Kreuzer · Robbiano
Computational Commutative Algebra 1

Martin Kreuzer · Lorenzo Robbiano

Computational Commutative Algebra 1

Springer

Martin Kreuzer
Lehrstuhl für Symbolic Computation
Fakultät für Mathematik und Informatik
Universität Passau
Innstraße 33
94032 Passau
Germany
martin.kreuzer@uni-passau.de

Lorenzo Robbiano
Università Genova
Dipartimento di Matematica
Via Dodecaneso, 35
16146 Genova
Italy
robbiano@dima.unige.it

Foreword

> *Hofstadter's Law: It always takes longer than you think it will take,*
> *even if you take into account Hofstadter's Law.*
> (Douglas R. Hofstadter)

Dear Reader,

what you are holding in your hands now is for you *a book*. But for us, for our families and friends, it has been known as *the book* over the last three years. Three years of intense work just to fill three centimeters of your bookshelf! This amounts to about one centimeter per year, or roughly two-fifths of an inch per year if you are non-metric. Clearly we had ample opportunity to experience the full force of Hofstadter's Law.

Writing a book about Computational Commutative Algebra is not unlike computing a Gröbner basis: you need unshakeable faith to believe that the project will ever end; likewise, you must trust in the Noetherianity of polynomial rings to believe that Buchberger's Algorithm will ever terminate. Naturally, we hope that the final result proves our efforts worthwhile. This is a book for learning, teaching, reading, and, most of all, enjoying the topic at hand.

Since neither of us is a native English speaker, the literary quality of this work is necessarily a little limited. Worries about our lack of linguistic sophistication grew considerably upon reading the following part of the introduction of "The Random House College Dictionary"

> An educated speaker will transfer from informal *haven't* to formal *have not*. The uneducated speaker who informally uses *I seen* or *I done gone* may adjust to the formal mode with *I have saw* and *I have went*.

Quite apart from being unable to distinguish between the informal and formal modes, we were frequently puzzled by such elementary questions as: is there another word for synonym? Luckily, we were able to extricate ourselves from the worst mires thanks to the generous aid of John Abbott and Tony Geramita. They provided us with much insight into British English and American English, respectively. However, notwithstanding their illuminating help, we were sometimes unable to discover the ultimate truth: should I be an ideal *in* a ring R or an ideal *of* a ring R? Finally, we decided to be non-partisan and use both.

Having revealed the names of two of our main aides, we now abandon all pretence and admit that *the book* is really a joint effort of many people. We especially thank Alessio Del Padrone who carefully checked every detail of the main text and test-solved all of the exercises. The tasks of proof-reading and checking tutorials were variously carried out by John Abbott, Anna Bigatti, Massimo Caboara, Robert Forkel, Tony Geramita, Bettina Kreuzer, and Marie Vitulli. Anna Bigatti wrote or improved many of the CoCoA programs we present, and also suggested the tutorials about Toric Ideals and Diophantine Systems and Integer Programming. The tutorial about Strange Polynomials comes from research by John Abbott. The tutorial about Elimination of Module Components comes from research in the doctoral thesis of Massimo Caboara. The tutorial about Splines was conceived by Jens Schmidbauer. Most tutorials were tested, and in many cases corrected, by the students who attended our lecture courses. Our colleagues Bruno Buchberger, Dave Perkinson, and Moss Sweedler helped us with material for jokes and quotes.

Moral help came from our families. Our wives Bettina and Gabriella, and our children Chiara, Francesco, Katharina, and Veronika patiently helped us to shoulder the problems and burdens which writing a book entails. And from the practical point of view, this project could never have come to a successful conclusion without the untiring support of Dr. Martin Peters, his assistant Ruth Allewelt, and the other members of the staff at Springer Verlag.

Finally, we would like to mention our favourite soccer teams, Bayern München and Juventus Turin, as well as the stock market mania of the late 1990s: they provided us with never-ending material for discussions when our work on *the book* became too overwhelming.

<div align="right">

Martin Kreuzer and Lorenzo Robbiano,
Regensburg and Genova, June 2000

</div>

Contents

Introduction

It seems to be a common practice of book readers to glance through the introduction and skip the rest. To discourage this kind of behaviour, we tried to make this introduction sufficiently humorous to get you hooked, and sufficiently vague to tempt you to read on.

