```
r;
//->    characteristic : 0
//->    number of vars : 3
//->         block   1 : ordering dp
//->                   : names    e f h
//->         block   2 : ordering C
//->    noncommutative relations:
//->     fe=ef-h
//->     he=eh+2e
//->     hf=fh-2f
```

The non–commutative multiplication between polynomials is carried out, as soon as the symbol `*` is used.

```
fe; // "commutative" syntax, not correct
//-> ef
f*e; // correct non-commutative syntax
//-> ef-h
```

SINGULAR Example 1.9.4 (quantum deformation of $U(\mathfrak{so}_3)$). Consider the algebra $U_q'(\mathfrak{so}_3)$, which is a non–standard (quantum) deformation of the algebra $U(\mathfrak{so}_3)$. The quantum parameter q is invertible. It is considered to be either a free parameter (that is, we work over the transcendental field extension $K(q)$) or a primitive root of unity (then we work over the simple algebraic field extension $K[q]/\mu(q)$, where $\mu(q)$ is the corresponding minimal polynomial). Computation in both cases is possible in SINGULAR.

The algebra $U_q'(\mathfrak{so}_3)$ is defined as

$$K\langle x,y,z \mid yx = q\cdot xy - \sqrt{q}z,\ zx = \frac{1}{q}\cdot xz + \frac{1}{\sqrt{q}}y,\ zy = q\cdot yz - \sqrt{q}x\rangle.$$

Hence, we have $c_{12} = q, c_{13} = \frac{1}{q}, c_{23} = q$ and $d_{12} = -\sqrt{q}z,\ d_{13} = \frac{1}{\sqrt{q}}y,$ $d_{23} = -\sqrt{q}x$.

Let us consider q as a free parameter and, moreover, set $Q := \sqrt{q}$.

```
ring s  = (0,Q),(x,y,z),dp;
matrix C[3][3];
C[1,2] = Q2;
C[1,3] = 1/Q2;
C[2,3] = Q2;
matrix D[3][3];
D[1,2] = -Q*z;
D[1,3] = 1/Q*y;
D[2,3] = -Q*x;
ncalgebra(C,D);
```

We obtain the following relations in the non–commutative ring `s`:

```
//->    noncommutative relations:
//->     yx=(Q2)*xy+(-Q)*z
//->     zx=1/(Q2)*xz+1/(Q)*y
//->     zy=(Q2)*yz+(-Q)*x
```

Many important algebras are predefined in numerous procedures of the libraries `ncalg.lib`, `nctools.lib` and `qmatrix.lib`, distributed with SINGULAR.

In the library `ncalg.lib`, there are procedures defining the universal enveloping algebras $U(\mathfrak{sl}_n)$, $U(\mathfrak{gl}_n)$, $U(\mathfrak{so}_m)$, $U(\mathfrak{sp}_m)$, $U(\mathfrak{g}_2)$, $U(\mathfrak{f}_4)$, $U(\mathfrak{e}_6)$, $U(\mathfrak{e}_7)$, $U(\mathfrak{e}_8)$. Moreover, there are procedures for the quantized enveloping algebras $U_q(\mathfrak{sl}_2)$, $U_q(\mathfrak{sl}_3)$ and the non–standard quantum deformation $U_q'(\mathfrak{so}_3)$.

Weyl, Heisenberg, exterior algebras, as well as finite dimensional algebras (given via multiplication table between generators) are implemented in the library `nctools.lib`. The ring of quantum matrices $\mathcal{O}_q(M_n)$ can be set with the procedure `quantMat` from `qmatrix.lib`. This procedure can be used for defining the algebras $\mathcal{O}_q(GL_n)$ and $\mathcal{O}_q(SL_n)$ as factor algebras of $\mathcal{O}_q(M_n)$.

Having defined some interesting non–commutative algebras we start with describing Gröbner bases for left ideals.

Let $A = K\langle x_1,\dots,x_n \mid x_jx_i = c_{ij}x_ix_j + d_{ij}, 1 \le i < j \le n\rangle$ be a G–algebra over a field K. Since A has a PBW basis, we call an element $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ of this basis, i.e. a standard word, a *monomial* in A,

and denote the set of monomials from A by $\mathrm{Mon}(A)$. Note that, although A is a quotient algebra of T_n the set $\mathrm{Mon}(A)$ coincides with Mon_n defined in Definition 1.1.3. A *term* in A is an element of A of the form cx^α with $c \in K$ and x^α a monomial.

Definition 1.9.5. Let A be a G–algebra in n variables.

(1) A total ordering $<$ on $\mathrm{Mon}(A)$ is called a *a (global) monomial ordering* on A, if it is a global monomial ordering on Mon_n in the sense of Definition 1.2.2, that is, if the following conditions hold:
- $<$ is a well–ordering,
- $\forall \alpha, \beta, \gamma \in \mathbb{N}^n$ such that $x^\alpha < x^\beta$, we have $x^{\alpha+\gamma} < x^{\beta+\gamma}$.

(2) Since $\mathrm{Mon}(A)$ is a K–basis of A, any $f \in A \setminus \{0\}$ can be written uniquely as $f = c_\alpha x^\alpha + g$ with $c_\alpha \in K \setminus \{0\}$, x^α a monomial, and $x^\beta < x^\alpha$ for any nonzero term $c_\beta x^\beta$ of g. We define

$$\begin{array}{lcll} \mathrm{LM}(f) & = & x^\alpha & \in \mathrm{Mon}(A), \quad \text{the } \textit{leading monomial} \text{ of } f, \\ \mathrm{LC}(f) & = & c_\alpha & \in K \setminus \{0\}, \quad \text{the } \textit{leading coefficient} \text{ of } f, \\ \mathrm{LE}(f) & = & \alpha & \in \mathbb{N}^n, \quad \text{the } \textit{leading exponent} \text{ of } f. \end{array}$$

(3) We say that x^α *divides* the monomial x^β, if $\alpha_i \leq \beta_i \ \forall i = 1 \ldots n$ and denote it by $x^\alpha | x^\beta$.

Example 1.9.6. Consider two exponent vectors $\alpha = (1,1)$ and $\beta = (1,2)$ from $\mathbb{N}^2$. Let A be a G–algebra in the variables $x = \{x_1, x_2\} = \{y, \partial\}$, and let $m_1 = x^\alpha = y\partial$ and $m_2 = x^\beta = y\partial^2$, hence $m_1 \mid m_2$. However, the left division of m_2 by m_1 gives various answers in different algebras. For example, in the commutative polynomial ring $R = K[y, \partial]$, we have $m_2 = \partial m_1$, whereas in the *first quantized Weyl algebra* $A_q = K(q)\langle y, \partial \mid \partial y = q^2 x\partial + 1\rangle$, we obtain $m_2 = q^{-2} \cdot \partial \cdot m_1 - q^{-2}\partial$.

Definition 1.9.7. Let S be any subset of a G–algebra A.

- We define $\mathcal{L}(S) \subseteq \mathbb{N}^n$ to be the monoid ideal (with respect to addition) in $\mathbb{N}^n$, generated by the leading exponents of the elements of S, that is

$$\mathcal{L}(S) = {}_{\mathbb{N}^n}\langle \alpha \mid \exists s \in S \ \ \mathrm{LE}(s) = \alpha \rangle.$$

  We call $\mathcal{L}(S)$ a *monoid ideal of leading exponents*. By Dixon's Lemma (Lemma 1.2.6), $\mathcal{L}(S)$ is finitely generated, i.e. there exist $\alpha_1, \ldots, \alpha_m \in \mathbb{N}^n$, such that $\mathcal{L}(S) = {}_{\mathbb{N}^n}\langle \alpha_1, \ldots, \alpha_m \rangle$.
- The *span of leading monomials of* S is defined to be the K–vector space spanned by the set $\{x^\alpha \mid \alpha \in \mathcal{L}(S)\} \subseteq \mathrm{Mon}(A)$. We denote it by $L(S) := {}_K\langle \{x^\alpha \mid \alpha \in \mathcal{L}(S)\} \rangle \subseteq A$.

Definition 1.9.8. Let $<$ be a monomial ordering on the G–algebra A, $I \subset A$ a left ideal and $G \subset I$ a finite subset. G is called a *left Gröbner basis* of I if for any $f \in I \setminus \{0\}$ there exists $g \in G$ satisfying $\mathrm{LM}(g) \mid \mathrm{LM}(f)$.

Remark 1.9.9. In commutative rings, one usually defines Gröbner basis via leading ideals (cf. Definition 1.6.1). In general, it is impossible to adapt this definition in the context of G–algebras. One of the reasons is that for $S \subset A$, $L(S)$ is just a K–vector subspace of A and is not, in general, an ideal.

Let us define $L'(S) = {}_A\langle\{\mathrm{LM}(f) \mid f \in S\}\rangle$ to be the left leading ideal of a finite set S. Recall, that for a commutative algebra A, a finite set S is a Gröbner basis of an ideal I, if $S \subset I$ and $L'(S) = L'({}_A\langle S\rangle) = L'(I)$.

Consider the *Weyl algebra* $A = K\langle x, \partial | \partial x = x\partial + 1\rangle$, the set $S = \{x\partial + 1, x\}$ and $I = {}_A\langle S\rangle$. I is a proper left ideal and $\{x\}$ is a reduced left Gröbner basis of I. Hence, the K–vector spaces $L(I)$ and $L(\{x\})$ are equal, but $L'(I) = {}_A\langle\{x\partial, x\}\rangle = A \neq L'(\{x\}) = {}_A\langle x\rangle$.

Proposition 1.9.10. *Let $<$ be a monomial ordering on the G–algebra A, $I \subset A$ a left ideal and $G \subset I$ a finite subset. Then the following conditions are equivalent:*

- *G is a left Gröbner basis of I,*
- *$L(G) = L(I)$ as K–vector spaces,*
- *$\mathcal{L}(G) = \mathcal{L}(I)$ as monoid ideals in $\mathbb{N}^n$.*

Let us now introduce the notion of a normal form or *divison with remainder* in the non–commutative setting.

Definition 1.9.11. Denote by $\mathcal{G}$ the set of all finite ordered subsets of the G–algebra A. A map $\mathrm{NF} : A \times \mathcal{G} \to A, \quad (f, G) \mapsto \mathrm{NF}(f|G)$, is called a *(left) normal form* on A if:

(1) For all $f \in A$, $G \in \mathcal{G}$
  (i) $\mathrm{NF}(0 \mid G) = 0$,
  (ii) $\mathrm{NF}(f \mid G) \neq 0 \quad \Rightarrow \quad \mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G)$,
  (iii) $f - \mathrm{NF}(f \mid G) \in {}_A\langle G\rangle$.
(2) Let $G = \{g_1, \ldots, g_s\} \in \mathcal{G}$ and $f \in A$. Then

$$f - \mathrm{NF}(f \mid G) = \sum_{i=1}^{s} a_i g_i, \ a_i \in A, \ s \geq 0,$$

is either 0 or $\mathrm{LM}(\Sigma_{i=1}^{s} a_i g_i) \geq \mathrm{LM}(a_i g_i)$ for all i such that $a_i g_i \neq 0$. We say that $f - \mathrm{NF}(f|G)$ (or, by abuse of notation, f) has a *(left) standard representation* with respect to G.

Lemma 1.9.12. *Let $I \subset A$ be a left ideal, $G \subset I$ a left Gröbner basis of I and $\mathrm{NF}(\cdot \mid G)$ a left normal form on A with respect to G.*

(1) For any $f \in A$, we have $f \in I \iff \mathrm{NF}(f \mid G) = 0$.
(2) If $J \subset A$ is a left ideal with $I \subset J$, then $L(I) = L(J)$ implies $I = J$. In particular, G generates I as a left ideal.
(3) If $\mathrm{NF}(\cdot \mid G)$ is a reduced left normal form, then it is unique.

Definition 1.9.13. Let $f, g \in A \setminus \{0\}$ with $\mathrm{LM}(f) = x^\alpha$ and $\mathrm{LM}(g) = x^\beta$. Set $\gamma := \mathrm{lcm}(\alpha, \beta)$ and define the *(left) s–polynomial* of f and g to be

$$\mathrm{LeftSpoly}(f, g) := x^{\gamma-\alpha} f - \frac{\mathrm{LC}(x^{\gamma-\alpha} f)}{\mathrm{LC}(x^{\gamma-\beta} g)} x^{\gamma-\beta} g.$$

Remark 1.9.14.

(1) It is easy to see that $\mathrm{LM}(\mathrm{LeftSpoly}(f, g)) < \mathrm{LM}(f \cdot g)$ holds. If $\mathrm{LM}(g) \mid \mathrm{LM}(f)$, say $\mathrm{LM}(g) = x^\beta$ and $\mathrm{LM}(f) = x^\alpha$, then the s–polynomial is especially simple:

$$\mathrm{LeftSpoly}(f, g) = f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(x^{\alpha-\beta} g)} x^{\alpha-\beta} g,$$

and $\mathrm{LM}\big(\mathrm{LeftSpoly}(f, g)\big) < \mathrm{LM}(f)$ holds.

(2) Let A be a G–algebra, where all the relations are of the form $\{x_j x_i = x_i x_j + d_{ij}\}$. Then, there is an easier formula for the s–polynomial, namely

$$\mathrm{LeftSpoly}(f, g) := x^{\gamma-\alpha} f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} x^{\gamma-\beta} g,$$

which looks exactly like the formula in the Definition 1.6.9.

As before, we assume that A is a G–algebra and $<$ is a fixed global monomial ordering on A.

Algorithm 1.9.15. LeftNF($f \mid G$)

Input: $f \in A,\ G \in \mathcal{G}$;
Output: $h \in A$, a left normal form of f with respect to G.

- $h := f$;
- while $((h \neq 0)$ and $(G_h := \{g \in G :\ \mathrm{LM}(g) \mid \mathrm{LM}(h)\} \neq \emptyset))$
  choose any $g \in G_h$;
  $h := \mathrm{LeftSpoly}(h, g)$;
- return h;

Algorithm 1.9.16. LeftGröbnerBasis(G)

Input: $G \in \mathcal{G}$;
Output: $S \in \mathcal{G}$, a left Gröbner basis of the left submodule $I = {}_A\langle G\rangle \subset A$.

- $S := G$;
- $P := \{(f, g) \mid f, g \in S\} \subset S \times S$;
- while ($P \neq \emptyset$)
  choose $(f, g) \in P$;
  $P := P \setminus \{(f, g)\}$;
  $h :=$ LeftNF$\big(\ \mathrm{LeftSpoly}(f, g) \mid S\big)$;

```
        if ( h ≠ 0 )
           P := P ∪ {(h, f) | f ∈ S};
           S := S ∪ {h};
  return S;
```

As one can see, with the chosen setup, we are able to keep the form of the algorithms exactly as in the commutative case. However, since we use left s–polynomials, left normal forms, and compute left Gröbner bases respectively, the proofs are somewhat different.

Theorem 1.9.17 (Left Buchberger's Criterion). *Let $I \subset A$ be a left ideal and $G = \{g_1, \ldots, g_s\}$, $g_i \in I$. Let* $\mathrm{LeftNF}(\cdot \mid G)$ *be a left normal form on A with respect to G. Then the following are equivalent:*

(1) G is a left Gröbner basis of I,
(2) $\mathrm{LeftNF}(f \mid G) = 0$ *for all $f \in I$,*
(3) each $f \in I$ has a left standard representation with respect to G,
(4) $\mathrm{LeftNF}\big(\mathrm{LeftSpoly}(g_i, g_j) | G\big) = 0$ *for $1 \leq i, j \leq s$.*

The practical computation of Gröbner bases in non–commutative algebras can be extremely time and space consuming already for small examples, much more than in the commutative case. It is therefore important to know which criteria for discarding useless pairs continue to hold. We point out, that the generalization of the *chain criterion* (Lemma 2.5.10) holds in the LeftGröbnerBasis algorithm over G–algebras with no restrictions, whereas the *product criterion* (Exercise 1.7.1) does not hold in general. However, for some cases it is possible to use a weaker statement.

Lemma 1.9.18 (Generalized Product Criterion). *Let A be a G–algebra, such that $\forall 1 \leq i < j \leq n$, $c_{ij} = 1$. That is, the relations of A are of the form $\{x_j x_i = x_i x_j + d_{ij}\}$.*

Let $f, g \in A$. Suppose that $\mathrm{LM}(f)$ *and* $\mathrm{LM}(g)$ *have no common factor, then* $\mathrm{LeftNF}(\mathrm{LeftSpoly}(f, g) | \{f, g\}) = fg - gf$.

Example 1.9.19. Let $A = U(\mathfrak{sl}_2)$ over the field $\mathbb{Q}$, that is $A = \mathbb{Q}\langle e, f, h \mid fe = ef - h,\ he = eh + 2e,\ hf = fh - 2f\rangle$. Let $I \subset A$ be the left ideal generated by $\{e^2, f\}$. We compute a left Gröbner basis of I with respect to the `dp` ordering.

Let $p_1 := e^2$, $p_2 := f$, then $S = \{p_1, p_2\}$ and $P = \{(p_1, p_2)\}$. Since p_1, p_2 do not have common factors, we apply the generalized product criterion and obtain

- $\mathrm{spoly}(p_1, p_2) \to e^2 f - f e^2 = 2eh + 2e$. It is not reducible by the elements of S, so $p_3 := eh + e$, $S := \{p_1, p_2, p_3\}$ and $P := \{(p_1, p_3), (p_2, p_3)\}$.
- $\mathrm{spoly}(p_1, p_3) = h p_1 - e p_3 = 3e^2 = 3p_1$, hence $\mathrm{NF}(\mathrm{spoly}(p_1, p_3) \mid S) = 0$.
- $\mathrm{spoly}(p_2, p_3) \to p_3 p_2 - p_2 p_3 = 2ef - h^2 - h =: g$. $\mathrm{NF}(g \mid S) = g - 2ep_2 = -(h^2 + h)$, so $p_4 := h^2 + h$, $S := \{p_1, p_2, p_3, p_4\}$ and $P := \{(p_1, p_4), (p_2, p_4), (p_3, p_4)\}$.

- $\text{spoly}(p_1, p_4) \to p_1p_4 - p_4p_1 = -8e^2h - 20e^2 =: g$, then $\text{NF}(g \mid S) = g + 8ep_3 + 12p_1 = 0$.
- $\text{spoly}(p_2, p_4) = p_2p_4 - p_4p_2 = 4fh - 2f =: g$, then $\text{NF}(g \mid S) = g - 4hp_2 - 6p_2 = 0$.
- $\text{spoly}(p_3, p_4) = hp_3 - ep_4 = 2(eh + e) = 2p_3$, so $\text{NF}(\text{spoly}(p_3, p_4) \mid S) = 0$.

$S = \{p_1, p_2, p_3, p_4\}$ and $P = \emptyset$.

Hence, after reordering the elements in an ascending way, we conclude that $S = \{f, h^2 + h, eh + h, e^2\}$ is a left Gröbner basis of I.

SINGULAR Example 1.9.20 (Left Gröbner basis). Let us compute the above example with SINGULAR. The command `std` computes a left Gröbner basis of its argument of type `ideal` or `module`.

```
LIB "ncalg.lib";
// load the library with the definition of U((sl_2)
def A = makeUsl(2); // set up U(sl_2)
setring A;
option(redSB);
option(redTail); // we wish to compute reduced bases
ideal I = e2,f;
ideal LI = std(I); LI;
//-> LI[1]=f
//-> LI[2]=h2+h
//-> LI[3]=eh+e
//-> LI[4]=e2
```

Above, we have sketched the left Gröbner basis theory. By replacing every left–sided with a right–sided action in the statements and proofs, one obtains a right Gröbner basis theory. However, it is not necessary to rewrite the algorithms, since we can compute with right ideals by using left Gröbner bases in opposite algebras.

Let A be an associative algebra over K. The *opposite algebra* A^{opp} is defined by taking the underlying vector-space of A and introducing a new "opposite" multiplication on it, by setting $f * g := g \cdot f$. Then, A^{opp} is an associative K–algebra, and $(A^{\text{opp}})^{\text{opp}} = A$.

Lemma 1.9.21. *Let A be a G–algebra, then A^{opp} is a G–algebra too.*

There is one–to–one correspondence between left (right) ideals of A and right (left) ideals of A^{opp}. Thus, in order to compute a right Gröbner basis of a left ideal I in A, we have to create the opposite algebra A^{opp} of A, compute the right ideal I^{opp} corresponding to I. Then, we compute a left Gröbner basis of I^{opp} and "oppose" the result back to A. This can be achieved by the following procedure:

```
proc rightStd(ideal I)
{
  def A = basering;
  def Aopp = opposite(A);
  setring Aopp;
  ideal Iopp = oppose(A,I);
  ideal Jopp = std(Iopp);
  setring A;
  ideal J = oppose(Aopp,Jopp);
  return(J);
}
```

The same principle applies to computation of right normal forms, right syzygies etc. The corresponding procedures `rightStd, rightNF, rightSyz, rightModulo` are implemented in the library `nctools.lib`.

SINGULAR Example 1.9.22 (Right Gröbner basis).

```
LIB "ncalg.lib";
def A = makeUsl(2);
setring A;
option(redSB);
option(redTail); // we wish to compute reduced bases
ideal I = e2,f;
ideal LI = std(I);
print(matrix(LI));  // a compact form of an ideal
//-> f,h2+h,eh+e,e2
ideal RI = rightStd(I);
print(matrix(RI));
//-> f,h2-h,eh+e,e2
```

As we can see, in this case the left and right bases differ only by one generator.

A *two–sided Gröbner basis* of an ideal I is a finite set of generators $F = \{f_1, \ldots, f_s\}$, such that F is a left and a right Gröbner basis of I. In particular, if F is a two–sided Gröbner basis of I, we have ${}_A\langle F\rangle = \langle F\rangle_A = {}_A\langle F\rangle_A = I$.

We use a special algorithm for computing two–sided Gröbner bases which is described in detail in [152] and which is behind the command `twostd`. Let us continue with the example before.

SINGULAR Example 1.9.23 (Two–sided Gröbner basis).

```
ideal I = e2,f;
ideal LI = std(I);
print(matrix(LI));  // a compact form of an ideal
//-> f,h2+h,eh+e,e2
```

```
ideal TI = twostd(I);
print(matrix(TI));
//-> h,f,e
```

Two–sided Gröbner bases are essential for computations in factor–algebras. Let A be a G–algebra and $T \subset A$ be a nonzero two–sided ideal, then there is a factor–algebra A/T which we call a *GR–algebra*. The data type `qring` in the non–commutative case corresponds to GR–algebras. The ideal T must be given as a two–sided Gröbner basis.

SINGULAR Example 1.9.24 (Computations in factor algebras).

```
LIB "ncalg.lib";
def A = makeUsl2();
setring A;
ideal T = 4*e*f+h^2-2*h; // central element in U(sl_2)
T = twostd(T);
T;
//-> T[1]=4ef+h2-2h
qring Q = twostd(T);
ideal I = e2,f;
ideal LI = std(I);
LI;
//-> LI[1]=h
//-> LI[2]=f
//-> LI[3]=e
```

As we can see, the left Gröbner basis of $\{e^2, f\}$ is very different, if we pass from $U(\mathfrak{sl}_2)$ to the factor algebra $U(\mathfrak{sl}_2)/\langle 4ef + h^2 - 2h\rangle$.

Many of the SINGULAR functions are available both for G–algebras and for GR–algebras. Among them are the functions for computing left syzygy modules (`syz`), left transformation matrices between bases (`lift`), left free resolutions (`nres`, `mres`) and many others.

1.9.1 Centralizers and Centers

In many applications we need natural subalgebras of a non–commutative G–algebra A, like the *centralizer* of a finite set $S \subset A$, defined to be $C_A(S) := \{f \in A \mid \ fs = sf \ \forall s \in S\}$, and the *center* of A, $Z(A) := C_A(A) = \{f \in A \mid \ fa = af \ \forall a \in A\}$. As one can easily see, $K \subseteq Z(A) \subset C_A(S)$ for any finite subset S of A. The computation of centers and centralizers is implemented in the library `central.lib` (cf. [172]). For a general G–algebra we do not have any information on the number of generators of the center and of their degree. Hence, both procedures `centralizer` and `center` need extra arguments. Namely, one sets an upper bound for the degree and, optionally, a

bound for the number of elements to be computed. Note, that although both procedures return data of the type `ideal`, the data consists of generators of a subalgebra.

SINGULAR Example 1.9.25 (Center and centralizer).

```
LIB "ncalg.lib";
LIB "central.lib";
def A0 = makeUsl2(); // U(sl_2) over the rationals
setring A0;
// compute the centralizer of f^2 up to degree 6
ideal C = centralizer(f^2,6); C;
// -> C[1]=f
// -> C[2]=4ef+h2-2h
ideal Z = center(5); Z;
// -> Z[1]=4ef+h2-2h
def A5 = makeUsl2(5); // U(sl_2) over Z/5Z
setring A5;
ideal Z = center(5); Z;
// -> Z[1]=ef-h2+2h
// -> Z[2]=h5-h
// -> Z[3]=f5
// -> Z[4]=e5
```

As we can see, the centralizers depend heavily on the ground field K of a given G–algebra. Let us demonstrate the computations for GR–algebras. We continue with the example above. Since the element $4ef + h^2 - 2h$ is central in $U(\mathfrak{sl}_2)$ for any K, it generates a principal two–sided ideal.

```
// we are in the algebra A5
ideal T = twostd(4ef+h2-2h);  T;
// -> T[1]=ef-h2+2h
qring Q = T;
// compute the centralizer of f^2 up to degree 6
ideal C = centralizer(f^2,6); C;
// -> C[1]=f
// -> C[2]=eh3-2eh2-eh+2e
// -> C[3]=h5-h
// -> C[4]=e5
// -> C[5]=e4h2-2e4h
```

1.9.2 Left Ideal Membership

In order to test whether a given polynomial lies in the given left ideal, we have to compute, according to Lemma 1.9.12, a left Gröbner basis of the ideal and then the left normal form of the polynomial with respect to the latter basis.

This method is also used for "canonizing" representatives of polynomials in factor algebras. Let us continue with Example 1.9.25.

The procedure `bracket(a, b)` returns $ab - ba$. Let us check, that `C[2]` and `C[5]` lie in the centralizer of f^2 in the algebra $U(\mathfrak{sl}_2)/\langle 4ef+h^2-2h\rangle$. For this, we use the left ideal membership approach by invoking `NF(b,std(0))` or, alternatively, `reduce(b,std(0))` for a polynomial b.

Recall, that, in a factor ring `std(0)` stands for the two–sided Gröbner basis of the ideal defining the factor ring, which has been constructed as `qring Q` in the Singular example 1.9.25.

```
poly b = bracket(C[2],f^2);  b;
// -> -2ef2h2+2fh4-ef2h-fh3-2ef2+2fh2+fh+f
NF(b,std(0));
// -> 0
b = bracket(C[5],f^2);  b;
// -> 2e4f2h-2e3fh3-e4f2-2e2h4-2e3fh-e2h3-2e2h2-e2h
reduce(b,std(0));
// -> 0
```

1.9.3 Intersection with Subalgebras (Elimination of Variables)

Let A be a G–algebra generated by $\{x_1, \ldots, x_n\}$ with structural matrices (c_{ij}) and (d_{ij}). For a fixed $r, 1 \leq r < n$, consider the subalgebra A_r, generated by the $\{x_{r+1}, \ldots, x_n\}$. We say, that A_r is an *essential* subalgebra (or *admissible* for elimination), if $\forall\ i, j$ such that $r+1 \leq i < j \leq n$, the polynomials d_{ij} involve only the variables $x_{r+1}, \ldots, x_n$.

Example 1.9.26 (Essential and non–essential subalgebras). Consider $A = U(\mathfrak{sl}_2)$ (see SINGULAR Example 1.9.3). $\{f, h\}$ generate an essential subalgebra (recall the relations $he = eh + 2e$ and $hf = fh - 2f$). However, the subalgebra generated by $\{e, f\}$ is not essential, since $fe = ef - h$ and hence, h is the third generator of this subalgebra. That is, the set $\{e, f, h\}$ generates the same algebra over K as the set $\{e, f\}$, namely the whole A. As a consequence, we cannot "eliminate" h from any ideal of A, since this would require the intersection with the subalgebra generated by $\{e, f\}$, which is A, and hence this would not change anything.

The notion of *elimination* of variables in the context of non–commutative algebras means the *intersection of an ideal with an essential subalgebra*.

Recall, that an *ordering* $<_r$ for $x_1, \ldots, x_n$ (cf. Definition 1.5.4) is said to have the elimination property for $x_1, \ldots, x_r$, if, for any $f \in A$, $\mathrm{LM}(f) \in A_r$ implies $f \in A_r$; it is then called an *elimination ordering*.

The following lemma is the constructive generalization of Lemma 1.8.3 to the class of G–algebras.

Lemma 1.9.27. *Let A be a G–algebra, generated by $\{x_1, \ldots, x_n\}$ and $I \subset A$ an ideal. Suppose, that the following conditions are satisfied for a fixed r, $1 \leq r < n$:*

- *the set $\{x_{r+1}, \ldots, x_n\}$ generates an essential subalgebra A_r,*
- *there exists an admissible elimination ordering [16] $<_r$ for $x_1, \ldots, x_r$.*

Then, if S is a left (resp. right) Gröbner basis of I with respect to $<_r$, $S \cap A_r$ is a left (resp. right) Gröbner basis of $I \cap A_r$.

Note, that both conditions in Lemma 1.9.27 are automatically satisfied in a commutative polynomial ring as well as in a free associative algebra.

The SINGULAR command `eliminate` works along the lines of Lemma 1.9.27. At first it checks whether B is essential and, if it is the case, the check of the admissibility of the elimination ordering is performed. If one of these conditions is not satisfied, the corresponding error message is returned.

SINGULAR Example 1.9.28 (Intersection with essential subalgebras).

```
LIB "ncalg.lib";
def  U = makeUsl2(); // U(sl_2) over the rationals
setring U;
ring A = 0,(a),dp;
def  UA = U + A;
setring UA;
```

The algebra `UA` corresponds to $U(\mathfrak{sl}_2) \otimes_K K[a]$, in particular, a commutes with e, f and h in `UA`.

```
poly  p = 4*e*f+h^2-2*h - a;
// p is a central element of UA
ideal I = e^3, f^3, h^3-4*h, p;
// intersect I with the ring K[a]
ideal J = eliminate(I,e*f*h);
J;
//-> J[1]=a3-32a2+192a
```

Hence, ${}_{U(\mathfrak{sl}_2)\otimes_K K[a]}\langle 4ef + h^2 - 2h - a\rangle \cap K[a] = \langle a(a-8)(a-24)\rangle$. From Example 1.9.26 we know, that $\{e, f\}$ does not generate an essential subalgebra. Let us see what happens if we try to intersect it with this subalgebra (i.e. "eliminate" h).

```
eliminate(I,h);
//-> ? no elimination possible: subalgebra is not admissible
//-> ? error occurred in line 13: ‘eliminate(I,h);‘
```

[16] that is, satisfying the ordering condition in Definition 1.9.1 and having the elimination property for $x_1, \ldots, x_r$.

Since a commutes with e, f and h we can eliminate a, that is intersect I with the subalgebra $U(\mathfrak{sl}_2) \subset U(\mathfrak{sl}_2) \otimes_K K[a]$. Moreover, we can intersect I with the subalgebra $K[h] \subset U(\mathfrak{sl}_2) \otimes_K K[a]$, being achieved by eliminating e, f and a.

```
eliminate(I,e*f*a);
//-> _[1]=h3-4h
```

SINGULAR Example 1.9.29 (No elimination ordering exists). Let $A = K\langle p, q \mid qp = pq+q^2\rangle$ be a G–algebra for a fixed ordering $<$. In particular $q^2 < pq$ and hence $q < p$ holds. An elimination ordering for q requires that $q > p$ holds, which is a contradiction to the ordering condition for the G–algebra A.

```
ring s = 0,(p,q),dp;
ncalgebra(1,q^2); // setting the relation qp = pq + q^2
ideal I = p+q, p2+q2;
eliminate(I,q);
//-> Bad ordering at 1,2
//-> ? no elimination possible: ordering condition violated
//-> ? error occurred in STDIN line 4: `eliminate(I,q);`
```

The first line of the error message says, that the ordering condition is violated for the relation between the 1st and 2nd variable. However, we can intersect the ideal with the subalgebra $K[q]$.

```
eliminate(I,p);
//-> _[1]=q2
```

1.9.4 Kernel of a Left Module Homomorphism

Let A be a GR–algebra. Consider a left A–module homomorphism

$$\phi: \quad A^m/U \longrightarrow A^n/V \quad e_i \longmapsto \Phi_i, \quad \Phi \in Mat(n \times m, A),$$

where $U \subset A^m$ and $V \subset A^n$. The kernel of a homomorphism ϕ can be computed with the procedure `modulo` (compare SINGULAR Example 2.1.26).

SINGULAR Example 1.9.30 (Kernel of module homomorphism). Let $A = U(\mathfrak{sl}_2)/I$, where the two–sided ideal I is generated by $\{e^2, f^2, h^2 - 1\}$. Let us study the endomorphisms $\tau : A \to A$.

```
LIB "ncalg.lib";
def A0 = makeUsl2();  setring A0;
option(redSB);  option(redTail);
ideal I = e2,f2,h2-1;
I = twostd(I);
print(matrix(I));     // ideal in a compact form
//-> h2-1,fh-f,eh+e,f2,2ef-h-1,e2
```

From the two–sided Gröbner basis of I, we can read off that A is 4–dimensional over K with basis $\{1, e, f, h\}$.

```
qring A  = I;        // we move to a GR--algebra A
ideal Ke = modulo(e,0);
Ke = std(Ke+std(0)); // normalize Ke w.r.t. the factor ideal
Ke;
//->  Ke[1]=h-1      // the kernel of e
//->  Ke[2]=e
ideal Kh = modulo(h-1,0);
Kh = std(Kh+std(0));
Kh;                  // the kernel of h-1
//->  Kh[1]=h+1
//->  Kh[2]=f
```

Computing with more endomorphisms, we get the following information on their kernels.
For non–zero $k \in \mathbb{K}$, $\ker(\tau : 1 \mapsto e + k) = \ker(\tau : 1 \mapsto f + k) = 0$.
For $k^2 \neq 1$, $\ker(\tau : 1 \mapsto h + k) = 0$.
$\ker(\tau : 1 \mapsto e) = \ker(\tau : 1 \mapsto h + 1) = {}_A\langle e, h - 1\rangle$.
$\ker(\tau : 1 \mapsto f) = \ker(\tau : 1 \mapsto h - 1) = {}_A\langle f, h + 1\rangle$.

1.9.5 Left Syzygy Modules

Let A be an associative algebra and A^n the canonical free module of rank n over A. A *left* (resp. *right*) *syzygy* of elements $f_1, \ldots, f_m$ from A^n is an m–tuple $(a_1, \ldots, a_m)$, $a_i \in A$ such that $\sum_{i=1}^m a_i f_i = 0$ (resp. $\sum_{i=1}^m f_i a_i = 0$). It can be shown, that the set of all left (resp. right) syzygies forms a left (resp. right) A–module.

We can view the elements $f_i \in A^n$ as columns of a matrix $F \in Mat(n \times m, A)$. It is convenient to view a single left syzygy, which is an element of A^m, as a column in a matrix. If the left syzygy module is generated by s elements, it can be represented by a matrix $S \in Mat(m \times s, A)$ and then $S^T \cdot F^T = 0$ holds where S^T and F^T denote the transposed matrices. Similar remarks apply to right syzygies.

The command `syz` computes the first (left) syzygy module of a given set of elements. The higher syzygy modules are defined as successive syzygies of syzygies etc.

SINGULAR Example 1.9.31 (Syzygies).
Consider the algebra $U_q'(\mathfrak{so}_3)$ (Example 1.9.30), specializing the quantum parameter Q at the primitive 6th root of unity. The corresponding minimal polynomial for the algebraic field extension is $Q^2 - Q + 1$.

```
LIB "ncalg.lib";
def R = makeQso3(3);
```

```
setring R;
option(redSB); option(redTail); // for reduced output
ideal K = x+y+z,y+z,z;
module S = syz(K);        // the (left) syzygy module of K
print(S);
//-> (Q-1),       (-Q+1)*z,   (Q-1)*y,
//-> (Q)*z+(-Q+1),(Q-1)*z+(Q),(Q)*x+(-Q+1)*y,
//-> y+(-Q)*z,    x+(-Q),     (-Q)*x-1
```

The columns of the above matrix generate the (left) syzygy module of K. Let us check the property ($S^T \cdot F^T = 0$) of a syzygy matrix from above.

```
ideal tst = ideal(transpose(S)*transpose(K));
print(matrix(tst));
//-> 0,0,0
```

It is easy to see, that the (left) Gröbner basis of the ideal K is $\{x, y, z\}$. Let us compute the first syzygy module of this set of generators.

```
K = x,y,z;
S = syz(K);
print(S);
//-> (Q-1),0,            0,
//-> (Q)*z,-z2-1,        (Q)*yz+(-Q)*x,
//-> y,    (-Q)*yz+(Q)*x,y2+1
```

There are quadratic terms in the generators. It is important to mention, that the command `syz` does not return a left Gröbner basis of the first syzygy module. However, one can force it to return a Gröbner basis by setting the option `returnSB` as follows

```
option(returnSB);
S = syz(K);
print(S);
//-> (Q-1),(-Q+1)*y,-z,
//-> (Q)*z,(-Q)*x,  (-Q+1),
//-> y,    1,       (-Q)*x
```

The latter generators of the syzygy module are linear.

1.9.6 Left Free Resolutions

Computing syzygy modules of a module M iteratively, we get a free left resolution (cf. Definition 2.4.10) of M. If M is a finitely presented A–module, where A is a G–algebra in n variables, we know that this process stops at most after n steps.

The commands `nres` and `mres` compute free left resolutions and the command `minres` minimizes a given resolution also in the non–commutative setting.

SINGULAR Example 1.9.32 (Resolution with `nres` and `minres`). In the algebra $A = U(\mathfrak{sl}_2)$ we consider the ideal I, generated by $\{e^2, f\}$. Its left Gröbner basis has been computed in example 1.9.19 and SINGULAR example 1.9.20. Now we want to compute a left free resolution of the latter set of generators.

```
LIB "ncalg.lib";
def A = makeUsl2();  setring A;
option(redSB);  option(redTail);
ideal I = e2,f;
ideal J = groebner(I);
resolution F = nres(J,0);
F;
//->  1      4      4      1
//-> A <--  A <--  A <--  A
//-> 0      1      2      3
//-> resolution not minimized yet
print(matrix(F[1]));             // F[1] is the left map
//-> f,h2+h,eh+e,e2
print(matrix(F[2]));             // F[2] is the middle map
//-> 0,   h2+5h+6,eh+3e,e2,
//-> 0,   -f,     -1,   0,
//-> e,   0,      -f,   -2,
//-> -h+3,0,      0,    -f
print(matrix(F[3]));             // F[3] is the right map
//-> f2,
//-> -e,
//-> ef,
//-> -fh+f
```

With the help of `minres`, we can minimize a given resolution.

```
resolution MF = minres(F);
print(matrix(MF[1]));
//-> f,e2
print(matrix(MF[2]));
//-> e3,      e2f2-6efh-6ef+6h2+18h+12,
//-> -ef-2h+6,-f3
print(matrix(MF[3]));
//-> f2,
//-> -e
```

Applying `mres` produces the same result as the two commands `nres` and `minres` together.

1.9.7 Betti Numbers in Graded GR–algebras

A graded G–algebra in n variables is characterized by the following property: $\forall\ 1 \leq i < j \leq n$ the polynomials $x_i x_j + d_{ij}$ are weighted homogeneous. A graded GR–algebra is a factor algebra of a G–algebra modulo a two–sided ideal T, whose two–sided Gröbner basis consists of weighted homogeneous polynomials.

The Betti numbers (see Definition 2.4.10) of graded objects in graded GR–algebras can be computed with the procedure `betti`.