0.1 What Is This Book About?

The title of this book is "Computational Commutative Algebra 1". In other words, it treats that part of commutative algebra which is suitable for explicit computer calculations. Or, if you prefer, the topic is that part of computer algebra which deals with commutative objects like rings and modules. Or, as one colleague put it jokingly, the topic could be called "computative algebra".

This description immediately leads us to another question. What is commutative algebra? It is the study of that area of algebra in which the important operations are commutative, particularly commutative rings and modules over them. We shall assume throughout the book that the reader has some elementary knowledge of algebra: the kinds of objects one studies should be familiar (groups, rings, fields, etc.), as should some of the basic constructions (homomorphisms, residue class rings, etc.). The commutative algebra part of this book is the treatment of polynomials in one or more indeterminates. To put this in a more fancy way, we could say that the generality we shall be able to deal with is the theory of finitely generated modules over finitely generated algebras over a field.

This leaves us with one last unexplained part of the title. What does the "1" refer to? You guessed it! There will be a second volume called "Computational Commutative Algebra 2". In the course of writing this book, we found that it was impossible to concentrate all the material we had planned in one volume. Thus, in the (hopefully) not so distant future we will be back with more. Meanwhile, we suggest you get acquainted with the next 300 or so pages, and we are confident that this will keep you busy for a while.

Although the fundamental ideas of Computational Commutative Algebra are deeply rooted in the development of mathematics in the 20th century, their full power only emerged in the last twenty years. One central notion which embodies both the old and the new features of this subject is the notion of a *Gröbner basis*.

0.2 What Is a Gröbner Basis?

The theory of Gröbner bases is a wonderful example of how an idea used to solve one problem can become the key for solving a great variety of other problems in different areas of mathematics and even outside mathematics. The introduction of Gröbner bases is analogous to the introduction of i as a solution of the equation $x^2 + 1 = 0$. After i has been added to the reals, the field of complex numbers arises. The astonishing fact is that in this way not only $x^2 + 1 = 0$ has a solution, but also every other polynomial equation over the reals has a solution.

Suppose now that we want to address the following problem. Let

$$f_1(x_1, \ldots, x_n) = 0, \ \ldots \ , f_s(x_1, \ldots, x_n) = 0$$

be a system of polynomial equations defined over an arbitrary field, and let $f(x_1, \ldots, x_n) = 0$ be an additional polynomial equation. How can we decide if $f(x_1, \ldots, x_n) = 0$ holds for all solutions of the initial system of equations? Naturally, this depends on where we look for such solutions. In any event, part of the problem is certainly to decide whether f belongs to the ideal I generated by $f_1, \ldots, f_s$, i.e. whether there are polynomials $g_1, \ldots, g_s$ such that $f = g_1 f_1 + \cdots + g_s f_s$. If $f \in I$, then every solution of $f_1 = \cdots = f_s = 0$ is also a solution of $f = 0$.

The problem of deciding whether or not $f \in I$ is called the *Ideal Membership Problem*. It can be viewed as the search for a solution of $x^2 + 1 = 0$ in our analogy. As in the case of the introduction of i, once the key tool, namely a Gröbner basis of I, has been found, we can solve not only the Ideal Membership Problem, but also a vast array of other problems.

Now, what *is* a Gröbner basis? It is a special system of generators of the ideal I with the property that the decision as to whether or not $f \in I$ can be answered by a simple division with remainder process. Its importance for practical computer calculations comes from the fact that there is an explicit algorithm, called Buchberger's Algorithm, which allows us to find a Gröbner basis starting from any system of generators $\{f_1, \ldots, f_s\}$ of I.

0.3 Who Invented This Theory?

As often happens, there are many people who may lay claim to inventing some aspects of this theory. In our view, the major step was taken by B. Buchberger in the mid-sixties. He formulated the concept of Gröbner bases and, extending a suggestion of his advisor W. Gröbner, found an algorithm to compute them, and proved the fundamental theorem on which the correctness and termination of the algorithm hinges.

For many years the importance of Buchberger's work was not fully appreciated. Only in the eighties did researchers in mathematics and computer science start a deep investigation of the new theory. Many generalizations and a wide variety of applications were developed. It has now become clear that the theory of Gröbner bases can be widely used in many areas of science. The simplicity of its fundamental ideas stands in stark contrast to its power and the breadth of its applications. Simplicity and power: two ingredients which combine perfectly to ensure the continued success of this theory.

For instance, researchers in commutative algebra and algebraic geometry benefitted immediately from the appearance of specialized computer algebra systems such as CoCoA, Macaulay, and Singular. Based on advanced implementations of Buchberger's Algorithm for the computation of Gröbner bases, they allow the user to study examples, calculate invariants, and explore objects one could only dream of dealing with before. The most fascinating feature of these systems is that their capabilities come from tying together deep ideas in both mathematics and computer science.

It was only in the nineties that the process of establishing computer algebra as an independent discipline started to take place. This contributed a great deal to the increased demand to learn about Gröbner bases and inspired many authors to write books about the subject. For instance, among others, the following books have already appeared.

1) W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*
2) T. Becker and V. Weispfenning, *Gröbner Bases*
3) B. Buchberger and F. Winkler (eds.), *Gröbner Bases and Applications*
4) D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms*
5) D. Eisenbud, *Commutative Algebra with a View toward Algebraic Geometry*, Chapter 15
6) B. Mishra, *Algorithmic algebra*
7) W. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*
8) F. Winkler, *Polynomial Algorithms in Computer Algebra*
9) R. Fröberg, *An Introduction to Gröbner Bases*

Is there any need for another book on the subject? Clearly we think so. For the remainder of this introduction, we shall try to explain why. First we should explain how the contents of this book relate to the books listed above.

0.4 Now, What Is This Book *Really* About?

Instead of dwelling on generalities and the virtues of the theory of Gröbner bases, let us get down to some nitty-gritty details of *real mathematics*. Let us examine some concrete problems whose solutions we shall try to explain in this book. For instance, let us start with the Ideal Membership Problem mentioned above.

Suppose we are given a polynomial ring $P = K[x_1, \ldots, x_n]$ over some field K, a polynomial $f \in P$, and some other polynomials $f_1, \ldots, f_s \in P$ which generate an ideal $I = (f_1, \ldots, f_s) \subseteq P$.

Question 1 *How can we decide whether $f \in I$?*

In other words, we are asking whether it is possible to find polynomials $g_1, \ldots, g_s \in P$ such that $f = g_1 f_1 + \cdots + g_s f_s$. In such a relation, many terms can cancel on the right-hand side. Thus there is no obvious *a priori* bound on the degrees of $g_1, \ldots, g_s$, and we cannot simply convert this question to a system of linear equations by comparing coefficients.

Next we suppose we are given a finitely generated K-algebra R specified by generators and relations. This means that we have a representation $R = P/I$ with P and I as above.

Question 2 *How can we perform addition and multiplication in R?*

Of course, if $f_1, f_2 \in P$ are representatives of residue classes $r_1, r_2 \in R$, then $f_1 + f_2$ (resp. $f_1 f_2$) represents the residue class $r_1 + r_2$ (resp. $r_1 r_2$). But this depends on the choice of representatives, and if we want to check whether two different results represent the same residue class, we are led back to Question 1. A much better solution would be to have a "canonical" representative for each residue class, and to compute the canonical representative of $r_1 + r_2$ (resp. $r_1 r_2$).

More generally, we can ask the same question for modules. If M is a finitely generated R-module, then M is also a finitely generated P-module via the surjective homomorphism $P \longrightarrow R$, and, using generators and relations, the module M has a presentation of the form $M \cong P^r/N$ for some P-submodule $N \subseteq P^r$.

Question 3 *How can we perform addition and scalar multiplication in M?*

Let us now turn to a different problem. For polynomials in one indeterminate, there is a well-known and elementary algorithm for doing division with remainder. If we try to generalize this to polynomials in n indeterminates, we encounter a number of difficulties.

Question 4 *How can we perform polynomial division for polynomials in n indeterminates? In other words, is there a "canonical" representation $f = q_1 f_1 + \cdots + q_s f_s + p$ such that $q_1, \ldots, q_s \in P$ and the remainder $p \in P$ is "small"?*

Again we find a connection with Question 2. If we can define the polynomial division in a canonical way, we can try to use the remainder p as the canonical representative of the residue class of f in R. Even if we are able to perform the basic operations in R or M, the next step has to be the possibility of computing with ideals (resp. submodules). Suppose we have further polynomials $g_1, \ldots, g_t \in P$ which generate an ideal $J = (g_1, \ldots, g_t)$.