SINGULAR Example 1.9.33 (Betti numbers).

```
ring r = 0,(x,d,q),dp;
matrix D[3][3];
D[1,2]=q^2;
ncalgebra(1,D);
ideal I = x,d,q;
option(redSB); option(redTail);
resolution R = mres(I,0);
R;
//->  1      3      3      1
//-> r <--  r <--  r <--  r
//-> 0      1      2      3
print(betti(R),"betti");
//->            0     1     2     3
//-> ------------------------------
//->     0:     1     3     3     1
//-> ------------------------------
//-> total:     1     3     3     1
```

1.9.8 Gel'fand–Kirillov Dimension

The standard SINGULAR command `dim` computes the Krull dimension of a module or an ideal. In the non–commutative case, the Gel'fand–Kirillov dimension GKdim [180] plays a similar important role as the Krull dimension in the commutative case. Note, that for an ideal I in the polynomial ring $K[\mathbf{x}] = K[x_1, \ldots, x_n]$, the Krull dimension $\dim(I)$ and the Gel'fand–Kirillov dimension $\mathrm{GKdim}(I)$ of $K[\mathbf{x}]/I$ coincide.

The algorithm for computing the Gel'fand–Kirillov (or, shortly, GK) dimension [38, 154] uses Gröbner bases. It is implemented in the library `gkdim.lib`.

SINGULAR Example 1.9.34 (Gel'fand–Kirillov Dimension).

In this example we compute the Gel'fand–Kirillov dimensions of some modules which appeared in the examples 1.9.3, 1.9.22, 1.9.28, and 1.9.30 before.

```
LIB "gkdim.lib";
LIB "ncalg.lib";
def A = makeUsl(2); // set up U(sl_2)
setring A;
ideal I  = e2,f;
ideal LI = std(I);
GKdim(LI);
//-> 0
ideal TI = twostd(I);
GKdim(TI);
//-> 0
ideal Z = 4*e*f + h^2 - 4*h;
Z = std(Z);
GKdim(Z);
//-> 2
ring B = 0,(a),dp;
def  C = A + B;
setring C;
ideal I = e^3, f^3, h^3-4*h, 4*e*f+h^2-2*h - a;
I = std(I);
GKdim(I);
//-> 0
ideal J = eliminate(I,e*f*h);
GKdim(J);
//-> 3
setring A;
resolution F = nres(LI,0); // we computed it before
GKdim(F[1]); // this is LI itself
//-> 0
GKdim(F[2]);
//-> 3
GKdim(F[3]);
//-> 3
```

2. Modules

Module theory may, perhaps, best be characterized as linear algebra over a ring. While classical commutative algebra was basically ideal theory, modules are in the centre of modern commutative algebra as a unifying approach. Formally, the notion of a module over a ring is the analogue of the notion of a vector space over a field, in the sense that a module is defined by the same axioms, except that we allow ring elements as scalars and not just field elements. Just as vector spaces appear naturally as the solution sets of systems of linear equations over a field, modules appear as solution sets of such systems over a ring. However, contrary to vector spaces, not every module has a basis and this makes linear algebra over a ring much richer than linear algebra over a field.

This chapter contains the basic definitions and constructions in connection with modules with some emphasis on syzygies and free resolutions. Modules over special rings, such as graded rings and principal ideal domains, are treated in a special section.

Again, every construction is accompanied by concrete computational examples.

2.1 Modules, Submodules and Homomorphisms

This section contains the most elementary definitions and properties of modules. As far as the theory is completely analogous to that of vector spaces, we leave the verification of such results as exercises, with a few exceptions, in order to give some examples on how to proceed.

Definition 2.1.1. Let A be a ring. A set M, together with two operations $+ : M \times M \to M$ (*addition*) and $\cdot : A \times M \to M$ (*scalar multiplication*) is called *A–module* if

(1) $(M, +)$ is an abelian group.
(2) $(a + b) \cdot m = a \cdot m + b \cdot m$
$a \cdot (m + n) = a \cdot m + a \cdot n$
$(ab) \cdot m = a \cdot (b \cdot m)$
$1 \cdot m = m$
for all $a, b \in A$ and $m, n \in M$.

Example 2.1.2.

(1) Let A be a ring, then A is an A–module with the ring operation.
(2) If $A = K$ is a field, then A–modules are just K–vector spaces.
(3) Every abelian group is a $\mathbb{Z}$–module with scalar multiplication

$$n \cdot x := \underbrace{x + \cdots + x}_{n \text{ times}} .$$

(4) Let $I \subset A$ be an ideal, then I and A/I are A–modules with the obvious addition and scalar multiplication.
(5) Let A be a ring and $A^n = \{(x_1, \ldots, x_n) \mid x_i \in A\}$ the n–fold Cartesian product of A, then A^n is, in a canonical way, an A–module (with the component–wise addition and scalar multiplication).
(6) Let K be a field and $A = K[x]$ the polynomial ring in one variable x. An A–module M can be considered as a K–vector space M together with a linear map $\varphi : M \to M$ defined by $\varphi(m) := x \cdot m$ for all $m \in M$. On the other hand, given a K–vector space M and a linear map $\varphi : M \to M$, then we can give M the structure of a $K[x]$–module defining $x \cdot m := \varphi(m)$ for all $m \in M$.
(7) Let $\varphi : A \to B$ be a ring map, and set $a \cdot b := \varphi(a) \cdot b$ for $a \in A$ and $b \in B$. This defines an A–module structure on B. The ring B together with this structure is called an *A–algebra*.

Definition 2.1.3.

(1) Let M, N be A–modules. A map $\varphi : M \to N$ is called *A–module homomorphism* (or simply homomorphism) if, for all $a \in A$ and $m, n \in M$,
   a) $\varphi(am) = a\varphi(m)$,
   b) $\varphi(m + n) = \varphi(m) + \varphi(n)$.
   We also say that φ is *A–linear* or just *linear*. If $N = M$, then φ is called an *endomorphism*.
(2) The set of all A–module homomorphisms from M to N is denoted by $\mathrm{Hom}_A(M, N)$.
(3) A bijective A–module homomorphism is called *isomorphism* (the inverse is automatically a homomorphism, Exercise 2.1.12).
(4) M is called *isomorphic* to N, denoted by $M \cong N$, if there exists an isomorphism $M \to N$.
(5) If $\varphi : A \to B$ and $\psi : A \to C$ are two ring maps then a ring map $\alpha : B \to C$ is called an *A–algebra map* or a *homomorphism of A–algebras* if it is an A–module homomorphism, that is, if $\alpha \circ \varphi = \psi$.

Lemma 2.1.4. *Define two operations on* $\mathrm{Hom}_A(M, N)$ *by*

$$(\varphi + \psi)(m) := \varphi(m) + \psi(m) ,$$
$$(a\varphi)(m) := a \cdot \varphi(m) .$$

Then $\mathrm{Hom}_A(M, N)$ *is an A–module.*

The proof is left as Exercise 2.1.1. The module

$$M^* := \mathrm{Hom}_A(M, A)$$

is called the *dual module* of M.

Lemma 2.1.5. *Let M, N, L be A–modules and $\varphi : M \to N$ be an A–module homomorphism. Define $\phi : \mathrm{Hom}_A(N, L) \to \mathrm{Hom}_A(M, L)$ by $\phi(\lambda) := \lambda \circ \varphi$ and $\psi : \mathrm{Hom}_A(L, M) \to \mathrm{Hom}_A(L, N)$ by $\psi(\lambda) := \varphi \circ \lambda$. Then ϕ and ψ are A–module homomorphisms.*

Proof. This is just a formal verification of the definition. To give an example, we show that ϕ is an A–module homomorphism. The proof for ψ is similar and left to the reader.

Let $\lambda, \mu \in \mathrm{Hom}_A(N, L)$, $a \in A$ and $m \in M$ arbitrary. Then

$$\begin{aligned}
\big(\phi(a\lambda)\big)(m) &= \big((a\lambda) \circ \varphi\big)(m) = (a\lambda)\big(\varphi(m)\big) = a \cdot \lambda\big(\varphi(m)\big) \\
&= \big(a \cdot (\lambda \circ \varphi)\big)(m) = \big(a\phi(\lambda)\big)(m)\,, \\
\big(\phi(\lambda + \mu)\big)(m) &= \big((\lambda + \mu) \circ \varphi\big)(m) = (\lambda + \mu)\big(\varphi(m)\big) = \lambda\big(\varphi(m)\big) + \mu\big(\varphi(m)\big) \\
&= (\lambda \circ \varphi)(m) + (\mu \circ \varphi)(m) = \big(\phi(\lambda) + \phi(\mu)\big)(m)\,.
\end{aligned}$$

Since m is arbitrary, we have $\phi(a\lambda) = a \cdot \phi(\lambda)$ and $\phi(\lambda + \mu) = \phi(\lambda) + \phi(\mu)$. □

Let us first consider a homomorphism $\varphi : A^n \to A^m$. If $\{e_1, \ldots, e_n\}$ denotes the *canonical basis* of A^n (that is, $e_i = (0, \ldots, 1, \ldots, 0)$, 1 at place i), then any $x \in A^n$ is a unique linear combination $x = x_1 e_1 + \cdots + x_n e_n$, $x_i \in A$. Hence, $\varphi(e_i)$ has a unique representation as

$$\varphi(e_i) = \sum_{j=1}^{n} M_{ji} e_j, \qquad i = 1, \ldots, n\,.$$

By linearity of φ we obtain, if we write x as a column vector,

$$\varphi(x) = \begin{pmatrix} M_{11} & \ldots & M_{1n} \\ \vdots & & \vdots \\ M_{m1} & \ldots & M_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = M \cdot x$$

where $M = (M_{ij})$ is an $m \times n$–matrix with entries in A. That is, φ is given by a matrix $M \in \mathrm{Mat}(m \times n, A)$ and any such M defines a homomorphism $A^n \to A^m$. We identify these homomorphisms with matrices. This is all as for vector spaces over a field. In particular, the addition and scalar multiplication of homomorphisms correspond to addition and scalar multiplication of matrices. The composition of linear maps corresponds to matrix multiplication.

SINGULAR Example 2.1.6 (matrix operations). A matrix in SINGULAR is a matrix with polynomial entries, hence they can be defined only when a basering is active. This applies also to matrices with numbers as entries (compare SINGULAR Examples 1.1.8 and 1.1.9). A matrix is filled with entries from left to right, row by row, spaces are allowed.

```
ring A = 0,(x,y,z),dp;
matrix M[2][3] = 1, x+y, z2,        //2x3 matrix
                 x,   0, xyz;
matrix N[3][3] = 1,2,3,4,5,6,7,8,9; //3x3 matrix

M;                                  //lists all entries of M
//-> M[1,1] = 1
//-> M[1,2]=x+y
//-> M[1,3]=z2
//-> M[2,1]=x
//-> M[2,2]=0
//-> M[2,3]=xyz

print(N);                          //displays N as usual
//-> 1,2,3,                        //if the entries are small
//-> 4,5,6,
//-> 7,8,9

print(M+M);                        //addition of matrices
//-> 2, 2x+2y,2z2,
//-> 2x,0,    2xyz

print(x*N);
//-> x, 2x,3x,                     //scalar multiplication
//-> 4x,5x,6x,
//-> 7x,8x,9x

print(M*N);                       //multiplication of matrices
//-> 7z2+4x+4y+1,8z2+5x+5y+2,9z2+6x+6y+3,
//-> 7xyz+x,     8xyz+2x,    9xyz+3x

M[2,3];                           //access to single entry
//-> xyz
M[2,3]=37;                        //change single entry
print(M);
//-> 1,x+y,z2,
//-> x,0,  37
```

Further matrix operations are contained in the library `matrix.lib`. There is a procedure `pmat` in `inout.lib` which formats matrices similarly to `print`,

but allows additional parameters, for example to show only the first terms of each entry for big matrices.

```
LIB "matrix.lib"; LIB "inout.lib";

print(power(N,3));             //exponentiation of matrices
//-> 468, 576, 684,
//-> 1062,1305,1548
//-> 1656,2034,2412

pmat(power((x+y+z)*N,3),15);//show first 15 terms of entries
//-> 468x3+1404x2y+1 576x3+1728x2y+1 684x3+2052x2y+2
//-> 1062x3+3186x2y+ 1305x3+3915x2y+ 1548x3+4644x2y+
//-> 1656x3+4968x2y+ 2034x3+6102x2y+ 2412x3+7236x2y+

matrix K = concat(M,N);  //concatenation
print(K);
//-> 1,x+y,z2,1,2,3,
//-> x,0,  37,4,5,6,
//-> 0,0,  0, 7,8,9

ideal(M);              //converts matrix to ideal
//-> _[1]=1            //same as 'flatten' from matrix.lib
//-> _[2]=x+y
//-> _[3]=z2
//-> _[4]=x
//-> _[5]=0
//-> _[6]=37

print(unitmat(5));     //5x5 unit matrix
//-> 1,0,0,0,0,
//-> 0,1,0,0,0,
//-> 0,0,1,0,0,
//-> 0,0,0,1,0,
//-> 0,0,0,0,1,
```

Besides matrices, there are integer matrices which do not need a ring. These are mainly used for bookkeeping or storing integer results. The operations are the same as for matrices.

```
intmat I[2][3]=1,2,3,4,5,6;
I;
//-> 1,2,3,
//-> 4,5,6
```

We construct now the matrices corresponding to the linear maps of Lemma 2.1.5.

SINGULAR Example 2.1.7 (maps induced by Hom).
Let $\varphi : A^n \to A^m$ be the linear map defined by the $m \times n$–matrix $M = (M_{ij})$ with entries in A, $\varphi(x) = M \cdot x$. We want to compute the induced map

$$\varphi^* : \mathrm{Hom}(A^m, A^s) \to \mathrm{Hom}(A^n, A^s)\,.$$

To do so, we identify $\mathrm{Hom}(A^n, A^s) = A^{sn}$ and $\mathrm{Hom}(A^m, A^s) = A^{ms}$, using Exercise 2.1.14.

Let $\{e_1, \ldots, e_n\}$, $\{f_1, \ldots, f_m\}$, $\{h_1, \ldots, h_s\}$ denote the canonical bases of A^n, A^m, A^s, respectively. Then $\varphi(e_i) = \sum_{j=1}^m M_{ji} f_j$. Moreover, if $\{\sigma_{ij}\}$, $\{\kappa_{ij}\}$ are the bases of $\mathrm{Hom}(A^m, A^s)$, respectively $\mathrm{Hom}(A^n, A^s)$, defined by $\sigma_{ij}(f_\ell) = \delta_{j\ell} h_i$,[1] respectively $\kappa_{ij}(e_\ell) = \delta_{j\ell} h_i$, then

$$\begin{aligned}\varphi^*(\sigma_{ij})(e_k) = \sigma_{ij} \circ \varphi(e_k) = \sigma_{ij}\left(\sum_{\ell=1}^m M_{\ell k} f_\ell\right) = \sum_{\ell=1}^m M_{\ell k}\delta_{j\ell} h_i \\ = M_{jk} h_i = \sum_{\ell=1}^n M_{j\ell}\delta_{\ell k} h_i = \sum_{\ell=1}^n M_{j\ell}\kappa_{i\ell}(e_k)\,.\end{aligned}$$

This implies $\varphi^*(\sigma_{ab}) = \sum_{c=1}^n M_{bc}\kappa_{ac}$. To obtain the $sn \times sm$–matrix R defining φ^*, we order the basis elements σ_{ij} and κ_{ij} as follows

$$\begin{gathered}\{\sigma_{11}, \sigma_{12}, \ldots, \sigma_{1m}, \sigma_{21}, \sigma_{22}, \ldots\ldots, \sigma_{s1}, \sigma_{s2}, \ldots, \sigma_{sm}\}\,, \\ \{\kappa_{11}, \kappa_{12}, \ldots, \kappa_{1n}, \kappa_{21}, \kappa_{22}, \ldots\ldots, \kappa_{s1}, \kappa_{s2}, \ldots, \kappa_{sn}\}\,,\end{gathered}$$

and set, for $a, d = 1, \ldots, s$, $b = 1, \ldots, m$, $c = 1, \ldots, n$,

$$i := (d-1)n + c, \quad j := (a-1)m + b\,.$$

Then

$$R_{ij} = \begin{cases} 0, & d \neq a, \\ M_{bc} & d = a\,. \end{cases}$$

We program this in a short procedure: given a matrix M, defining a homomorphism $A^n \to A^m$, and an integer s, the procedure `kontraHom` returns a matrix defining $R : \mathrm{Hom}(A^m, A^s) \to \mathrm{Hom}(A^n, A^s)$.

```
proc kontraHom(matrix M,int s)
{
   int n,m=ncols(M),nrows(M);
   int a,b,c;
   matrix R[s*n][s*m];
   for(b=1;b<=m;b++)
   {
      for(a=1;a<=s;a++)
      {
```

[1] Here $\delta_{j\ell}$ is the *Kronecker symbol* ($\delta_{j\ell} = 0$ if $j \neq \ell$ and $\delta_{jj} = 1$).

```
            for(c=1;c<=n;c++)
            {
               R[(a-1)*n+c,(a-1)*m+b]=M[b,c];
            }
         }
      }
      return(R);
   }
```

Let us try an example.

```
   ring A=0,(x,y,z),dp;
   matrix M[3][3]=1,2,3,
                  4,5,6,
                  7,8,9;

   print(kontraHom(M,2));
   //-> 1,4,7,0,0,0,
   //-> 2,5,8,0,0,0,
   //-> 3,6,9,0,0,0,
   //-> 0,0,0,1,4,7,
   //-> 0,0,0,2,5,8,
   //-> 0,0,0,3,6,9
```

This procedure is contained as `kontrahom` in `homolog.lib`. Note that for $s = 1$, the dual map, that is, the transposed matrix, is computed.

Similarly, we can compute the map

$$\varphi_* : \mathrm{Hom}(A^s, A^n) \to \mathrm{Hom}(A^s, A^m).$$

If $\{\sigma_{ij}\}$ and $\{\kappa_{ij}\}$ are defined as before as bases of $\mathrm{Hom}(A^s, A^n)$, respectively $\mathrm{Hom}(A^s, A^m)$, then one checks that $\varphi_*(\sigma_{ab}) = \sum_{c=1}^{m} M_{ca}\kappa_{cb}$.

We obtain the following procedure: given $M : A^n \to A^m$ and s, `kohom` returns $R : \mathrm{Hom}(A^s, A^n) \to \mathrm{Hom}(A^s, A^m)$.

```
   proc kohom(matrix M,int s)
   {
      int n,m=ncols(M),nrows(M);
      int a,b,c;
      matrix R[s*m][s*n];
      for(b=1;b<=s;b++)
      {
         for(a=1;a<=m;a++)
         {
            for(c=1;c<=n;c++)
            {
               R[(a-1)*s+b,(c-1)*s+b]=M[a,c];
```

```
            }
         }
      }
      return(R);
}
```

As an example use the matrix defined above.

```
print(kohom(M,2));
//-> 1,0,2,0,3,0,
//-> 0,1,0,2,0,3,
//-> 4,0,5,0,6,0,
//-> 0,4,0,5,0,6,
//-> 7,0,8,0,9,0,
//-> 0,7,0,8,0,9
```

This procedure is contained as `kohom` in `homolog.lib`.

Definition 2.1.8. Let M be an A–module. A non–empty subset $N \subset M$ is called a *submodule* of M if, for all $m, n \in N$ and $a \in A$,

(1) $m + n \in N$,
(2) $a \cdot m \in N$.

Note that every submodule of an A–module is itself an A–module.

Remark 2.1.9. Every element of A^n is represented as

$$x = x_1 e_1 + \cdots + x_n e_n = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad x_i \in A\,,$$

that is, as a linear combination in terms of the canonical basis or as a (column, respectively row) vector. Both representations are used in SINGULAR. An element of A^n is called a *vector*.

SINGULAR Example 2.1.10 (submodules of A^n). We shall explain how to declare submodules of A^n in SINGULAR, where A is any ring of SINGULAR. In the same way as ideals $I \subset A$ are given by elements of A as generators, submodules are given by vectors in A^n as generators. The canonical basis elements e_i of A^n are denoted by `gen(i)` in SINGULAR.

```
ring   A=0,(x,y,z),dp;
module M=[xy-1,z2+3,xyz],[y4,x3,z2];
M;
//-> M[1]=xyz*gen(3)+xy*gen(1)+z2*gen(2)+3*gen(2)-gen(1)
//-> M[2]=y4*gen(1)+x3*gen(2)+z2*gen(3)
```

M is the submodule of $\mathbb{Q}[x,y,z]^3$ generated by the two (column) vectors $(xy-1, z^2+3, xyz)$ and (y^4, x^3, z^2). The output is given as linear combination of the canonical basis. SINGULAR understands both formats as input.

```
ideal  I=x2+y2+z2;
qring  Q=std(I);         //create quotient ring mod I
module M=fetch(A,M);     //map M from A to Q
```

Here we consider M as a submodule in $(\mathbb{Q}[x,y,z]/\langle x^2+y^2+z^2\rangle)^3$.

Definition 2.1.11. Let $\varphi : M \to N$ be an A–module homomorphism. The *kernel* of φ, $\mathrm{Ker}(\varphi)$ is defined by $\mathrm{Ker}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$. The *image* of φ, $\mathrm{Im}(\varphi)$, is defined by $\mathrm{Im}(\varphi) := \{\varphi(m) \mid m \in M\}$.

Lemma 2.1.12. $\mathrm{Ker}(\varphi)$ *and* $\mathrm{Im}(\varphi)$ *are submodules of* M*, respectively* N*.*

The easy proof is left as Exercise 2.1.6.

SINGULAR Example 2.1.13 (kernel and image of a module homomorphism).

```
ring A=0,(x,y,z),(c,dp);
matrix M[2][3]=x,xy,z,x2,xyz,yz;
print(M);
//->x, xy,  z,
//->x2,xyz,yz
```

To compute the kernel of a module homomorphism means to solve a system of linear equations over a ring. The `syz` command, which is based on Gröbner basis computations is, hence, a generalization of Gaussian elimination from fields to rings (see Section 2.5).

```
module Ker=syz(M);
Ker;
//-> Ker[1]=[y2z-yz2,xz-yz,-x2y+xyz]
```

For the image, there is nothing to compute. The column vectors of M generate the image.

```
module Im=M[1],M[2],M[3];
Im;
//-> Im[1]=[x,x2]
//-> Im[2]=[xy,xyz]
//-> Im[3]=[z,yz]
```

Definition 2.1.14.

(1) Let M be an A–module and $N \subset M$ be a submodule. We define the *quotient module* or *factor module* M/N by

$$M/N := \{m + N \mid m \in M\}\,.$$

That is, M/N is the set of equivalence classes of elements of M, where $m, n \in M$ are equivalent if $m - n \in N$. An equivalence class is denoted by $m + N$ or by $[m]$. Each element in the class $m + N$ is called a *representative* of the class.

(2) Let $\varphi : M \to N$ be an A–module homomorphism, then

$$\operatorname{Coker}(\varphi) := N/\operatorname{Im}(\varphi)$$

is called the *cokernel* of φ.

Lemma 2.1.15. *With the canonical operations, by choosing representatives,*

$$(m + N) + (n + N) := (m + n) + N\,, \quad a \cdot (m + N) := am + N$$

the set M/N is an A–module. N, the equivalence class of $0 \in M$ is the 0–element in M/N. The map $\pi : M \to M/N$, $\pi(m) := m + N$ is a surjective A–module homomorphism.

The proof is left as Exercise 2.1.7. We just show that the addition is well–defined (independent of the chosen representatives). If $(m' + N)$ and $(n' + N)$ are other representatives, then $m - m'$, $n - n' \in N$.

Hence, $(m + n) - (m' + n') = (m - m') + (n - n') \in N$, which shows that $(m + n) + N = (m' + n') + N$.

Proposition 2.1.16. *Let $\varphi : M \to N$ be an A–module homomorphism, then*

$$\operatorname{Im}(\varphi) \cong M/\operatorname{Ker}(\varphi)\,.$$

Proof. Define a map $\lambda : M/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ by $\lambda\big(m + \operatorname{Ker}(\varphi)\big) := \varphi(m)$. It is easy to see that λ is well–defined, that is, does not depend on the choice of the representative m. λ is surjective by definition. To see that λ is injective, let $\lambda\big(m + \operatorname{Ker}(\varphi)\big) = 0$. That is, $\varphi(m) = 0$, and, hence, $m \in \operatorname{Ker}(\varphi)$. But then $m + \operatorname{Ker}(\varphi) = \operatorname{Ker}(\varphi)$ which is the 0–element in $M/\operatorname{Ker}(\varphi)$. One can also easily check that λ is an A–module homomorphism. □

Corollary 2.1.17. *Let $L \supset M \supset N$ be A–modules, then*

$$(L/N)/(M/N) \cong L/M\,.$$

Proof. The inclusion $N \subset M$ induces a homomorphism $\pi : L/N \to L/M$ of A–modules. Obviously, π is surjective and $\operatorname{Ker}(\pi) = M/N$. Therefore, the corollary is a consequence of Proposition 2.1.16. □

Definition 2.1.18.

(1) Let M be an A–module and $M_i \subset M$ be submodules, $i \in I$. We define the *sum* of the M_i by

$$\sum_{i\in I} M_i := \left\{ \sum_{i\in I} m_i \;\middle|\; m_i \in M_i, \;\; m_i \neq 0 \text{ only for finitely many } i \right\} .$$

(2) Let $J \subset A$ be an ideal and M an A–module. We define JM by

$$JM := \left\{ \sum_{i\in I} a_i m_i \;\middle|\; I \text{ finite}, \quad a_i \in J, \quad m_i \in M \right\} .$$

(3) An A–module M is called *finitely generated* if $M = \sum_{i=1}^{n} A \cdot m_i$ for suitable $m_1, \ldots, m_n \in M$. We then write $M = \langle m_1, \ldots, m_n \rangle$, and $m_1, \ldots, m_n$ are called *generators* of M. A module generated by one element is called a *cyclic module*.

(4) Let M be an A–module. The *torsion submodule* $\mathrm{Tors}(M)$ is defined by

$$\mathrm{Tors}(M) := \{ m \in M \mid \exists \text{ a non–zerodivisor } a \in A \text{ with } am = 0 \} .$$

A module M is called *torsion free* if $\mathrm{Tors}(M) = 0$. M itself is called a *torsion module* if $\mathrm{Tors}(M) = M$.

(5) Let $N, P \subset M$ be submodules, then the *quotient* $N : P$ is defined by

$$N : P := N :_A P := \{ a \in A \mid aP \subset N \} .$$

In particular, the *annihilator* of P is

$$\mathrm{Ann}(P) := \mathrm{Ann}_A(P) := \langle 0 \rangle : P = \{ a \in A \mid aP = 0 \} .$$

Note that the module quotient is a generalization of the ideal quotient.

(6) There is still another quotient. Let $I \subset A$ be an ideal, then the *quotient of P by I in M* is

$$P :_M I := \{ m \in M \mid I \cdot m \subset P \} .$$

(7) Let M_i, $i \in I$, be A–modules. The *direct sum* $\bigoplus_{i\in I} M_i$ is defined by

$$\bigoplus_{i\in I} M_i = \{ (m_i)_{i\in I} \mid m_i \in M_i, \; m_i \neq 0 \text{ for only finitely many } i \} .$$

The *direct product* $\prod_{i\in I} M_i$ is defined by

$$\prod_{i\in I} M_i = \{ (m_i)_{i\in I} \mid m_i \in M_i \} .$$

Note that for a finite index set $I = \{1, \ldots, n\}$ the direct sum and the direct product coincide and are denoted as

$$M_1 \oplus \cdots \oplus M_n .$$

(8) Let M be an A–module. M is called *free* if $M \cong \bigoplus_{i\in I} A$. The cardinality of the index set I is called the *rank* of M. A subset $S \subset M$ is called a *basis* of M if every $m \in M$ can be written in a unique way as a finite linear combination $m = a_1m_1 + \cdots + a_nm_n$ with $m_i \in S$ and $a_i \in A$, for some n (depending on m).
If A is a field the modules are vector spaces and every module is free. In general, this is not true. The $\mathbb{Z}$–module $\mathbb{Z}/\langle 2\rangle$ is not free. More generally, a module M with $\mathrm{Tors}(M) \neq 0$ cannot be free (Exercise 2.1.9).

Lemma 2.1.19. *The sum of submodules of an A–module, the product of an ideal with an A–module, the direct sum and the direct product of A–modules are again A–modules. The module quotient of two submodules of an A–module is an ideal in A. The quotient of a submodule by an ideal is a submodule of M. The torsion module* $\mathrm{Tors}(M)$ *is a submodule of M.*

The proof is left as Exercise 2.1.8.

SINGULAR Example 2.1.20 (sum, intersection, module quotient). The sum of two modules is generated by the union of the generators, the "+" lets SINGULAR simplify the union by deleting 0's and identical generators.

```
ring A=0,(x,y,z),(c,dp);//the ordering (c,..) has the effect
module M=[xy,xz],[x,x]; //that the vectors are internally
module N=[y2,z2],[x,x]; //represented component-wise.
M+N;
//-> _[1]=[xy,xz]        //the output is, as the internal
//-> _[2]=[y2,z2]        //representation, component-wise
//-> _[3]=[x,x]
```

`intersect` and `quotient` require standard basis computations.

```
intersect(M,N);         //intersection, see Section 2.8.3
//-> _[1]=[x,x]
//-> _[2]=[xy2,xz2]

quotient(M,N);          //M:N, see Section 2.8.4
//-> _[1]=x

quotient(N,M);
//-> _[1]=y+z

qring Q=std(x5);        //quotient ring Q[x,y,z]/<x5>
module M=fetch(A,M);    //map M from A to Q
module Null;            //creates zero-module
M;
//-> M[1]=[xy,xz]
//-> M[2]=[x,x]
```

```
Null;                    //the zero-module
//-> Null[1]=0

quotient(Null,M);        //the annihilator of M
//-> _[1]=x4
```

Proposition 2.1.21. *Let M be an A-module and $N_1, N_2 \subset M$ submodules, then $(N_1 + N_2)/N_1 \cong N_2/N_1 \cap N_2$.*

Proof. The inclusion $N_2 \subset N_1 + N_2$ induces an A-module homomorphism $\pi : N_2 \to (N_1 + N_2)/N_1$. Obviously π is surjective and $\mathrm{Ker}(\pi) = N_1 \cap N_2$. Now we can use Proposition 2.1.16. □

Lemma 2.1.22. *Let M be an A–module. M is finitely generated if and only if $M \cong A^n/L$ for a suitable $n \in \mathbb{N}$ and a suitable submodule $L \subset A^n$. Equivalently, there exists a surjective homomorphism $\varphi : A^n \twoheadrightarrow M$.*

Proof. Assume that $M = \langle x_1, \ldots, x_n \rangle$ and consider the A–module homomorphism $\varphi : A^n \to M$ defined by $\varphi(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i x_i$. φ is surjective because $x_1, \ldots, x_n$ generate M. Let $L := \mathrm{Ker}(\varphi)$ then Proposition 2.1.16 implies that $M \cong A^n/L$.

Now assume $M \cong A^n/L$ for some submodule $L \subset A^n$. Let $\{e_1, \ldots, e_n\}$ be a basis of A^n, then the preimages of $x_1 := e_1 + L, \ldots, x_n := e_n + L$ generate M. □

Let M be a finitely generated A–module and $M \cong A^n/L$ for some submodule $L \subset A^n$. If L is also finitely generated, then $L \cong A^m/N$ for a suitable submodule $N \subset A^m$ and we have homomorphisms $A^m \twoheadrightarrow A^m/N \cong L \subset A^n \twoheadrightarrow A^n/L \cong M$. Therefore, M is isomorphic to the cokernel of a homomorphism $\varphi : A^m \to A^n$, the composition $A^n \to A^m/N \cong L \subset A^n$. Fixing bases in A^m and A^n, φ is given by an $n \times m$–matrix, which we also denote by φ.

Definition 2.1.23. Let M be an A–module. M is called of *finite presentation* if there exists an $n \times m$–matrix φ such that M is isomorphic to the cokernel of the map $A^m \xrightarrow{\varphi} A^n$. φ is called a *presentation matrix* of M. We write $A^m \xrightarrow{\varphi} A^n \to M \to 0$ to denote a presentation of M.

Constructive module theory is concerned with modules of finite presentation, that is, with modules which can be given as the cokernel of some matrix. All operations with modules are then represented by operations with the corresponding presentation matrices. We shall see below (Proposition 2.1.29) that every finitely generated module over a Noetherian ring is finitely presented. As polynomial rings and localizations thereof are Noetherian (Lemma 1.4.8), every finitely generated module over these rings is of finite presentation.

We shall see how we can actually compute with finitely generated modules over the rings $K[x_1, \ldots, x_n]_>$ (for any monomial ordering $>$, cf. Chapter 1),

or, more generally, over quotient rings A of those. To start with, we must know how to represent a module within SINGULAR. Since any finitely generated module over $K[x]_>$ has a presentation matrix with polynomial entries, and, as we know how to define polynomial matrices, we can define arbitrary finitely generated A–modules in SINGULAR by giving a polynomial presentation matrix. In fact, for arbitrary modules, there is no other way, we have to know a presentation matrix.

However, submodules of A^n (which is a special class, since they are, for example, torsion free, see Exercise 2.1.8) can be given just by a set of generators, that is, by m vectors of A^n. Given the generators, we can *compute* the presentation matrix by using the `syz` command, which is based on Gröbner bases (Section 2.5). Giving m vectors in A^n is, up to numbering, the same as giving an $n \times m$–matrix over A. Since we can only give ordered lists of generators, this is indeed the same.

Thus, defining a matrix or a module in SINGULAR can be interpreted in two ways: either as the presentation matrix of the factor module of A^n or as the submodule of A^n generated by the columns of the matrix.

SINGULAR Example 2.1.24 (submodules, presentation of a module).
SINGULAR distinguishes between modules and matrices. For matrices see Example 2.1.6. A module is always given by generators, either with brackets, or as a linear combination of the canonical generators `gen(1),...,gen(n)` of A^n, where only the non–zero coefficients have to be given. The last (sparse) representation is internally used. Matrices, however, are represented internally non–sparse, therefore, it is recommended to use modules instead of matrices for large input.

SINGULAR assumes a module to be a submodule of A^n if, for some generator, `gen(n)` has a non–zero coefficient, and if, for each generator, the coefficients of `gen(i)` are zero for $i > n$.

```
ring A = 0,(x,y,z),dp;
module N = [xy,0,yz],[0,xz,z2]; //submodule of A^3,
N;                              //2 generators
//-> N[1]=xy*gen(1)+yz*gen(3)   //output in sparse format
//-> N[2]=xz*gen(2)+z2*gen(3)

LIB "inout.lib";           //library for formatting output
show(N);                   //shows the generators as vectors
//-> // module, 2 generator(s)
//-> [xy,0,yz]
//-> [0,xz,z2]

print(N);                  //the corresponding matrix
//-> xy,0,
```

```
//-> 0,xz,
//-> yz,z2
```

Modules may be added and multiplied with a polynomial or an ideal. Not that addition of modules means, as for ideals, the sum of modules, which is quite different from the sum of matrices.

```
show(N+x*N);
//-> [xy,0,yz]
//-> [0,xz,z2]
//-> [x2y,0,xyz]
//-> [0,x2z,xz2]
```

There are type conversions from matrix to module, and from module to matrix: `module(matrix)` creates a module with generators the columns of the matrix, `matrix(module)` creates a matrix with columns the generators of the module. `module(matrix(module))` restores the original module and `matrix(module(matrix))` restores the original matrix.

```
module M = [xy,yz],[xz,z2]; //submodule of A^2
matrix MM = M;              //automatic type conversion,
MM;                         // same as matrix MM=matrix(M);
//-> MM[1,1]=xy
//-> MM[1,2]=xz
//-> MM[2,1]=yz
//-> MM[2,2]=z2
```

The operations on modules are operations as submodules. However, as explained above, `M` (or, better, `matrix(M)`) can be considered as the presentation matrix

$$A^2 \xrightarrow{\begin{pmatrix} xy & xz \\ yz & z^2 \end{pmatrix}} A^2$$

of the module A^2/M.

On the other hand, if M is considered as a submodule of A^2, then we can compute a presentation as

```
module K = syz(M);            //computes the kernel of M
show(K);
//-> K[1]=[-z,y]
```

This means that $A \xrightarrow{\begin{pmatrix} -z \\ y \end{pmatrix}} A^2 \to M \to 0$ is a presentation of M.

Lemma 2.1.25. *Let M, N be two A–modules with presentations*

$$A^m \xrightarrow{\varphi} A^n \xrightarrow{\pi} M \to 0 \text{ and } A^r \xrightarrow{\psi} A^s \xrightarrow{\kappa} N \to 0\,.$$

(1) Let $\lambda : M \to N$ be an A–module homomorphism, then there exist A–module homomorphisms $\alpha : A^m \to A^r$ and $\beta : A^n \to A^s$ such that the following diagram commutes:

$$\begin{array}{ccccccc} A^m & \xrightarrow{\varphi} & A^n & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\lambda} & & \\ A^r & \xrightarrow{\psi} & A^s & \xrightarrow{\kappa} & N & \longrightarrow & 0 \end{array} \tag{2.1}$$

that is, $\beta \circ \varphi = \psi \circ \alpha$ and $\lambda \circ \pi = \kappa \circ \beta$.

(2) Let $\beta : A^n \to A^s$ be an A–module homomorphism such that $\beta\big(\operatorname{Im}(\varphi)\big) \subset \operatorname{Im}(\psi)$. Then there exist A–module homomorphisms $\alpha : A^m \to A^r$ and $\lambda : M \to N$ such that the corresponding diagram (as in (2.1)) commutes.

Proof. (1) Let $\{e_1, \ldots, e_n\}$ be a basis of A^n and choose $x_i \in A^s$ such that $\kappa(x_i) = \lambda \circ \pi(e_i)$, $i = 1, \ldots, n$. We define $\beta\left(\sum_{i=1}^n a_i e_i\right) = \sum_{i=1}^n a_i x_i$. Obviously, β is an A–module homomorphism and $\lambda \circ \pi = \kappa \circ \beta$. Let $\{f_1, \ldots, f_m\}$ be a basis of A^m. Then $\kappa \circ \beta \circ \varphi(f_i) = \lambda \circ \pi \circ \varphi(f_i) = 0$. Therefore, there exist $y_i \in A^r$ such that $\psi(y_i) = \beta \circ \varphi(f_i)$. We define $\alpha\left(\sum_{i=1}^n b_i f_i\right) = \sum_{i=1}^n b_i y_i$. Again α is an A–module homomorphism and $\psi \circ \alpha = \beta \circ \varphi$.

(2) Define $\lambda(m) = \kappa \circ \beta(f)$, for some $f \in A^n$ with $\pi(f) = m$. This definition does not depend on the choice of f, because $\operatorname{Ker}(\pi) = \operatorname{Im}(\varphi)$ and $\beta\big(\operatorname{Im}(\varphi)\big) \subset \operatorname{Im}(\psi) = \operatorname{Ker}(\kappa)$. Obviously, λ is an A–module homomorphism satisfying $\lambda \circ \pi = \kappa \circ \beta$. We can define α as in (1).