Question 5 *How can we perform elementary operations on ideals or submodules? More precisely, how can we compute systems of generators of the following ideals?*

a) $I \cap J$
b) $I :_P J = \{f \in P \mid f \cdot J \subseteq I\}$
c) $I :_P J^\infty = \{f \in P \mid f \cdot J^i \subseteq I \text{ for some } i \in \mathbb{N}\}$

The cases of computing $I + J$ and $I \cdot J$ are obviously easy. It turns out that the keys to the solution of this last question are the answers to our next two problems, namely the problems of computing syzygy modules and elimination modules.

Question 6 *How can we compute the module of all* syzygies *of* $(f_1, \ldots, f_s)$, *i.e. the* P-*module*

$$\mathrm{Syz}_P(f_1, \ldots, f_s) = \{(g_1, \ldots, g_s) \in P^s \mid g_1 f_1 + \cdots + g_s f_s = 0\}?$$

Question 7 *How can we solve the* Elimination Problem, *i.e. for* $1 \le m < n$, *how can we find the ideal* $I \cap K[x_1, \ldots, x_m]$?

As we shall see, the answers to those questions have numerous applications. For instance, after we have studied the arithmetic of finitely generated K-algebras $R = P/I$ and of finitely generated R-modules M, the next natural problem is to do computations with homomorphisms between such objects.

Suppose $M_1 = P^{r_1}/N_1$ and $M_2 = P^{r_2}/N_2$ are two finitely generated R-modules, and $\varphi : M_1 \longrightarrow M_2$ is an R-linear map which is given explicitly by an $r_2 \times r_1$-matrix of polynomials.

Question 8 *How can we compute presentations of the kernel and the image of* φ?

And the following question gives a first indication that we may also try to use Computational Commutative Algebra to compute objects which are usually studied in homological algebra.

Question 9 *Is it possible to compute a presentation of the finitely generated* P-*module* $\mathrm{Hom}_P(M_1, M_2)$?

Now suppose $R = P/I$ and $S = Q/J$ are two finitely generated K-algebras, where $Q = K[y_1, \ldots, y_m]$ is another polynomial ring and $J \subseteq Q$ is an ideal. Furthermore, suppose that $\psi : R \longrightarrow S$ is a K-algebra homomorphism which is explicitly given by a list of polynomials in Q representing the images $\psi(x_1 + I), \ldots, \psi(x_n + I)$.

Question 10 *How can we compute presentations of the kernel and the image of ψ? And how can we decide for a given element of S whether it is in the image of ψ?*

Finally, one of the most famous applications of Computational Commutative Algebra is the possibility to solve polynomial systems of equations.

Question 11 *How can we check whether the system of polynomial equations*

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$$

has solutions in $\overline{K}^n$, where $\overline{K}$ is the algebraic closure of K, and whether the number of those solutions is finite or infinite?

Question 12 *If the system of polynomial equations*

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$$

has only finitely many solutions $(a_1, \ldots, a_n) \in \overline{K}^n$, how can we describe them? For instance, can we compute the minimal polynomials of the elements $a_1, \ldots, a_n$ over K? And how can we tell which of the combinations of the zeros of those polynomials solve the system of equations?

These and many related questions will be answered in this book. For a similar description of the contents of Volume 2 we refer the reader to its introduction. Here we only mention that it will contain three more chapters called

Chapter IV   The Homogeneous Case
Chapter V   Hilbert Functions
Chapter VI   Further Applications of Gröbner Bases

Let us end this discussion by pointing out one important choice we made. From the very beginning we have developed the theory for submodules of free modules over polynomial rings, and not just for their ideals. This differs markedly from the common practice of introducing everything only in the case of ideals and then leaving the appropriate generalizations to the reader.

Naturally, there is a trade-off involved here. We have to pay for our generality with slight complications lingering around almost every corner. This suggests that the usual exercises "left to the reader" by other authors could harbour a few nasty mines. But much more importantly, in our view Gröbner basis theory is *intrinsically* about modules. Buchberger's Algorithm, his Gröbner basis criterion, and other central notions and results deal with

syzygies. In any case, the set of all syzygies is a module, not an ideal. Therefore a proper introduction to Gröbner basis theory cannot avoid submodules of free modules. In fact, we believe this book shows that there is no reason to avoid them.

Finally, we would like to point out that even if you are only interested in the theory of polynomial ideals, often you still have to be able to compute with modules, for instance if you want to compute some invariants which are derived from the free resolution of the ideal. Without modules, a number of important applications of this theory would have to remain conspicuously absent!

0.5 What Is This Book *Not* About?

The list of topics which we do *not* talk about is too long to be included here, but for instance it contains soccer, chess, gardening, and our other favourite pastimes.

Computational Commutative Algebra is part of a larger field of investigation called *symbolic computation* which some people also call *computer algebra.* Covering this huge topic is beyond the scope of our book. So, what is symbolic computation about? Abstractly speaking, it deals with those algorithms which allow modern computers to perform computations involving symbols, and not only numbers.

Unlike your math teacher, computers do not object to symbolic simplification and rewriting of formulas such as

$$\frac{\cancel{6}4}{1\cancel{6}} = 4 \qquad \text{and} \qquad \frac{\cancel{9}5}{1\cancel{9}} = 5 \qquad \text{and} \qquad \tfrac{1}{6} + \left(\tfrac{1}{3} \times \tfrac{1}{2}\right) = \left(\tfrac{1}{6} + \tfrac{1}{3}\right) \times \left(\tfrac{1}{6} + \tfrac{1}{2}\right)$$

More seriously, symbolic computation includes topics such as computational group theory, symbolic integration, symbolic summation, quantifier elimination, etc., which we shall not touch here.

Another circle of questions which we avoid is concerned with computability, recursive functions, decidability, and so on. Almost all of our algorithms will be formulated for polynomials and vectors of polynomials with coefficients in an arbitrary field. Clearly, if you want to implement those algorithms on a computer, you will have to assume that the field is *computable.* This means (approximately) that you have to be able to store an element of your field in finitely many memory cells of the computer, that you can check in finitely many steps whether two such representations correspond to the same field element, and you have to provide algorithms for performing the four basic operations $+, -, \times, \div$, i.e. sequences of instructions which perform these operations in finitely many steps.

For us, this assumption does not present any problem at all, since for concrete implementations we shall always assume that the base field is one of the fields implemented in CoCoA, and those fields are computable.

Moreover, we are not going to give a detailed account of the history of the topics we discuss. Likewise, although at the end of the book you will find some references, we decided not to cite everything everywhere. More correctly, we did not cite anything anywhere. If you want additional information about the historical development, you can look into the books mentioned above. For specific references to recent research papers, we recommend that you use electronic preprint and review services. The number of papers in Computational Commutative Algebra is growing exponentially, and unlike Gröbner basis computations, it does not seem likely that it will end eventually. If all else fails, you can also drop an e-mail to us, and we will try to help you.

Finally, we do not talk about complexity issues. We shall mainly be content with proving that our algorithms terminate after finitely many steps. Unfortunately, this finite number of steps could be so large that the actual termination of the calculation occurs well beyond our lifetimes! In fact, it is known that the computation of a Gröbner basis has *doubly-exponential* worst-case time complexity. In layman's terms this means that we should worry that no computation of any Gröbner basis ever terminates in our lifetimes. Fortunately, the practical experiences of mathematicians are not that dramatic. The computation of the Gröbner basis of a *reasonable* ideal or module *usually* terminates in a *reasonable* amount of time.

Nevertheless, it is an important topic to study how long a computer calculation will actually take. For instance, in Appendix C we give some hints which can help you speed up your CoCoA programs. The main reason that we have not delved more into complexity considerations is that we are not specialists in this subject and we feel that we cannot contribute many meaningful remarks in this direction.

If you are interested in practical applications of Computational Commutative Algebra, the complexity issues you are going to encounter are of a different nature anyway. Usually, they cannot be solved by theoretical considerations. Instead, they require a good grasp of the underlying mathematical problem and a concerted effort to improve your program code.

0.6 Are There any Applications of This Theory?

Definitely, yes! Computational Commutative Algebra has many applications, some of them in other areas of mathematics, and some of them in other sciences. Amongst others, we shall see some easy cases of the following applications.