□

SINGULAR Example 2.1.26 (computation of Hom).
With the notations of Lemma 2.1.25 we obtain the following commutative diagram:

$$\begin{array}{ccccc} \operatorname{Hom}(M,N) & \longrightarrow & \operatorname{Hom}(A^n,N) & \xrightarrow{\varphi_N^*} & \operatorname{Hom}(A^m,N) \\ & & \uparrow & & \uparrow \\ & & \operatorname{Hom}(A^n,A^s) & \xrightarrow{\varphi^*} & \operatorname{Hom}(A^m,A^s) \\ & & \uparrow{\scriptstyle j} & & \uparrow{\scriptstyle i} \\ & & \operatorname{Hom}(A^n,A^r) & \longrightarrow & \operatorname{Hom}(A^m,A^r)\,, \end{array}$$

the maps being defined as in Lemma 2.1.5. In particular, $\varphi_N^*(\sigma) = \sigma \circ \varphi$, $\varphi^*(\sigma) = \sigma \circ \varphi$, $i(\sigma) = \psi \circ \sigma$, and $j(\sigma) = \psi \circ \sigma$. Lemma 2.1.25 and Proposition 2.4.3 below imply that

$$\operatorname{Hom}(M,N) = \operatorname{Ker}(\varphi_N^*) \cong \varphi^{*-1}\big(\operatorname{Im}(i)\big) \big/ \operatorname{Im}(j)\,.$$

Using the SINGULAR built–in command `modulo`, which is explained below, we have (identifying, as before, $\mathrm{Hom}(A^n, A^s) = A^{sn}$ and $\mathrm{Hom}(A^m, A^s) = A^{ms}$)

$$D := \varphi^{*-1}\big(\mathrm{Im}(i)\big) = \mathrm{Ker}\big(A^{ns} \xrightarrow{\overline{\varphi^*}} A^{ms}/\,\mathrm{Im}(i)\big) = \texttt{modulo}\,(\varphi^*, i)\,,$$

which is given by a $ns \times k$–matrix with entries in A, and we can compute $\mathrm{Hom}(M, N)$ as

$$\varphi^{*-1}\big(\mathrm{Im}(i)\big)/\,\mathrm{Im}(j) = A^k\big/\,\mathrm{Ker}\big(A^k \xrightarrow{\overline{D}} A^{ns}/\,\mathrm{Im}(j)\big) = A^k\big/\,\texttt{modulo}\,(D, j)\,.$$

Finally, we obtain the following procedure with $F = \varphi^*$, $B = i$, $C = j$.

```
proc Hom(matrix M, matrix N)
{
  matrix F = kontraHom(M,nrows(N));
  matrix B = kohom(N,ncols(M));
  matrix C = kohom(N,nrows(M));
  matrix D = modulo(F,B);
  matrix E = modulo(D,C);
  return(E);
}
```

Here is an example.

```
ring A=0,(x,y,z),dp;
matrix M[3][3]=1,2,3,
               4,5,6,
               7,8,9;
matrix N[2][2]=x,y,
               z,0;

print(Hom(M,N));      //a 6x6 matrix
//-> 0,0,0,0,y,x,
//-> 0,0,0,0,0,z,
//-> 1,0,0,0,0,0,
//-> 0,1,0,0,0,0,
//-> 0,0,1,0,0,0,
//-> 0,0,0,1,0,0
```

We explain the `modulo` command: let the matrices $M \in \mathrm{Mat}(m \times n, A)$, respectively $N \in \mathrm{Mat}(m \times s, A)$, represent linear maps

$$\begin{array}{ccc} A^n & \xrightarrow{\;M\;} & A^m \\ & & \uparrow{\scriptstyle N} \\ & & A^s\,. \end{array}$$

Then $\texttt{modulo}(M,N) = \mathrm{Ker}\big(A^n \xrightarrow{\overline{M}} A^m/\mathrm{Im}(N)\big)$, where $\overline{M}$ is the map induced by M; more precisely, $\texttt{modulo}(M,N)$ returns a set of vectors in A^n which generate $\mathrm{Ker}(\overline{M})$ [2]. Hence, `matrix(modulo(M,N))` is a presentation matrix for the quotient $(\mathrm{Im}(M)+\mathrm{Im}(N))/\mathrm{Im}(N)$. The computation is explained in SINGULAR Example 2.8.9.

Definition 2.1.27. Let M be an A–module. Then M is called *Noetherian* if every submodule $N \subset M$ is finitely generated.

Note that, in particular, a ring A is a Noetherian A–module if and only if it is a Noetherian ring (cf. Definition 1.3.4).

Lemma 2.1.28.

(1) Submodules and quotient modules of Noetherian modules are Noetherian.
(2) Let $N \subset M$ be A–modules, then M is Noetherian if and only if N and M/N are Noetherian.
(3) Let M be an A–module, then the following properties are equivalent:
  a) M is Noetherian.
  b) Every ascending chain of submodules

$$M_1 \subset M_2 \subset \ldots \subset M_k \subset \ldots$$

  becomes stationary.
  c) Every non–empty set of submodules of M has a maximal element (with regard to inclusion).

The proof is left as Exercise 2.1.9 (compare Proposition 1.3.6).

The following proposition relates Noetherian and finitely generated modules.

Proposition 2.1.29. *Let A be a Noetherian ring and M be a finitely generated A–module, then M is a Noetherian A–module.*

Proof. Using Lemma 2.1.22 and Lemma 2.1.28 we may assume that $M = A^n$ and prove the statement using induction on n. For $n = 1$ the statement follows by assumption. Let $n \geq 2$ and consider the projection $\pi : A^n \to A^{n-1}$, $(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_{n-1})$. Clearly, $\mathrm{Ker}(\pi) = \{(0, \ldots, 0, a) \mid a \in A\} \cong A$, and $A^{n-1} = A^n/\mathrm{Ker}(\pi)$. Hence, the result follows from Lemma 2.1.28 (2) and the induction hypothesis. □

Lemma 2.1.30 (Nakayama). *Let A be a ring and $I \subset A$ an ideal which is contained in the Jacobson radical of A. Let M be a finitely generated A–module and $N \subset M$ a submodule such that $M = IM + N$. Then $M = N$. In particular, if $M = IM$, then $M = 0$.*

[2] Using automatic type conversion, we can apply the `modulo`–command to modules as well as to matrices.

Proof. By passing to the quotient module it is enough to prove the lemma in the case $N = \langle 0 \rangle$. Assume $M \neq \langle 0 \rangle$ and let $m_1, \ldots, m_n$ be a minimal system of generators of M. Since $m_n \in M = IM$, we can choose $a_1, \ldots, a_n \in I$ such that $m_n = \sum_{i=1}^{n} a_i m_i$. This implies $(1 - a_n)m_n = \sum_{i=1}^{n-1} a_i m_i$.

By Exercise 1.4.4, $(1 - a_n)$ is a unit in A, and, therefore, $m_1, \ldots, m_{n-1}$ generate M, which is a contradiction to the minimality of the chosen system of generators. □

Corollary 2.1.31. *Let $(A, \mathfrak{m})$ be a local ring and M a finitely generated A–module. Let $m_1, \ldots, m_n \in M$ such that their classes form a system of generators for the $A/\mathfrak{m}$–vector space $M/\mathfrak{m}M$. Then $m_1, \ldots, m_n$ generate M.*

Proof. Let $N := \sum_i Am_i$ and consider the canonical map $N \to M \to M/\mathfrak{m}M$. This map is surjective, which implies $N + \mathfrak{m}M = M$. Thus, the corollary is a consequence of Lemma 2.1.30. □

Remark 2.1.32. With the assumptions of Corollary 2.1.31, $\{m_1, \ldots, m_n\}$ is a *minimal system of generators* of M if and only if their classes form a basis of $M/\mathfrak{m}M$, and then n is the dimension of the $A/\mathfrak{m}$–vector space $M/\mathfrak{m}M$.

Definition 2.1.33. Let $(A, \mathfrak{m})$ be a local ring and M an A–module. A presentation $A^m \xrightarrow{\varphi} A^n \to M \to 0$ of M is called a *minimal presentation* if $n = \dim_{A/\mathfrak{m}}(M/\mathfrak{m}M)$.

Note that $n = \dim_{A/\mathfrak{m}}(M/\mathfrak{m}M)$ if and only if $\varphi(A^m) \subset \mathfrak{m}A^n$, that is, the entries of the presentation matrix are in $\mathfrak{m}$ (Exercise 2.1.17).

How can we make a presentation φ of a module M minimal if it is not? If an entry φ_{ij} of φ is a unit, we can perform elementary row and column operations to produce a matrix $\tilde{\varphi}$ which has, except at position (i, j), only zeros in row i and column j. Elementary row, respectively column, operations mean that we multiply φ from the left, respectively right, with an invertible matrix. Hence $\mathrm{Coker}(\varphi) \cong \mathrm{Coker}(\tilde{\varphi})$, that is, $\tilde{\varphi}$ is a presentation matrix of a module isomorphic to M. But from $\tilde{\varphi}$ we can delete the ith row and the jth column without changing the cokernel.

Doing this, successively, with every entry which is a unit, we obtain a minimal presentation of (a module isomorphic to) M.

Note that this is nothing else but a Gauß reduction with a pivot element being a unit. If A is a field, then every element $\neq 0$ is a unit and we can carry out a complete Gauß reduction. The SINGULAR command `prune` produces a minimal presentation matrix.

SINGULAR Example 2.1.34 (minimal presentations, prune).

```
ring A=0,(x,y,z),ds;  //local ring with max. ideal <x,y,z>
module M=[0,xy-1,xy+1],[y,xz,xz];
print(M);
//-> 0,    y,
```

```
//-> -1+xy,xz,        //we have units in the first column
//-> 1+xy, xz

print(prune(M));
//-> -y+xy2,
//-> -2xz
```

Let $A = \mathbb{Q}[x,y,z]_{\langle x,y,z\rangle}$ and $N = A^3/M$, where M denotes the submodule of A^3 generated by the vectors $(0, xy-1, xy+1)$, (y, xz, xz). Then

$$A^2 \xrightarrow{\begin{pmatrix} 0 & y \\ xy-1 & xz \\ xy+1 & xz \end{pmatrix}} A^3 \longrightarrow N \longrightarrow 0$$

is a presentation. We computed, using the command `prune`, a minimal presentation of N:

$$A \xrightarrow{\begin{pmatrix} y-xy^2 \\ 2xz \end{pmatrix}} A^2 \longrightarrow N \longrightarrow 0\,.$$

```
ring B=0,(x,y,z),dp;              //non-local ring
module M=[0,xy-1,xy+1],[y,xz,xz]; //no units as entries
print(prune(M));
//-> 0,   y,
//-> xy-1,xz,
//-> xy+1,xz

M=[0,1,xy+1],[y,xz,xz];
print(M);
//-> 0,   y,
//-> 1,   xz,
//-> xy+1,xz

print(prune(M));
//-> y,
//-> -x2yz
```

Corollary 2.1.35 (Krull's intersection theorem). *Let A be a Noetherian ring, $I \subset A$ an ideal contained in the Jacobson radical and M a finitely generated A–module. Then $\bigcap_{k\in\mathbb{N}} I^k M = \langle 0\rangle$.*

Proof. Let $N := \bigcap_k I^k M$. N is a finitely generated A-module, since it is a submodule of the finitely generated module M over the Noetherian ring A. By Nakayama's Lemma it is sufficient to show that $IN = N$. Let

$$\mathfrak{M} := \{L \subset M \text{ submodule } \mid L \cap N = IN\}\,.$$

Since A is Noetherian, the set $\mathfrak{M}$ has a maximal element which we call L. It remains to prove that $I^k M \subset L$ for some k, because this implies

$N = I^k M \cap N \subset L \cap N = IN$. Since I is finitely generated, it suffices to prove that for any $x \in I$ there is some positive integer a such that $x^a M \subset L$. Let $x \in I$ and consider the chain of ideals $L :_M \langle x \rangle \subset L :_M \langle x^2 \rangle \subset \cdots$. This chain stabilizes because A is Noetherian.

Choose a with $L :_M \langle x^a \rangle = L :_M \langle x^{a+1} \rangle$. We claim that $x^a M \subset L$. By the maximality of L it is enough to prove that $(L + x^a M) \cap N \subset IN$ (note that, obviously, $IN \subset (L + x^a M) \cap N$). Let $m \in (L + x^a M) \cap N$, $m = n + x^a s$, with $n \in L$, $s \in M$. Now $xm - xn = x^{a+1} s \in IN + L = L$, which implies $s \in L :_M \langle x^{a+1} \rangle = L :_M \langle x^a \rangle$. Therefore, $x^a s \in L$ and, consequently, $m \in L$. This implies $m \in L \cap N = IN$. □

Definition 2.1.36. Let A be a ring, $S \subset A$ be a multiplicatively closed subset and M be an A–module.

(1) We define the *localization of M with respect to S*, $S^{-1}M$, as follows:

$$S^{-1}M := \left\{ \frac{m}{s} \;\middle|\; m \in M,\ s \in S \right\}$$

where m/s denotes the equivalence class of $(m, s) \in M \times S$ with respect to the following equivalence relation:

$$(m, s) \sim (m', s') :\Longleftrightarrow \exists\ s'' \in S, \text{ such that } s''(s'm - sm') = 0\,.$$

Moreover, on $S^{-1}M$ we define an addition and multiplication with ring elements by the same formulæ as for the quotient field (see before Definition 1.4.4). We shall also use the notation M_S instead of $S^{-1}M$. If $S = \{1, f, f^2, \ldots\}$ then we write M_f instead of $S^{-1}M$. If $S = A \setminus P$, P a prime ideal, we write M_P instead of $S^{-1}M$.

(2) Let $\varphi : M \to N$ be an A–module homomorphism, then we define the induced $S^{-1}A$–module homomorphism,

$$\varphi_S : M_S \longrightarrow N_S\,, \quad \frac{m}{s} \longmapsto \frac{\varphi(m)}{s}\,.$$

Note that the latter is, indeed, a well–defined $S^{-1}A$–module homomorphism (Exercise 2.1.19).

Proposition 2.1.37. *Let A be a ring, $S \subset A$ be a multiplicatively closed subset, M, N be A–modules and $\varphi : M \to N$ be an A–module homomorphism. Then*

(1) $\mathrm{Ker}(\varphi_S) = \mathrm{Ker}(\varphi)_S$.
(2) $\mathrm{Im}(\varphi_S) = \mathrm{Im}(\varphi)_S$.
(3) $\mathrm{Coker}(\varphi_S) = \mathrm{Coker}(\varphi)_S$.

In particular, localization with respect to S is an *exact functor*. That is, if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of A–modules, then $0 \to M'_S \to M_S \to M''_S \to 0$ is an exact sequence of A_S–modules (cf. Definition 2.4.1).

Proof. (1) follows, since $\varphi_S(m/s) = 0$ if and only if there exists some $s' \in S$ such that $s'\varphi(m) = 0$, that is, $s'm \in \mathrm{Ker}(\varphi)$. (2) is clear by definition of φ_S. Finally, using Exercise 2.1.20, we have

$$\mathrm{Coker}(\varphi_S) = N_S/\operatorname{Im}(\varphi_S) = N_S/\operatorname{Im}(\varphi)_S = \big(N/\operatorname{Im}(\varphi)\big)_S\,,$$

which implies (3). □

Proposition 2.1.38. *Let A be a ring, M be an A–module. The following conditions are equivalent:*

(1) $M = \langle 0\rangle$.
(2) $M_P = \langle 0\rangle$ *for all prime ideals* P.
(3) $M_{\mathfrak{m}} = \langle 0\rangle$ *for all maximal ideals in* $\mathfrak{m}$.

Proof. The only non–trivial part is to prove (3) $\Rightarrow$ (1). Let $m \in M$ and assume $\mathrm{Ann}(m) \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $m/1 \neq 0$ in $M_{\mathfrak{m}}$ contradicting the assumption $M_{\mathfrak{m}} = \langle 0\rangle$. This implies that the annihilator of every element $m \in M$ is A, that is, $M = \langle 0\rangle$, since $1 \in A$. □

Corollary 2.1.39. *Let A be ring, M, N A–modules, and $\varphi : M \to N$ an A–module homomorphism. Then φ is injective (respectively surjective) if and only if $\varphi_{\mathfrak{m}}$ is injective (respectively surjective) for all maximal ideals* $\mathfrak{m}$.[3]

Proof. The corollary is an immediate consequence of Proposition 2.1.37 and Proposition 2.1.38. □

Definition 2.1.40. Let A be a ring and M an A–module. The *support* of M, $\mathrm{supp}(M)$, is defined by

$$\mathrm{supp}(M) := \{P \subset A \text{ prime ideal } \mid M_P \neq \langle 0\rangle\}\,.$$

Lemma 2.1.41. *Let A be a ring and M a finitely generated A–module. Then* $\mathrm{supp}(M) = \{P \subset A \text{ prime ideal } \mid P \supset \mathrm{Ann}(M)\} =: V\big(\mathrm{Ann}(M)\big)$.

Proof. Assume that $\mathrm{Ann}(M) \not\subset P$, then there exists some $s \in \mathrm{Ann}(M)$ satisfying $s \notin P$. Let $m \in M$, then $sm = 0$. This implies $m/1 = sm/s = 0$ in M_P and, therefore, $M_P = \langle 0\rangle$.

On the other hand, if $M_P = \langle 0\rangle$, then $A_P = \mathrm{Ann}(M_P) = \big(\mathrm{Ann}(M)\big)_P$ (Exercise 2.1.24) implies that $\mathrm{Ann}(M) \not\subset P$. □

For flatness properties of $S^{-1}M$ see Exercise 7.3.1.

[3] This means that injectivity (respectively surjectivity) is a local property.

Exercises

2.1.1. Prove Lemma 2.1.4.

2.1.2. Let $\varphi : M \to N$ be a bijective module homomorphism. Show that φ^{-1} is a homomorphism.

2.1.3. Let A be a ring and M an A–module. Prove that $\mathrm{Hom}_A(A, M) \cong M$ and give an example which shows that, in general, $\mathrm{Hom}_A(M, A) \ncong M$.

2.1.4. Prove that isomorphisms between A–modules define an equivalence relation on the set of all A–modules.

2.1.5. Complete the proof of Lemma 2.1.5.

2.1.6. Prove Lemma 2.1.12.

2.1.7. Prove Lemma 2.1.15.

2.1.8. Prove Lemma 2.1.19.

2.1.9. Prove Lemma 2.1.28.

2.1.10. Let A be a ring, M an A–module and $I \subset A$ an ideal. Prove that M/IM has a canonical A/I–module structure.

2.1.11. Let A be a ring and $\varphi : A^n \to A^s$ an isomorphism of free A–modules. Prove that $n = s$.

2.1.12. Let A be a ring and M an A–module. Prove that M is, in a natural way, an $A/\operatorname{Ann}(M)$–module.

2.1.13. Let A be a ring and M an A–module. Prove that $\mathrm{Tors}(M)$ is a submodule of M.

2.1.14. Let A be a ring, and let $M = \bigoplus_{i=1}^n M_i$, N be A–modules. Prove that $\mathrm{Hom}_A(M, N) \cong \bigoplus_{i=1}^n \mathrm{Hom}_A(M_i, N)$, $\mathrm{Hom}_A(N, M) \cong \bigoplus_{i=1}^n \mathrm{Hom}_A(N, M_i)$. In particular, $\mathrm{Hom}(A^n, A^m) \cong A^{m \cdot n}$.

2.1.15. Let K be a field and M a $K[x]$–module which is finite dimensional as K–vector space. Prove that M is a torsion module.

2.1.16. Let A be an integral domain and $I \subset A$ be an ideal. Prove that I is a free A–module if and only if I can be generated by one element.

2.1.17. Let $(A, \mathfrak{m})$ be a local ring and M an A–module with presentation $A^m \xrightarrow{\varphi} A^n \to M \to 0$. Prove that this presentation is minimal if and only if $\varphi(A^m) \subset \mathfrak{m}A^n$.

2.1.18. Let $(A, \mathfrak{m})$ be a local ring and $A^m \cong A^s \oplus N$ for a suitable A–module N. Prove that $N \cong A^{m-s}$.

2.1.19. Prove (with the notations of Definition 2.1.36) that $S^{-1}M$ is an $S^{-1}A$–module. Prove that φ_S is well–defined and an $S^{-1}A$–module homomorphism.

2.1.20. Let A be a ring, $S \subset A$ be a multiplicatively closed subset and M, N be A–modules with $N \subset M$. Prove that $(M/N)_S \cong M_S/N_S$.

2.1.21. Prove that a module homomorphism is injective if and only if its kernel is zero.

2.1.22. Let A be a ring and $P_1, \ldots, P_m$ prime ideals. Let $\langle 0 \rangle \neq M$ be a finitely generated A–module such that $M_{P_j} \neq \langle 0 \rangle$ for all j. Prove that there exists $x \in M$ such that $x \notin P_j M_{P_j}$ for all j.

2.1.23. Let A be a ring, M an A–module and N, L submodules of M. Prove that $N = L$ if and only if $N_P = L_P$ for all prime ideals P.

2.1.24. Let A be a ring, $S \subset A$ be a multiplicatively closed subset and M a finitely generated A–module. Prove that $\operatorname{Ann}(S^{-1}M) = S^{-1}\operatorname{Ann}(M)$.

2.1.25. Compute the kernel and image of the following homomorphism: $A^3 \xrightarrow{M} A^2$ with $A = \mathbb{Q}[x, y, z]$ and $M = \left(\begin{smallmatrix} xy & xz & yz \\ x-1 & y-1 & z-1 \end{smallmatrix}\right)$.

2.1.26. Compute a minimal presentation of the A–module M with $M = A^3/\left\langle \begin{pmatrix} 1 \\ xy-1 \\ xz \end{pmatrix}, \begin{pmatrix} 0 \\ yz-1 \\ xy \end{pmatrix} \right\rangle$ and $A = \mathbb{Q}[x, y, z]_{\langle x,y,z \rangle}$.

2.1.27. Compute the support of the module of Exercise 2.1.26.

2.2 Graded Rings and Modules

Definition 2.2.1. A *graded ring* A is a ring together with a direct sum decomposition $A = \bigoplus_{\nu \geq 0} A_\nu$, where the A_ν are abelian groups satisfying $A_\nu A_\mu \subset A_{\nu+\mu}$ for all $\nu, \mu \geq 0$.

A *graded K–algebra*, K a field, is a K–algebra which is a graded ring such that A_ν is a K–vector space for all $\nu \geq 0$, and $A_0 = K$.

The A_ν are called *homogeneous components* and the elements of A_ν are called *homogeneous* elements of *degree* ν.

Remark 2.2.2. Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a graded ring, then A_0 is a subring of A. This follows since $1 \cdot 1 = 1$, hence $1 \in A_0$. For a K–algebra A, this implies already $K \subset A_0$, but to be a graded K–algebra we require even $K = A_0$.

Example 2.2.3.

(1) Let K be a field and $A = K[x_1, \ldots, x_n]$. Moreover, let $w = (w_1, \ldots, w_n)$ be a vector of positive integers, and let A_d be the K–vector space generated by all monomials x^α with $\text{w–deg}(x^\alpha) = d$. Then $A = \bigoplus_{\nu \geq 0} A_\nu$ is a graded K–algebra. Namely, $A_0 = K$, and for each i we have $x_i \in A_{w_i}$. The elements of A_d are called *quasihomogeneous* or *weighted homogeneous* polynomials of (*weighted*) *degree* d with respect to the weights $w_1, \ldots, w_n$. If $w_1 = \cdots = w_n = 1$ we obtain the usual notion of homogeneous polynomials.

(2) Let A be any ring, then $A_0 := A$ and $A_\nu := 0$ for $\nu > 0$ defines a (trivial) structure of a graded ring for A.
(3) Let A be a Noetherian K–algebra, $I \subset A$ be an ideal, then

$$\mathrm{Gr}_I(A) := \bigoplus_{\nu \geq 0} I^\nu / I^{\nu+1}$$

is a graded K–algebra in a natural way. If $(A, \mathfrak{m})$ is a local ring, then all homogeneous components of $\mathrm{Gr}_\mathfrak{m}(A) = \bigoplus_{\nu \geq 0} \mathfrak{m}^\nu / \mathfrak{m}^{\nu+1}$ are finite dimensional vector spaces over $A/\mathfrak{m}$.

Definition 2.2.4. Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a graded ring. An A–module M, together with a direct sum decomposition $M = \bigoplus_{\mu \in \mathbb{Z}} M_\mu$ into abelian groups is called a *graded A–module* if $A_\nu M_\mu \subset M_{\nu+\mu}$ for all $\nu \geq 0$, $\mu \in \mathbb{Z}$.

The elements from M_ν are called *homogeneous* of *degree* ν. If $m = \sum_\nu m_\nu$, $m_\nu \in M_\nu$ then m_ν is called the *homogeneous part of degree* ν of m.

Example 2.2.5. Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a graded K–algebra and consider the free module $A^m = \bigoplus_{i=1}^m A e_i$, $e_i = (0, \ldots, 1, \ldots, 0)$ with 1 at the i–th place. Let $\nu_1, \ldots, \nu_m \in \mathbb{Z}$, define $\deg(e_i) := \nu_i$, and let M_ν be the A_0–module generated by all $f e_i$ with $f \in A_{\nu - \nu_i}$, then $A^m = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$ is a graded A–module.

Definition 2.2.6. Let $M = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$ be a graded A–module and define $M(d) := \bigoplus_{\nu \in \mathbb{Z}} M(d)_\nu$ with $M(d)_\nu := M_{\nu+d}$. Then $M(d)$ is a graded A–module, especially $A(d)$ is a graded A–module. $M(d)$ is called the *d–th twist* or the *d–th shift* of M.

Lemma 2.2.7. *Let $M = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$ be a graded A–module and $N \subset M$ a submodule. The following conditions are equivalent:*

(1) N is graded with the induced grading, that is, $N = \bigoplus_{\nu \in \mathbb{Z}} (M_\nu \cap N)$.
(2) N is generated by homogeneous elements.
(3) Let $m = \sum m_\nu$, $m_\nu \in M_\nu$. Then $m \in N$ if and only if $m_\nu \in N$ for all ν.

The proof is easy and left as Exercise 2.2.1.

Definition 2.2.8. A submodule $N \subset M$, satisfying the equivalent conditions of Lemma 2.2.7, is called a *graded* (or *homogeneous*) submodule. A graded submodule of a graded ring is called a *graded ideal* or *homogeneous ideal* .

Remark 2.2.9. Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a graded ring, and let $I \subset A$ be a homogeneous ideal. Then the quotient A/I has an induced structure as graded ring: $A/I = \bigoplus_{\nu \geq 0} (A_\nu + I)/I \cong \bigoplus_{\nu \geq 0} A_\nu / (I \cap A_\nu)$.

Definition 2.2.10. Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a graded ring and $M = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$, $N = \bigoplus_{\nu \in \mathbb{Z}} N_\nu$ be graded A–modules. A homomorphism $\varphi : M \to N$ is called *homogeneous* (or *graded*) of degree d if $\varphi(M_\nu) \subset N_{\nu+d}$ for all ν. If φ is homogeneous of degree zero we call φ just *homogeneous*.

Example 2.2.11. Let M be a graded A–module and $f \in A_d$ then the multiplication with f defines a graded homomorphism $M \to M$ of degree d. It also defines a graded homomorphism $M \to M(d)$ of degree 0.

Lemma 2.2.12. *Let A be a graded ring and M, N be graded A–modules. Let $\varphi : M \to N$ be a homogeneous A–module homomorphism, then* $\mathrm{Ker}(\varphi)$, $\mathrm{Coker}(\varphi)$ *and* $\mathrm{Im}(\varphi)$ *are graded A–modules with the induced grading.*

Proof. Let $M = \bigoplus_{i\in\mathbb{Z}} M_i$ and $N = \bigoplus_{i\in\mathbb{Z}} N_i$, and define $K_i := \mathrm{Ker}(\varphi) \cap M_i$. Then, clearly, $\bigoplus_{i\in\mathbb{Z}} K_i \subset \mathrm{Ker}(\varphi)$. Moreover, let $m = \sum_{i=1}^{k} m_i$, $m_i \in M_i$ and assume that $\varphi(m) = 0$. Then $\varphi(m) = \sum_i \varphi(m_i) = 0$, with $\varphi(m_i) \in N_i$. This implies $\varphi(m_i) = 0$, that is, $m_i \in K_i$ and, therefore, $\mathrm{Ker}(\varphi) = \bigoplus_{i\in\mathbb{Z}} K_i$.
The other statements can be proved similarly. □

Example 2.2.13. Let A be a graded ring, $M = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$ a graded A–module and $N \subset M$ a homogeneous submodule. Let $N_\nu := N \cap M_\nu$, then the quotient M/N has an induced structure as graded A–module:

$$M/N = \bigoplus_{\nu\in\mathbb{Z}} (M_\nu + N)/N \cong \bigoplus_{\nu\in\mathbb{Z}} M_\nu/N_\nu\,.$$

Lemma 2.2.14. *Let $A = \bigoplus_{\nu\geq 0} A_\nu$ be a Noetherian graded K–algebra and $M = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$ be a finitely generated A–module. Then*

(1) there exist $m \in \mathbb{Z}$ such that $M_\nu = \langle 0\rangle$ for $\nu < m$;
(2) $\dim_K M_\nu < \infty$ *for all ν.*

Proof. (1) is obvious because M is finitely generated and a graded A–module. To prove (2) it is enough to prove that M_ν is a finitely generated A_0–module for all ν.

By assumption M is finitely generated and we may choose finitely many homogeneous elements $m_1, \ldots, m_k$ to generate M. Assume that $m_i \in M_{e_i}$ for $i = 1, \ldots, k$, then $\sum_i A_{n-e_i} \cdot m_i = M_n$ (with the convention $A_\nu = 0$ for $\nu < 0$). This implies that M_n is a finitely generated A_0–module because the A_ν are finitely generated A_0–modules. □

SINGULAR Example 2.2.15 (graded rings and modules).
We give examples here on how to work with graded rings and modules.

First we consider the ideal $\langle y^3 - z^2, x^3 - z\rangle$ in $A = \mathbb{Q}[x, y, z]$. This ideal is homogeneous if we consider $\mathbb{Q}[x, y, z]$ as a graded ring with weights $w_1 = 1$, $w_2 = 2$, $w_3 = 3$. Note that it is not homogeneous in $\mathbb{Q}[x, y, z]$ with the usual graduation.

```
ring A=0,(x,y,z),dp;
ideal I=y3-z2,x3-z;
qhweight(I);
//-> 1,2,3
```

The SINGULAR command `homog(I)` checks whether `I` is homogeneous with respect to the weights given to the variables of the basering (if no weights are assigned explicitly, all weights are assumed to be 1).

```
homog(I);
//-> 0

ring B=0,(x,y,z),wp(1,2,3);
ideal I=fetch(A,I);
homog(I);
//-> 1
```

Next we consider $B = \mathbb{Q}[x, y, z]$ as a graded ring with weights $w_1 = 1$, $w_2 = 2$, $w_3 = 3$, and a B–module $M = \left\langle \begin{pmatrix} y^3-z^2 \\ x^3-z \end{pmatrix}, \begin{pmatrix} x^3 \\ 1 \end{pmatrix} \right\rangle$. Then M is a homogeneous submodule of B^2 if we consider B^2 as graded B–module with $\deg\big((1,0)\big) = 0$ and $\deg\big((0,1)\big) = 3$. This can be seen as follows:

```
module M=[y3-z2,x3-z],[x3,1];
homog(M);
//-> 1
```

M is homogeneous. SINGULAR defines internally a corresponding *attribute*.

```
attrib(M,"isHomog");      //asks for attributed weights
//-> 0,3
```

The degree of (1,0) is 0 and the degree of (0,1) is 3.

The grading for M being homogeneous is not uniquely determined. We can also use $\deg\big((1,0)\big) = 4$ and $\text{degree}\big((0,1)\big) = 7$.

```
intvec v=4,7;
attrib(M,"isHomog",v);    //sets externally an attribute,
attrib(M,"isHomog");      //without changing the module
//-> 4,7
```

Exercises

2.2.1. Prove Lemma 2.2.7.

2.2.2. Prove the remaining statements of Lemma 2.2.12.

2.2.3. Let A be a graded ring and M a graded A–module. Show that the annihilator $\text{Ann}_A(M)$ is a homogeneous ideal.

2.2.4. Let I_1, I_2 be homogeneous ideals in a graded ring. Show that $I_1 + I_2$, $I_1 \cdot I_2$, $I_1 \cap I_2$, $I_1 : I_2$ and $\sqrt{I_1}$ are homogeneous.

2.2.5. Let A be a graded ring. A homogeneous ideal $I \subset A$ is prime if and only if for any two *homogeneous* elements $f, g \in A$, $f \cdot g \in I$ implies $f \in I$ or $g \in I$.

2.2.6. Prove the homogeneous version of Nakayama's Lemma: let A be a graded K–algebra and $\mathfrak{m}$ the ideal generated by the elements of positive degree. Let M be a finitely generated, graded A–module and $N \subset M$ a graded submodule. If $N + \mathfrak{m}M = M$ then $N = M$.

2.2.7. Test whether the following ideals in $K[x, y, z]$ are homogeneous w.r.t. suitable weights, $\langle y^5 - z^2,\ x^3 - z,\ x^6 - y^5 \rangle$, $\langle y^5 - z^2,\ x^3 - z,\ x^7 - y^5 \rangle$.

2.3 Standard Bases for Modules

For our intended applications of standard bases, but also for an elegant proof of Buchberger's standard basis criterion, we have to extend the notion of monomial orderings to the free module $K[x]^r = \bigoplus_{i=1}^r K[x]e_i$, where

$$e_i = (0, \ldots, 1, \ldots, 0) \in K[x]^r$$

denotes the i–th canonical basis vector of $K[x]^r$ with 1 at the i–th place. We call

$$x^\alpha e_i = (0, \ldots, x^\alpha, \ldots, 0) \in K[x]^r$$

a *monomial (involving component i)*.

Definition 2.3.1. Let $>$ be a monomial ordering on $K[x]$. A *(module) monomial ordering* or a *module ordering* on $K[x]^r$ is a total ordering $>_m$ on the set of monomials $\{x^\alpha e_i \mid \alpha \in \mathbb{N}^n, i = 1, \ldots, r\}$, which is compatible with the $K[x]$–module structure including the ordering $>$, that is, satisfying

(1) $x^\alpha e_i >_m x^\beta e_j \implies x^{\alpha+\gamma} e_i >_m x^{\beta+\gamma} e_j$,
(2) $x^\alpha > x^\beta \implies x^\alpha e_i >_m x^\beta e_i$,

for all $\alpha, \beta, \gamma \in \mathbb{N}^n$, $i, j = 1, \ldots, r$.

Two module orderings are of particular practical interest:

$$x^\alpha e_i > x^\beta e_j :\Longleftrightarrow i < j \text{ or } (i = j \text{ and } x^\alpha > x^\beta),$$

giving priority to the components, denoted by $(c, >)$, and

$$x^\alpha e_i > x^\beta e_j :\Longleftrightarrow x^\alpha > x^\beta \text{ or } (x^\alpha = x^\beta \text{ and } i < j),$$

which gives priority to the monomials in $K[x]$, denoted by $(>, c)$.
Note that, by the second condition of Definition 2.3.1, each component of $K[x]^r$ carries the ordering of $K[x]$. Hence, $>_m$ is a well-ordering on $K[x]^r$ if and only if $>$ is a well–ordering on $K[x]$. We call $>_m$ *global*, respectively *local*, respectively *mixed*, if this holds for $>$ respectively.

In the case of a well–ordering it makes sense to define a module ordering without fixing a ring ordering, only requiring (1) (cf. [53]). In the general case, this could lead to standard bases which do not generate the module (Exercise 2.3.5).

Now we fix a module ordering $>_m$ and denote it also with $>$. Since any vector $f \in K[x]^r \setminus \{0\}$ can be written uniquely as

$$f = cx^\alpha e_i + f^*$$

with $c \in K \setminus \{0\}$ and $x^\alpha e_i > x^{\alpha^*} e_j$ for any non–zero term $c^* x^{\alpha^*} e_j$ of f^* we can define as before

$$\begin{aligned} \mathrm{LM}(f) &:= x^\alpha e_i\,, \\ \mathrm{LC}(f) &:= c\,, \\ \mathrm{LT}(f) &:= cx^\alpha e_i \end{aligned}$$

and call it the *leading monomial*, *leading coefficient* and *leading term*, respectively, of f. $\mathrm{tail}(f) := f - \mathrm{LT}(f)$ is called the *tail* of f. Moreover, for $G \subset K[x]^r$ we call

$$L_>(G) := L(G) := \langle\, \mathrm{LM}(g) \mid g \in G \setminus \{0\} \,\rangle_{K[x]} \subset K[x]^r$$

the *leading submodule* of $\langle G \rangle$. In particular, if $I \subset K[x]^r$ is a submodule, then $L_>(I) = L(I)$ is called the *leading module* of I.

As from $K[x]$ to $K[x]_>$ these definitions carry over naturally from $K[x]^r$ to $K[x]^r_>$.

Note that the set of monomials of $K[x]^r$ may be identified with $\mathbb{N}^n \times E^r \subset \mathbb{N}^n \times \mathbb{N}^r = \mathbb{N}^{n+r}$, $E^r = \{e_1, \ldots, e_r\}$ where e_i is considered as an element of $\mathbb{N}^r$. The natural partial order on $\mathbb{N}^{n+r}$ induces a partial order $\geq_{\mathrm{nat}}$ on the set of monomials, which is given by

$$x^\alpha e_i \leq_{\mathrm{nat}} x^\beta e_j \;:\Longleftrightarrow\; i = j \text{ and } x^\alpha \mid x^\beta \;\Longleftrightarrow:\; x^\alpha e_i \mid x^\beta e_j$$

(we say that $x^\beta e_j$ is *divisible by* $x^\alpha e_i$ if $i = j$ and $x^\alpha \mid x^\beta$). For any set of monomials $G \subset K[x]^r$ and any monomial $x^\alpha e_i$, we have

$$x^\alpha e_i \notin \langle G \rangle_{K[x]} \iff x^\alpha e_i \text{ is not divisible by any element of } G.$$

Hence, Dickson's Lemma for $\mathbb{N}^m$ (m arbitrary) is equivalent to the statement that any monomial submodule of $K[x]^r$ (r arbitrary) is finitely generated.

Let $>$ be a fixed monomial ordering. Again we write

$$R := K[x]_> = S_>^{-1} K[x]$$

to denote the localization of $K[x]$ with respect to $>$. Since $R^r \subset K[[x]]^r$, we can talk about the power series expansion of elements of R^r.

The theory of standard bases for ideals carries over to modules almost without any changes. We formulate the relevant definitions and theorems but omit the proofs, since they are practically identical to the ideal case.

We fix a module ordering on R^r. As for ideals, we define:

Definition 2.3.2.

(1) Let $I \subset R^r$ be a submodule. A finite set $G \subset I$ is called a *standard basis* of I if and only if $L(G) = L(I)$, that is, for any $f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $\mathrm{LM}(g) \mid \mathrm{LM}(f)$.
(2) If the ordering is a well–ordering then a standard basis G is called a *Gröbner basis*. In this case $R = K[x]$ and, hence, $G \subset I \subset K[x]^r$.
(3) A set $G \subset R^r$ is called *interreduced* if $0 \notin G$ and if $\mathrm{LM}(g) \notin L(G \setminus \{g\})$ for each $g \in G$. An interreduced standard basis is also called *minimal*.
(4) For $f \in R^r$ and $G \subset R^r$ we say that f is *reduced with respect to* G if no monomial of the power series expansion of f is contained in $L(G)$.
(5) A set $G \subset R^r$ is called *reduced* if $0 \notin G$ and if each $g \in G$ is reduced with respect to $G \setminus \{g\}$, $\mathrm{LC}(g) = 1$, and if, moreover, $\mathrm{tail}(g)$ is reduced with respect to G. For $>$ a well–ordering, this just means that for each $g \in G \subset K[x]^r$, $\mathrm{LM}(g)$ does not divide any monomial of any element of $G \setminus \{g\}$.

Definition 2.3.3. Let $\mathcal{G}$ denote the set of all finite ordered subsets $G \subset R^r$.

(1) A map
$$\mathrm{NF} : R^r \times \mathcal{G} \to R^r,\ (f, G) \mapsto \mathrm{NF}(f \mid G)\,,$$
is called a *normal form* on R^r if for all $f \in R^r$ and $G \in \mathcal{G}$, $\mathrm{NF}(0 \mid G) = 0$, and
   a) $\mathrm{NF}(f \mid G) \neq 0 \Rightarrow \mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G)$,
   b) If $G = \{g_1, \ldots, g_s\}$ then $f - \mathrm{NF}(f|g)$ (or f) has a *standard representation* with respect to $\mathrm{NF}(- \mid G)$, that is,
$$f - \mathrm{NF}(f \mid G) = \sum_{i=1}^{s} a_i g_i,\ \ a_i \in R\,,\ \ s \geq 0\,,$$
   satisfying $\mathrm{LM}(\sum_{i=1}^{s} a_i g_i) \geq \mathrm{LM}(a_i g_i)$ for all i such that $a_i g_i \neq 0$.
   NF is called a *reduced normal form* if, moreover, $\mathrm{NF}(f \mid G)$ is reduced with respect to G for all $G \in \mathcal{G}$.
(2) NF is called a *weak normal form* if, instead of b), only condition b') holds:
   b') for each $f \in R^r$ and each $G \in \mathcal{G}$ there exists a unit $u \in R$ such that uf has a standard representation with respect to $\mathrm{NF}(- \mid G)$.
(3) Similarly to Definition 1.6.5 (2) *polynomial weak normal forms* are defined.

Remark 2.3.4. In the same manner as for ideals, a reduced normal form exists for global orderings. We just have to apply $\mathrm{NF}(- \mid G)$ not only to f but successively to $\mathrm{tail}(f)$ until it terminates (cf. Algorithm 1.6.11). For non–global orderings, this procedure may not terminate.