Applications in Algebraic Geometry

- Hilbert's Nullstellensatz (see Section 2.6)
- Affine varieties (see Tutorial 27)

- Projective spaces and Graßmannians (see Tutorial 35)
- Saturation (for computing the homogeneous vanishing ideal of a projective variety, see Section 3.5 and Volume 2)
- Systems of polynomial equations (see Section 3.7)
- Primary decompositions (for computing irreducible components of varieties, see Tutorial 43)
- Projective Varieties (see Volume 2)
- Homogenization (for computing projective closures, see Volume 2)
- Set-theoretic complete intersections (see Volume 2)
- Dimensions of affine and projective varieties (see Volume 2)
- Ideals of points (see Volume 2)

Applications in Number Theory

- Modular arithmetic, factoring polynomials over finite fields (see Tutorials 3 and 6)
- Computations in the field of algebraic numbers (see Tutorials 17 and 18)
- Magic squares (see Volume 2)

Applications in Homological Algebra

- Computation of syzygy modules (see Section 3.1)
- Kernels, images and liftings of module homomorphisms (see Section 3.3)
- Computation of Hom-modules (see Section 3.3)
- Ext-modules and the depth of a module (see Tutorial 33)
- Graded free resolutions (see Volume 2)

Applications in Combinatorics

- Monomial ideals and modules (see Section 1.3)
- Graph colourings (see Tutorial 26)
- Toric ideals (see Tutorial 38)

Practical and Other Applications

- Splines (see Tutorial 28)
- Diophantine Systems and Integer Programming (see Tutorial 36 and 38)
- Strange Polynomials (see Tutorial 42)
- Mathematical Finance: Modern Portfolio Theory (see Tutorial 44)
- Photogrammetry (see Volume 2)
- Chess Puzzles (see Volume 2)
- Statistics: Design of Experiments (see Volume 2)
- Automatic Theorem Proving (see Volume 2)

0.7 How Was This Book Written?

In our opinion, any plan for writing a book should include a set of rules which the authors intend to follow consistently. This *metarule* is more difficult to comply with than one thinks, and indeed many books appear to have been written in a more liberal manner. Strictly following a set of rules seems to be in contrast with the freedom of choosing different approaches to different problems. On the other hand, too much freedom sometimes leads to situations which, in our opinion, *cheat* the reader.

For instance, one of our most important rules is that statements called Lemma, Proposition, Theorem, etc. have to be followed by a complete proof, and the development of the theory should be as self-contained as possible. In particular, we avoid relegating proofs to exercises, giving a proof which consists of a reference which is not specific, giving a proof which consists of a reference hard to verify, because it uses different assumptions and/or notation, and giving a proof which consists of a reference to a later part of the book.

Another fundamental rule is that the notation used in this book is consistent throughout the book and always as close as possible to the notation of the computer algebra system CoCoA. It is clear that, in an emerging field like computer algebra, the notation is still in flux and few conventions hold uniformly. We think that the situation in computer algebra is even worse than elsewhere. Just look at the following table which presents the different terminologies and the notation used for some fundamental objects in our references listed in Subsection 0.3. Its second row contains our choices which agree with CoCoA.

Given a non-zero polynomial f in a polynomial ring $K[x_1, \ldots, x_n]$ and an ordering σ on the set of products of powers of indeterminates, we let $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the largest element (with respect to σ) in the support of f and $c \in K$ its coefficient in f.

	$x_1^{\alpha_1} \cdots x_n^{\alpha_n}$	Notation	$c \cdot x_1^{\alpha_1} \ldots x_n^{\alpha_n}$	Notation
	leading term	$\mathrm{LT}_\sigma(f)$	(none)	$\mathrm{LM}_\sigma(f)$
1)	leading power product	$\mathrm{lp}(f)$	leading term	$\mathrm{lt}(f)$
2)	head term	$\mathrm{HT}(f)$	head monomial	$\mathrm{HM}(f)$
3)	leading power product	$\mathrm{LPP}_\prec(f)$	leading monomial	$\mathrm{LM}_\prec(f)$
4)	leading monomial	$\mathrm{LM}(f)$	leading term	$\mathrm{LT}(f)$
5)	initial monomial	(none)	initial term	$\mathrm{in}_>(f)$
6)	head term	$\mathrm{Hterm}(f)$	head monomial	$\mathrm{Hmono}(f)$
7)	initial monomial	$\mathrm{in}(f), \mathrm{M}(f)$	leading term	$\mathrm{lt}(f), \mathrm{L}(f)$
8)	leading power product	$\mathrm{lpp}(f)$	initial	$\mathrm{in}(f)$
9)	leading monomial	$\mathrm{lm}(f)$	leading term	$\mathrm{lt}(f)$

A further constraint is that we have tried to structure each section according to the following scheme: introduction, body, exercises, tutorials.