However, for an arbitrary module ordering $>$, we can always find a weak normal form NF with the following property which is stronger than 1.a from Definition 2.3.3: if, for any $f \in K[x]^r$ and $G = \{g_1, \ldots, g_s\} \in \mathcal{G}$,

$$\mathrm{NF}(f \mid G) = f_1 e_1 + \cdots + f_r e_r \in K[x]^r \,,$$

then $\mathrm{LM}(f_i e_i) \notin L(G)$ for all i with $f_i \neq 0$.

Proof. We may assume that $\mathrm{LM}(f_1 e_1) = \mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G)$ and proceed by induction on r, to show that we can successively reduce $\sum_{j=1}^{r} f_j e_j$ with respect to G to obtain the above property. Let $f^{(2)} := f_2 e_2 + \cdots + f_r e_r$, and let $G^{(2)} := \{g \in G \mid \mathrm{LM}(g) \notin K[x]e_1\}$. We consider the images

$$\overline{f}^{(2)} := \pi(f^{(2)}) \,, \quad \overline{G}^{(2)} := \pi(G^{(2)})$$

under the canonical projection $\pi : \bigoplus_{i=1}^{r} Re_i \to \bigoplus_{i=2}^{r} Re_i$. Then, by induction hypothesis, we can assume that there exists a weak normal form

$$\mathrm{NF}\big(\overline{f}^{(2)} \mid \overline{G}^{(2)}\big) = f_2^{(2)} e_2 + \cdots + f_r^{(2)} e_r$$

such that $\mathrm{LM}(f_j^{(2)} e_j) \notin L(\overline{G}^{(2)}) = L(G) \cap \bigoplus_{i=2}^{r} K[x]e_i$ for $j = 2, \ldots, r$. Let

$$u^{(2)} \overline{f}^{(2)} = \sum_{j=2}^{r} f_j^{(2)} e_j + \sum_{g \in G^{(2)}} a_g^{(2)} \overline{g}$$

be a standard representation with respect to $\overline{G}^{(2)}$ ($u^{(2)}$ a unit in R). Then, by construction,

$$u^{(2)} f^{(2)} - \sum_{g \in G^{(2)}} a_g^{(2)} g = f_1^{(2)} e_1 + \sum_{j=2}^{r} f_j^{(2)} e_j$$

for some $f_1^{(2)}$ such that either $\mathrm{LM}(f_1^{(2)} e_1) \leq \mathrm{LM}(f^{(2)})$ or $f_1^{(2)} = 0$. Now, it is easy to see that

$$(u^{(2)} f_1 + f_1^{(2)}) e_1 + \sum_{j=2}^{r} f_j^{(2)} e_j$$

is a weak normal form for f with respect to G with the required property. □

Lemma 2.3.5. *Let $I \subset R^r$ be a submodule, $G \subset I$ a standard basis of I and $\mathrm{NF}(- \mid G)$ a weak normal form on R^r with respect to G.*

(1) For any $f \in R^r$ we have $f \in I$ if and only if $\mathrm{NF}(f \mid G) = 0$.

(2) If $J \subset R^r$ is a submodule with $I \subset J$, then $L(I) = L(J)$ implies $I = J$.
(3) $I = \langle G \rangle_R$, that is, G generates I as an R–module.
(4) If $\mathrm{NF}(\_ \mid G)$ is a reduced normal form, then it is unique.

The proof is the same as for ideals. Also the notion of s–polynomial carries over to modules.

Definition 2.3.6. Let $f, g \in R^r \setminus \{0\}$ with $\mathrm{LM}(f) = x^\alpha e_i$, $\mathrm{LM}(g) = x^\beta e_j$. Let

$$\gamma := \mathrm{lcm}(\alpha, \beta) := \big(\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n)\big)$$

be the least common multiple of α and β and define the s–polynomial of f and g to be

$$\mathrm{spoly}(f, g) := \begin{cases} x^{\gamma-\alpha} f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot x^{\gamma-\beta} g, & \text{if } i = j \\ 0, & \text{if } i \neq j\,. \end{cases}$$

Definition 2.3.7. For a monomial $x^\alpha e_i \in K[x]^r$ set

$$\deg x^\alpha e_i := \deg x^\alpha = \alpha_1 + \cdots + \alpha_n\,.$$

For $f \in K[x]^r \setminus \{0\}$, let $\deg f$ be the maximal degree of all monomials occurring in f. We define the *ecart* of f as

$$\mathrm{ecart}\,(f) := \deg f - \deg \mathrm{LM}(f)\,.$$

Similarly to Definition 1.7.5 one can define the weighted ecart and interpret the ecart as $\deg_t\big(\mathrm{LM}(f^h)\big)$ for the homogenization of f with respect to a new variable t.

The Algorithms 1.6.10 (NFBuchberger), 1.6.11 (redNFBuchberger) carry over verbatim to the module case if we replace $K[x]$ by $K[x]^r$. Similarly for the Algorithms 1.7.1 (Standard), 1.7.6 (NFMora) and 1.7.8 (StandardBasis). However, for the sake of completeness, we shall formulate them for modules, omitting the proofs.

Let $>$ be any monomial ordering on R^r and assume that a weak normal form algorithm NF on R^r is given.

Algorithm 2.3.8 (Standard(G,NF)).

Input: $G \in \mathcal{G}$, NF a weak normal form algorithm.
Output: $S \in \mathcal{G}$ such that S is a standard basis of $I = \langle G \rangle_R \subset R^r$.

- $S = G$;
- $P = \{(f, g) \mid f, g \in S,\ f \neq g\}$;

- while $(P \neq \emptyset)$
  choose $(f, g) \in P$;
  $P = P \setminus \{(f, g)\}$;
  $h = \mathrm{NF}\big(\mathrm{spoly}(f, g) \mid S\big)$;
  If $(h \neq 0)$
    $P = P \cup \{(h, f) \mid f \in S\}$;
    $S = S \cup \{h\}$;
- return S;

Let $>$ be any monomial ordering on $K[x]^r$, $R = K[x]_>$.

Algorithm 2.3.9 (NFMora($f \mid G$)).

Input: $f \in K[x]^r$, $G = \{g_1, \ldots, g_s\} \subset K[x]^r$.

Output: $h \in K[x]^r$ a weak normal form of f with respect to G, such that there exists a standard representation $uf = h + \sum_{i=1}^{s} a_i g_i$ with $a_i \in K[x]$, $u \in S_>$.

- $h = f$;
- $T = G$;
- while$\big(h \neq 0$ and $T_h = \big\{g \in T \mid \mathrm{LM}(g)$ divides $\mathrm{LM}(h)\big\} \neq \emptyset\big)$
  choose $g \in T_h$ with ecart(g) minimal;
  if (ecart$(g) >$ ecart(h))
    $T = T \cup \{h\}$;
  $h = \mathrm{spoly}(h, g)$;
- return h;

SINGULAR Example 2.3.10 (normal form).

```
ring A=0,(x,y,z),(c,dp);
module I=[x,y,1],[xy,z,z2];
vector f=[zx,y2+yz-z,y];
reduce(f,I);
//-> // ** I is no standardbasis
//-> [0,y2-z,y-z]

reduce(f,std(I));
//-> [0,0,z2-z]
```

We have seen in SINGULAR Example 1.6.13 that the normal form may not be unique, in particular, if we do not have a standard basis for I.

Let $>$ be any monomial ordering on $K[x]^r$, $R = K[x]_>$.

Algorithm 2.3.11 (StandardBasis(G)).

Input: $G = \{g_1, \ldots, g_s\} \subset K[x]^r$.

Output: $S = \{h_1, \ldots, h_t\} \subset K[x]^r$ such that S is a standard basis of $I = \langle G \rangle_R \subset R^r$.

- $S =$ STANDARD(G,NFMORA);
- return S;

SINGULAR Example 2.3.12 (standard bases).
The example shows the influence of different orderings to standard bases.

```
ring A=0,(x,y,z),(c,dp);
module I=[x+1,y,1],[xy,z,z2];
std(I);
//-> _[1]=[0,xy2-xz-z,-xz2+xy-z2]
//-> _[2]=[y,y2-z,-z2+y]
//-> _[3]=[x+1,y,1]

ring B=0,(x,y,z),dp;
module I=fetch(A,I);
std(I);
//-> _[1]=x*gen(1)+y*gen(2)+gen(3)+gen(1)
//-> _[2]=y2*gen(2)-z2*gen(3)+y*gen(3)+y*gen(1)-z*gen(2)

ring C=0,(x,y,z),lp;
module I=fetch(A,I);
std(I);
//-> _[1]=y2*gen(2)+y*gen(3)+y*gen(1)-z2*gen(3)-z*gen(2)
//-> _[2]=x*gen(1)+y*gen(2)+gen(3)+gen(1)

ring D=0,(x,y,z),(c,ds);
module I=fetch(A,I);
std(I);
//-> _[1]=[1+x,y,1]
//-> _[2]=[0,z+xz-xy2,-xy+z2+xz2]

ring E=0,(x,y,z),ds;
module I=fetch(A,I);
std(I);
//-> _[1]=gen(3)+gen(1)+x*gen(1)+y*gen(2)
//-> _[2]=z*gen(2)+xy*gen(1)+z2*gen(3)
```

Similarly to Chapter 1 we also have *Buchberger's criterion*.

Theorem 2.3.13. *Let $I \subset R^r$ be a submodule and $G = \{g_1, \ldots, g_s\} \subset I$. Let $\mathrm{NF}(- \mid G)$ be a weak normal form on R^r with respect to G. Then the following are equivalent:*

(1) G is a standard basis of I.

(2) $\mathrm{NF}(f \mid G) = 0$ *for all* $f \in I$.
(3) Each $f \in I$ *has a standard representation with respect to* $\mathrm{NF}(- \mid G)$.
(4) G *generates* I *and* $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) = 0$ *for* $i, j = 1, \ldots, s$.
(5) G *generates* I *and* $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G_{ij}\big) = 0$ *for some* $G_{ij} \subset G$ *and* $i, j = 1, \ldots, s$.

Proof. The proof of $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5)$ is similar to the proof of Theorem 1.7.3.

The proof of $(5) \Rightarrow (1)$ will be given in Section 2.5. This proof needs the equivalence of (1) and (2). We prove now that $(2) \Rightarrow (1)$. Let $f \in I$ then (2) implies $\mathrm{NF}(f \mid G) = 0$, and there exists a unit $u \in R^*$ such that uf has a standard representation $uf = \sum_i a_i g_i$ with $\mathrm{LM}(f) \geq \mathrm{LM}(a_i g_i)$. Therefore, there exists some i such that $\mathrm{LM}(f) = \mathrm{LM}(a_i g_i)$. This implies that $\mathrm{LM}(g_i) \mid \mathrm{LM}(f)$, which proves that G is a standard basis of I. □

Exercises

2.3.1. Verify that the proofs for Lemma 2.3.5 and that the algorithms carry over from the ideal case of Chapter 1.

2.3.2. Let $R = K[x]$, and let $M = (m_{ij})$ be an $n \times n$–matrix with entries in R. Consider the matrix (M, E) obtained by concatenating M with the $n \times n$–unit matrix E, and let $v_1, \ldots, v_n \in R^{2n}$ be the rows of (M, E). On the free R–module $R^{2n} = \bigoplus_{i=1}^{2n} Re_i$, $e_1 = (1, 0, \ldots, 0)$, $\ldots$, $e_{2n} = (0, \ldots, 0, 1)$, consider the ordering defined by $x^\alpha e_i < x^\beta e_j$ if $i > j$ or if $i = j$ and $x^\alpha < x^\beta$.

Let $\{w_1, \ldots, w_m\} \subset R^{2n}$ be the reduced standard basis of $\langle v_1, \ldots, v_n \rangle$, with $\mathrm{LM}(w_1) > \cdots > \mathrm{LM}(w_m)$. Prove that M is invertible if and only if $m = n$ and $\mathrm{LM}(w_i) = e_i$ for $i = 1, \ldots, m$, and then $w_1, \ldots, w_m$ are the rows of (E, M^{-1}).

2.3.3. Let $I \subset K[x]^r$ be a submodule, $x = (x_1, \ldots, x_n)$, and let $>$ be a global module ordering on $K[x]^r$. Prove that

$$K[x]^r \;\cong\; I \oplus \left(\bigoplus_{m \notin L[I]} K \cdot m \right) \quad .$$

2.3.4. Compute the normal form of $\binom{x+y}{y-1}$ w.r.t. the module $M \subset K[x, y]^2$ generated by the vectors $\binom{x^2}{xy}$, $\binom{x}{y^2}$, and the ordering `(c,dp)`.

2.3.5. Let K be a field and $R = K[x]$ the polynomial ring in one variable. Consider on $K[x]^2$ the following ordering:

$$\begin{aligned} x^\alpha e_i > x^\beta e_j \;:\Longleftrightarrow\; & i > j \;\text{ or }\; (i = j = 1 \text{ and } \alpha < \beta) \\ & \text{or }\; (i = j = 2 \text{ and } \alpha > \beta)\,. \end{aligned}$$

Prove that $\{(1+x)e_1,\, e_2\}$ is a standard basis of $K[x]^2$ (w.r.t. $>$), but it does not generate $K[x]^2$ (as $K[x]$-module).

The following exercises (2.3.6) – (2.3.12) are related to the behaviour of *standard bases under specialization*. Let, in these exercises, R be an integral domain, $R[x] = R[x_1, \ldots, x_n]$, and let $>$ be a fixed monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$. The set $S_> = \{f \in R[x] \mid \mathrm{LT}(F) = 1\}$ is multiplicatively closed and the localization of $R[x]$ with respect to $S_>$ is

$$R[x]_> = S_>^{-1}R[x] = \left\{ \frac{f}{g} \;\middle|\; f, g \in R[x],\, \mathrm{LT}(g) = 1 \right\} .$$

If $>$ is global, then $R[x]_> = R[x]$ and if $>$ is local then $R[x]_> = R[x]_{\langle x_1,\ldots,x_n\rangle}$, the localization of $R[x]$ with respect to the prime ideal $\langle x_1, \ldots, x_n\rangle$ (check this).

2.3.6. Let $\mathcal{G}$ denote the set of finite ordered sets $G \subset R[x]^r_>$, where $>$ is a fixed module ordering on the set of monomials $\{x^\alpha e_i\}$. Call a function

$$\mathrm{NF} : R[x]^r_> \times \mathcal{G} \to R[x]^r_>,\ (f, g) \mapsto \mathrm{NF}(f \mid G)\,,$$

a *pseudo normal form* on $R[x]^r_>$, if the following holds:

(1) $\mathrm{NF}(f \mid G) \neq 0 \Rightarrow \mathrm{LM}\big(\mathrm{NF}(f \mid G)\big)$ is not divisible by $\mathrm{LM}(g)$ for all $g \in G$.
(2) For all $f \in R[x]^r_>$ and $G = \{g_1, \ldots, g_s\} \in \mathcal{G}$ there exists a $u \in R[x]_>$ with $\mathrm{LT}(u)$ a product of leading coefficients of elements of G such that uf has a standard representation with respect to $\mathrm{NF}(- \mid G)$, that is,

$$uf = \mathrm{NF}(f \mid G) + \sum_{i=1}^{s} a_i g_i,\ a_i \in R[x]_>\,,$$

such that $\mathrm{LM}(r) \geq \mathrm{LM}(a_i g_i)$ for all i with $a_i g_i \neq 0$.

NF is called *polynomial* if, for $f \in R[x]^r$, $G \subset R[x]^r$, then $u, a_i \in R[x]$. Define, in this situation, the s–polynomial of $f, g \in R[x]_> \setminus \{0\}$, $\mathrm{LT}(f) = ax^\alpha e_i$, $\mathrm{LT}(g) = bx^\beta e_j$, as

$$\mathrm{spoly}\,(f, g) = \begin{cases} bx^{\gamma-\alpha}f - ax^{\gamma-\beta}g & \text{if } i = j\,, \\ 0 & \text{if } i \neq j\,, \end{cases}$$

where $\gamma = \mathrm{lcm}(\alpha, \beta)$.

Show the following: if we use this definition of s–polynomial, the algorithms NFBuchberger (for global orderings), respectively NFMora (for arbitrary orderings) from Chapter 1, Section 1.6, respectively Chapter 2, Section 2.3, define a pseudo normal form on $R[x]^r_>$ (where the element u itself from (2) is a product of leading coefficients of elements of G for NFBuchberger). We call NFBuchberger, respectively NFMora, with the above s–polynomial *normal forms without division* .

2.3.7. Show the following generalization of *Buchberger's criterion*.
Let $I \subset R[x]^r_>$ be a $R[x]_>$–submodule, NF a pseudo normal form on $R[x]^r_>$ and $G = \{g_1, \ldots, g_0\} \subset I$ satisfying

(1) G generates I as $R[x]_>$–module;
(2) $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) = 0$ for all $1 \leq i < j \leq s$.

Then, for any maximal ideal $\mathfrak{m} \subset R$ such that $\mathrm{LC}(g_i) \notin \mathfrak{m}$ for all i, the set $\{\overline{g_1}, \ldots, \overline{g_s}\}$ is a standard basis of $I \cdot (R/\mathfrak{m})[x]_>$. Here $\overline{g_i}$ denotes the residue class of g_i in $(R/\mathfrak{m})[x]$.
(Hint: compare the proof of Theorem 2.5.9.)

We call G a *pseudo standard basis* of I if it satisfies the above conditions (1) and (2). Show that Algorithm 2.3.8, STANDARD(G,NF), returns a pseudo standard basis if NF is a pseudo normal form. (Note that a pseudo standard basis is not a standard basis over a ring, as defined in Remark 1.6.14.)

2.3.8. Let K be a field, $R = K[t] = K[t_1, \ldots, t_p]$, $K[t, x] = R[x_1, \ldots, x_n]$ and $\{g_1, \ldots, g_s\} \subset K[t, x]^r$ a pseudo standard basis of the submodule $I \subset K[t, x]^r_>$. Set $h_i = \mathrm{LC}(g_i) \in K[t]$ and $h = h_1 \cdot \ldots \cdot h_s$. Then, for any t_0 with $h(t_0) \neq 0$, show that $\{g_1(t_0, x), \ldots, g_s(t_0, x)\}$ is a standard basis of $(I|_{t=t_0})K[x]_>$.

2.3.9. Let $\{g_1, \ldots, g_s\} \subset \mathbb{Z}[x]^r = \mathbb{Z}[x_1, \ldots, x_n]^r$ be a pseudo standard basis of the submodule $I \subset \mathbb{Z}[x]^r_>$. Set $m_i = \mathrm{LC}(g_i) \in \mathbb{Z}$ and $m = m_1 \cdot \ldots \cdot m_s$. Then, for any prime number p such that $p \nmid m$, $\{\overline{g_1}, \ldots, \overline{g_s}\}$ is a standard basis of $I \cdot \mathbb{Z}/p\mathbb{Z}[x]_>$.

2.3.10. Consider $f := x^3 + y^3 + z^4 + ax^2yz + bxy^2z$, where a and b are parameters. Let $d := \dim_K K[x, y, z]/\langle f_x, f_y, f_z\rangle$, where K is the field $\mathbb{Q}$ or $\mathbb{F}_p$, p a prime. Hence, $d = d(a, b, p)$ depends on $(a, b) \in K^2$ and the characteristic p ($p = 0$ if $K = \mathbb{Q}$). Show

(1) $d(a, b, p) < \infty$ if and only if $p \notin \{2, 3\}$.
(2) For $p \notin \{2, 3\}$, we have

$$\begin{array}{ll} d(a,b,p) = 24 & \text{if } a \neq 0 \text{ and } b \neq 0 \text{ and } a^3 \neq b^3 \\ d(0,b,p) = 21 & \text{if } b \neq 0 \\ d(a,0,p) = 21 & \text{if } a \neq 0 \\ d(a,a,p) = 15 & \text{if } a \neq 0 \\ d(0,0,p) = 12\,. & \end{array}$$

(Hint: use the previous exercises.)

Note that SINGULAR avoids divisions in standard basis computations if the options `intStrategy` and `contentSB` are set.

2.3.11. Let $M = M(a, b) \subset \mathbb{Q}^2$ be the submodule generated by the vectors $[ax^2, (a + 3b)x^3y + z^4]$, $[(a - 2b)3y^3 + xyz, by^3]$, $[5az^4, (a + b)z^2]$ with a, b parameters. Compute a *comprehensive Gröbner basis* of M, that is, a system of generators which is a Gröbner basis of $M(a, b)$ for all $a, b \in \mathbb{Q}$ for the ordering `(c,ds)`.

(Hint: start with a Gröbner basis in the `ring R=(0,a,b),(x,y,z),(c,ds)` and then distinguish cases, as in Exercise 2.3.10, and take the union of all Gröbner bases.)

2.3.12. Show that the system of equations

$$\begin{array}{ll} x^3+yz+y+z=0 & x+y=1 \\ y^4+xz+x+z=0 & x+z=1 \\ z^5+xy+x+y=0 & y+z=1 \end{array}$$

has no solution in $\overline{\mathbb{F}}_p^3$ for *all* prime numbers p, where $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$.

2.4 Exact Sequences and free Resolutions

Definition 2.4.1. A sequence of A–modules and homomorphisms

$$\cdots \to M_{k+1} \xrightarrow{\varphi_{k+1}} M_k \xrightarrow{\varphi_k} M_{k-1} \to \cdots$$

is called a *complex* if $\operatorname{Ker}(\varphi_k) \supset \operatorname{Im}(\varphi_{k+1})$. It is called *exact at* M_k if

$$\operatorname{Ker}(\varphi_k) = \operatorname{Im}(\varphi_{k+1})\,.$$

It is called *exact* if it is exact at all M_k. An exact sequence

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

is called a *short exact sequence*.

Example 2.4.2.

(1) $0 \to M \xrightarrow{\varphi} N$ is exact if and only if φ is injective.
(2) $M \xrightarrow{\varphi} N \to 0$ is exact if and only if φ is surjective.
(3) $0 \to M \xrightarrow{\varphi} N \to 0$ is exact if and only if φ is an isomorphism.
(4) $0 \to M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$ is a short exact sequence if and only if φ is injective, ψ is surjective and ψ induces an isomorphism $M_2/\operatorname{Im}(\varphi) \cong M_3$.
(5) $0 \to M_1 \xrightarrow{\varphi} M_1 \oplus M_2 \xrightarrow{\psi} M_2 \to 0$ with $\varphi(x) = (x,0)$, $\psi(x,y) = y$ is exact.

Proposition 2.4.3. *Let M', M, M'' be A–modules.*

(1) Let $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ be a complex. The complex is exact if and only if, for all A–modules N, the sequence

$$0 \to \operatorname{Hom}(M'',N) \xrightarrow{\psi^*} \operatorname{Hom}(M,N) \xrightarrow{\varphi^*} \operatorname{Hom}(M',N)$$

is exact. Here $\psi^*(\lambda) := \lambda \circ \psi$ and $\varphi^*(\sigma) := \sigma \circ \varphi$.

(2) Let $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$ *be a complex. The complex is exact if and only if, for all* A*–modules* N*,*

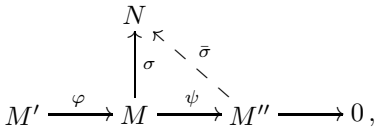
$$0 \to \mathrm{Hom}(N, M') \xrightarrow{\varphi_*} \mathrm{Hom}(N, M) \xrightarrow{\psi_*} \mathrm{Hom}(N, M'')$$

is exact. Here $\varphi_*(\lambda) = \varphi \circ \lambda$ *and* $\psi_*(\sigma) = \psi \circ \sigma$*.*

Proof. We prove (1). The proof of (2) is similar and left as Exercise 2.4.4. Assume that $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ is exact and consider the sequence

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{\psi^*} \mathrm{Hom}(M, N) \xrightarrow{\varphi^*} \mathrm{Hom}(M', N)\,,$$

which is a complex, since $\varphi^* \circ \psi^* = (\psi \circ \varphi)^*$. We have to show that it is, indeed, exact: let $\psi^*(\lambda) = \lambda \circ \psi = 0$, then, since ψ is surjective, $\lambda = 0$. Hence, ψ^* is injective. Let $\sigma \in \mathrm{Hom}(M, N)$ with $\varphi^*(\sigma) = \sigma \circ \varphi = 0$,



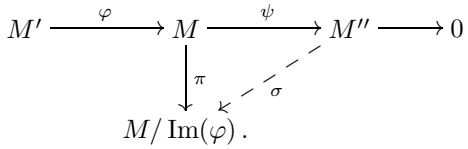
and define $\bar\sigma : M'' \to N$ by $\bar\sigma(m'') = \sigma(m)$ for some $m \in M$ with $\psi(m) = m''$. $\bar\sigma$ is well–defined because $\mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$ and $\sigma \circ \varphi = 0$. We have $\psi^*(\bar\sigma) = \sigma$ and, hence, $\mathrm{Im}(\psi^*) \supset \mathrm{Ker}(\varphi^*)$.

Assume now that $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\psi^*} \mathrm{Hom}(M, N) \xrightarrow{\varphi^*} \mathrm{Hom}(M', N)$ is exact for all A–modules N, that is,

- ψ^* is injective;
- $\mathrm{Im}(\psi^*) = \mathrm{Ker}(\varphi^*)$.

To prove that ψ is surjective, we consider $N := M''/\,\mathrm{Im}(\psi)$ and the canonical map $\pi : M'' \to N$. Then $\psi^*(\pi) = \pi \circ \psi = 0$. Because ψ^* is injective we obtain $\pi = 0$ and, therefore, $N = 0$, that is, ψ is surjective.

To prove that $\mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$ we choose $N = M/\,\mathrm{Im}(\varphi)$ and $\pi : M \to N$ the canonical morphism. Then $\varphi^*(\pi) = \pi \circ \varphi = 0$. Hence, $\pi \in \mathrm{Im}(\psi^*)$, that is, $\pi = \psi^*(\sigma) = \sigma \circ \psi$ for a suitable $\sigma : M'' \to N$, as shown in the diagram



This implies that $\mathrm{Im}(\varphi) \supset \mathrm{Ker}(\psi)$, the inverse inclusion being satisfied by assumption. □

Remark 2.4.4. Let

$$0 \to M_n \xrightarrow{\varphi_n} M_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \to M_2 \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0 \to 0$$

be a sequence of A–modules. The sequence is exact if and only if $\mathrm{Im}(\varphi_1) = M_0$, $\mathrm{Ker}(\varphi_n) = 0$ and $\mathrm{Ker}(\varphi_i) = \mathrm{Im}(\varphi_{i+1})$ for $i = 1, \ldots, n-1$. If the sequence is exact, this defines short exact sequences

$$\begin{array}{l} 0 \to \mathrm{Ker}(\varphi_1) \to M_1 \xrightarrow{\varphi_1} \mathrm{Im}(\varphi_1) \to 0 \\ 0 \to \mathrm{Ker}(\varphi_2) \to M_2 \xrightarrow{\varphi_2} \mathrm{Im}(\varphi_2) \to 0 \\ \vdots \qquad\qquad\qquad\quad \vdots \\ 0 \to \mathrm{Ker}(\varphi_n) \to M_n \xrightarrow{\varphi_n} \mathrm{Im}(\varphi_n) \to 0\,. \end{array}$$

Conversely, if short exact sequences

$$\begin{array}{l} 0 \to K_1 \to M_1 \to M_0 \to 0 \\ 0 \to K_2 \to M_2 \to K_1 \to 0 \\ \vdots \qquad\quad \vdots \\ 0 \to 0 \to M_n \to K_{n-1} \to 0 \end{array}$$

are given, then they obviously lead to a long exact sequence

$$0 \to M_n \to M_{n-1} \to \cdots \to M_1 \to M_0 \to 0\,.$$

Definition 2.4.5. Let A be a ring and $\mathcal{C}$ be a class of A–modules. A map $\lambda : \mathcal{C} \to \mathbb{Z}$ is called *additive function* if $\lambda(M) = \lambda(M') + \lambda(M'')$ for every short exact sequence $0 \to M' \to M \to M'' \to 0$ with $M', M, M'' \in \mathcal{C}$.

Example 2.4.6.

(1) Let K be a field and $\mathcal{C}$ be the class of all finite dimensional K–vector spaces. Then $\lambda : \mathcal{C} \to \mathbb{Z}$ defined by $\lambda(V) = \dim_K(V)$ is additive.
(2) Let $\mathcal{C}$ be the class of finitely generated abelian groups, that is, finitely generated $\mathbb{Z}$–modules. It will be proved in Section 2.6 that every finitely generated $\mathbb{Z}$–module M decomposes as $M = F \oplus \mathrm{Tors}(M)$, with F a free module. Defining $\lambda(M) = \mathrm{rank}(F)$ we obtain an additive map $\lambda : \mathcal{C} \to \mathbb{Z}$.

Proposition 2.4.7. *Let $\mathcal{C}$ be a class of A–modules which contains all submodules and factor modules of each of its elements and let $\lambda : \mathcal{C} \to \mathbb{Z}$ be additive. If*

$$0 \to M_n \xrightarrow{\varphi_n} M_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \to M_1 \xrightarrow{\varphi-1} M_0 \to 0$$

is an exact sequence with $M_0, \ldots, M_n \in \mathcal{C}$, then $\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$.

Proof. We consider the short exact sequences

$$0 \longrightarrow \operatorname{Ker}(\varphi_i) \longrightarrow M_i \longrightarrow \operatorname{Im}(\varphi_i) \longrightarrow 0\,, \quad i = 1, \ldots, n\,.$$

The additivity of λ implies

$$\begin{aligned}
\lambda(M_1) &= \lambda\big(\operatorname{Ker}(\varphi_1)\big) + \lambda(M_0)\,,\\
\lambda(M_2) &= \lambda\big(\operatorname{Ker}(\varphi_2)\big) + \lambda\big(\operatorname{Ker}(\varphi_1)\big)\,,\\
&\vdots\\
\lambda(M_n) &= \lambda\big(\operatorname{Ker}(\varphi_n)\big) + \lambda\big(\operatorname{Ker}(\varphi_{n-1})\big)\,.
\end{aligned}$$

Taking the alternating sum, we obtain

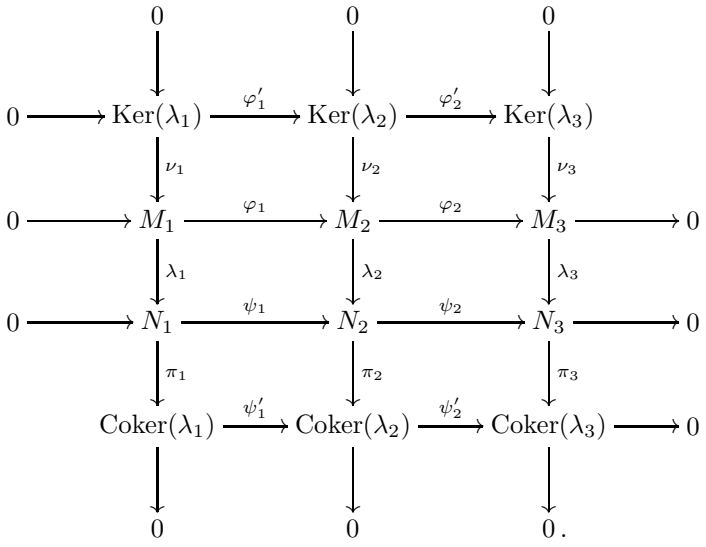
$$\sum_{i=1}^{n}(-1)^{i-1}\lambda(M_i) = \lambda(M_0) + (-1)^{n-1}\lambda\big(\operatorname{Ker}(\varphi_n)\big)\,.$$

But $\operatorname{Ker}(\varphi_n) = 0$ and λ being additive implies that $\lambda\big(\operatorname{Ker}(\varphi_n)\big) = 0$. □

Lemma 2.4.8 (Snake Lemma). *Let* $0 \to M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \to 0$ *and* $0 \to N_1 \xrightarrow{\psi_1} N_2 \xrightarrow{\psi_2} N_3 \to 0$ *be short exact sequences of A–modules. Moreover, let* $\lambda_i : M_i \to N_i$, $i = 1, 2, 3$, *be module homomorphisms such that the induced diagram commutes, that is,* $\lambda_3 \circ \varphi_2 = \psi_2 \circ \lambda_2$ *and* $\lambda_2 \circ \varphi_1 = \psi_1 \circ \lambda_1$. *Then there is an exact sequence*

$$\begin{aligned}
0 \to \operatorname{Ker}(\lambda_1) \to \operatorname{Ker}(\lambda_2) \to \operatorname{Ker}(\lambda_3)&\\
\to \operatorname{Coker}(\lambda_1) \to \operatorname{Coker}(\lambda_2) \to \operatorname{Coker}(\lambda_3) \to 0\,.&
\end{aligned}$$

Proof. The sequences $0 \to \operatorname{Ker}(\lambda_i) \xrightarrow{\nu_i} M_i \xrightarrow{\lambda_i} N_i \xrightarrow{\pi_i} \operatorname{Coker}(\lambda_i) \to 0$ are exact and lead to the following diagram:



It is not difficult to see that the canonically defined φ_i' (restriction of the φ_i) and ψ_i' make the diagram commutative, that is,

$$\pi_3 \circ \psi_2 = \psi_2' \circ \pi_2, \;\; \pi_2 \circ \psi_1 = \psi_1' \circ \pi_1, \;\; \varphi_2 \circ \nu_2 = \nu_3 \circ \varphi_2' ,$$
$$\nu_2 \circ \varphi_1' = \varphi_1 \circ \nu_1, \;\; \lambda_3 \circ \varphi_2 = \psi_2 \circ \lambda_2 \text{ and } \lambda_2 \circ \varphi_1 = \psi_1 \circ \lambda_1 .$$

We have to prove that the first and the last row are exact. This is left as an exercise.

The important part of the proof is to define the connecting homomorphism $d : \mathrm{Ker}(\lambda_3) \to \mathrm{Coker}(\lambda_1)$ and prove that $\mathrm{Ker}(d) = \mathrm{Im}(\varphi_2')$ and $\mathrm{Im}(d) = \mathrm{Ker}(\psi_1')$.

Let $x \in \mathrm{Ker}(\lambda_3)$ and choose $y \in M_2$ with $\varphi_2(y) = x$.[4] Then

$$0 = \lambda_3(x) = \lambda_3 \circ \varphi_2(y) = \psi_2 \circ \lambda_2(y) .$$

The exactness of the third row of the diagram implies that there exists a unique $z \in N_1$ with $\psi_1(z) = \lambda_2(y)$. We define $d(x) := \pi_1(z)$.

We have to prove that this definition is independent of the choice of y. Let $\overline{z} \in N_1$ with $\psi_1(\overline{z}) = \lambda_2(\overline{y})$ and $\varphi_2(\overline{y}) = x$. Then $\varphi_2(y - \overline{y}) = 0$ implies that $y - \overline{y} = \varphi_1(u)$ for a suitable $u \in M_1$. Therefore,

$$\psi_1(z - \overline{z}) = \lambda_2(y - \overline{y}) = \lambda_2 \circ \varphi_1(u) = \psi_1 \circ \lambda_1(u) .$$

But ψ_1 is injective, hence $z = \overline{z} + \lambda_1(u)$. It follows that $\pi_1(z) = \pi_1(\overline{z})$. This proves that d is well–defined.

It is not difficult to see that d is, indeed, a module homomorphism. We shall prove now that $\mathrm{Ker}(d) = \mathrm{Im}(\varphi_2')$.

Let $x \in \mathrm{Ker}(d)$. This implies, by definition of d, that there exist $z \in N_1$ and $y \in M_2$ such that $\psi_1(z) = \lambda_2(y)$, $\varphi_2(y) = x$ and $\pi_1(z) = 0$. Let $u \in M_1$ such that $z = \lambda_1(u)$. Then $\lambda_2(y) = \psi_1(z) = \psi_1 \circ \lambda_1(u) = \lambda_2 \circ \varphi_1(u)$, whence, $y - \varphi_1(u) \in \mathrm{Ker}(\lambda_2)$. But $\varphi_2'\big(y - \varphi_1(u)\big) = \varphi_2\big(y - \varphi_1(u)\big) = \varphi_2(y) = x$. It follows that $\mathrm{Ker}(d) \subset \mathrm{Im}(\varphi_2')$.

On the other hand, let $x \in \mathrm{Im}(\varphi_2')$. Then $x = \varphi_2(y)$, $y \in \mathrm{Ker}(\lambda_2)$ implies $\psi_1(0) = 0 = \lambda_2(y)$, that is, $d(x) = 0$ by definition of d. Thus we have shown the equality $\mathrm{Ker}(d) = \mathrm{Im}(\varphi_2')$.

To prove that $\mathrm{Im}(d) = \mathrm{Ker}(\psi_1')$ let $\overline{x} \in \mathrm{Im}(d)$, that is, $\overline{x} = \pi_1(z)$ such that there exists a $y \in M_2$ with $\lambda_2(y) = \psi_1(z)$. But

$$0 = \pi_2 \circ \lambda_2(y) = \pi_2 \circ \psi_1(z) = \psi_1' \circ \pi_1(z) = \psi_1'(\overline{z})$$

and, therefore, $\mathrm{Im}(d) \subset \mathrm{Ker}(\psi_1')$. Now let $\overline{z} \in \mathrm{Ker}(\psi_1')$ and choose a preimage $z \in N_1$, $\pi(z) = \overline{z}$. Then $0 = \psi_1'(\overline{z}) = \psi_1' \circ \pi_1(z) = \pi_2 \circ \psi_1(z)$. Therefore, there exists some $y \in M_2$ with $\lambda_2(y) = \psi_1(z)$. Then $\overline{z} = d\big(\varphi_2(y)\big)$, which proves that $\mathrm{Ker}(\psi_1') \subset \mathrm{Im}(d)$. □

[4] Since ν_3 is the canonical inclusion, we simplify the notations by identifying $\nu_3(x)$ and x.

Proposition 2.4.9. *Let*

$$\cdots \to M_{k+1} \xrightarrow{\varphi_{k+1}} M_k \xrightarrow{\varphi_k} M_{k-1} \to \dots$$

be an exact sequence of A–modules and $x \in A$ a non–zerodivisor for all M_k, then the induced sequence

$$\cdots \to M_{k+1}/xM_{k+1} \to M_k/xM_k \to M_{k-1}/xM_{k-1} \to \dots$$

is exact.

Proof. Because of Remark 2.4.4 it is enough to prove the proposition for short exact sequences. Consider an exact sequence

$$0 \to M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \to 0$$

then the multiplication by x induces injective maps $M_i \to M_i$, $i = 1, 2, 3$. Using the Snake Lemma (Lemma 2.4.8) we obtain that the induced sequence

$$0 \to M_1/xM_1 \to M_2/xM_2 \to M_3/xM_3 \to 0$$

is exact. □

Definition 2.4.10. Let A be a ring and M a finitely generated A–module. A *free resolution* of M is an exact sequence [5]

$$\dots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \dots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$

with finitely generated free A–modules F_i for $i \geq 0$. We say that a free resolution has *(finite) length* n if $F_k = 0$ for all $k > n$ and n is minimal with this property.

If $(A, \mathfrak{m})$ is a local ring, then a free resolution as above is called *minimal* if $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ for $k \geq 1$, and then $b_k(M) := \operatorname{rank}(F_k)$, $k \geq 0$, is called the *k–th Betti number* of M.

The following theorem shows that the Betti numbers of M are, indeed, well–defined.

Theorem 2.4.11. *Let $(A, \mathfrak{m})$ be a local Noetherian ring and M be a finitely generated A–module, then M has a minimal free resolution. The rank of F_k in a minimal free resolution is independent of the resolution. If M has a minimal resolution of finite length n,*

[5] Frequently the complex of free A-modules

$$F_\bullet : \dots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \dots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow 0$$

is called a free resolution of M.

$$0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

and if

$$0 \to G_m \to G_{m-1} \to \cdots \to G_0 \to M \to 0$$

is any free resolution, then $m \geq n$.

Proof. Let $m_1, \ldots, m_{s_0}$ be a minimal set of generators of M and consider the surjective map $\varphi_0 : F_0 := A^{s_0} \to M$ defined by $\varphi_0(a_1, \ldots, a_{s_0}) = \sum_{i=1}^{s_0} a_i m_i$. Because of Nakayama's Lemma, $m_1, \ldots, m_{s_0}$ induces a basis of the vector space $M/\mathfrak{m}M$. Hence, φ_0 induces an isomorphism $\overline{\varphi}_0 : F_0/\mathfrak{m}F_0 \cong M/\mathfrak{m}M$. Let K_1 be the kernel of φ_0. Then $K_1 \subset \mathfrak{m}F_0$. K_1 is a submodule of a finitely generated module over a Noetherian ring, hence finitely generated. As before, we can find a surjective map $F_1 := A^{s_1} \to K_1$, where s_1 is the minimal number of generators of K_1.

Let $\varphi_1 : F_1 \to F_0$ be defined by the composition $F_1 \to K_1 \hookrightarrow F_0$. As $K_1 \subset \mathfrak{m}F_0$, it follows that $\varphi_1(F_1) \subset \mathfrak{m}F_0$. Up to now, we have constructed the exact sequence $F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$.

Continuing like this we obtain a minimal free resolution for M. To show the invariance of the Betti numbers, we consider two minimal resolutions of M:

$$\cdots \xrightarrow{\varphi_{n+1}} F_k \to \ldots \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$
$$\cdots \xrightarrow{\psi_{n+1}} G_k \to \ldots \xrightarrow{\psi_1} G_0 \xrightarrow{\psi_0} M \to 0\,.$$

We have $F_0/\mathfrak{m}F_0 \cong M/\mathfrak{m}M \cong G_0/\mathfrak{m}G_0$ and, therefore, $\operatorname{rank}(F_0) = \operatorname{rank}(G_0)$. Let $\{f_1, \ldots, f_{s_0}\}$, respectively $\{g_1, \ldots, g_{s_0}\}$, be bases of F_0, respectively G_0. As $\{\psi_0(g_i)\}$ generate M, we have $\varphi_0(f_i) = \sum_j h_{ij} \cdot \psi_0(g_j)$ for some $h_{ij} \in A$. The matrix (h_{ij}) defines a map $h_1 : F_0 \to G_0$. The induced map $\overline{h}_1 : F_0/\mathfrak{m}F_0 \to G_0/\mathfrak{m}G_0$ is an isomorphism. In particular, we derive that $\det(h_{ij}) \neq 0 \mod \mathfrak{m}$. This implies that $\det(h_{ij})$ is a unit in A and h_1 is an isomorphism. Especially, h_1 induces an isomorphism $\operatorname{Ker}(\varphi_0) \xrightarrow{\sim} \operatorname{Ker}(\psi_0)$. As φ_1 and ψ_1, considered as matrices, have entries in $\mathfrak{m}$, and since we have surjections $F_1 \to \operatorname{Ker}(\varphi_0)$ and $G_1 \to \operatorname{Ker}(\psi_0)$, it follows, as before, that $\operatorname{rank}(F_1) = \operatorname{rank}(G_1)$. Now we can continue like this and obtain the invariance of the Betti numbers.

To prove the last statement, let

$$0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

be a minimal free resolution with $F_n \neq \langle 0 \rangle$ and

$$0 \to G_m \to G_{m-1} \to \cdots \to G_0 \to M \to 0$$

be any free resolution. We have to prove that $m \geq n$. This can be proved in a similar way to the previous step. With the same idea, one can prove that there are injections $h_i : F_i \to G_i$ for all $i \leq n$. □

SINGULAR Example 2.4.12 (resolution and Betti numbers).
SINGULAR has several commands, based on different algorithms, to compute free resolutions, see also Section 2.5. `mres` computes, for modules over local rings and for homogeneous modules over graded rings (cf. Definition 2.4.13), a minimal free resolution. More precisely, let $A = \texttt{matrix}(I)$, then `mres(I,k)` computes a free resolution of $\mathrm{Coker}(A) = F_0/I$ [6]

$$\ldots \to F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \to F_0/I \to 0\,,$$

where the columns of the matrix φ_1 are a minimal set of generators of I if the basering is local or if I is homogeneous. If k is not zero then the computation stops after k steps and returns a list of modules $M_i = \texttt{module}(\varphi_i)$, $i = 1 \ldots k$. `mres(I,0)` stops computation after, at most, $n+2$ steps, where n is the number of variables of the basering. Note that the latter suffices to compute all non-zero modules of a minimal free resolution if the basering is not a quotient ring (cf. Theorem 2.5.15).

In some cases it is faster to use the SINGULAR commands `res` (or `sres`, or `lres`) and then to apply `minres` to minimize the computed resolution.

```
ring A=0,(x,y),(c,ds);
ideal I=x,y;
resolution Re=mres(I,0);
```

Typing `Re;` displays a pictorial description of the computed resolution, where the exponents are the ranks of the free modules and the lower index i corresponds to the index of the respective free module F_i in the resolution of $M = A/I$ (see Definition 2.4.10).

```
Re;
//->  1      2      1
//-> A  <-- A  <-- A
//->
//-> 0      1      2
```

The corresponding list of matrices φ_i is displayed when typing `print(Re);`. More precisely, `Re[i]` $= \mathrm{Im}(\varphi_i)$, hence the columns of φ_i are given by the generators of `Re[i]`.

```
print(Re);
//-> [1]:
//->    _[1]=x
//->    _[2]=y
//-> [2]:
//->    _[1]=[y,-x]
```

[6] To obtain a minimal free resolution of F_0/I, use `mres(prune(I),0)`.

This is an example of the resolution of $\mathbb{Q} = A/\langle x, y\rangle$, as $A = \mathbb{Q}[x,y]_{\langle x,y\rangle}$–module:

$$0 \to \mathbb{Q}[x,y]_{\langle x,y\rangle} \xrightarrow{\binom{y}{-x}} \mathbb{Q}[x,y]^2_{\langle x,y\rangle} \xrightarrow{(x,y)} \mathbb{Q}[x,y]_{\langle x,y\rangle} \to \mathbb{Q} \to 0\ .$$

We can see that the Betti numbers $b_k(A/\langle x,y\rangle)$ are 1, 2 and 1. Let us compute them with SINGULAR:

```
betti(Re);          //intmat of Betti numbers
//-> 1,2,1
```

Now we consider an example of a cyclic infinite minimal resolution of the module $M = R^2/\langle \binom{x}{0}, \binom{0}{y}\rangle$ over the local ring $R = A/\langle xy\rangle$ with $A = \mathbb{Q}[x,y]_{\langle x,y\rangle}$.

```
qring R=std(xy);
module M=[x,0],[0,y];
resolution Re=mres(M,4);     //mres(M,k) stops at F_k
Re;
//->  2      2      2      2      2
//-> R  <-- R  <-- R  <-- R  <-- R
//->
//-> 0      1      2      3      4
```

Let us have a look at the matrices in the computed resolution:

```
print(Re);
//-> [1]:
//->    _[1]=[x]
//->    _[2]=[0,y]
//-> [2]:
//->    _[1]=[y]
//->    _[2]=[0,x]
//-> [3]:
//->    _[1]=[x]
//->    _[2]=[0,y]
//-> [4]:
//->    _[1]=[y]
//->    _[2]=[0,x]
```

Definition 2.4.13. Let K be a field, A be a graded K–algebra and M a graded A–module: a *homogeneous free resolution* of M is a resolution

$$\cdots \to F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \to \ldots \xrightarrow{\varphi_1} F_0 \to M \to 0$$

such that the F_k are finitely generated free A–modules,

$$F_k = \bigoplus_{j\in\mathbb{Z}} A(-j)^{b_{j-k,k}}\ ,$$

and the φ_k are homogeneous maps (of degree 0). Such a resolution is called *minimal*, if $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$, where $\mathfrak{m}$ is the ideal generated by all elements of positive degree. Then the numbers $b_{j,k} =: b_{j,k}(M)$ are called *graded Betti numbers* of M and $b_k(M) := \sum_j b_{j,k}(M)$ is called the *k–th Betti number* of M.

The following theorem shows that the graded Betti numbers of M are well–defined.

Theorem 2.4.14. *Let K be a field, A be a graded K–algebra and M be a finitely generated graded A–module. Then M has a minimal free resolution. The numbers $b_{j,k}$ and, in particular, the rank of F_k, in a minimal free resolution are independent of the resolution.*

The proof is similar to the proof of Theorem 2.4.11 and left as Exercise 2.4.3.

SINGULAR Example 2.4.15 (homogeneous resolution and graded Betti numbers).
We compute a minimal resolution of a homogeneous module $M = A/I$, with $A = \mathbb{Q}[w, x, y, z]$ and $I = \langle xyz, wz, x + y\rangle$, and compute its graded Betti numbers.

```
ring A = 0,(w,x,y,z),(c,dp);
ideal I = xyz, wz, x+y;
resolution Re = mres(I,0);
Re;
//->  1      3      3      1
//-> A <--  A <--  A <--  A
//->
//-> 0      1      2      3

print(Re);       //display the matrices in the resolution
//-> [1]:
//->    _[1]=x+y
//->    _[2]=wz
//->    _[3]=y2z
//-> [2]:
//->    _[1]=[0,y2,-w]
//->    _[2]=[wz,-x-y]
//->    _[3]=[y2z,0,-x-y]
//-> [3]:
//->    _[1]=[x+y,y2,-w]
//-> [4]:
//->    _[1]=0
```

To show the correct format of the matrices, we use `print(matrix(Re[i]))`:

```
print(matrix(Re[2]));
//-> 0, wz,  y2z,
//-> y2,-x-y,0,
//-> -w,0,   -x-y
```

We compute the matrix of graded Betti numbers $\big(b_{j,k}(A/I)\big)$: [7]

```
betti(Re);
//-> 1,1,0,0,
//-> 0,1,1,0,
//-> 0,1,2,1
```

The print command allows attributes, like `"betti"`, to format the output:

```
print(betti(Re),"betti");   //display graded Betti numbers
//->            0     1     2     3
//-> ----------------------------
//->     0:     1     1     -     -
//->     1:     -     1     1     -
//->     2:     -     1     2     1
//-> ----------------------------
//-> total:     1     3     3     1
```

Hence, we have computed the following (minimal) homogeneous free resolution (written as displayed by `Re;`):

$$0 \longleftarrow A/I \longleftarrow A(0) \xleftarrow{(x+y,wz,xyz)} \begin{matrix} A(-1) \\ \oplus \\ A(-2) \\ \oplus \\ A(-3) \end{matrix} \xleftarrow{\begin{pmatrix} 0 & wz & y^2z \\ y^2 & -x-y & 0 \\ -w & 0 & -x-y \end{pmatrix}} \begin{matrix} A(-4) \\ \oplus \\ A(-3) \\ \oplus \\ A(-4) \end{matrix} \xleftarrow{\begin{pmatrix} x+y \\ yz \\ -w \end{pmatrix}} A(-5) \longleftarrow 0\,.$$

Exercises

2.4.1. Let M, N be A–modules and $0 \to M \xrightarrow{\varphi} N \xrightarrow{\psi} A^s \to 0$ be an exact sequence, then this sequence splits, that is, there exists an isomorphism $\lambda : M \oplus A^s \to N$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & A^s & \longrightarrow & 0 \\ & & \| & & \uparrow{\scriptstyle \lambda} & & \| & & \\ 0 & \longrightarrow & M & \xrightarrow[i]{} & M \oplus A^s & \xrightarrow[\pi]{} & A^s & \longrightarrow & 0 \end{array}$$

is commutative ($\lambda \circ i = \varphi,\ \psi \circ \lambda = \pi$).

[7] Note that $b_{j,k}(I) = b_{j-1,k+1}(A/I)$ for all $k \geq 0$.

2.4.2. Let $A = \mathbb{Q}[x,y]_{\langle x,y\rangle}/\langle xy\rangle$. Compute the Betti numbers of the A–module $M = \langle \binom{x^2}{y}, \binom{x}{y} \rangle$.

2.4.3. Prove Theorem 2.4.14.
(Hint: Use the fact that kernel and image of a homogeneous map are graded with the induced grading and choose in every step a minimal system of generators using Nakayama's Lemma (Exercise 2.2.6)).

2.4.4. Prove (2) of Proposition 2.4.3.

2.4.5. With the notations of the Snake Lemma (Lemma 2.4.8) prove that

(1) $0 \to \mathrm{Ker}(\lambda_1) \to \mathrm{Ker}(\lambda_2) \to \mathrm{Ker}(\lambda_3)$,
(2) $\mathrm{Coker}(\lambda_1) \to \mathrm{Coker}(\lambda_2) \to \mathrm{Coker}(\lambda_3) \to 0$,

are exact sequences.

2.4.6. Let A be a ring and $S \subset A$ a multiplicatively closed subset. Let $M' \to M \to M''$ be an exact sequence of A–modules. Prove that the induced sequence $M'_S \to M_S \to M''_S$ of $S^{-1}A$–modules is exact.

2.4.7. Let A be a ring and $\cdots \to M_{i+1} \to M_i \to M_{i-1} \to \cdots$ be a complex of A–modules. Prove that the complex is exact if and only if the induced complexes $\cdots \to (M_{i+1})_P \to (M_i)_P \to (M_{i-1})_P \to \cdots$ of A_P–modules are exact for all prime ideals $P \subset A$.

2.4.8. Compute a minimal free resolution of $\mathbb{Q}$ as $\mathbb{Q}[x_1,\ldots,x_n]$–module for small n by using SINGULAR. Do you see a pattern, at least for the Betti numbers?

(Hint: if you do not succeed, you may have a look at Sections 2.5 and 7.6.)

2.4.9. Let $A = \mathbb{Q}[x,y,z]_{\langle x,y,z\rangle}/\langle x^3+y^3+z^3\rangle$. Use SINGULAR to compute several steps of a minimal free resolution of $\langle x,y,z\rangle$ as A–module, until you see a periodicity. Prove that the resolution is infinite.

2.5 Computing Resolutions and the Syzygy Theorem

Let K be a field and $>$ a monomial ordering on $K[x]^r$. Again R denotes the localization of $K[x]$ with respect to $S_>$.

We shall give a method, using standard bases, to compute syzygies and, more generally, free resolutions of finitely generated R–modules. Syzygies and free resolutions are very important objects and basic ingredients for many constructions in homological algebra and algebraic geometry. On the other hand, the use of syzygies gives a very elegant way to prove Buchberger's criterion for standard bases. Moreover, a close inspection of the syzygies of the generators of an ideal allows detection of useless pairs during the computation of a standard basis.

In the following definition R can be an arbitrary ring.

Definition 2.5.1. A *syzygy* or *relation* between k elements $f_1, \ldots, f_k$ of an R–module M is a k–tuple $(g_1, \ldots, g_k) \in R^k$ satisfying

$$\sum_{i=1}^{k} g_i f_i = 0\,.$$

The set of all syzygies between $f_1, \ldots, f_k$ is a submodule of R^k. Indeed, it is the kernel of the ring homomorphism

$$\varphi : F_1 := \bigoplus_{i=1}^{k} R\varepsilon_i \longrightarrow M\,, \quad \varepsilon_i \longmapsto f_i\,,$$

where $\{\varepsilon_1, \ldots, \varepsilon_k\}$ denotes the canonical basis of R^k. φ surjects onto the R–module $I := \langle f_1, \ldots, f_k\rangle_R$ and

$$\mathrm{syz}(I) := \mathrm{syz}(f_1, \ldots, f_k) := \mathrm{Ker}(\varphi)$$

is called the *module of syzygies* of I with respect to the generators $f_1, \ldots, f_k$. [8]

Remark 2.5.2. If R is a local (respectively graded) ring and $\{f_1, \ldots, f_k\}$, $\{g_1, \ldots, g_k\}$ are minimal sets of (homogeneous) generators of I then

$$\mathrm{syz}(f_1, \ldots, f_k) \cong \mathrm{syz}(g_1, \ldots, g_k)\,,$$

hence, $\mathrm{syz}(I)$ is well–defined up to (graded) isomorphism (cf. Exercises 2.5.7 and 2.5.8). More generally, setting $\mathrm{syz}_0(I) := I$, the modules

$$\mathrm{syz}_k(I) := \mathrm{syz}\big(\mathrm{syz}_{k-1}(I)\big)\,,$$

$k \geq 1$, are well–defined up to (graded) isomorphisms. We call $\mathrm{syz}_k(I)$ the *k–th syzygy module* of I. [9]

Note that the k–th Betti number $b_k(I)$ is the minimal number of generators for the k–th syzygy module $\mathrm{syz}_k(I)$. Moreover, in the homogeneous case, the graded Betti number $b_{j,k}(I)$ is the minimal number of generators of the k–th syzygy module $\mathrm{syz}_k(I)$ in degree $j + k$.

[8] In general, the notion $\mathrm{syz}(I)$ is a little misleading, because it depends on the chosen system of generators of I. But it can be proved (cf. Exercise 2.5.6) that for $I = \langle f_1, \ldots, f_k\rangle = \langle g_1, \ldots, g_s\rangle$,

$$\mathrm{syz}(f_1, \ldots, f_k) \oplus R^s \cong \mathrm{syz}(g_1, \ldots, g_s) \oplus R^k\,.$$

For this reason, we keep using the notation $\mathrm{syz}(I)$ as long as we are not interested in a special system of generators.

[9] We also write $\mathrm{syz}^R(I)$, respectively $\mathrm{syz}^R_k(I)$, if we want to emphasize the basering R.

The following lemma provides a method to compute syzygies for submodules of R^r, $R = K[x]_>$, $x = (x_1, \ldots, x_n)$.

Lemma 2.5.3. *Let $I = \langle f_1, \ldots, f_k\rangle_R \subset R^r = \bigoplus_{i=1}^r Re_i$, with $e_1, \ldots, e_r$ the canonical basis of R^r. Consider the canonical embedding*

$$R^r \subset R^{r+k} = \bigoplus_{i=1}^{r+k} Re_i$$

and the canonical projection $\pi : R^{r+k} \to R^k$. Let $G = \{g_1, \ldots, g_s\}$ be a standard basis of $F = \langle f_1 + e_{r+1}, \ldots, f_k + e_{r+k}\rangle_R$ with respect to an elimination ordering for $e_1, \ldots, e_r$ (for example, the ordering $(c, <)$: $x^\alpha e_i < x^\beta e_j$ if $j < i$ or $j = i$ and $x^\alpha < x^\beta$). Suppose that $\{g_1, \ldots, g_\ell\} = G \cap \bigoplus_{i=r+1}^{r+k} Re_i$, then

$$\operatorname{syz}(I) = \langle \pi(g_1), \ldots, \pi(g_\ell)\rangle\,.$$

Proof. $G \cap \bigoplus_{i=r+1}^{r+k} Re_i$ is a standard basis of $F \cap \bigoplus_{i=r+1}^{r+k} Re_i$ (see Lemma 2.8.2, below). On the other hand, $\pi\big(F \cap \bigoplus_{i=r+1}^{r+k} Re_i\big) = \operatorname{syz}(I)$. Namely, let $h \in F \cap \bigoplus_{i=r+1}^{r+k} Re_i$, that is, $h = \sum_{\nu=r+1}^{r+k} h_\nu e_\nu = \sum_{j=1}^k b_j(f_j + e_{r+j})$ for suitable $b_j \in R$. This implies that $\sum_{j=1}^k b_j f_j = 0$ and $b_j = h_{r+j}$.

Conversely, if $h = (h_1, \ldots, h_k) \in \operatorname{syz}(I)$, that is, if $\sum_{\nu=1}^k h_\nu f_\nu = 0$, then $\sum_{\nu=1}^k h_\nu(f_\nu + e_{r+\nu}) \in F \cap \bigoplus_{i=r+1}^{r+k} Re_i$. □

Algorithm 2.5.4 (SYZ$(f_1, \ldots, f_k)$).
Let $>$ be any monomial ordering on $\operatorname{Mon}(x_1, \ldots, x_n)$ and $R = K[x]_>$.

Input: $f_1, \ldots, f_k \in K[x]^r$.
Output: $S = \{s_1, \ldots, s_\ell\} \subset K[x]^k$ such that $\langle S\rangle = \operatorname{syz}(f_1, \ldots, f_k) \subset R^k$.

- $F := \{f_1 + e_{r+1}, \ldots, f_k + e_{r+k}\}$, where $e_1, \ldots, e_{r+k}$ denote the canonical generators of $R^{r+k} = R^r \oplus R^k$ such that $f_1, \ldots, f_k \in R^r = \bigoplus_{i=1}^r Re_i$;
- compute a standard basis G of $\langle F\rangle \subset R^{r+k}$ with respect to $(c, >)$;
- $G_0 := G \cap \bigoplus_{i=r+1}^{r+k} Re_i = \{g_1, \ldots, g_\ell\}$, with $g_i = \sum_{j=1}^k a_{ij} e_{r+j}$, $i = 1, \ldots, \ell$;
- $s_i := (a_{i1}, \ldots a_{ik})$, $i = 1, \ldots, \ell$;
- return $S = \{s_1, \ldots, s_\ell\}$.

SINGULAR Example 2.5.5 (syzygies).
We apply first the built–in command `syz`, while, in the second example, we proceed as in Lemma 2.5.3 (resp. Algorithm 2.5.4). The latter method gives more flexibility in choosing a faster ordering for specific examples.

```
ring R=0,(x,y,z),(c,dp);
ideal I=xy,yz,xz;
module M=syz(I);   //the module of syzygies of xy,yz,xz
```

```
M;
//-> M[1]=[0,x,-y]
//-> M[2]=[z,0,-y]

module T=[xy,1,0,0],[yz,0,1,0],[xz,0,0,1];
module N=std(T);
N;            //the first two elements give the syzygies
//-> N[1]=[0,0,x,-y]
//-> N[2]=[0,z,0,-y]
//-> N[3]=[yz,0,1]
//-> N[4]=[xz,0,0,1]
//-> N[5]=[xy,1]
```

Remark 2.5.6. Let R be a ring, $I = \langle f_1, \ldots, f_s \rangle \subset R$ an ideal, and

$$\overline{M} = \langle \overline{m}_1, \ldots, \overline{m}_k \rangle \subset (R/I)^r$$

a submodule. Then $\overline{M}$ is an R– as well as an R/I–module, and we denote by $\mathrm{syz}\big(\overline{M}\big) := \mathrm{syz}^R(\overline{m}_1, \ldots, \overline{m}_k)$ and $\mathrm{syz}^{R/I}\big(\overline{M}\big) := \mathrm{syz}^{R/I}\big(\overline{m}_1, \ldots, \overline{m}_k\big)$ the respective modules of syzygies. They can be computed as follows: let $e_1, \ldots, e_r$ be the canonical basis of R^r, and let $m_1, \ldots, m_k \in R^r$ be representatives of $\overline{m}_1, \ldots, \overline{m}_k$. Moreover, let

$$M := \langle m_1, \ldots, m_k, f_1 e_1, \ldots, f_1 e_r, \ldots, f_s e_1, \ldots, f_s e_r \rangle \subset R^r$$

and $\mathrm{syz}(M) = \{s_1, \ldots, s_\ell\}$, where $s_i = (s_{i1}, \ldots, s_{iN})$, $N = k + rs$. Then

$$\mathrm{syz}\big(\overline{M}\big) = \langle \overline{s}_1, \ldots, \overline{s}_\ell \rangle \subset R^k\,,$$

where $\overline{s}_i = (s_{i1}, \ldots, s_{ik})$, $i = 1, \ldots, \ell$. Now $\mathrm{syz}^{R/I}\big(\overline{M}\big)$ is the image of $\mathrm{syz}\big(\overline{M}\big)$ when projecting modulo I.

Successively computing syzygies of syzygies, we obtain an algorithm to compute free resolutions up to any given length.

Algorithm 2.5.7 (Resolution(I, m)).
Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$ and $R = K[x]_>$.

Input: $f_1, \ldots, f_k \in K[x]^r$, $I = \langle f_1, \ldots, f_k \rangle \subset R^r$, and m a positive integer.
Output: A list of matrices $A_1, \ldots, A_m$ with $A_i \in \mathrm{Mat}(r_{i-1} \times r_i, K[x])$, $i = 1, \ldots, m$, such that

$$\ldots \longrightarrow R^{r_m} \xrightarrow{A_m} R^{r_{m-1}} \longrightarrow \ldots \longrightarrow R^{r_1} \xrightarrow{A_1} R^r \longrightarrow R^r/I \longrightarrow 0$$

is a free resolution of R^r/I.

- $i := 1$;
- $A_1 := \mathrm{matrix}(f_1, \ldots, f_k) \in \mathrm{Mat}(r \times k, K[x])$;

- while $(i < m)$
  $i := i + 1$;
  $A_i := \mathrm{syz}(A_{i-1})$;
- return $A_1, \ldots, A_m$.

With the notation of Definition 2.5.1, we shall now define a monomial ordering on F_1, the free R–module containing $\mathrm{syz}(I)$, $I = \langle f_1, \ldots, f_k \rangle \subset R^r =: F_0$, $f_i \neq 0$ for all i, which behaves perfectly well with respect to standard bases of syzygies. This ordering was first introduced and used by Schreyer [204].

We define the *Schreyer ordering* as follows

$$x^\alpha \varepsilon_i >_1 x^\beta \varepsilon_j :\Longleftrightarrow \mathrm{LM}(x^\alpha f_i) > \mathrm{LM}(x^\beta f_j) \text{ or}$$
$$\mathrm{LM}(x^\alpha f_i) = \mathrm{LM}(x^\beta f_j) \text{ and } i > j.$$

The left–hand side $>_1$ is the new ordering on F_1 and the right–hand side $>$ is the given ordering on F_0. The same ordering on R is induced by $>$ and $>_1$. Note that the Schreyer ordering depends on $f_1, \ldots, f_k$.

Now we are going to prove Buchberger's criterion, which states that $G = \{f_1, \ldots, f_k\}$ is a standard basis of $I = \langle f_1, \ldots, f_k \rangle$, if, for all $i < j$, $\mathrm{NF}\big(\mathrm{spoly}(f_i, f_j) \mid G_{ij}\big) = 0$ for suitable $G_{ij} \subset G$. We give a proof by using syzygies, which works for arbitrary monomial orderings and which is different from Schreyer's (cf. [204], [205]) original proof (cf. also [66]), although the basic ideas are due to Schreyer. Our proof gives, at the same time, a proof of Schreyer's result that the syzygies derived from a standard representation of $\mathrm{spoly}(f_i, f_j)$ form a standard basis of $\mathrm{syz}(I)$ for the Schreyer ordering.

We introduce some notations. For each $i \neq j$ such that f_i and f_j have their leading terms in the same component, say $\mathrm{LM}(f_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(f_j) = x^{\alpha_j} e_\nu$, we define the monomial

$$m_{ji} := x^{\gamma - \alpha_i} \in K[x]\,,$$

where $\gamma = \mathrm{lcm}(\alpha_i, \alpha_j)$. If $c_i = \mathrm{LC}(f_i)$ and $c_j = \mathrm{LC}(f_j)$ then

$$m_{ji} f_i - \frac{c_i}{c_j} m_{ij} f_j = \mathrm{spoly}(f_i, f_j)\,.$$

Assume that we have a standard representation

$$m_{ji} f_i - \frac{c_i}{c_j} m_{ij} f_j = \sum_{\nu=1}^{k} a_\nu^{(ij)} f_\nu, \quad a_\nu^{(ij)} \in R\,.$$

For $i < j$ such that $\mathrm{LM}(f_i)$ and $\mathrm{LM}(f_j)$ involve the same component, define

$$s_{ij} := m_{ji} \varepsilon_i - \frac{c_i}{c_j} m_{ij} \varepsilon_j - \sum_\nu a_\nu^{(ij)} \varepsilon_\nu.$$

Then $s_{ij} \in \mathrm{syz}(I)$ and it is easy to see that

Lemma 2.5.8. *With the notations introduced above,* $\mathrm{LM}(s_{ij}) = m_{ji}\varepsilon_i$.

Proof. Since $\mathrm{LM}(m_{ij}f_j) = \mathrm{LM}(m_{ji}f_i)$ and $i < j$, the definition of $>_1$ gives $m_{ji}\varepsilon_i > m_{ij}\varepsilon_j$. From the defining property of a standard representation we obtain

$$\mathrm{LM}(a_\nu^{(ij)} f_\nu) \leq \mathrm{LM}\Big(m_{ji}f_i - \frac{c_i}{c_j} m_{ij} f_j\Big) < \mathrm{LM}(m_{ji}f_i)$$

and, hence, the claim. □

Theorem 2.5.9. *Let* $G = \{f_1, \ldots, f_k\}$ *be a set of generators of* $I \subset R^r$. *Let*

$$M := \big\{(i,j) \,\big|\, 1 \leq i < j \leq k\,,\ \mathrm{LM}(f_i), \mathrm{LM}(f_j) \text{ involve the same component}\big\}\,,$$

and let $J \subset M$. *Assume that*

- $\mathrm{NF}\big(\mathrm{spoly}(f_i, f_j) \,\big|\, G_{ij}\big) = 0$ *for some* $G_{ij} \subset G$ *and* $(i,j) \in J$.
- $\big\langle \{m_{ji}\varepsilon_i \mid (i,j) \in J\} \big\rangle = \big\langle \{m_{ji}\varepsilon_i \mid (i,j) \in M\} \big\rangle$ *for* $i = 1, \ldots, r$.

Then the following statements hold:

(1) G *is a standard basis of* I *(*Buchberger's criterion*).*
(2) $S := \{s_{ij} \mid (i,j) \in J\}$ *is a standard basis of* $\mathrm{syz}(I)$ *with respect to the Schreyer ordering. In particular,* S *generates* $\mathrm{syz}(I)$.

Proof. We give a proof of (1) and (2) at the same time (recall the notations of Definition 2.5.1).

Take any $f \in I$ and a preimage $g \in F_1$ of f,

$$g = \sum_{i=1}^{k} a_i\varepsilon_i,\ f = \varphi(g) = \sum_{i=1}^{k} a_i f_i\,.$$

This is possible as G generates I. In case (1), we assume $f \neq 0$, in case (2) $f = 0$.

Consider a standard representation of ug, u a unit,

$$ug = h + \sum_{(i,j)\in J} a_{ij}s_{ij}, \quad a_{ij} \in R\,,$$

where $h = \sum_j h_j\varepsilon_j \in F_1$ is a normal form of g with respect to S for some weak normal form on F_1 (we need only know that it exists). We can assume, if $h \neq 0$,

$$h = h_1\varepsilon_1 + \cdots + h_k\varepsilon_k$$

and $\mathrm{LM}(h_\nu\varepsilon_\nu) \notin \langle \mathrm{LM}(s_{ij}) \,|_{(i,j)\in J}\rangle = \langle m_{ji}\varepsilon_i \,|_{(i,j)\in J}\rangle$ by Lemma 2.5.8 and Remark 2.3.4 for all ν such that $h_\nu \neq 0$. This shows

$$m_{j\nu} \nmid \mathrm{LM}(h_\nu)$$

for all ν, j such that f_j and f_ν have the leading term in the same component.

Since $ug - h \in \langle S\rangle \subset \mathrm{syz}(I)$, we obtain

$$uf = \varphi(ug) = \varphi(h) = \sum_j h_j f_j\,.$$

Assume that for some $j \neq \nu$, $\mathrm{LM}(h_j f_j) = \mathrm{LM}(h_\nu f_\nu)$ and let $\mathrm{LM}(f_\nu) = x^{\alpha_\nu} e_k$, $\mathrm{LM}(f_j) = x^{\alpha_j} e_k$. Then $\mathrm{LM}(h_\nu f_\nu)$ is divisible by $x^{\alpha_\nu} e_k$ and by $x^{\alpha_j} e_k$, hence,

$$\mathrm{lcm}(x^{\alpha_\nu}, x^{\alpha_j}) \mid \mathrm{LM}(h_\nu f_\nu) = \mathrm{LM}(h_\nu) x^{\alpha_\nu} e_k\,.$$

But $m_{j\nu} = \mathrm{lcm}(x^{\alpha_\nu}, x^{\alpha_j})/x^{\alpha_\nu}$. This contradicts $m_{j\nu} \nmid \mathrm{LM}(h_\nu)$.

In case (1) we obtain $\mathrm{LM}(f) = \mathrm{LM}(h_\nu f_\nu) \in L(G)$ for some ν and, hence, G is a standard basis by definition. In case (2) it shows that $h \neq 0$ leads to a contradiction and S is a standard basis by Theorem 2.3.13, (2) $\Rightarrow$ (1), which was already proved. □

Lemma 2.5.10 (Chain Criterion). *With the notations of Theorem 2.5.9 assume that $(i,j) \in M$ and $(j,\ell) \in M$. Let $\mathrm{LM}(f_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(f_j) = x^{\alpha_j} e_\nu$ and $\mathrm{LM}(f_\ell) = x^{\alpha_\ell} e_\nu$. If x^{α_j} divides $\mathrm{lcm}(x^{\alpha_i}, x^{\alpha_\ell})$ then $m_{\ell i}\varepsilon_i \in \langle m_{ji}\varepsilon_i\rangle$. In particular, if $s_{i\ell}, s_{ij} \in S$ then $S \setminus \{s_{i\ell}\}$ is already a standard basis of* $\mathrm{syz}(I)$.

Proof. $x^{\alpha_j} \mid \mathrm{lcm}(x^{\alpha_i}, x^{\alpha_\ell})$ implies that $\mathrm{lcm}(x^{\alpha_i}, x^{\alpha_j}) \mid \mathrm{lcm}(x^{\alpha_i}, x^{\alpha_\ell})$. Dividing by x^{α_i} we obtain that m_{ji} divides $m_{\ell i}$. □

Remark 2.5.11. The chain criterion can be used to refine the Standard Basis Algorithm 2.3.8. If (f_i, f_j), (f_i, f_ℓ) and (f_j, f_ℓ) are in the pair set P and (with the notations of the lemma) $x^{\alpha_j} \mid \mathrm{lcm}(x^{\alpha_i}, x^{\alpha_\ell})$ then we can delete (f_i, f_ℓ) from P. For a generalization of the criterion cf. [168]. Note that the *Product Criterion* (Exercise 1.7.1) is only applicable for modules with all module components 0 except one.

We want to illustrate this with the following example.

Example 2.5.12. Let $I = \langle u^5 - v^5, v^5 - x^5, x^5 - y^5, y^5 - z^5, u^4v + v^4x + x^4y + y^4z + z^4u\rangle \subset \mathbb{Q}[u,v,x,y,z]$. The reduced standard basis of this ideal with respect to the ordering `dp` has 149 elements.

Using Buchberger's criterion (Theorem 2.3.13), we see that during the computation of the standard basis $\binom{149}{2} = 11026$ pairs have to be considered.

In the implementation of Buchberger's algorithm in SINGULAR, the chain criterion is applied 10288 times and the product criterion 166 times. Therefore, instead of reducing 11026 s–polynomials, we only need to consider 572 (about 5 %) of them. This shows that these criteria have an enormous influence on the performance of Buchberger's algorithm.

We shall now see, as an application, that Hilbert's syzygy theorem holds for the rings $R = K[x]_>$, stating that each finitely generated R–module has a free resolution of length at most n, the number of variables.

Lemma 2.5.13. *Let $G = \{g_1, \dots, g_s\}$ be a minimal standard basis of the submodule $I \subset R^r = \bigoplus_{i=1}^r Re_i$ such that $\mathrm{LM}(g_i) \in \{e_1, \dots, e_r\}$ for all i. Let J denote the set of indices j such that $e_j \notin \{\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)\}$. Then*

$$I = \bigoplus_{i=1}^{s} Rg_i, \qquad R^r/I \cong \bigoplus_{j \in J} Re_j\,.$$

Proof. The set $G' := G \cup \{e_j \mid j \in J\}$ is R–linearly independent, since the leading terms are. This shows that both sums above are direct.

Let $f \in R^r$ and consider a weak normal form h of f with respect to G'. Assuming $h \neq 0$, we would have $\mathrm{LM}(h) \notin \langle e_1, \dots, e_r\rangle$, a contradiction. Hence, $h = 0$, that is, $f \in I + \langle\{e_j \mid j \in J\}\rangle$. □

Lemma 2.5.14. *Let $G = \{g_1, \dots, g_s\}$ be a standard basis of $I \subset R^r$, ordered in such a way that the following holds: if $i < j$ and $\mathrm{LM}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(g_j) = x^{\alpha_j} e_\nu$ for some ν, then $\alpha_i \geq \alpha_j$ lexicographically. Let s_{ij} denote the syzygies defined above. Suppose that $\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)$ do not depend on the variables $x_1, \dots, x_k$. Then the $\mathrm{LM}(s_{ij})$, taken with respect to the Schreyer ordering, do not depend on $x_1, \dots, x_{k+1}$.*

Proof. Given s_{ij}, then $i < j$ and $\mathrm{LM}(g_i)$ and $\mathrm{LM}(g_j)$ involve the same component, say e_ν. By assumption, $\mathrm{LM}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(g_j) = x^{\alpha_j} e_\nu$ satisfy $\alpha_i = (0, \dots, \alpha_{i,k+1}, \dots)$ and $\alpha_j = (0, \dots, \alpha_{j,k+1}, \dots)$ with $\alpha_{i,k+1} \geq \alpha_{j,k+1}$. Therefore, $\mathrm{LM}(s_{ij}) = m_{ji}\varepsilon_i$, $m_{ji} = x^{\mathrm{lcm}(\alpha_i, \alpha_j) - \alpha_i}$, does not depend on x_{k+1}. □

Applying the lemma successively to the higher syzygy modules, we obtain

Theorem 2.5.15 (Hilbert's Syzygy Theorem). *Let $>$ be any monomial ordering on $K[x] = K[x_1, \dots, x_n]$, and let $R = K[x]_>$ be the associated ring. Then any finitely generated R–module M has a free resolution*

$$0 \to F_m \to F_{m-1} \to \cdots \to F_0 \to M \to 0$$

of length $m \leq n$, where the F_i are free R–modules.

Proof. Since R is Noetherian, M has a presentation

$$0 \to I \to F_0 \to M \to 0\,,$$

with $F_0 = \bigoplus_{i=1}^{r_0} Re_i$, and I being finitely generated. Let $G = \{g_1, \dots, g_s\}$ be a standard basis of I and assume that the $\mathrm{LM}(g_i)$ do not depend on the variables $x_1, \dots, x_k$, $k \geq 0$. By Theorem 2.5.9, the syzygies $s_{ij} =: s_{ij}^{(1)}$ are a standard basis of $\mathrm{syz}(I)$ and, by Lemma 2.5.14, we may assume that the $\mathrm{LM}(s_{ij}^{(1)})$ do not depend on $x_1, \dots, x_{k+1}$. Hence, we obtain an exact sequence

$$0 \to \mathrm{Ker}(\varphi_1) = \mathrm{syz}(I) \to F_1 \xrightarrow{\varphi_1} F_0 \to M \to 0$$

$F_1 = \bigoplus_{i=1}^{s} R\varepsilon_i$, $\varphi_1(\varepsilon_i) = g_i$, with $\mathrm{syz}(I)$ satisfying analogous properties as I. We can, therefore, construct by induction an exact sequence

$$0 \to \mathrm{Ker}(\varphi_{n-k}) \to F_{n-k} \xrightarrow{\varphi_{n-k}} F_{n-k-1} \to \ldots \xrightarrow{\varphi_2} F_1 \to F_0 \to M \to 0$$

with F_i free of rank r_i and $\mathrm{Ker}(\varphi_{n-k})$ given by a standard basis $\{s_{ij}^{(n-k)}\}$ such that none of the variables appears in $\mathrm{LM}(s_{ij}^{(n-k)})$. By Lemma 2.5.13, the quotient $F_{n-k}/\mathrm{Ker}(\varphi_{n-k})$ is a free R–module, and replacing F_{n-k} by $F_{n-k}/\mathrm{Ker}(\varphi_{n-k})$ we obtain the desired free resolution. □

Algorithm 2.5.16 (SResolution).
Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_r)$, $R = K[x]_>$.

Input: $>_m$ any module ordering on R^r, $\emptyset \neq G = \{g_1, \ldots, g_k\} \subset K[x]^r$ an interreduced standard basis of $I = \langle G \rangle \subset R^r$ w.r.t. $>_m$.

Output: A list of matrices $A_1, \ldots, A_m$ with $A_i \in \mathrm{Mat}(r_{i-1} \times r_i, K[x])$, $i = 1, \ldots, m$, such that $m \leq n$ and

$$0 \longrightarrow R^{r_m} \xrightarrow{A_m} R^{r_{m-1}} \longrightarrow \ldots \longrightarrow R^{r_1} \xrightarrow{A_1} R^r \longrightarrow R^r/I \longrightarrow 0$$

is a free resolution.

- Renumber the elements $g_1, \ldots, g_k$ of G such that the following holds: if $i < j$ and $\mathrm{LM}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(g_j) = x^{\alpha_j} e_\nu$ for some ν, then $\alpha_i >_{lp} \alpha_j$.
- Set $A_1 = (g_1, \ldots, g_k) \in \mathrm{Mat}(r \times k, K[x])$.
- With the notations of Theorem 2.5.9, choose a subset $J \subset M$ such that $\big\langle \{m_{ji}\varepsilon_i \mid (i,j) \in J\} \big\rangle \supset \{m_{ji}\varepsilon_i \mid (i,j) \in M\}$ for $i = 1, \ldots, r$.
- For $(i,j) \in J$ compute a standard representation

$$u_{ij} \cdot \mathrm{spoly}(g_i, g_j) = \sum_{\nu=1}^{k} a_\nu^{(ij)} g_\nu \,,$$

$u_{ij} \in K[x] \cap R^*$, $a_\nu^{(ij)} \in K[x]$, and set[10]

$$s_{ij} := u_{ij} m_{ji} \varepsilon_i - \frac{c_i}{c_j} u_{ij} m_{ij} \varepsilon_j - \sum_{\nu=1}^{k} a_\nu^{(ij)} \varepsilon_\nu \,.$$

- Set $S := \mathrm{InterReduction}(\{s_{ij} \mid (i,j) \in J\})$.
- If, for each $s \in S$, $\mathrm{LM}(s) \in \{\varepsilon_1, \ldots, \varepsilon_k\}$ (where the leading monomial is taken w.r.t. the Schreyer ordering $>_1$)
  then
  set $J' := \big\{1 \leq j \leq k \,\big|\, \varepsilon_j \notin \{\mathrm{LM}(s) \mid s \in S\}\big\}$,

[10] Recall $c_i = \mathrm{LC}(g_i)$ and $m_{ji} = x^{\gamma - \alpha_i}$ with $\gamma = \mathrm{lcm}(\alpha_i, \alpha_j)$ and $\mathrm{LM}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(g_j) = x_{\alpha_j} e_\nu$.

delete in the matrix A_1 all columns with index $j \notin J'$,
return(A_1),
else
list $L = A_1$, SResolution($>_1, S$),
return(L).

Note that the free resolution computed by SResolution($>_m, G$) is, in general, not minimal (in the local, respectively homogeneous case). But, it can be *minimized* afterwards, following the procedure described on page 127 (applying Gaussian elimination and deleting rows and columns of the corresponding matrices), with the only difference that each column operation on the matrix A_i has to be succeeded by a certain row operation on A_{i+1} (and vice versa, cf. Exercise 2.5.4).

Example 2.5.17. Let $R := K[x,y,z]$ with degree reverse lexicographical ordering $>_{dp}$, let $>_m = (c, >_{dp})$, and consider

$$G := \{yz + z^2, y^2 + xz, xy + z^2, z^3, xz^2, x^2z\}$$

(which is an interreduced standard basis of $I := \langle G\rangle \subset R$). After renumbering the elements of G such that $\mathrm{LM}(g_1) >_{lp} \mathrm{LM}(g_2) >_{lp} \cdots >_{lp} \mathrm{LM}(g_6)$, we obtain

$$A_1 := (\underbrace{x^2z}_{g_1}, \underbrace{xy+z^2}_{g_2}, \underbrace{xz^2}_{g_3}, \underbrace{y^2+xz}_{g_4}, \underbrace{yz+z^2}_{g_5}, \underbrace{z^3}_{g_6}) \in \mathrm{Mat}(1\times 6, K[x,y,z])\,.$$

The respective monomials $m_{ji}\varepsilon_i$, $1 \le i < j \le 6$, are given in the following table:

$_i\backslash^j$	2	3	4	5	6
1	$y\varepsilon_1$	$z\varepsilon_1$	$y^2\varepsilon_1$	$y\varepsilon_1$	$z^2\varepsilon_1$
2	$--$	$z^2\varepsilon_2$	$y\varepsilon_2$	$z\varepsilon_2$	$z^3\varepsilon_2$
3	$--$	$--$	$y^2\varepsilon_3$	$y\varepsilon_3$	$z\varepsilon_3$
4	$--$	$--$	$--$	$z\varepsilon_4$	$z^3\varepsilon_4$
5	$--$	$--$	$--$	$--$	$z^2\varepsilon_5$

Hence, we may choose

$$J := \big\{(1,2),(1,3),(2,4),(2,5),(3,5),(3,6),(4,5),(5,6)\big\}$$

and compute

$$\begin{aligned}
s_{1,2} &= y\varepsilon_1 - xz\varepsilon_2 + x\varepsilon_6\,,\\
s_{1,3} &= z\varepsilon_1 - x\varepsilon_3\,,\\
s_{2,4} &= y\varepsilon_2 - x\varepsilon_4 + \varepsilon_1 - z\varepsilon_5 + \varepsilon_6\,,\\
s_{2,5} &= z\varepsilon_2 - x\varepsilon_5 + \varepsilon_3 - \varepsilon_6\,,\\
s_{3,5} &= y\varepsilon_3 - xz\varepsilon_5 + x\varepsilon_6\,,\\
s_{3,6} &= z\varepsilon_3 - x\varepsilon_6\,,
\end{aligned}$$

$s_{4,5} = z\varepsilon_4 - y\varepsilon_5 - \varepsilon_3 + z\varepsilon_5 - \varepsilon_6\,,$
$s_{5,6} = z^2\varepsilon_5 - y\varepsilon_6 - z\varepsilon_6\,.$

The set $S := \{s_{1,2}, s_{1,3}, s_{2,4}, s_{2,5}, s_{3,5}, s_{3,6}, s_{4,5}, s_{5,6}\}$ is an interreduced standard basis for $\mathrm{syz}(I)$ (w.r.t. the Schreyer ordering $>_1$), and we are left with computing SRESOLUTION$(>_1, S)$. By accident, the elements of S are already ordered as needed, and we set

$$A_2 := \begin{pmatrix} y & z & 1 & 0 & 0 & 0 & 0 & 0 \\ -xz & 0 & y & z & 0 & 0 & 0 & 0 \\ 0 & -x & 0 & 1 & y & z & -1 & 0 \\ 0 & 0 & -x & 0 & 0 & 0 & z & 0 \\ 0 & 0 & -z & -x & -xz & 0 & -y+z & z^2 \\ x & 0 & 1 & -1 & x & -x & -1 & -y-z \end{pmatrix}.$$

We see that the set M of pairs (i,j), $1 \le i < j \le 8$, such that the leading monomials of the i–th and j–th element of S involve the same components consists of precisely 3 elements: $M = \big\{(1,2), (3,4), (5,6)\big\}$. We compute

$s^{(1)}_{1,2} = z\varepsilon_1 - y\varepsilon_2 + xz\varepsilon_4 - x\varepsilon_5 - x\varepsilon_6\,,$
$s^{(1)}_{3,4} = z\varepsilon_3 - y\varepsilon_4 - \varepsilon_2 + \varepsilon_5 + x\varepsilon_7 + \varepsilon_8\,,$
$s^{(1)}_{5,6} = z\varepsilon_5 - y\varepsilon_6 + x\varepsilon_8\,,$

Again, $S^{(1)} := \big\{s^{(1)}_{1,2}, s^{(1)}_{3,4}, s^{(1)}_{5,6}\big\}$ is an interreduced standard basis for $\mathrm{syz}(\langle S\rangle)$. Since the leading monomials of the elements of $S^{(1)}$ (w.r.t. the Schreyer ordering $>_2$) involve different components, SRESOLUTION$(>_2, S^{(1)})$ returns

$$A_3 := \begin{pmatrix} z & 0 & 0 \\ -y & -1 & 0 \\ 0 & z & 0 \\ xz & -y & 0 \\ -x & 1 & z \\ -x & 0 & -y \\ 0 & x & x \\ 0 & 1 & x \end{pmatrix}.$$

Finally, we have computed the free resolution

$$0 \longrightarrow R^3 \xrightarrow{A_3} R^8 \xrightarrow{A_2} R^6 \xrightarrow{A_1} R \longrightarrow R/I \longrightarrow 0\,.$$

Note that I is a *homogeneous* ideal, hence R/I has the structure of a graded K-algebra. Now we can easily derive the *Betti numbers* of R/I from the computed (non–minimal) free resolution (without computing the minimal resolution). To do so, we consider the matrices A_1, A_2, A_3 mod $\mathfrak{m} = \langle x, y, z\rangle$, apply Gaussian elimination in $K = R/\mathfrak{m}$ as indicated above (for minimizing the resolution), and delete the respective rows and columns (cf. also Exercise

2.5.4). We obtain that $b_3(R/I) = 2$, $b_2(R/I) = 4$, $b_1(R/I) = 3$, $b_0(R/I) = 1$, that is, the minimal resolutions of R/I look as follows

$$0 \longrightarrow R^2 \longrightarrow R^4 \longrightarrow R^3 \longrightarrow R \longrightarrow R/I \longrightarrow 0\,.$$

The implemented algorithm `sres` in SINGULAR is a modification of SRESOLUTION. For efficiency reasons the generators (with leading monomials in the same components) are not ordered lexicographically but with respect to $>_{dp}$. Hence, `sres` does not necessarily compute a free resolution of finite length, but stops the computation after $n+1$ steps (n being the number of variables of the basering). Anyhow, we can obtain the Betti numbers (using the built–in command `betti`), respectively minimize the obtained resolution (using `minres`).

SINGULAR Example 2.5.18 (Schreyer resolution).

```
ring R=0,(x,y,z),(c,dp);
ideal I=yz+z2,y2+xz,xy+z2,z3,xz2,x2z;
```

First compute a minimal free resolution of R/I:

```
resolution Re=mres(I,0);
Re;
//->  1      3      4      2
//-> R  <-- R  <-- R  <-- R
//->
//-> 0      1      2      3
```

Display the matrices in the resolution:

```
print(Re);
//-> [1]:
//->    _[1]=yz+z2
//->    _[2]=y2+xz
//->    _[3]=xy+z2
//-> [2]:
//->    _[1]=[0,xy+z2,-y2-xz]
//->    _[2]=[y2+xz,-yz-z2]
//->    _[3]=[xy+z2,0,-yz-z2]
//->    _[4]=[x2-yz,-xz+z2,-xz+yz]
//-> [3]:
//->    _[1]=[0,x-z,x-y,-y-z]
//->    _[2]=[z,z,-x,y]
```

Now apply the modification of Schreyer's algorithm to compute a free resolution for R/I and display the matrices:

```
resolution Se=sres(I,0);
Se;
//->  1      6      8      3
//-> R  <-- R  <-- R  <-- R
//->
//-> 0      1      2      3
//-> resolution not minimized yet

print(Se);
//-> [1]:
//->    _[1]=x2z
//->    _[2]=xz2
//->    _[3]=z3
//->    _[4]=xy+z2
//->    _[5]=y2+xz
//->    _[6]=yz+z2
//-> [2]:
//->    _[1]=[z,-x]
//->    _[2]=[y,0,x,-xz]
//->    _[3]=[0,z,-x]
//->    _[4]=[0,y,z,-z2]
//->    _[5]=[0,0,y+z,0,0,-z2]
//->    _[6]=[1,0,1,y,-x,-z]
//->    _[7]=[0,1,-1,z,0,-x]
//->    _[8]=[0,-1,-1,0,z,-y+z]
//-> [3]:
//->    _[1]=[y,-z,0,x]
//->    _[2]=[0,0,y+z,-z,x,0,-z2]
//->    _[3]=[-1,0,-1,1,-1,z,-y+z,x]
```

Finally, let us minimize the computed resolution:

```
print(minres(Se));
//-> [1]:
//->    _[1]=xy+z2
//->    _[2]=y2+xz
//->    _[3]=yz+z2
//-> [2]:
//->    _[1]=[-2y2-xz-yz,2xy+xz-yz,-x2+y2+xz+yz]
//->    _[2]=[-xz-z2,-xz+z2,x2+xy-yz+z2]
//->    _[3]=[-yz-z2,yz+z2,xy-y2-xz+z2]
//->    _[4]=[yz+z2,yz+z2,-xy-y2-xz-z2]
//-> [3]:
//->    _[1]=[-z,-y,x+y,-y]
//->    _[2]=[0,y+z,-z,x]
```

Exercises

2.5.1. Find a standard basis with respect to the lexicographical ordering and a standard basis of the syzygies for $I = \langle x^2, y^2, xy + yz \rangle$. Compare Schreyer's method and the method of Lemma 2.5.3.

2.5.2. Let $I \subset K[x_1, \ldots, x_n]$ be a homogeneous ideal. Give an algorithm to compute a minimal resolution of $K[x_1, \ldots, x_n]/I$, modifying the algorithm RESOLUTION.

2.5.3. Compute a minimal resolution for $I = \langle x^2, y^2, xy + yz \rangle \subset K[x, y, z]$.

2.5.4. Give an algorithm to obtain a minimal resolution in the case of local rings from Schreyer's resolution.

2.5.5. Prove *Schanuel's Lemma*: Let R be a Noetherian ring and M a finitely generated R–module. Moreover, assume that the following sequences are exact:

$$0 \longrightarrow K_1 \longrightarrow R^{n_1} \xrightarrow{\pi_1} M \longrightarrow 0\,,$$
$$0 \longrightarrow K_2 \longrightarrow R^{n_2} \xrightarrow{\pi_2} M \longrightarrow 0\,.$$

Then $K_1 \oplus R^{n_2} \cong K_2 \oplus R^{n_1}$.
(Hint: Prove that both of them are isomorphic to $\mathrm{Ker}(R^{n_1} \oplus R^{n_2} \xrightarrow{\pi_1+\pi_2} M)$.)

2.5.6. Let R be a Noetherian ring and $M = \langle f_1, \ldots, f_k \rangle = \langle g_1, \ldots, g_s \rangle \subset R^r$. Prove that $\mathrm{syz}(f_1, \ldots, f_k) \oplus R^s \cong \mathrm{syz}(g_1, \ldots, g_s) \oplus R^k$.

2.5.7. Let R be a local Noetherian ring, let M be a finitely generated R-module, and let $\{f_1, \ldots, f_k\}$, $\{g_1, \ldots, g_k\}$ be two minimal sets of generators. Prove that $\mathrm{syz}(f_1, \ldots, f_k) \cong \mathrm{syz}(g_1, \ldots, g_k)$, and conclude that the k–th syzygy module $\mathrm{syz}_k(M)$ is well–defined up to isomorphism.

2.5.8. Let R be a local Noetherian graded K–algebra, K a field, and let M be a finitely generated graded R-module. Show that, for a system of homogeneous generators $\{f_1, \ldots, f_k\}$ of M, the module of syzygies $\mathrm{syz}(f_1, \ldots, f_k)$ is a homogeneous submodule of R^k.

Moreover, show that for two minimal systems of homogeneous generators $\{f_1, \ldots, f_k\}$, $\{g_1, \ldots, g_k\}$ of M, the modules of syzygies are isomorphic as graded R–modules.

Conclude that the k–th syzygy module $\mathrm{syz}_k(M)$ is well–defined up to graded isomorphism and that the Betti numbers of M depend only on the graded isomorphism class of M.

2.5.9. Let $f, g \in K[x]$. Prove that $\gcd(f, g)$ and $\mathrm{lcm}(f, g)$ can be computed using the syzygies of f and g. Write a SINGULAR procedure to compute the gcd and lcm.

2.6 Modules over Principal Ideal Domains

In this section we shall study the structure of finitely generated modules over principal ideal domains. It will be proved that they can be decomposed in a unique way into a direct sum of cyclic modules with special properties. Examples are given for the case of a univariate polynomial ring over a field. We show how this decomposition can be computed by using standard bases (actually, we need only interreduction).

Theorem 2.6.1. *Let R be a principal ideal domain and M a finitely generated R–module, then M is a direct sum of cyclic modules.*

Proof. Let $R^m \to R^n \to M \to 0$ be a presentation of M given by the matrix $A = (a_{ij})$ with respect to the bases $B = \{e_1, \ldots, e_n\}$, $B' = \{f_1, \ldots, f_m\}$ of R^n, R^m, respectively. If A is the zero–matrix, then $M \cong R^n$, and we are done. Otherwise, we may assume that $a_{11} \neq 0$. We shall show that, for a suitable choice of the bases, the presentation matrix has *diagonal form*, that is, $a_{ij} = 0$ if $i \neq j$. For some $k > 1$ with $a_{k1} \neq 0$, let h be a generator of the ideal $\langle a_{11}, a_{k1}\rangle$, and let $a, b, c, d \in R$ be such that $h = aa_{11} + ba_{k1}$, $a_{11} = ch$, $a_{k1} = dh$ (we choose $a := 1,\ b := 0,\ c := 1$ if $\langle a_{11}\rangle = \langle a_{11}, a_{k1}\rangle$). Now we change the basis B to $\bar{B} = \{ce_1 + de_k, e_2, \ldots, e_{k-1}, -be_1 + ae_k, e_{k+1}, \ldots, e_n\}$. $\bar{B}$ is a basis because $\det \left(\begin{smallmatrix} c & -b \\ d & a \end{smallmatrix}\right) = 1$. Let $\bar{A} = (\bar{a}_{ij})$ be the presentation matrix with respect to this basis, then $\bar{a}_{11} = h$ and $\bar{a}_{k1} = 0$, while $\bar{a}_{i1} = a_{i1}$ for $i \neq 1, k$. Note that the first row of A and $\overline{A}$ are equal if and only if $\langle a_{11}\rangle = \langle a_{11}, a_{k1}\rangle$. Doing this with every $k > 1$, we may assume that $a_{k1} = 0$ for $k = 2, \ldots, n$.

Now, applying the same procedure to the transposed matrix ${}^tA$ (which corresponds to base changes in B'), we obtain a matrix ${}^tA_1$,

$$A_1 = \begin{pmatrix} a_{11}^{(1)} & 0 & \ldots & 0 \\ a_{21}^{(1)} & a_{22}^{(1)} & \ldots & a_{2m}^{(1)} \\ \vdots & & & \vdots \\ a_{n1}^{(1)} & a_{n2}^{(1)} & \ldots & a_{nm}^{(1)} \end{pmatrix},$$

with the property: $\langle a_{11}\rangle \subset \langle a_{11}^{(1)}\rangle$ and $a_{21}^{(1)} = \cdots = a_{n1}^{(1)} = 0$, if $\langle a_{11}\rangle = \langle a_{11}^{(1)}\rangle$.

Repeating this procedure, if $\langle a_{11}\rangle \subsetneq \langle a_{11}^{(1)}\rangle$, we obtain matrices $A_2, \ldots, A_\ell$ such that $\langle a_{11}\rangle \subset \langle a_{11}^{(1)}\rangle \subset \cdots \subset \langle a_{11}^{(\ell)}\rangle$. The ring R is Noetherian and, therefore, we find an ℓ such that $\langle a_{11}^{(\ell)}\rangle = \langle a_{11}^{(\ell+1)}\rangle$. This implies that, in the matrix $A_{\ell+1}$, $a_{1j}^{(\ell+1)} = 0$ for all j and $a_{j1}^{(\ell+1)} = 0$ for all j. After this step, we may assume that, for the matrix A, with respect to the bases B and B', $a_{11} \neq 0$, $a_{1j} = 0$ and $a_{j1} = 0$ for all $j > 1$.

Now we use induction to prove that, for suitable changes of $\{e_2, \ldots, e_n\}$ and $\{f_2, \ldots, f_m\}$, the presentation matrix A has diagonal form, that is, $a_{ij} = 0$ for $i \neq j$. Let M_i be the submodule of M generated by the image

of the i–th basis element. Then $M = \bigoplus_{i=1}^{n} M_i$ and $M_i \cong R/\langle a_{ii}\rangle$ if $i \leq m$, respectively $M_i \cong R$ if $i > m$. □

From the proof of Theorem 2.6.1 we deduce the following algorithm to compute a diagonal form of a presentation matrix of a module over the polynomial ring $K[x]$, K a field.

Algorithm 2.6.2 (DIAGONALFORM).

Input: A matrix A with entries in $K[x]$.
Output: A matrix D in diagonal form such that $D = BAC$ for invertible matrices B, C with entries in $K[x]$.

- if A has no non–zero entry, return A;
- exchange rows and columns to obtain $a_{11} \neq 0$;
- while there exist $i > 1$ such that $a_{1i} \neq 0$ or $a_{i1} \neq 0$
  $A :=$ ROWNF(A);
  $A :=$ transpose (ROWNF(transpose(A)));
- let $A = \begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix}$, then return $\begin{pmatrix} a_{11} & 0 \\ 0 & \text{DIAGONALFORM}(A') \end{pmatrix}$.

We use the following procedure ROWNF(A) to obtain zeros in the first column of the matrix, except at the place $(1,1)$. Let $A = (a_{ij})$ be an $n \times m$–matrix with entries in $K[x]$ and assume that $a_{11} \neq 0$.

Input: $A = (a_{ij})$ an $n \times m$–matrix with entries in $K[x]$, $a_{11} \neq 0$.
Output: ROWNF(A), an $n \times m$–matrix, such that ROWNF(A) $= C \cdot A$ for a suitable invertible matrix C, and the first column is of the form ${}^t(h, 0, \ldots, 0)$ with $h \mid a_{11}$.

- For $i = 2, \ldots, n$
  compute $h := \gcd(a_{11}, a_{i1})$;
  choose $a, b, c, d \in K[x]$, such that $h = aa_{11} + ba_{i1}$, $a_{11} = ch$, $a_{i1} = dh$ (if a_{11} divides a_{i1} then choose $a := 1$, $b := 0$, $c := 1$);
  change A by multiplying the first row with a and add to it the b–th multiple of the i–th row;
  change A by subtracting from the i–th row the d–th multiple of the (new) first row;
- return A.

SINGULAR Example 2.6.3 (diagonal form).
In this example we shall use the SINGULAR command `interred` to diagonalize a matrix. This command replaces the procedure ROWNF in Algorithm 2.6.2. In the ring $K[x]$ (with the two possible orderings `dp` and `ds`) consider, on $K[x]^n = \bigoplus_{i=1}^{n} K[x]e_i$, the ordering $>$ = `(C,dp)`, respectively `(C,ds)`. Recall that $x^\alpha e_i < x^\beta e_j$ if $i < j$, or if $i = j$, $x^\alpha <_{dp} x^\beta$ (respectively $x^\alpha <_{ds} x^\beta$).

The command `interred` applied to a matrix interreduces the columns of the matrix considered as elements of $K[x]^n$ (which is, in the case of one

variable, the same as to compute a standard basis). The result is an upper triangular matrix (the columns are ordered with respect to their leading terms, the first column with the smallest leading term).

```
proc diagonalForm(matrix M)
{
  int n=nrows(M);
  int m=ncols(M);
  matrix N,K;
  matrix L[n][m];
  while(N!=M)
  {
     N=M;
     M=L;
     K=transpose(interred(transpose(interred(N))));
     M[1..nrows(K),1..ncols(K)]=K;
  }
  return(N);
}
```

Here are two examples:

```
option(redSB);
ring R=0,(x),(C,dp);

matrix M[2][3]=(x2+1)^2,0,     0,
               0,      x3-x-1,0;
matrix N1[2][2]=1, 1,
               2,-2;
matrix N2[3][3]=1,2, 3,
               4,5, 6,
               7,8,-1;
M=N1*M*N2;
print(M);
//->x4+4x3+2x2-4x-3,  2x4+5x3+4x2-5x-3,   3x4+6x3+6x2-6x-3,
//->2x4-8x3+4x2+8x+10,4x4-10x3+8x2+10x+14,6x4-12x3+12x2+12x+18
```

Let us diagonalize M:

```
diagonalForm(M);
//-> _[1,1]=x7+x5-x4-x3-2x2-x-1
//-> _[1,2]=0
//-> _[1,3]=0
//-> _[2,1]=0
//-> _[2,2]=1
//-> _[2,3]=0
```

The second example:

```
matrix M0[5][5]=1, 1,0, 0,0,
                3,-1,0, 0,0,
                0, 0,1, 1,0,
                0, 0,3,-1,0,
                0, 0,0, 0,2;
matrix N[5][5]=1, 1, -1,  1,-1,
               2, 2,  1,  1, 0,
              -1, 2,  2,  1, 1,
              -2, 1,  1, -1, 0,
               1, 2, -2,  1, 1;
```

Now we want to compute $M = N^{-1}M_0N - xE_5$[11] and its normal form:

```
M=lift(N,freemodule(nrows(N)))*M0*N-x*freemodule(5);
print(M);
//-> -x+29/50,-71/50,  -143/50,1/25,    -71/50,
//-> 16/25,   -x+66/25,3/25,   58/25,   16/25,
//-> -24/25,  -24/25,  -x+8/25,-12/25,  -24/25,
//-> -12/25,  -12/25,  29/25,  -x-56/25,-12/25,
//-> -13/10,  -13/10,  -19/10, -7/5,    -x+7/10

print(diagonalForm(M));
//-> x2-4,0,  0,   0,0,
//-> 0,   x-2,0,   0,0,
//-> 0,   0,  x2-4,0,0,
//-> 0,   0,  0,   1,0,
//-> 0,   0,  0,   0,1
```

Corollary 2.6.4. *Let R be a principal ideal domain and M a finitely generated R–module. If M is torsion free, then M is free.*

In the following we further analyze the structure of modules over a principal ideal domain in order to obtain a unique decomposition.

Proposition 2.6.5. *Let R be a principal ideal domain and M a finitely generated R–module, then $M = F \oplus \mathrm{Tors}(M)$, F a free submodule of M. If $M \cong R^n \oplus T$, T a torsion module, then $R^n \cong F$ and $T \cong \mathrm{Tors}(M)$.*

Proof. $M/\mathrm{Tors}(M)$ is torsion free and, therefore, because of Corollary 2.6.4, free. Let $x_1, \ldots, x_s \in M$ be representatives of a basis of $M/\mathrm{Tors}(M)$, then $F := \langle x_1, \ldots, x_s \rangle$ is a free module and $F \cap \mathrm{Tors}(M) = \langle 0 \rangle$. This implies that $M = F \oplus \mathrm{Tors}(M)$.

To prove the second part, note that $\mathrm{Tors}(R^n \oplus T) = T$ and T is mapped via the isomorphism $M \cong R^n \oplus T$ to $\mathrm{Tors}(M)$. □

[11] Here E_n denotes the $n \times n$ unit matrix.

Proposition 2.6.6. *Let R be a principal ideal domain and M a finitely generated torsion R–module. Let $\langle f\rangle = \mathrm{Ann}(M)$ and $f = p_1^{c_1}\cdot\ldots\cdot p_n^{c_n}$, with p_i prime and $\langle p_i, p_j\rangle = R$ for $i \neq j$.*[12] *Let $T_{p_i}(M) := \{x \in M \mid p_i^{c_i}x = 0\}$. Then*

$$M = \bigoplus_{i=1}^{n} T_{p_i}(M)\,.$$

Proof. Let $x \in T_{p_i}(M) \cap \sum_{j\neq i} T_{p_j}(M)$. Then $p_i^{c_i}x = 0$ and

$$p_1^{c_1}\cdot\ldots\cdot p_{i-1}^{c_{i-1}}\cdot p_{i+1}^{c_{i+1}}\cdot\ldots\cdot p_n^{c_n}x = 0\,.$$

But $\langle p_i^{c_i}, p_1^{c_1}\cdot\ldots\cdot p_{i-1}^{c_{i-1}}\cdot p_{i+1}^{c_{i+1}}\cdot\ldots\cdot p_n^{c_n}\rangle = R$, because $\langle p_i, p_j\rangle = R$ for $i \neq j$ and p_i is prime for all i (Exercise 2.6.7). This implies that $x = 0$, that is, $T_{p_i}(M) \cap \sum_{j\neq i} T_{p_j}(M) = \langle 0\rangle$.

Let $x \in M$, and choose $a, b \in R$ such that $ap_n^{c_n} + bp_1^{c_1}\cdot\ldots\cdot p_{n-1}^{c_{n-1}} = 1$. We write $x = x' + x_n$ with $x' := ap_n^{c_n}x$ and $x_n := bp_1^{c_1}\cdot\ldots\cdot p_{n-1}^{c_{n-1}}x$, and obtain $x_n \in T_{p_n}(M)$ and $p_1^{c_1}\cdot\ldots\cdot p_{n-1}^{c_{n-1}}x' = 0$. Using induction, we can continue to decompose x' and obtain $x = x_1 + \cdots + x_n \in \sum_{i=1}^{n} T_{p_i}(M)$. □

Proposition 2.6.7. *Let R be a principal ideal domain, M a torsion R–module and $\mathrm{Ann}(M) = \langle p^c\rangle$, p prime. Then $M = \bigoplus_{i=1}^{s} C_i$ with cyclic R–modules C_i such that $\mathrm{Ann}(C_i) = \langle p^{n_i}\rangle$, $n_1 \geq \cdots \geq n_s$. The numbers $n_1, \ldots, n_s$ are uniquely determined by M.*

Proof. Set $M_i := \{x \in M \mid p^i x = 0\}$, which are submodules of M satisfying $M_i \supset M_{i-1}$, $i = 1, \ldots, c$. The factor modules M_i/M_{i-1} are annihilated by p, hence, $R/\langle p\rangle$–vector spaces. Let $m_1 := \dim_{R/\langle p\rangle} M_c/M_{c-1}$ and choose $x_1, \ldots, x_{m_1} \in M$ representing a basis of M_c/M_{c-1}. Then $px_1, \ldots, px_{m_1}$ are linearly independent, considered as elements in M_{c-1}/M_{c-2}: assume that $\sum_{i=1}^{m_1} h_i p x_i \in M_{c-2}$ for some $h_1, \ldots, h_{m_1} \in R$, then $p^{c-2}\cdot\sum_{i=1}^{m_1} h_i p x_i = 0$. Therefore, $p^{c-1}\cdot\sum_{i=1}^{m_1} h_i x_i = 0$, that is, $\sum_{i=1}^{m_1} h_i x_i \in M_{c-1}$, which implies $h_1 = \cdots = h_{m_1} = 0$, due to the choice of $x_1, \ldots, x_{m_1}$.

Now, choose elements $x_{m_1+1}, \ldots, x_{m_2} \in M_{c-1}$ such that $px_1, \ldots, px_{m_1}$, $x_{m_1+1}, \ldots, x_{m_2}$ represent a basis of M_{c-1}/M_{c-2} ($m_1 = m_2$ is possible). Continuing like this, we obtain a sequence $x_1, \ldots, x_{m_c} \in M$ such that, for $\nu = 0, \ldots, c-1$, the set

$$\{p^\nu x_1, \ldots, p^\nu x_{m_1}, p^{\nu-1}x_{m_1+1}, \ldots, p^{\nu-1}x_{m_2}, \ldots, x_{m_\nu+1}, \ldots, x_{m_{\nu+1}}\}$$

induces an $R/\langle p\rangle$–basis of $M_{c-\nu}/M_{c-\nu-1}$ (with the convention $m_0 = 0$).

For $i = 1, \ldots, m_c$, define $C_i := \langle x_i\rangle$ and n_i by $\mathrm{Ann}(C_i) = \langle p^{n_i}\rangle$. Obviously, $\sum_{i=1}^{m_c} C_i = M$, and we have to show $C_i \cap \sum_{j\neq i} C_j = \langle 0\rangle$: if $\sum_{i=1}^{m_c} h_i x_i = 0$ for some $h_i \in R$ then $\sum_{i=1}^{m_1} h_i p^{c-1} x_i = 0$ and, therefore, p divides h_i for

[12] Such a decomposition always exists and is uniquely determined up to permutations and multiplication with units. This is proved in the Exercises 1.3.4, 1.3.5 and later in Chapter 4.

$i = 1, \ldots, m_1$. This implies $p^{c-2}\left(\sum_{i=1}^{m_1}(h_i/p)\cdot px_i + \sum_{i=m_1+1}^{m_2} h_i x_i\right) = 0$ and, therefore, p divides h_i/p for $i = 1, \ldots, m_1$ and h_i for $i = m_1 + 1, \ldots, m_2$. Continuing like this we obtain that $p^{c-\nu}$ divides h_i for $i = m_\nu + 1, \ldots, m_{\nu+1}$ and $\nu = 0, \ldots, c-1$. This implies $h_i x_i = 0$ for all i, and we conclude that $C_i \cap \sum_{j\neq i} C_j = \langle 0\rangle$.

It remains to prove that $n_1, \ldots, n_s$ are uniquely determined by M. By construction of the x_i and definition of n_i we have $n_{m_k+1} = \ldots = n_{m_{k+1}} = c - k$, $k = 0, \ldots, c-1$. Therefore, $m_1, \ldots, m_c$ and $n_1, \ldots, n_s$ determine each other. But $m_1, \ldots, m_c$ are give by the equations $\sum_{i=1}^{k} m_i = \dim_{R/\langle p\rangle} M_{c-k+1}/M_{c-k}$, $k = 1, \ldots, c$. □

Summarizing the results obtained, we have the following theorem:

Theorem 2.6.8. *Let R be a principal ideal domain and M a finitely generated R–module, then M is a direct sum of cyclic modules, $M = \bigoplus_{i=1}^{s} C_i$. The cyclic modules C_i are free or $\mathrm{Ann}(C_i) = \langle p_i^{n_i}\rangle$, p_i prime. The number of the free cyclic modules, the prime ideals $\langle p_i\rangle$ and the numbers n_i are uniquely determined by M.*

$p_1^{n_1}, \ldots, p_s^{n_s} \in R$ are called the *elementary divisors* of M, respectively of the torsion submodule $\mathrm{Tors}(M)$.

Corollary 2.6.9. *Let R be a principal ideal domain and M be a finitely generated R–module, then M is a direct sum of cyclic modules, $M = \bigoplus_{i=1}^{r} D_i$ such that $\mathrm{Ann}(D_1) \subset \mathrm{Ann}(D_2) \subset \cdots \subset \mathrm{Ann}(D_s)$. The ideals $\mathrm{Ann}(D_i)$ are uniquely determined.*

Proof. We use Theorem 2.6.8 and write

$$M = C_1 \oplus \cdots \oplus C_t \oplus C_{1,1} \cdots \oplus C_{1,n_1} \oplus \cdots \oplus C_{r,1} \oplus \cdots \oplus C_{r,n_r}$$

such that $C_1, \ldots, C_t$ are free and $\mathrm{Ann}(C_{ij}) = \langle p_i^{m_{i,j}}\rangle$ and $m_{i,1} \leq \cdots \leq m_{i,n_i}$, p_i prime. Let $D_i := C_i$ for $i = 1, \ldots, t$. Define $D_{t+1} := \bigoplus_{i=1}^{r} C_{i,n_i}$ then

$$\langle 0\rangle = \mathrm{Ann}(D_1) = \cdots = \mathrm{Ann}(D_t) \subset \mathrm{Ann}(D_{t+1}) = \langle p_1^{m_{1,n_1}} \cdot \ldots \cdot p_r^{m_{r,n_r}}\rangle\,.$$

We continue in this manner, defining $D_{t+k} = \bigoplus_{i=1}^{r} C_{i,n_i-k}$ with the convention $C_{i,n_i-k} = \langle 0\rangle$ if $n_i - k \leq 0$. Then

$$\mathrm{Ann}(D_{t+k}) = \left\langle p_1^{m_{1,n_1-k+1}} \cdot \ldots \cdot p_r^{m_{r,n_r-k+1}}\right\rangle\,,$$

with the convention $m_{i,n_i-k+1} = 0$ if $n_i - k + 1 \leq 0$. It remains to prove that the D_i are cyclic. This will be done in the following lemma. □

Lemma 2.6.10. *Let R be a ring and $f, g \in R$ such that $\langle f, g\rangle = R$, then $R/\langle f\rangle \oplus R/\langle g\rangle \cong R/\langle f \cdot g\rangle$.*

Proof. Consider the map $\pi : R \to R/\langle f\rangle \oplus R/\langle g\rangle$ defined by

$$\pi(h) = (h \mod \langle f\rangle,\ h \mod \langle g\rangle)\,.$$

This map is surjective: Let $a, b \in R$ such that $af + bg = 1$. If

$$(h \bmod \langle f\rangle,\, k \bmod \langle g\rangle) \in R/\langle f\rangle \oplus R/\langle g\rangle$$

then $h - k = a(h-k)f + b(h-k)g$, that is,

$$h - a(k-h)f = k + b(h-k)g =: c$$

and $\pi(c) = (h \mod \langle f\rangle,\ k \mod \langle g\rangle)$.

Let $h \in \mathrm{Ker}(\pi) = \langle f\rangle \cap \langle g\rangle$, that is, $h = h_1 f = h_2 g$ for some $h_1, h_2 \in R$. But, by the above, $h_2 = ah_2 f + bh_2 g = (ah_2 + bh_1)f$, which implies $h \in \langle fg\rangle$. Finally, we obtain $\mathrm{Ker}(\pi) = \langle fg\rangle$, therefore, $R/\langle f \cdot g\rangle \cong R/\langle f\rangle \oplus R/\langle g\rangle$. □

SINGULAR Example 2.6.11 (cyclic decomposition).
To obtain the complete decomposition as in Theorem 2.6.8, we have to diagonalize the presentation matrix of a given module and factorize the diagonal elements.

```
option(redSB);
ring R=0,(x),(C,dp);

matrix M0[5][5]=1, 1,0,0,0,
                -2,-1,0,0,0,
                 0, 0,2,1,0,
                 0, 0,0,2,0,
                 0, 0,0,0,3;
matrix N[5][5]=1, 1, -1,  1,-1,
               2, 2,  1,  1, 0,
              -1, 2,  2,  1, 1,
              -2, 1,  1, -1, 0,
               1, 2, -2,  1, 1;
```

Now we compute the matrix $M = N^{-1}M_0N - xE_5$:

```
matrix M=lift(N,freemodule(nrows(N)))*M0*N-x*freemodule(5);
print(M);
//-> -x-9/10,-183/50, -59/50,  -43/25,  29/50,
//-> -6/5,   -x+18/25,-11/25,  -19/25,  16/25,
//-> -11/5,  -52/25,  -x+54/25,-34/25,  1/25,
//-> 12/5,   99/25,   52/25,   -x+83/25,-12/25,
//-> -1/2,   1/10,    -17/10,  1/5,     -x+17/10

N=diagonalForm(M);
```

```
print(N);
//-> x5-7x4+17x3-19x2+16x-12,0,0,0,0,
//-> 0,                      1,0,0,0,
//-> 0,                      0,1,0,0,
//-> 0,                      0,0,1,0,
//-> 0,                      0,0,0,1
```

This shows that the module defined by the presentation matrix M is isomorphic to $\mathbb{Q}[x]/\langle x^5-7x^4+17x^3-19x^2-16x-12\rangle$.

```
factorize(N[1,1]);
//->[1]:
//->   _[1]=1
//->   _[2]=x-3
//->   _[3]=x2+1
//->   _[4]=x-2
//->[2]:
//->   1,1,1,2
```

This shows that the decomposition of the module defined by the presentation matrix M is $\mathbb{Q}[x]/\langle x-3\rangle \oplus \mathbb{Q}[x]/\langle x^2+1\rangle \oplus \mathbb{Q}[x]/\langle x-2\rangle$.

Let us be given a finite presentation for a module N,

$$K[x]^m \xrightarrow{M} K[x]^n \xrightarrow{\pi} N \longrightarrow 0\,,$$

with presentation matrix M (with respect to the canonical basis). Algorithm 2.6.2 transforms M into a diagonal matrix, but it does not return the transformation matrices. The following procedure computes invertible matrices B and C with entries in $K[x]$ such that $MB = CD$ with D a matrix in diagonal form. Instead of M we consider the matrix

$$\begin{pmatrix} 0 & E_m \\ E_n & M \end{pmatrix} \in \mathrm{GL}(n+m, K[x])\,,$$

(E_n denoting the $n \times n$ unit matrix), and perform on this matrix appropriate row and column operations to obtain

$$\begin{pmatrix} 0 & B \\ F & D \end{pmatrix} \in \mathrm{GL}(n+m, K[x])\,,$$

with D an $n \times m$–matrix in diagonal form. Then, by construction, we obtain that $M \cdot B = C \cdot D$ with $C := F^{-1}$.

If $f_1, \ldots, f_n$ are the columns of C and if the matrix D has the entries $p_1, \ldots, p_k \in K[x]$, $k = \min\{n, m\}$, on the diagonal, then $N = \bigoplus_{i=1}^{n} \langle \pi(f_i)\rangle$ and $\langle \pi(f_i)\rangle \cong K[x]/\langle p_i\rangle$, for $i \leq k$, respectively $\langle \pi(f_i)\rangle \cong K[x]$, for $i > k$.

```
proc extendedDiagonalForm(matrix M)
{
   int n=nrows(M);
   int m=ncols(M);
   intvec v=1..n;
   intvec w=n+1..n+m;
   intvec u=1..m;
   intvec x=m+1..n+m;
   matrix E=unitmat(n);
   matrix B=unitmat(m);
   matrix N=M;            //to keep M for the test
   matrix D,K;

   while(D!=N)
   {
      D=N;
      K=transpose(interred(transpose(concat(E,D))));
      E=submat(K,v,v);
      N=submat(K,v,w);
      K=interred(transpose(concat(transpose(B),transpose(N))));
      K=simplify(K,1);    //here we normalize
      B=submat(K,u,u);
      N=submat(K,x,u);
   }
   matrix C=inverse(E);
   if(M*B!=C*D){ERROR("something went wrong");}  //test
   list Re=B,C,D;
   return(Re);
}
```

Let us apply the procedure to an example:

```
LIB"matrix.lib";
LIB"linalg.lib";
matrix M1[2][2]=x2+1,  0,
                0   ,x-1;
matrix N1[2][2]=1, 1,
                1, 2;
matrix N2[2][2]=0,-1,
                1, 1;
M=N1*M1*N2;
print(M);
//->  x-1, -x2+x-2,
//-> 2x-2,-x2+2x-3

list L=extendedDiagonalForm(M);
```

```
print(L[1]);
//-> 1,        0,
//-> 1/2x2-1/2,1/2

print(L[2]);
//-> -1/2x,    -1/2x2+1/2x-1,
//-> -1/2x+1/2,-1/2x2+x-3/2

print(L[3]);
//-> x3-x2+x-1,0,
//-> 0,        1
```

Proposition 2.6.12. *Let V be a finite dimensional K–vector space, and let $\varphi : V \to V$ be an endomorphism. Then V can be considered as $K[x]$–module via φ, setting $xv := \varphi(v)$ for $v \in V$. Let M be the matrix corresponding to φ with respect to a fixed basis $\{b_1, \ldots, b_n\}$, and define $\pi : K[x]^n \to V$ by $\pi(e_i) := b_i$, where $\{e_1, \ldots, e_n\}$ is the canonical basis of $K[x]^n$. Then*

$$K[x]^n \xrightarrow{M-xE} K[x]^n \xrightarrow{\pi} V \longrightarrow 0\,,$$

is a presentation of the $K[x]$–module V. [13]

Remark 2.6.13. Any finitely generated torsion $K[x]$–module N can be obtained in the way described in Proposition 2.6.12: let $\langle f \rangle = \mathrm{Ann}(N)$, then $K[x]/\langle f \rangle$ is a finite dimensional K–vector space and N is a finitely generated $K[x]/\langle f \rangle$–module. This implies that N is a finite dimensional K–vector space and multiplication by x defines the above endomorphism $\varphi : N \to N$.

Proof of Proposition 2.6.12. By definition of the $K[x]$–module structure, we have $\pi \circ (M - xE) = 0$. Diagonalizing the matrix $M - xE$ as in Theorem 2.6.1 does not change its determinant. In particular, the product of the diagonal elements of the diagonal form of $M - xE$ is the characteristic polynomial of M, which has degree n. This implies that

$$\dim_K K[x]^n / \operatorname{Im}(M - xE) = n = \dim(V)$$

and, therefore, $V \cong K[x]^n / \operatorname{Im}(M - xE)$. □

Remark 2.6.14. Let M be an $n \times n$–matrix with entries in K and consider, as in Proposition 2.6.12, K^n via M as $K[x]$–module. Let $B, C \in \mathrm{GL}(n, K[x])$ be invertible matrices such that

$$C^{-1} \cdot (M - xE) \cdot B \;=\; D \;=\; \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \in \mathrm{Mat}(n \times n, K[x])$$

[13] Note that $\det(M - xE)$ is the *characteristic polynomial* of M, E being the unit matrix.

is the diagonal form corresponding to $M - xE$ (as computed by `extendedDiagonalForm(M-xE)`). Let $f_1, \ldots, f_n$ be the columns of $C = (c_{ij})$, that is, a basis of $K[x]^n$ with $f_i = \sum_{j=1}^n c_{ij} e_j$, $\{e_1, \ldots, e_n\}$ being the canonical basis of $K[x]^n$. We use this notation also for the canonical basis of K^n.

Setting $v_i := \sum_{j=1}^n c_{ij}(M) \cdot e_j \in K^n$ (that is, replacing x by M in f_i), we obtain that $\langle v_i \rangle_{K[x]} \cong K[x]/\langle d_i \rangle$, and $K^n = \bigoplus_{i=1}^n \langle v_i \rangle_{K[x]}$ is a decomposition of K^n as $K[x]$–module into a direct sum of cyclic modules [14]. Finally, we can factorize the d_i and split the submodules $\langle v_i \rangle$ into direct sums, using Lemma 2.6.10. If $d_i = \prod_j d_{ji}^{\rho_{ji}}$ is a decomposition into irreducible polynomials, then $\langle v_i \rangle = \bigoplus_j V_{ij}$, where

$$V_{ij} := \left\{ w \in \langle v_i \rangle \;\middle|\; d_{ji}^{\rho_{ji}} w = 0 \right\} = \left\langle \prod_{k \neq j} d_{ki}^{\rho_{ki}} \cdot v_i \right\rangle \cong K[x]/\langle d_{ji}^{\rho_{ji}} \rangle \,.$$

The $V_{ij} \subset K^n$ are *invariant subspaces* for the endomorphism $M : K^n \to K^n$, that is, $M \cdot V_{ij} \subset V_{ij}$. Moreover,

$$\det(M - xE) = \det(C) \cdot \det(B)^{-1} \cdot \prod_{i=1}^n d_i = \det(C) \cdot \det(B)^{-1} \cdot \prod_{i,j} d_{ji}^{\rho_{ji}} \,,$$

that is, the characteristic polynomial of M is (up to multiplication by a non–zero constant) equal to $\prod_{i,j} d_{ji}^{\rho_{ji}}$.

This leads to a procedure for computing a decomposition of M into block matrices as shown in the example below.

If the characteristic polynomial splits into linear factors (for instance, if the field K is algebraically closed), we obtain the decomposition corresponding to the *Jordan normal form* of M. In the general case, a better decomposition is given by the *rational normal form*, treated in Exercise 2.6.3.

SINGULAR Example 2.6.15 (Jordan normal form).
We start with a matrix M whose characteristic polynomial does not split into linear factors, but which is already in the form described in Remark 2.6.14. We conjugate M by some invertible matrix N and, finally, compute the original form (up to normalization), according to the procedure described in Remark 2.6.14. The same method leads to the Jordan normal form of a matrix if its characteristic polynomial splits into linear factors.

```
ring R=0,(x),(C,dp);
matrix M[5][5]=1, 1,0,0,0,
              -2,-1,0,0,0,
               0, 0,2,1,0,
               0, 0,0,2,0,
               0, 0,0,0,2;
```

[14] Note that some of the v_i may be zero.

```
matrix N[5][5]=1,2, 2, 2,-1 ,          //an invertible
               1,1, 2, 1, 1,           //matrix over Q
              -1,1, 2,-1, 2,
              -1,1, 1,-1, 2,
               1,2,-1, 2, 1;
M=lift(N,freemodule(nrows(N)))*M*N;    //inverse(N)*M*N
print(M);
//-> -3/2,-21,-53/2,-8,  -14,
//-> 5/4, -6, -35/4,-1/2,-13/2,
//-> -1,  1,  3,    -1,  2,
//-> 3/4, 18, 87/4, 13/2,27/2,
//-> -3/2,2,  3/2,  -1,  4
```

We want to compute the normal form of M according to Remark 2.6.14:

```
matrix A = M-x*freemodule(5);          //the matrix M-xE
LIB"linalg.lib";
option(redSB);
list L = extendedDiagonalForm(A);      //A*L[1]=L[2]*L[3]

print(L[2]);                           //the new basis
//-> 0,          0,    -53/3250,-8/24375,       -14/24375
//-> 0,          -1/650,-7/1300,-1/48750,         -1/3750
//-> 168/1625,   1/325,-1/1625x+3/1625,-1/24375,  2/24375
//-> -3451/24375,-1/390,87/6500,-1/24375x+1/3750, 9/16250
//-> -2798/24375,-2/975,3/3250,-1/24375,-1/24375x+4/24375

print(L[3]);                           //the diagonal form
//-> x4-4x3+5x2-4x+4,0,  0,0,0,        //of M-xE
//-> 0,              x-2,0,0,0,
//-> 0,              0,  1,0,0,
//-> 0,              0,  0,1,0,
//-> 0,              0,  0,0,1
```

At this level we know that the vector space $\mathbb{Q}^5$ considered as $\mathbb{Q}[x]$–module, where x acts via the matrix M, is isomorphic to

$$\mathbb{Q}[x]/\langle x^4-4x^3+5x^2-4x+4\rangle \oplus \mathbb{Q} =: V_1 \oplus V_2\,,$$

where V_1 and V_2 are invariant subspaces.

```
matrix V1[5][4]=concat(L[1][1],M*L[1][1],M*M*L[1][1],
                                       M*M*M*L[1][1]);
matrix V2[5][1]=L[1][2];               //the 2 invariant
                                       //subspaces
list F=factorize(L[2][1,1]);
```

```
F;
//-> [1]:
//->    _[1]=1
//->    _[2]=x2+1
//->    _[3]=x-2
//-> [2]:
//->    1,1,2
```

The first diagonal element of `L[3]` does not split into linear factors over $\mathbb{Q}$.

We need a procedure to compute the matrix $p(B)$, where $p \in \mathbb{Q}[x]$ is a polynomial and B a matrix.

```
proc polyOfEndo(matrix B,poly p)
{
  int i;
  int d=nrows(B);
  matrix A=coeffs(p,var(1));
  matrix E[d][d]=freemodule(d);
  matrix C[d][d]=A[1,1]*E;
  for(i=2;i<=nrows(A);i++)
  {
     E=E*B;
     C=C+A[i,1]*E;
  }
  return(C);
}
```

Now we are able to compute bases for the invariant subspaces V_1, V_2. Since V_2 is already one–dimensional, we need only to consider V_1.

```
matrix S=polyOfEndo(M,F[1][3]^2); //the decomposition of V1
matrix V11=std(S*V1);
print(V11);
//-> -4,1,
//-> -1,-1,
//-> 0, 0,
//-> 3, 0,
//-> 0, 1

S=polyOfEndo(M,F[1][2]);
matrix V12=std(S*V1);
print(V12);
//-> -9776,13195,
//-> -7107,14214,
//-> 4888, -17258,
//-> 7107, 0,
//-> 0,    7107
```

We test whether we obtained bases, that is, whether $V_{11} \oplus V_{12} \oplus V_2 = \mathbb{Q}^5$, and whether the subspaces V_{11} and V_{12} are invariant.

```
matrix B=concat(V11,V12,V2);
det(B);                          //we obtained a basis
//-> -28428
reduce(M*V11,std(V11));          //subspaces are invariant
//-> _[1]=0
//-> _[2]=0
reduce(M*V12,std(V12));
//-> _[1]=0
//-> _[2]=0
reduce(M*V2,std(V2));
//-> _[1]=0
```

Compute the matrix with respect to the new bases, given by the invariant subspaces.

```
matrix C=lift(B,M*B);       //the matrix M with respect to
print(C);                   //the basis B
//-> -1/2,-5/4,0,         0,          0,
//-> 1,   1/2, 0,         0,          0,
//-> 0,   0,   11501/4738,-18225/9476,0,
//-> 0,   0,   225/2369,  7451/4738,  0,
//-> 0,   0,   0,         0,          2
```

We compute special bases to obtain the normal form.

```
matrix v[5][1]=V12[1];      //special basis for normal form
B=concat(V11,M*v-2*v,v,V2);
C=lift(B,M*B);              //the matrix M with respect to
print(C);                   //the basis B
//-> -1/2,-5/4,0,0,0,
//-> 1,   1/2, 0,0,0,
//-> 0,   0,   2,1,0,
//-> 0,   0,   0,2,0,
//-> 0,   0,   0,0,2
```

Hence, we obtain, up to normalization, the original matrix M we started with.

Exercises

2.6.1. Prove that Corollary 2.6.9 implies Theorem 2.6.8.

2.6.2. Write a SINGULAR procedure to compute the Jordan normal form of an endomorphism under the assumptions that the characteristic polynomial splits into linear factors over the ground field.

2.6.3. Write a SINGULAR procedure to compute the *rational normal form* of an endomorphism, that is, a block in the matrix corresponding to a cyclic submodule has the shape

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & & & & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix},$$

where $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is the characteristic polynomial.
(Hint: compute $V = \bigoplus_i \langle v_i \rangle_{K[x]}$, a decomposition of the K–vector space V into a direct sum of cyclic $K[x]$–modules as in SINGULAR Example 2.6.15. Then consider in $\langle v_i \rangle_{K[x]}$ the K–basis $v_i, xv_i, x^2v_i, \ldots$)

2.6.4. Write a SINGULAR procedure using Algorithm 2.6.2 to diagonalize the presentation matrix for modules over the ring $K[x]$, respectively $K[x]_{\langle x \rangle}$.

2.6.5. Let A be a principal ideal domain and K its quotient field. Prove that K is not a free A–module and that K/A is not a direct sum of cyclic modules.

2.6.6. Let $A = K[x]$ be the polynomial ring in one variable, $a_1, \ldots, a_r \in A$, and $M := A/\langle a_1 \rangle \oplus \cdots \oplus A/\langle a_r \rangle$. Give an algorithm to compute the decomposition of M as in Corollary 2.6.9.

2.6.7. Let R be a principal ideal domain and $p_1, \ldots, p_n \in R$ prime elements such that $\langle p_i, p_j \rangle = R$ for $i \neq j$. Prove that $\langle p_i^{c_i}, p_1^{c_1} \cdot \ldots \cdot p_{i-1}^{c_{i-1}} p_{i+1}^{c_{i+1}} \cdot \ldots \cdot p_n^{c_n} \rangle = R$ for $c_1, \ldots, c_n \in \mathbb{N}$.

2.6.8. Use SINGULAR to compute the Jordan normal form of $\begin{pmatrix} 3 & -1 & 2 \\ 1 & 1 & 2 \\ 2 & -2 & 2 \end{pmatrix}$.

2.7 Tensor Product

Let A be a ring, and let M, N, and P be A–modules. Let $B(M, N; P)$ be the A–module of bilinear maps $M \times N \to P$. In this section we want to construct a module $M \otimes_A N$, the tensor product of M and N, together with a bilinear map $M \times N \to M \otimes_A N$, $(m, n) \mapsto m \otimes n$, such that this map induces a canonical isomorphism

$$B(M, N; P) \cong \mathrm{Hom}_A(M \otimes_A N, P)$$

of A–modules, and study its properties. The tensor product reduces the theory of bilinear maps to linear maps, for the price that the modules become more complicated.

Let $\sigma : M \times N \to P$ be a *bilinear map*, that is, for all $a \in A$, $m, m' \in M$, $n, n' \in N$,

$$\begin{aligned} &\text{(B1)} \quad \sigma(am, n) = \sigma(m, an) = a\sigma(m, n)\,, \\ &\text{(B2)} \quad \sigma(m + m', n) = \sigma(m, n) + \sigma(m', n)\,, \\ &\text{(B3)} \quad \sigma(m, n + n') = \sigma(m, n) + \sigma(m, n')\,. \end{aligned}$$

To obtain the isomorphism above, the elements of type $m \otimes n$ of the module to construct have to satisfy the following properties:

$$\begin{aligned} &\text{(T1)} \quad (am) \otimes n = m \otimes (an) = a(m \otimes n)\,, \\ &\text{(T2)} \quad (m + m') \otimes n = m \otimes n + m' \otimes n\,, \\ &\text{(T3)} \quad m \otimes (n + n') = m \otimes n + m \otimes n'\,, \end{aligned}$$

for all $a \in A$, $m, m' \in M$, $n, n' \in N$. The properties (T1)–(T3) imply the bilinearity of the map $(m, n) \mapsto m \otimes n$.

To obtain a "minimal" module with this property, the following is necessary: $M \otimes_A N$ is generated by $\{m \otimes n \mid m \in M,\, n \in N\}$ and

(T4) all relations between the generators $\{m \otimes n\}$ are generated by relations of type (T1), (T2) and (T3).

This motivates the following definition:

Definition 2.7.1. Let T be the free A–module generated by the pairs (m, n), $m \in M$, $n \in N$, and let U be the submodule of T generated by the elements

$$\begin{aligned} &(am, n) - a(m, n)\,, \\ &(m, an) - a(m, n)\,, \\ &(m + m', n) - (m, n) - (m', n)\,, \\ &(m, n + n') - (m, n) - (m, n')\,, \end{aligned}$$

with $a \in A$, $m, m' \in M$ and $n, n' \in N$.

Then we define the *tensor product* $M \otimes_A N$ of M and N to be the A–module T/U, and denote by $m \otimes n$ the equivalence class of (m, n) in T/U.

Proposition 2.7.2. *There are canonical isomorphisms of A–modules*

(1) $B(M, N; P) \cong \mathrm{Hom}_A(M \otimes_A N, P)$,
(2) $B(M, N; P) \cong \mathrm{Hom}_A\big(M, \mathrm{Hom}_A(N, P)\big)$.

Proof. To prove (1), let $\varphi : M \otimes_A N \to P$ be a homomorphism. Then the properties (T1), (T2) and (T3) imply that $\phi(\varphi)(m, n) := \varphi(m \otimes n)$ defines a bilinear map $\phi(\varphi) : M \times N \to P$. Thus, we obtain a map

$$\phi : \mathrm{Hom}_A(M \otimes_A N, P) \longrightarrow B(M, N; P), \quad \varphi \longmapsto \phi(\varphi)\,,$$

which is obviously A–linear.

If $\phi(\varphi) = 0$ then $\varphi(m \otimes n) = 0$ for all $m \in M$, $n \in N$. Because $M \otimes_A N$ is generated by the elements of the form $m \otimes n$, this implies that $\varphi = 0$.

To see that ϕ is surjective, let $\sigma : M \times N \to P$ be a bilinear map. Then we can define a linear map $\varphi : M \otimes_A N \to P$ by setting $\varphi(m \otimes n) := \sigma(m, n)$. This map is well–defined and linear by the properties (B1), (B2), (B3) of σ. Obviously, $\phi(\varphi) = \sigma$ and, therefore, ϕ is an isomorphism.

To prove (2), let $\varphi : M \to \mathrm{Hom}_A(N, P)$ be a homomorphism and define $\psi(\varphi)(m, n) := \varphi(m)(n)$. Thus,

$$\psi : \mathrm{Hom}_A\big(M, \mathrm{Hom}_A(N, P)\big) \longrightarrow B(M, N; P)$$

is a map which is obviously A–linear.

If $\psi(\varphi) = 0$ then $\varphi(m)(n) = 0$ for all $m \in M$, $n \in N$. This implies that $\varphi(m)$ is the zero map for all m and, therefore, $\varphi = 0$. Now let $\sigma : M \times N \to P$ be a bilinear map, then we can define a linear map $\varphi : M \to \mathrm{Hom}_A(N, P)$ by setting $\varphi(m)(n) := \sigma(m, n)$ and obtain $\psi(\varphi) = \sigma$. This implies that ψ is an isomorphism. □

The following properties of the tensor product are easy to prove and, therefore, left as an exercise (Exercise 2.7.1).

Proposition 2.7.3. *Let M, M', N, N', and P be A–modules, let $S \subset A$ be a multiplicatively closed subset, and let $\varphi : M \to M'$ and $\psi : N \to N'$ be A–module homomorphisms. Then we have the following isomorphisms of A–modules, respectively $S^{-1}A$–modules,*

(1) $M \otimes_A N \cong N \otimes_A M$,
(2) $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$,
(3) $A \otimes_A M \cong M$,
(4) $(M \oplus N) \otimes_A P \cong (M \otimes_A P) \oplus (N \otimes_A P)$,
(5) $S^{-1}(M \otimes_A N) \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N$,

Moreover,

(6) $(\varphi \otimes \psi)(m \otimes n) := \varphi(m) \otimes \psi(n)$ *defines a homomorphism*

$$\varphi \otimes \psi : M \otimes_A N \to M' \otimes_A N' .$$

Example 2.7.4.

(1) $A^r \otimes_A A^s \cong A^{rs}$, and if $\{e_1, \ldots, e_r\}$, respectively $\{f_1, \ldots, f_r\}$, is a basis for A^r, respectively A^s, then $\{e_i \otimes f_j \mid i = 1, \ldots, r,\ j = 1, \ldots, s\}$ is a basis for $A^r \otimes_A A^s$.

(2) Let $\varphi : A^r \to A^s$ and $\psi : A^p \to A^q$ be linear maps, defined by the matrices $M = (m_{ij})_{i,j}$ (with respect to the bases $\{e_1, \ldots, e_r\}$ of A^r and $\{f_1, \ldots, f_s\}$ of A^s), respectively $N = (n_{ij})_{i,j}$ (with respect to the bases $\{g_1, \ldots, g_p\}$ of A^p and $\{h_1, \ldots, h_q\}$ of A^q). Then $\varphi \otimes \psi$ has the matrix $(m_{ca}n_{db})_{a,b;c,d}$ (with respect to the bases $\{e_1 \otimes g_1, e_1 \otimes g_2, \ldots, e_r \otimes g_p\}$

of $A^r \otimes_A A^p$ and $\{f_1 \otimes h_1, f_1 \otimes h_2, \ldots, f_s \otimes h_q\}$ of $A^s \otimes_A A^q$). More precisely, if

$$\varphi(e_a) = \sum_{c=1}^{s} m_{ca} f_c\,, \quad \psi(g_b) = \sum_{d=1}^{q} n_{db} h_d$$

then

$$(\varphi \otimes \psi)(e_a \otimes g_b) = \sum_{c=1}^{s} \sum_{d=1}^{q} m_{ca} n_{db} \cdot f_c \otimes h_d\,.$$

If $i = (c-1)q + d$ and $j = (a-1)p + b$ then the element in the i–th row and j–th column of the matrix of $\varphi \otimes \psi$ is $m_{ca} n_{db}$.

SINGULAR Example 2.7.5 (tensor product of maps).
Let M, N be matrices defining maps $\varphi : A^r \to A^s$, respectively $\psi : A^p \to A^q$. The matrix of $\varphi \otimes \psi$ can be computed as follows:

```
proc tensorMaps(matrix M, matrix N)
{
   int r=ncols(M);
   int s=nrows(M);
   int p=ncols(N);
   int q=nrows(N);
   int a,b,c,d;
   matrix R[s*q][r*p];
   for(b=1;b<=p;b++)
   {
      for(d=1;d<=q;d++)
      {
         for(a=1;a<=r;a++)
         {
            for(c=1;c<=s;c++)
            {
               R[(c-1)*q+d,(a-1)*p+b]=M[c,a]*N[d,b];
            }
         }
      }
   }
   return(R);
}
```

Let us try an example.

```
ring A=0,(x,y,z),dp;
matrix M[3][3]=1,2,3,4,5,6,7,8,9;
matrix N[2][2]=x,y,0,z;
print(M);
```

```
//-> 1,2,3,
//-> 4,5,6,
//-> 7,8,9
print(N);
//-> x,y,
//-> 0,z

print(tensorMaps(M,N));
//->  x, y,2x,2y,3x,3y,
//->  0, z, 0,2z, 0,3z,
//-> 4x,4y,5x,5y,6x,6y,
//->  0,4z, 0,5z, 0,6z,
//-> 7x,7y,8x,8y,9x,9y,
//->  0,7z, 0,8z, 0,9z
```

The next theorem gives a very important property of the tensor product.

Theorem 2.7.6. *Let $M \xrightarrow{i} N \xrightarrow{\pi} P \to 0$ be an exact sequence of A–modules, and L an A–module, then*

$$M \otimes_A L \xrightarrow{i\otimes 1_L} N \otimes_A L \xrightarrow{\pi\otimes 1_L} P \otimes_A L \to 0$$

is exact (the tensor product is right exact).

Proof. We know from Section 2.4 that it is enough to prove that

$$0 \to \mathrm{Hom}_A(P \otimes_A L, S) \to \mathrm{Hom}_A(N \otimes_A L, S) \to \mathrm{Hom}_A(M \otimes_A L, S)$$

is exact for all A–modules S.

Using both isomorphisms of Proposition 2.7.2, we see that this is equivalent to the exactness of

$$0 \to \mathrm{Hom}_A\big(P, \mathrm{Hom}_A(L,S)\big) \to \mathrm{Hom}_A\big(N, \mathrm{Hom}_A(L,S)\big) \to \mathrm{Hom}_A\big(M, \mathrm{Hom}_A(L,S)\big).$$

This is the left exactness of Hom already proved in Section 2.4. □

Example 2.7.7. Let $A = \mathbb{Z}$ and consider the exact sequence $0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/\langle 2\rangle \to 0$, $i(x) = 2x$, then

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/\langle 2\rangle \xrightarrow{i\otimes 1} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/\langle 2\rangle \xrightarrow{\pi\otimes 1} \mathbb{Z}/\langle 2\rangle \to 0$$

is exact but $i \otimes 1$ is not injective.

Namely, $(i\otimes 1)\big(a\otimes(b+\langle 2\rangle)\big) = 2a\otimes(b+\langle 2\rangle) = a\otimes\langle 2\rangle = 0$. That is, $i\otimes 1$ is, in fact, the zero map.

Corollary 2.7.8. *Let* $A^r \xrightarrow{\varphi} A^s \xrightarrow{\pi} M \to 0$ *and* $A^p \xrightarrow{\psi} A^q \xrightarrow{\lambda} N \to 0$ *be presentations of the* A*–modules* M *and* N*, then*

$$A^{sp+rq} = (A^s \otimes_A A^p) \oplus (A^r \otimes_A A^q) \xrightarrow{\sigma} A^{sq} = A^s \otimes_A A^q \xrightarrow{\pi\otimes\lambda} M \otimes_A N \to 0$$

is a presentation of the tensor product $M \otimes_A N$*, where* σ *is the composition of the addition* $A^{sq} \oplus A^{sq} \xrightarrow{+} A^{sq}$ *and* $(1_{A^s} \otimes \varphi) \oplus (\varphi \otimes 1_{A^s})$.

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \uparrow & & \uparrow & & \uparrow & \\
A^r \otimes_A N & \xrightarrow{\varphi\otimes 1} & A^s \otimes_A N & \xrightarrow{\pi\otimes 1} & M \otimes_A N & \longrightarrow & 0 \\
\uparrow{\scriptstyle 1\otimes\lambda} & & \uparrow{\scriptstyle 1\otimes\lambda} & \nearrow{\scriptstyle \pi\otimes\lambda} & \uparrow{\scriptstyle 1\otimes\lambda} & & \\
A^r \otimes_A A^q & \xrightarrow{\varphi\otimes 1} & A^s \otimes_A A^q & \xrightarrow{\pi\otimes 1} & M \otimes_A A^q & \longrightarrow & 0 \\
\uparrow{\scriptstyle 1\otimes\psi} & & \uparrow{\scriptstyle 1\otimes\psi} & & \uparrow{\scriptstyle 1\otimes\psi} & & \\
A^r \otimes_A A^p & \xrightarrow{\varphi\otimes 1} & A^s \otimes_A A^p & \xrightarrow{\pi\otimes 1} & M \otimes_A A^p & \longrightarrow & 0\,.
\end{array}$$

Because of Theorem 2.7.6 the rows and columns are exact. An easy diagram chase shows that $\pi\otimes\lambda$ is surjective and $\mathrm{Ker}(\pi\otimes\lambda) = \mathrm{Im}(1\otimes\psi)+\mathrm{Im}(\varphi\otimes 1)$. □

SINGULAR Example 2.7.9 (tensor product of modules).
Let φ and ψ be matrices describing presentations of the modules M, respectively N. We give a procedure for computing the presentation matrix of $M \otimes_A N$ as described in Corollary 2.7.8.

```
LIB"matrix.lib";

proc tensorMod(matrix Phi, matrix Psi)
{
   int s=nrows(Phi);
   int q=nrows(Psi);
   matrix A=tensorMaps(unitmat(s),Psi);  //I_s tensor Psi
   matrix B=tensorMaps(Phi,unitmat(q));  //Phi tensor I_q
   matrix R=concat(A,B);                 //sum of A and B
   return(R);
}
```

We consider an example:

```
ring A=0,(x,y,z),dp;
matrix M[3][3]=1,2,3,4,5,6,7,8,9;
matrix N[2][2]=x,y,0,z;
```

```
print(M);
//-> 1,2,3,
//-> 4,5,6,
//-> 7,8,9

print(N);
//-> x,y,
//-> 0,z

print(tensorMod(M,N));
//-> x,y,0,0,0,0,1,0,2,0,3,0,
//-> 0,z,0,0,0,0,0,1,0,2,0,3,
//-> 0,0,x,y,0,0,4,0,5,0,6,0,
//-> 0,0,0,z,0,0,0,4,0,5,0,6,
//-> 0,0,0,0,x,y,7,0,8,0,9,0,
//-> 0,0,0,0,0,z,0,7,0,8,0,9
```

For further applications we need a criterion for $\sum_i m_i \otimes n_i$ to be zero.

Proposition 2.7.10. *Let M and N be A–modules, $m_i \in M$ for $i \in I$, and $N = \langle n_i \mid i \in I \rangle$. Then $\sum_{i\in I} m_i \otimes n_i = 0$[15] if and only if there exist $a_{ij} \in A$ and $\bar{m}_j \in M$, for $i \in I$ and $j \in J$, such that $\sum_{j\in J} a_{ij}\bar{m}_j = m_i$ for all $i \in I$, and $\sum_{i\in I} a_{ij} n_i = 0$ for all $j \in J$.*

Proof. Suppose $\sum_{j\in J} a_{ij}\bar{m}_j = m_i$ and $\sum_{i\in I} a_{ij} n_i = 0$, then

$$\sum_{i\in I} m_i \otimes n_i = \sum_{i\in I}\Big(\sum_{j\in J} a_{ij}\bar{m}_j\Big) \otimes n_i = \sum_{j\in J}\Big(\bar{m}_j \otimes \sum_{i\in I} a_{ij} n_i\Big) = 0\,.$$

To prove the other direction, we consider first the special case that N is free and $\{n_i\}_{i\in I}$ is a basis of N. Using Proposition 2.7.3 (3), (4), we obtain that $\sum_{i\in I} m_i \otimes n_i \mapsto \sum_{i\in I} m_i$ induces an isomorphism $M \otimes_A N \cong \bigoplus_{i\in I} M$. This implies that $\sum_{i\in I} m_i \otimes n_i = 0$ if and only if $m_i = 0$ for all $i \in I$.

Now let N be arbitrary, and let $F_1 \xrightarrow{\lambda} F_0 \xrightarrow{\pi} N \to 0$ be a presentation of N such that there is a basis $\{e_i\}_{i\in I}$ of F_0 with $\pi(e_i) = n_i$ for all $i \in I$. Using Theorem 2.7.6, we obtain that the induced sequence

$$M \otimes_A F_1 \xrightarrow{1\otimes\lambda} M \otimes_A F_0 \xrightarrow{1\otimes\pi} M \otimes_A N \to 0$$

is exact, too. In these terms our assumption reads $(1 \otimes \pi)\big(\sum_{i\in I} m_i \otimes e_i\big) = 0$, which implies $\sum_{i\in I} m_i \otimes e_i = \sum_{j\in J} \bar{m}_j \otimes f_j$ for suitable $\bar{m}_j \in M$, $f_j \in \mathrm{Im}(\lambda)$ (using the exactness of the induced sequence). Let $f_j =: \sum_{i\in I} a_{ij} e_i$, $j \in J$, then $\sum_{i\in I} m_i \otimes e_i - \sum_{i\in I}\big(\sum_{j\in J} a_{ij}\bar{m}_j\big) \otimes e_i = 0$. This is the situation of our special case and, therefore, $m_i = \sum_{j\in J} a_{ij}\bar{m}_j$ for all $i \in I$. On the other hand, $f_j \in \mathrm{Im}(\lambda) = \mathrm{Ker}(\pi)$ and, therefore, $\sum_{i\in I} a_{ij} n_i = 0$. □

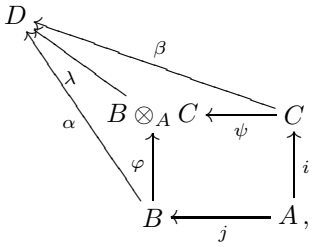
[15] Of course, there are only finitely many indices $i \in I$ with $m_i \neq 0$ in such a sum.

Now we turn to the tensor product of algebras.

Proposition 2.7.11. *Let B, C be A–algebras, then $B \otimes_A C$ is an A–algebra having the following* universal property*: for any commutative diagram*

$$\begin{array}{ccc} D & \xleftarrow{\beta} & C \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle i} \\ B & \xleftarrow[j]{} & A \end{array}$$

of A–algebras, there exists a unique A–algebra homomorphism $\lambda : B \otimes_A C \to D$ such that the diagram



with $\psi : c \mapsto 1 \otimes c$ and $\varphi : b \mapsto b \otimes 1$, commutes.

Proof. It is easy to see that $B \otimes_A C$ together with the multiplication defined by $(b \otimes c)(b' \otimes c') := (bb') \otimes (cc')$ is an A–algebra and φ and ψ are A–algebra homomorphisms such that $\varphi \circ j = \psi \circ i$.

To prove the second part of the proposition we set $\lambda(b \otimes c) := \alpha(b)\beta(c)$. If λ is well–defined, then it is obviously an A–algebra homomorphism, making the diagram commutative, and it is uniquely determined. That is, we have to prove that $\sum_{\ell \in L} b_\ell \otimes c_\ell = 0$ implies $\sum_{\ell \in L} \alpha(b_\ell)\beta(c_\ell) = 0$. Let $\{x_i\}_{i \in I}$ be a set of generators of C as an A–module, and let $c_\ell = \sum_{i \in I} c_{\ell i} x_i$ for some $c_{\ell i} \in A$. Then

$$0 = \sum_{\ell \in L} b_\ell \otimes c_\ell = \sum_{i \in I} \left(\sum_{\ell \in L} c_{\ell i} b_\ell \right) \otimes x_i \,.$$

Using Proposition 2.7.10, we obtain some $\bar{b}_j \in B$ and $a_{ij} \in A$, $j \in J$, such that $\sum_{j \in J} a_{ij} \bar{b}_j = \sum_{\ell \in L} c_{\ell i} b_\ell$ and $\sum_{i \in I} a_{ij} x_i = 0$ for all j. Now

$$\begin{aligned} \sum_{\ell \in L} \alpha(b_\ell)\beta(c_\ell) &= \sum_{\ell \in L} \alpha(b_\ell)\beta\left(\sum_{i \in I} c_{\ell i} x_i \right) = \sum_{i \in I} \alpha\left(\sum_{\ell \in L} c_{\ell i} b_\ell \right) \beta(x_i) \\ &= \sum_{i \in I} \alpha\left(\sum_{j \in J} a_{ij} \bar{b}_j \right) \beta(x_i) = \sum_{j \in J} \alpha(\bar{b}_j)\beta\left(\sum_{i \in I} a_{ij} x_i \right) = 0 \,. \end{aligned}$$

□

Corollary 2.7.12. *Let A, B, C be as in Proposition 2.7.11 and T be an A–algebra having the universal property described in 2.7.11, then there exists a unique isomorphism $T \cong B \otimes_A C$.*

Proof. We leave the proof as Exercise 2.7.3. □

Corollary 2.7.13. *Let $B = A[x_1, \ldots, x_n]/I$ and $C = A[y_1, \ldots, y_m]/J$, then $B \otimes_A C = A[x_1, \ldots, x_n, y_1, \ldots, y_m]/\langle I, J\rangle$.*

Proof. We use Corollary 2.7.12. Let

$$\begin{array}{ccc} D & \xleftarrow{\beta} & C \\ \uparrow{\scriptstyle \alpha} & & \uparrow \\ B & \longleftarrow & A \end{array}$$

be a commutative diagram of A–algebras. We define a ring map

$$\lambda : A[x_1, \ldots, x_n, y_1, \ldots, y_m]/\langle I, J\rangle \longrightarrow D$$

by setting $\lambda(x_i + \langle I, J\rangle) := \alpha(x_i + I)$ and $\lambda(y_i + \langle I, J\rangle) := \beta(y_i + J)$. If λ is well–defined then it obviously has the minimal property required for the tensor product. To prove that this is the case, let $F \in \langle I, J\rangle$, that is, we can write $F = \sum_i G_i g_i + \sum_j H_j h_j$ for suitable $g_i \in I$, $h_j \in J$, $G_i \in A[y_1, \ldots, y_m]$, $H_j \in A[x_1, \ldots, x_n]$. Then $\lambda(F) = \sum_i \beta(G_i)\alpha(g_i) + \sum_j \alpha(H_j)\beta(h_j)$. But we have $\alpha(g_i) = 0$, $\beta(h_j) = 0$, which implies that $\lambda(F) = 0$. □

SINGULAR Example 2.7.14 (tensor product of rings).
In the following, we apply Corollary 2.7.12 to compute the tensor product of rings: let $A := \mathbb{Q}[a, b, c]/\langle ab - c^2\rangle$, $B := \mathbb{Q}[x, y, z, a, b, c]/\langle x^2, y, ab - c^2\rangle$ and $C := \mathbb{Q}[u, v, a, b, c]/\langle uv, ab - c^2\rangle$, and let $A \to B$, $A \to C$ be the canonical maps.

```
ring A1=0,(a,b,c),dp;
ideal P=ab-c2;
qring A=std(P);                  // A=A1/P
poly p=abc;

ring B1=0,(x,y,z,a,b,c),dp;
ideal I=x2,y,ab-c2;
qring B=std(I);                  // B=B1/I
map ib=A,a,b,c;                  // the canonical map A-->B

ring C1=0,(u,v,a,b,c),lp;
ideal J=uv,ab-c2;
qring C=std(J);                  // C=C1/J
map ic=A,a,b,c;                  // the canonical map A-->C
```

We compute the tensor product $T = B \otimes_A C$, together with the maps $B \to T$ and $C \to T$:

```
ring T1=0,(x,y,z,u,v,a,b,c),dp; // B1 tensor C1 over A1
ideal K=imap(C1,J)+imap(B1,I);
qring T=std(K);                 // B tensor C over A
map jb=B,x,y,z,a,b,c;           // the canonical map B-->T
map jc=C,u,v,a,b,c;             // the canonical map C-->T
```

Finally, we check that the tensor product diagram commutes:

```
map psi=jc(ic);
map phi=jb(ib);
psi(p);
//-> abc
phi(p);
//-> abc
```

Exercises

2.7.1. Prove Proposition 2.7.3.

2.7.2. Let A be a ring, B an A–algebra, and M an A–module. Prove that $M \otimes_A B$ has a canonical B–module structure.

2.7.3. Prove Corollary 2.7.12.

2.7.4. Prove that $\mathbb{Z}/\langle a\rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle b\rangle = 0$ if a, b are coprime.

2.7.5. Let A be a ring, $I \subset A$ an ideal, and M an A–module. Prove that $M/IM \cong (A/I) \otimes_A M$.

2.7.6. Let A be a local ring and M, N finitely generated A–modules. Prove that $M \otimes_A N = 0$ implies $M = 0$ or $N = 0$.

2.7.7. Let $0 \to M \to N \to P \to 0$ be an exact sequence of A–modules and F a free A–module. Prove that

$$0 \to M \otimes_A F \to N \otimes_A F \to P \otimes_A F \to 0$$

is exact. (Hint: study the proof of Corollary 2.7.8.)

2.7.8. Let $\ldots \to F_i \to F_{i-1} \to \ldots \to F_0 \to 0$ be an exact sequence of A–modules and F a free A–module. Prove that

$$\ldots \to F_i \otimes_A F \to F_{i-1} \otimes_A F \to \ldots \to F_0 \otimes_A F \to 0$$

is exact.

2.7.9. Let A be a ring, let $a \in A$, and let M be an A–module. Prove that $\langle a \rangle \otimes_A M = \{a \otimes m \mid m \in M\}$.

2.7.10. Write a SINGULAR procedure to compute, for two ideals $I, J \subset K[x] = K[x_1, \ldots, x_n]$, the dimension of $K[x]/I \otimes_{K[x]} K[x]/J$.

2.7.11. Write a SINGULAR procedure to compute $\mathrm{Ker}(J \otimes_A M \to M)$, for $A = K[x_1, \ldots, x_n]/I$, $J \subset A$ an ideal and M a finitely generated A–module. Compute this kernel for $J = \langle x, y \rangle$, $M = A/J$ and $I = \langle x^2 + y^3 \rangle \subset \mathbb{Q}[x, y]$.

2.7.12. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$, let $>_1$ be a global monomial ordering on $\mathrm{Mon}(x)$ and $>_2$ be an arbitrary monomial ordering on $\mathrm{Mon}(y)$. Moreover, let $> = (>_1, >_2)$ be the corresponding product ordering on $\mathrm{Mon}(x, y)$. Show that there is an isomorphism of K–algebras

$$K[x, y]_> \xrightarrow{\cong} K[y]_{>_2} \otimes_K K[x]\,.$$

Show by an example that $K[x, y]_> \ncong K[y]_{>_2} \otimes_K K[x]_{>_1}$ if $>_1$ is local.

2.8 Operations on Modules and Their Computation

Throughout the following, let K be a field, $>$ a monomial ordering on $K[x]$, $x = (x_1, \ldots, x_n)$, and $R = K[x]_>$. Moreover, let $>_m$ be any module ordering on $K[x]^r$.

2.8.1 Module Membership Problem

The module membership problem can be formulated as follows:

Problem: Given polynomial vectors $f, f_1, \ldots, f_k \in K[x]^r$, decide whether $f \in I := \langle f_1, \ldots, f_k \rangle \subset R^r$ or not.

Solution: Compute a standard basis $G = \{g_1, \ldots, g_s\}$ of I with respect to $>_m$ and choose any weak normal form NF on R^r. Then

$$f \in I \iff \mathrm{NF}(f \mid G) = 0\,.$$

This is proved in Lemma 2.3.5. □

Additional Problem: If $f \in I = \langle f_1, \ldots, f_r \rangle \subset R^r$ then express f as a linear combination $uf = \sum_{i=1}^k g_i f_i$ with $u, g_i \in K[x]$, u a unit in R.

If $\{f_1, \ldots, f_k\}$ is a standard basis then we could compute a standard representation for f by applying NFMORA. For an arbitrary set of generators this is not possible, and we have to use a more tricky

Solution: Compute a standard basis G of $\mathrm{syz}(f, f_1, \ldots, f_k) \subset R^{k+1}$ w.r.t. the ordering $(c, >)$. Now choose any vector $h = (u, -g_1, \ldots, -g_k) \in G$ whose first component u satisfies $\mathrm{LM}(u) = 1$. Then $uf = \sum_{i=1}^k g_i f_i$.

Proof. By definition, $h = (u, -g_1, \ldots, -g_k) \in \mathrm{syz}(f, f_1, \ldots, f_k)$ if and only if $uf = \sum_{i=1}^{k} g_i f_i$. Moreover, for the chosen ordering $(c, >)$, $\mathrm{LM}(h) = \mathrm{LM}(u)\varepsilon_1$. Hence, $f \in I$ implies that we find a vector in G whose first component is a unit in R. □

The built–in commands in SINGULAR for this computation are `lift(I,f)` (which returns $g_1, \ldots, g_k$), respectively `division(f,I)` (which returns, additionally, the unit u).

SINGULAR Example 2.8.1 (module membership).

```
ring R=0,(x,y,z),(c,dp);
module M=[-z,-y,x+y,x],[yz+z2,yz+z2,-xy-y2-xz-z2];
vector v=[-xz-z2,-xz+z2,x2+xy-yz+z2];
reduce(v,std(M));
//-> [0,xy-xz+yz+z2,-xz-2yz+z2,-x2-xz]  //v is not in M

v=M[1]-x5*M[2];
v;
//-> [-x5yz-x5z2-z,-x5yz-x5z2-y,x6y+x5y2+x6z+x5z2+x+y,x]
reduce(v,std(M));
//-> 0                                   //v is in M
```

Now we want to express v in terms of generators of M.

```
syz(v+M);
//-> _[1]=[1,-1,x5]
```

This shows that $v = M[1] - x^5 M[2]$. By the built–in command `lift`, we obtain

```
lift(M,v);
//-> _[1,1]=1
//-> _[2,1]=-x5
```

In the local case one should use the built–in command `division` (cf. SINGULAR Example 1.8.2).

```
ring S=0,(x,y),(c,ds);
vector v=[x2,xy];
module M=[x+x3+y2,y3+y],[y,-x2+y2];
list L=division(v,M);
L;
//-> [1]:
//->     _[1,1]=x
//->     _[2,1]=-xy
//-> [2]:
//->     _[1]=0
//-> [3]:
//->     _[1,1]=1+x2
```

From the output, we read that $(1+x^2)\cdot v = x\cdot M[1] - xy\cdot M[2]$. The second entry of the list L is the remainder, which is 0.

2.8.2 Intersection with Free Submodules (Elimination of Module Components)

Let $R^r = \bigoplus_{i=1}^r Re_i$, where $\{e_1,\ldots,e_r\}$ denotes the canonical basis of R^r.

Problem: Given $f_1,\ldots,f_k \in K[x]^r$, $I = \langle f_1,\ldots,f_k\rangle \subset R^r$, find a (polynomial) system of generators for the submodule

$$I' := I \cap \bigoplus_{i=s+1}^{r} Re_i\,.$$

Elements of the submodule I' are said to be obtained from $f_1,\ldots,f_k$ *by eliminating* $e_1,\ldots,e_s$.

The following lemma is the basis for solving the elimination problem.

Lemma 2.8.2. *Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$ and $R = K[x]_>$. Moreover, let $I \subset R^r = \bigoplus_{i=1}^r Re_i$ be a submodule and S a standard basis of I w.r.t. the module ordering $>_m = (c,>)$ defined by*

$$x^\alpha e_i > x^\beta e_j \;:\Longleftrightarrow\; j<i \;\text{ or }\; (\,j=i \text{ and } x^\alpha > x^\beta\,)\,.$$

Then, for any $s = 0,\ldots,r-1$, $S' := S \cap \bigoplus_{i=s+1}^r Re_i$ is a standard basis of $I' = I \cap \bigoplus_{i=s+1}^r Re_i$ w.r.t. $(c,>)$. In particular, S' generates I'.

Proof. Let $h \in I'$, then we have to prove that there exists $f \in S'$ such that $\mathrm{LM}(f) \mid \mathrm{LM}(h)$.

Because S is a standard basis of I there exists $f \in S$ such that $\mathrm{LM}(f)$ divides $\mathrm{LM}(h)$. In particular, $\mathrm{LM}(f) \in \bigoplus_{i=s+1}^r K[x]e_i$. Now, by definition of the ordering, we obtain $f \in \bigoplus_{i=s+1}^r Re_i$, in particular, $f \in S'$. □

Hence, we obtain

Solution: Compute a standard basis $G = \{g_1,\ldots,g_s\}$ of I w.r.t. $(c,>)$. Then

$$G' := \left\{ g \in G \;\middle|\; \mathrm{LM}(g) \in \bigoplus_{i=s+1}^{r} K[x]e_i \right\}$$

is a standard basis for I'. □

SINGULAR Example 2.8.3 (elimination of module components).

```
ring R=0,(x,y,z),(c,dp);
module T=[xy,1,0,0],[yz,0,1,0],[xz,0,0,1];
module N=std(T);
N;
//-> N[1]=[0,0,x,-y]
//-> N[2]=[0,z,0,-y]
//-> N[3]=[yz,0,1]
//-> N[4]=[xz,0,0,1]
//-> N[5]=[xy,1]
```

From the output, we read

$$N \cap \bigoplus_{i=2}^{4} Re_i = \left\langle \begin{pmatrix} 0 \\ z \\ 0 \\ -y \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ x \\ -y \end{pmatrix} \right\rangle , \quad N \cap \bigoplus_{i=3}^{4} Re_i = \left\langle \begin{pmatrix} 0 \\ 0 \\ x \\ -y \end{pmatrix} \right\rangle .$$

2.8.3 Intersection of Submodules

Problem: Given $f_1, \ldots, f_k,\ h_1, \ldots, h_s \in K[x]^r$, let $I_1 = \langle f_1, \ldots, f_k \rangle R^r$ and $I_2 = \langle h_1, \ldots, h_s \rangle R^r$. We want to compute a (polynomial) system of generators for the intersection $I_1 \cap I_2$.

One solution would be to generalize the procedure described in Section 1.8.7 (cf. Exercise 2.8.3). Here we describe an alternative procedure, based on syzygies.

Lemma 2.8.4. *With the above assumptions, let $g \in K[x]^r$. Moreover, let $c_1, \ldots, c_{r+k+s} \in K[x]^{2r}$ be the columns of the $2r \times (r+k+s)$–matrix*

$$\left(\begin{array}{ccc|c|c} 1 & & 0 & & \\ & \ddots & & f_1 \ \ldots \ f_k & 0 \ \ldots \ 0 \\ 0 & & 1 & & \\ \hline 1 & & 0 & & \\ & \ddots & & 0 \ \ldots \ 0 & h_1 \ \ldots \ h_s \\ 0 & & 1 & & \end{array}\right) .$$

Then $g \in I_1 \cap I_2 \subset R^r$ if and only if g appears as the first r components of some $g' \in \operatorname{syz}(c_1, \ldots, c_{r+k+s}) \subset R^{r+k+s}$.

The proof is easy and left as Exercise 2.8.2.

Solution: Let $c_1, \ldots, c_{r+k+s} \in K[x]^{2r}$ be as in Lemma 2.8.4 and compute a generating set $M = \{p_1, \ldots, p_\ell\}$ of $\operatorname{syz}(c_1, \ldots, c_{r+k+s})$. The projections of $p_1, \ldots, p_\ell$ to their first r components generate $I_1 \cap I_2$. □

The corresponding SINGULAR command is `intersect(`I_1, I_2`)`.

SINGULAR Example 2.8.5 (intersection of submodules).

```
ring R=0,(x,y),(c,dp);
module I1=[x,y],[y,1];
module I2=[0,y-1],[x,1],[y,x];

intersect(I1,I2);
//-> _[1]=[y2-y,y-1]
//-> _[2]=[xy+y,x+1]
//-> _[3]=[x,y]
```

When using the procedure described before, we obtain a different set of generators:

```
vector c1=[1,0,1,0];
vector c2=[0,1,0,1];
vector c3=[x,y,0,0];
vector c4=[y,1,0,0];
vector c5=[0,0,0,y-1];
vector c6=[0,0,x,1];
vector c7=[0,0,y,x];
module M=c1,c2,c3,c4,c5,c6,c7;
syz(M);
//-> _[1]=[y,-y2+x+1,y,-x-1,y+1,0,-1]
//-> _[2]=[x,y,-1,0,-1,-1]
//-> _[3]=[y2-y,y-1,0,-y+1,x-1,0,-y+1]
```

From the output, we read that $I_1 \cap I_2$ is generated by the following vectors:

```
vector r1=[y,-y2+x+1];
vector r2=[x,y];
vector r3=[y2-y,y-1];
```

Both computations give the same module, for instance,

```
r1+y*r2;
//-> [xy+y,x+1]
```

2.8.4 Quotients of Submodules

Problem: Let I_1 and $I_2 \subset R^r$ be as in Section 2.8.3. Find a (polynomial) system of generators for the quotient

$$I_1 :_R I_2 = \left\{ g \in R \,\middle|\, gI_2 \subset I_1 \right\}.$$

Note that $I_1 :_R I_2 = \mathrm{Ann}_R\big((I_1 + I_2)/I_1\big)$, in particular, if $I_1 \subset I_2$, then we have $I_1 :_R I_2 = \mathrm{Ann}_R(I_2/I_1)$.

We proceed as in the ideal case (cf. Section 1.8.8):

Solution 1: Compute generating sets G_i of $I_1 \cap \langle h_i \rangle$, $i = 1, \ldots, s$, according to Section 2.8.3, "divide" the generators by the vector h_i, getting the generating set $G_i' = \{g \in R \mid gh_i \in G_i\}$ for $I_1 :_R \langle h_i \rangle$. Finally, compute the intersection $\bigcap_i (I_1 :_R \langle h_i \rangle)$, again according to 2.8.3. □

Note that there is a trick which can be used to "divide" by the vector h_i: let $G_i = \{v_1, \ldots, v_\ell\}$ and compute a generating system $\{w_1, \ldots, w_m\}$ for $\mathrm{syz}(v_1, \ldots, v_\ell, h_i)$. Then the last $(= (\ell+1)$–th) components of $w_1, \ldots, w_m$ generate the R–module $I_1 :_R \langle h_i \rangle$.

Solution 2: Define $h := h_1 + t_1 h_2 + \ldots + t_{s-1} h_s \in K[t_1, \ldots, t_{s-1}, x_1, \ldots, x_n]^r$, and compute a generating system for $(I_1 \cdot R[t]) :_{R[t]} \langle h \rangle_{R[t]}$, as before. Finally, eliminate $t_1, \ldots, t_{s-1}$ from $(I_1 \cdot R[t]) :_{R[t]} \langle h \rangle_{R[t]}$ (cf. Section 1.8.2). □

Let us consider the same problem for modules which are given by a presentation matrix.

Problem: Let $A = R/I$ for some ideal $I \subset R$, and let $\varphi : M_1 \to M_2$ be an A–module homomorphism, given by matrices B, B_1, B_2 with entries in R, such that the induced diagram

$$\begin{array}{ccccccc} A^r & \xrightarrow{B_1} & A^p & \longrightarrow & M_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle B} & & \downarrow{\scriptstyle \varphi} & & \\ A^s & \xrightarrow{B_2} & A^q & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

is commutative with exact rows. Compute generators for the ideal

$$\varphi(M_1) :_A M_2 = \mathrm{Ann}_A\big(M_2/\varphi(M_1)\big)\,.$$

Solution: Let $b_1, \ldots, b_p \in R^q$ and $g_1, \ldots, g_s \in R^q$ represent the columns of B and B_2, respectively, and let $\{e_1, \ldots, e_q\}$ denote the canonical basis of R^q. Then

$$\begin{aligned} \varphi(M_1) :_A M_2 &= \big((BA^p + \mathrm{Im}(B_2))/\,\mathrm{Im}(B_2)\big) :_A \big(A^q/\,\mathrm{Im}(B_2)\big) \\ &= \mathrm{Ann}_A\big(A^q/(BA^p + \mathrm{Im}(B_2))\big) \\ &= \langle g_1, \ldots, g_s, b_1, \ldots, b_p \rangle :_A \langle e_1, \ldots, e_q \rangle \\ &= \pi\big(\langle g_1, \ldots, g_s, b_1, \ldots, b_p \rangle + I \cdot R^q\big) :_R \langle e_1, \ldots, e_q \rangle\,, \end{aligned}$$

where $\pi : R \to A = R/I$ denotes the canonical projection. Hence, we can apply again the method from above. □

The built–in command in SINGULAR for this computation is `quotient(`I_1, I_2`)`, which also works over quotient rings of R.

SINGULAR Example 2.8.6 (quotient of submodules).

```
ring R=0,(x,y,z),(c,dp);
module I=[xy,xz],[yz,xy];
module J=[y,z],[z,y];
ideal K=quotient(I,J);
K;
//-> K[1]=x2y2-xyz2
reduce(K*J,std(I));       //test if KJ is contained in I
//-> _[1]=0
//-> _[2]=0
```

Since R has no zerodivisors, $\mathrm{Ann}_R(J) = \langle 0\rangle :_R J = \langle 0\rangle$, but the annihilator $\mathrm{Ann}_A(J)$ over the quotient ring $A = R/(I :_R J)$ is not trivial:

```
qring A=std(K);
module Null;
module J=[xy,xyz-x2y2],[xy2,y2x];
ideal ann=quotient(Null,J);          //annihilator of J
ann;
//-> ann[1]=xy-z2
```

Now let $M_1, M_2 \subset A^3$ be given by presentation matrices $B_1 \in \mathrm{Mat}(3\times 2, A)$, respectively, $B_2 \in \mathrm{Mat}(3\times 4, A)$, and let $\varphi : M_1 \to M_2$ be given by a matrix $B \in \mathrm{Mat}(3\times 3, A)$. We compute $\varphi(M_1) :_A M_2 = \mathrm{Ann}_A(M_2/\varphi(M_1))$.

```
module B1 = [x2,xy,y2],[xy,xz,yz];   //presentation of M1
module B  = [x,zx,zy],[y,zy,xy],[x+y,zx+zy,zy+xy];
module B2 = B[1],B[2],B1[1],B1[2];   //presentation of M2

reduce(B*B1,std(B2)); //test if im(B*B1) contained in im(B2)
//-> _[1]=0
//-> _[2]=0

quotient(B2+B,freemodule(3));        //the annihilator
//-> _[1]=x3y-xy2z
```

2.8.5 Radical and Zerodivisors of Modules

Let $A = R/I$ for some ideal $I \subset R$ and let M, N be two A–modules with $N \subset M$. Define the *radical of N in M* as the ideal

$$\mathrm{rad}_M(N) := \sqrt[M]{N} := \left\{ g \in A \;\middle|\; g^q M \subset N \text{ for some } q > 0 \right\}.$$

Problem: Solve the *radical membership problem* for modules, that is, decide whether $f \in A$ is contained in $\sqrt[M]{N}$, or not. [16]

[16] Cf. Exercises 4.1.13 – 4.1.15 to see how $\sqrt[M]{N}$ is related to a primary decomposition of M.

Solution: By Exercise 2.8.6, $\sqrt[M]{N} = \sqrt{\mathrm{Ann}_A(M/N)}$. Hence, we can compute generators for $\mathrm{Ann}_A(M/N) = N :_A M \subset A$ as in Section 2.8.4, and then we are reduced to solving the radical membership problem for ideals which was solved in Section 1.8.6. [17] □

A slightly different problem is the zerodivisor test:

Problem: Decide whether a given $f \in A$ is a zerodivisor of M, that is, whether there exists some $m \in M \setminus \{0\}$ such that $f \cdot m = 0$.

Solution: The element f defines an endomorphism $\varphi_f : M \to M$, $m \mapsto f \cdot m$, which is induced by $f \cdot E_r : A^r \to A^r$, with E_r the $r \times r$ unit matrix. It follows that f is a zerodivisor of M if and only if $\mathrm{Ker}(\varphi_f) \neq 0$. The computation of $\mathrm{Ker}(\varphi_f)$ is explained in Section 2.8.7. □

Note that $\mathrm{Ker}(\varphi_f)$ is a special case of the *quotient of a module by an ideal*

$$\mathrm{Ker}(\varphi_f) = \langle 0 \rangle :_M \langle f \rangle = \{m \in M \mid f \cdot m = 0\}.$$

Hence, f is a zerodivisor of $M = A^q/N$ if and only if $N :_{A^q} \langle f \rangle \neq 0$.

SINGULAR Example 2.8.7 (radical, zerodivisors of modules).
We check first whether a polynomial f is in the radical of N in A^3, with $A = Q[x,y,z]/\langle xy(xy - z^2)\rangle$.

```
ring R   = 0,(x,y,z),(c,dp);
ideal I  = x2y2-xyz2;
qring A  = std(I);
poly f   = xy*(y-z)*(y-1);
module N = [x,xz,y2],[y,yz,z2],[x2,xy,y2],[xy,xz,yz];
ideal ann= quotient(N,freemodule(3));   //annihilator of
                                        // Coker(N)
ring Rt  = 0,(t,x,y,z),dp;
ideal I  = imap(R,I);
ideal ann= imap(A,ann),I;
poly f   = imap(A,f);
ideal J  = ann,1-t*f;
eliminate(J,t);
//-> _[1]=1
```

Hence, f is contained in $\sqrt[A^3]{N}$, that is, some power of f maps A^3 to N. In particular, f should be a zerodivisor of A^3/N. Let us check this:

```
setring A;
size(quotient(N,f));
//-> 9
```

Hence, $N :_{A^3} \langle f \rangle \neq 0$ and f is a zerodivisor of A^3/N.

[17] If $M, N \subset A^r$ are given by generating systems $m_1, \ldots, m_p \in R^r$, $n_1, \ldots, n_q \in R^r$, then $\sqrt{N :_A M} = \sqrt{(\langle n_1, \ldots, n_q \rangle + I\,R^r) :_R \langle m_1, \ldots, m_p \rangle}$ mod I.

2.8.6 Annihilator and Support

Let $I = \langle f_1, \ldots, f_k \rangle \subset R$ be an ideal, and M an $A = R/I$–module. By Lemma 2.1.41, the *support of* M is the zero–set of the annihilator ideal of M,

$$\operatorname{supp}(M) = V\big(\operatorname{Ann}_A(M)\big)\,,$$

where $\operatorname{Ann}_A(M) = \{g \in A \mid gM = 0\} = \langle 0 \rangle :_A M$.

Problem: Compute a system of generators of some ideal $J \subset A$ satisfying

$$\operatorname{supp}(M) = V(J) = \{P \subset A \text{ prime ideal } \mid P \supset J\}$$

There are two cases of interest:

(I) $M \subset A^r$ is given by a system of generators $m_1, \ldots, m_s \in R^r$,

(II) M has the presentation $A^p \xrightarrow{B} A^q \to M \to 0$, given in form of a matrix $B \in \operatorname{Mat}(q \times p, R)$.

Note that $\operatorname{Ann}_R(M) = 0$ for $M \subset R^r$, since $R = K[x]_>$ has no zerodivisors. Hence, the first case is only interesting if $I \neq 0$.

Solution 1: We compute a system of generators for $J = \operatorname{Ann}_A(M)$.

In Case (I), this can be done by computing a system of generators for $\langle 0 \rangle :_A M$ as described in Section 2.8.4, with $A = R/I$ as basering. The latter means to compute a system of generators for the quotient $(I \cdot R^r) :_R \langle m_1, \ldots, m_r \rangle$, with R as basering and with $I \cdot R^r = \langle f_i e_j \mid 1 \leq i \leq k,\ 1 \leq j \leq r \rangle$,[18] and then to project modulo I.

In Case (II), we have $M \cong A^q / \operatorname{Im}(B)$ where $\operatorname{Im}(B) \subset A^q$ is the submodule generated by the columns of B. Hence, $\operatorname{Ann}_A(M) = \operatorname{Im}(B) :_A A^q$, and the generators of $\operatorname{Im}(B) :_A A^q$ computed as in Section 2.8.4 with A as basering, generate $\operatorname{Ann}_A(M)$. □

We shall see in Section 7.2 on Fitting ideals, that the 0–th *Fitting ideal* $F_0(M)$ satisfies also $\operatorname{supp}(M) = V\big(F_0(M)\big)$ (cf. Exercise 7.2.5). This leads to the following

Solution 2: We compute a system of generators for $J = F_0(M)$.

In Case (I), this can be done by computing a system of generators $\{b_1, \ldots, b_p\}$ of the module of syzygies $\operatorname{syz}^A(m_1, \ldots, m_s) \subset A^q$, cf. Remark 2.5.6. The b_i are the columns of a matrix B, defining a presentation $A^p \xrightarrow{B} A^q \to M \to 0$. Then the q–minors of B generate $F_0(M)$, cf. Definition 7.2.4.

In Case (II), it is clear that the q–minors of the presentation matrix B generate $F_0(M)$.

[18] Here $\{e_1, \ldots, e_r\}$ denotes the canonical basis of R^r.

SINGULAR Example 2.8.8 (annihilator and Fitting ideal).
We compute the annihilator and the Fitting ideal of a module $M = \mathrm{Coker}(B)$ given by a presentation matrix B over the quotient ring $A = R/I$, where $R = \mathbb{Q}[x, y, z, u]$ and $I = \langle x^2y^2 - xyz^2 \rangle$.

```
ring R   = 0,(x,y,z,u),dp;
ideal I  = x2y2-xyz2;
qring A  = std(I);
module B = [x,xz,y2],[y,yz,z2],[x2,xy,y2];
ideal ann= quotient(B,freemodule(3));
ideal fit= minor(B,3);
ann;                              //annihilator of Coker(B)
//-> ann[1]=x3z3-xy2z3+xy4-x2yz2
//-> ann[2]=x4yz2-xy2z4+xy4z-x2yz3
//-> ann[3]=x5z2-x2yz4+xy4-x2yz2

fit;                              //Fitting ideal of Coker(B)
//-> fit[1]=-x2y3z+x3z3+xy4-x2yz2
```

We now check that `fit` $\subset$ `ann` $\not\subset$ `fit`, but `ann`$^2 \subset$ `fit`, by counting the number of non–zero generators after reduction.

```
size(reduce(fit,std(ann)));
//-> 0
size(reduce(ann,std(fit)));
//-> 2
size(reduce(ann*ann,std(fit)));
//-> 0
```

2.8.7 Kernel of a Module Homomorphism

Let $A = R/I$ for some ideal $I \subset R$, let $U \subset A^n$, $V = \langle v_1, \ldots, v_s \rangle \subset A^m$ be submodules, and let $\varphi : A^n/U \to A^m/V$ be an A–module homomorphism defined by the matrix $B = (b_1, \ldots, b_n)$, $b_i \in A^m$.

Problem: Compute a system of generators in $A^n = \bigoplus_{i=1}^n Ae_i$ for $\mathrm{Ker}(\varphi)$.

Note that $f = \sum_{i=1}^n f_i e_i \in \mathrm{Ker}(\varphi)$ if and only if there exist $y_1, \ldots, y_s \in A$ such that $\sum_{i=1}^n f_i b_i = \sum_{j=1}^s y_j v_j$, in particular, $(f_1, \ldots, f_n, -y_1, \ldots, -y_s)$ is a syzygy of $b_1, \ldots, b_n$, $v_1, \ldots, v_s$. Hence, we obtain the following

Solution: Compute a system of generators $\{h_1, \ldots, h_\ell\}$ for the module of syzygies $\mathrm{syz}(b_1, \ldots, b_n, v_1, \ldots, v_s) \subset A^{n+s}$ (cf. Remark 2.5.6). Let $h'_i \in A^n$ be the vector obtained from h_i when omitting the last s components, $i = 1, \ldots, \ell$. Then $\{h'_1, \ldots, h'_\ell\}$ is a generating system for $\mathrm{Ker}(\varphi)$. □

SINGULAR Example 2.8.9 (kernel of a module homomorphism).

```
ring R=0,(x,y,z),(c,dp);
ideal I=x2y2-xyz2;
qring A=std(I);                    // quotient ring A=R/I
module V=[x2,xy,y2],[xy,xz,yz];
matrix B[3][2]=x,y,zx,zy,y2,z2;
module N=B[1],B[2],V[1],V[2];
module Re=syz(N);                  // syzygy module of N
module Ker;
int i;
for(i=1;i<=size(Re);i++){Ker=Ker+Re[i][1..2];}
Ker;                               // kernel of B
//-> Ker[1]=[xy2-yz2]
//-> Ker[2]=[y3z-x2z2-xyz2+y2z2-xz3+yz3,xy3-x2yz]
//-> Ker[3]=[x2yz-xz3]
//-> Ker[4]=[x3z+x2z2-xyz2-y2z2+xz3-yz3,x3y-xy2z]
//-> Ker[5]=[x3y-x2z2]

reduce(B*Ker,std(V));              // test
//-> _[1]=0
//-> _[2]=0
//-> _[3]=0
//-> _[4]=0
//-> _[5]=0
```

We can use the built–in command `modulo` (cf. SINGULAR Example 2.1.26).

```
modulo(B,V);
```

gives the same result as `Ker;`.

2.8.8 Solving Systems of Linear Equations

Let $I = \langle f_1, \ldots, f_k \rangle \subset R$ be an ideal, with $f_i \in K[x]$ polynomials, and let $S = R/I$. Moreover, let

$$\begin{array}{ccc} a_{11}Z_1 + \ldots + a_{1m}Z_m & = & b_1 \\ \vdots \qquad\qquad \vdots & & \vdots \\ a_{r1}Z_1 + \ldots + a_{rm}Z_m & = & b_r \end{array}$$

be a system of linear equations, with $a_{ij}, b_i \in K[x]$ and indeterminates Z_j. We can write the above system as a matrix equation $AZ = b$, where

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1m} \\ \vdots & & \vdots \\ a_{r1} & \ldots & a_{rm} \end{pmatrix}, \quad Z = \begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}.$$

A is called the *coefficient matrix* of the system and the concatenated matrix $(A \mid b)$ is called the *extended coefficient matrix*.

Problems:

(1) Check whether the system $AZ = b$ is solvable over S, and if so, then find a solution. That is, we are looking for a vector $z \in S^m$ such that the equation $Az = b$ holds in S^r. The set of all such solutions z is denoted by $\mathrm{Sol}_S(AZ = b)$.

(2) Consider the homogeneous system $AZ = 0$. The set of solutions is the kernel of the linear map $A : S^m \to S^r$ and, hence, a submodule of S^m. The problem is to find a set of generators of $\mathrm{Sol}_S(AZ = 0)$. Note that if $z \in \mathrm{Sol}_S(AZ = b)$ is a "special" solution of the inhomogeneous system, then $z + \mathrm{Sol}_S(AZ = 0) := \{z + w \mid w \in \mathrm{Sol}_S(AZ = 0)\}$ is the set of all solutions for $AZ = b$.

Solution 1: We assume that the a_{ij} and b_j are elements of a field F.[19] We create the ideal

$$E = \left\langle \sum_{j=1}^{m} a_{1j}Z_j - b_1 \, , \, \ldots \, , \, \sum_{j=1}^{m} a_{rj}Z_j - b_r \right\rangle$$

in $F[Z_1, \ldots, Z_m]$ and compute a reduced standard basis G of E with respect to a global monomial ordering. The system $AZ = b$ is solvable over F if and only if $G \neq \{1\}$ and then the solutions can be read from G.

In case $F = K(x_1, \ldots, x_n)$, the x_i are considered as parameters and if $AZ = b$ is not solvable over F this means that there is no vector $z(x)$ of rational functions, satisfying $AZ = b$. Hence $A(x) \cdot z(x) = b(x)$ has no solution for general x. Nevertheless, there may exist solutions for special x which satisfy some constraints. What we can do now is to create a ring with the x_i as variables, and then a standard basis of the ideal E in this ring, eventually, computes equations in the x_i such that $A(\overline{x}) \cdot Z = b(\overline{x})$ is solvable for all $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_n) \in S^n$ satisfying these equations (see SINGULAR Example 2.8.10 below).

Solution 2: We consider now the general case.

(1) $AZ = b$ is solvable over S if and only if b is in the image of the module homomorphism $A : S^m \to S^r$. Hence, we have to check whether b is contained in the submodule $\mathrm{Im}(A) \subset S^r$, generated by the columns $a_1, \ldots, a_m$ of A. If the latter is given, then we have to find $z_1, \ldots, z_m \in S$, such that $b = \sum_{i=1}^{m} z_i a_i$. However, this problem was already solved in Section 2.8.1.

[19] For instance, consider a_{ij}, b_j as elements of the quotient field $K(x_1, \ldots, x_n)$.

(2) Finding generators for $\mathrm{Sol}_S(AZ = 0)$ means nothing else but finding generators for $\mathrm{Ker}(A : S^m \to S^r)$, and this problem was solved in Section 2.8.7.

Note that solving over $K[x]/I$ means that the solution $z(p)$ satisfies the linear equation $A(p) \cdot z(p) = b(p)$ for p in the zero–set of $f_1, \ldots, f_k$ (*solving with polynomial constraints*).[20]

SINGULAR Example 2.8.10 (solving linear equations).
Consider the system of linear equations in x, y, z, u,

$$\begin{array}{rcl} 3x + y + z - u &=& a \\ 13x + 8y + 6z - 7u &=& b \\ 14x + 10y + 6z - 7u &=& c \\ 7x + 4y + 3z - 3u &=& d \end{array} \qquad (*)$$

where a, b, c, d are parameters. Moreover, we also consider the system $(**)$, which has the additional equation

$$x + y + z - u \;=\; 0\,.$$

We want to solve these systems by expressing x, y, z, u as functions of the parameters a, b, c, d if possible, respectively find conditions for the parameters such that the system is solvable.

Following Solution 1, we can express the systems $(*)$ and $(**)$ as ideals `E` and `EE` in a ring with a, b, c, d as parameters:

```
ring R = (0,a,b,c,d),(x,y,z,u),(c,dp);
ideal E =  3x +   y +  z -  u - a,
          13x +  8y + 6z - 7u - b,
          14x + 10y + 6z - 7u - c,
           7x +  4y + 3z - 3u - d;

ideal EE =  E, x + y + z - u;
```

Computing a reduced standard basis performs a complete Gaussian elimination, showing that there is a unique solution to the system $(*)$:

[20] Hilbert's Nullstellensatz 3.5.2 implies that, for a radical ideal I, to solve the system $AZ = b$ over $K[x]/I$ means nothing else but to look for polynomial vectors $z = (z_1, \ldots, z_m) \in K[x]^m$ such that $A(p) \cdot z(p) = b(p)$, for all $p \in V_{\overline{K}}(I)$. Here

$$V_{\overline{K}}(I) := \{p = (p_1, \ldots, p_n) \in \overline{K}^n \mid f_1(p) = \ldots = f_k(p) = 0\}$$

denotes the zero–set of I over the algebraic closure $\overline{K}$ of K.

The same remark applies for solving over $K[x]_{\langle x\rangle}/I$, except that we are looking for solutions in some Zariski open neighbourhood of 0, subject to the constraints $f_1 = \ldots = f_k = 0$ (cf. Appendix A.2).

```
option(redSB);
simplify(std(E),1);              //compute reduced SB
//-> _[1]=u+(6/5a+4/5b+1/5c-12/5d)
//-> _[2]=z+(16/5a-1/5b+6/5c-17/5d)
//-> _[3]=y+(3/5a+2/5b-2/5c-1/5d)
//-> _[4]=x+(-6/5a+1/5b-1/5c+2/5d)
```

We read the solution of $(*)$:

$$\begin{aligned} x &= \tfrac{1}{5}\cdot\left(6a-b+c-2d\right),\\ y &= \tfrac{1}{5}\cdot\left(-3a-2b+2c+d\right),\\ z &= \tfrac{1}{5}\cdot\left(-16a+b-6c+17d\right),\\ u &= \tfrac{1}{5}\cdot\left(-6a-4b-c+12d\right). \end{aligned}$$

Doing the same for `EE` gives 1:

```
std(EE);
//-> _[1]=1
```

This means that the system $(**)$ has no solution over the field $\mathbb{Q}(a,b,c,d)$, or, in other words, $(**)$ has no complex solutions for fixed *general* values of a,b,c,d. This is clear, since the extra equation for $(**)$, $x+y+z=u$ gives a linear condition in a,b,c,d for the solutions of $(*)$. Since general values of the parameters do not satisfy this equation, $(**)$ has no solution over the field of rational functions in a,b,c,d.

If we want to find conditions for a,b,c,d under which $(**)$ has a solution and then to solve it, we have to pass to a ring with a,b,c,d as variables. Since we have to solve for x,y,z,u, these variables have to come first.

```
ring R1 = 0,(x,y,z,u,a,b,c,d),(c,dp);
```

Now we compute a reduced standard basis (up to normalization) for the ideal generated by the rows of the system $(**)$.

```
ideal EE = imap(R,EE);
std(EE);
//-> _[1]=7a-2b+2c-4d
//-> _[2]=7u+8b-c-12d
//-> _[3]=7z+5b+2c-11d
//-> _[4]=7y+4b-4c+d
//-> _[5]=7x-b+c-2d
```

The first polynomial gives $7a-2b+2c-4d=0$, which must be satisfied by the parameters to have a solution for $(**)$. The remaining polynomials then give the solutions for x,y,z,u in terms of b,c,d (a has already been substituted).

Another method is to work directly on the (extended) coefficient matrix. The standard basis algorithm applied to a matrix operates on the module

generated by the columns of the matrix. Hence, in order to solve the linear system, we have to transpose the matrix and to make sure that the module ordering gives priority to the columns (for example, `(c,dp)`).

First we have to write two procedures which return the coefficient matrix, respectively the extended coefficient matrix, of an ideal, describing the system of linear equations as above.

```
LIB "matrix.lib";
proc coeffMat (ideal i)
{
   int ii;
   int n = nvars(basering);
   int m = ncols(i);
   matrix C[m][n];
   for ( ii=1; ii<=n; ii++)
   {
      C[1..m,ii] = i/var(ii);
   }
   return(C);
}

proc coeffMatExt(ideal i)
{
   matrix C = coeffMat(i);
   C = concat(C,transpose(jet(i,0)));
   return(C);
}
```

Now we consider again the above example, and, of course, obtain the same answers as before:

```
setring R;
matrix CE = coeffMatExt(EE);
matrix C = coeffMat(E);

setring R1;
matrix CE = imap(R,CE);
std(transpose(CE));
//-> _[1]=[0,0,0,0,7a-2b+2c-4d]
//-> _[2]=[0,0,0,7,8b-c-12d]
//-> _[3]=[0,0,7,0,5b+2c-11d]
//-> _[4]=[0,7,0,0,4b-4c+d]
//-> _[5]=[7,0,0,0,-b+c-2d]
```

Finally let us proceed as in Solution 2 with the above system $(**)$, already knowing that $7a - 2b + 2c - 4d = 0$ is the condition for solvability. Hence, we can work over the corresponding quotient ring.

```
ring R2 = 0,(x,y,z,u,a,b,c,d),(c,dp);
ideal p = 7a-2b+2c-4d;
qring qR= std(p);
matrix C = imap(R,C);
matrix CE= imap(R,CE);
matrix b[5][1]=CE[1..5,5];      //the r.h.s. of (**)
lift(C,b);
//-> __[1,1]=-1/7b+1/7c-2/7d
//-> __[2,1]=4/7b-4/7c+1/7d
//-> __[3,1]=5/7b+2/7c-11/7d
//-> __[4,1]=8/7b-1/7c-12/7d
```

Exercises

2.8.1. Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$ and $R = K[x]_>$, $x = (x_1,\ldots,x_n)$. Moreover, let $I \subset J \subset R^r$ be submodules and $f \in R^r/I$. Find a procedure to decide whether $f \in J/I$ or not.

2.8.2. Prove Lemma 2.8.4.

2.8.3. Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1,\ldots,x_n)$ and $R = K[x]_>$. Show that the procedure of Section 1.8.7 can be generalized to a procedure computing the intersection $I \cap J$ of two submodules $I, J \subset R^r$.

2.8.4. Use the `modulo` command to write a SINGULAR procedure to compute the quotient of two modules.

2.8.5. Let $R = \mathbb{Q}[x,y,z]/\langle x^2+y^2+z^2\rangle$, $M = R^3/\langle (x, xy, xz)\rangle$, and let $N = R^2/\langle (1,y)\rangle$. Moreover, let $\varphi = \varphi_A : M \to N$ be the R-module homomorphism given by the matrix

$$A = \begin{pmatrix} x^2+1 & y & z \\ yz & 1 & -y \end{pmatrix}.$$

(1) Compute $\mathrm{Ker}(\varphi)$.
(2) Test whether $(x^2, y^2) \in \mathrm{Im}(\varphi)$, or not.
(3) Compute $\mathrm{Im}(\varphi) \cap \big\{ f \in N \bigm| f \equiv (h,0) \mod \langle (x,1)\rangle \text{ for some } h \in R \big\}$.
(4) Compute $\mathrm{Ann}_R\big(\mathrm{Im}(\varphi)\big)$.

2.8.6. Let A be a ring, M an A–module and $N \subset M$ a submodule. Then

$$\sqrt[M]{N} := \big\{ g \in A \bigm| g^q M \subset N \text{ for some } q > 0 \big\},$$

is called the *radical of N in M*. Prove the following statements:

(1) $\sqrt[M]{N} = \sqrt{\mathrm{Ann}(M/N)} = \sqrt{N :_A M}$.
(2) $\sqrt[M]{N} = A$ if and only if $M = N$.
(3) $\sqrt[M]{N \cap N'} = \sqrt[M]{N} \cap \sqrt[M]{N'}$, for each submodule $N' \subset M$.
(4) $\sqrt[M]{N + N'} = \sqrt[M]{N} + \sqrt[M]{N'}$, for each submodule $N' \subset M$.