The introduction describes the content in a lively style, where *Italian* imagination overtakes *German* rigour. Metaphors, sketches of examples, and psychological motivations of the themes of the section are included here. The body is the technical part of the section. It includes definitions, theorems, proofs, etc. Very few compromises with imagination are accepted here. However, we always try to liven up the text by including examples.

Nothing special needs to be said about the exercises, except maybe that they are *supposed* to be easy. A careful reader of the book should succeed in solving them, and to make life even easier, we include some hints for selected exercises in the text, and some more in Appendix D. Then there is one of the main features of this book which we believe to be non-standard. At the end of every section there are *tutorials*.

0.8 What Is a Tutorial?

Almost all books about computer algebra include some exercises which require that actual computations be performed with the help of a computer algebra system. But in our opinion, the gap between the theory and actual computations is much too wide.

First of all, the algorithms in the text are usually presented in *pseudocode* which, in general, is completely different from the way you write a function in a computer algebra system. In fact, we have a hard time understanding precisely what pseudocode is, because it is not rigorously defined. Instead, we have tried to present all algorithms in the same way mathematicians formulate other theorems and to provide explicit and complete proofs of their finiteness and correctness. If the reader is asked to implement a certain algorithm as a part of some tutorial or exercise, these natural language descriptions should translate easily into computer code on a step-by-step basis.

Secondly, to narrow the gap between theory and computation even more, we decided to link the tutorials and some exercises with a specific computer algebra system, namely CoCoA. This does not mean that you cannot use another computer algebra system. It only means that there definitely *is* a solution using CoCoA.

Every tutorial develops a theme. Sometimes we anticipate later parts of the theory, or we step out a little from the main stream and provide some pointers to applications or other areas of interest. A tutorial is like a small section by itself which is not used in the main text of the book. Some effort on the part of the reader may be required to develop a small piece of theory or to implement certain algorithms. However, many suggestions and hints in the CoCoA style are there to guide you through the main difficulties.

0.9 What Is CoCoA?

CoCoA is a computer algebra system. It is freely available and may be found on the internet at the URL

<div align="center">

`http://cocoa.dima.unige.it`

</div>

CoCoA means "**Co**mputations in **Co**mmutative **A**lgebra". As we mentioned above, we suggest that you use CoCoA to solve the programming parts of the tutorials. The version of CoCoA we refer to in this book is CoCoA 4.

In Appendix A, we give some instructions on how you can download and install CoCoA on your computer. Then we show how you can start the program and how you can use it interactively. Before trying to solve the first tutorial, we think you should read through this appendix and those following it. The basic features of CoCoA, its syntax, and its data types are explained there.

If you have never used a computer algebra system before, you should definitely go through some of the examples on your computer. Play a little and get yourself acquainted with the system! Soon you will also learn how to use the on-line manual in order to get additional information.

Since the tutorials and some exercises require that you do some actual programming, we added Appendix B which gives a brief introduction to this topic. There you can find the basic commands for creating your own CoCoA functions, as well as some ideas on how you can organize your program development. In Appendix C we provide you with a number of examples of CoCoA programs which should help to get you started and which contain clues for certain tutorials.

0.10 And What Is This Book Good for?

> *Too often, mathematical results are terribly abused by teachers*
> *who take a cheap shortcut and simply refer to a result*
> *from the past, from another place, another context,*
> *totally underestimating the difficulty (and the importance)*
> *of transporting these ideas from one place to another.*
> *When that happens, the mathematics loses, the application loses,*
> *and most of all, the student loses.*
> (Peter Taylor)

From the very first glimpse, it should be clear to you that this book is not a typical undergraduate text. But it is primarily intended to serve as a textbook for courses in Computational Commutative Algebra at the undergraduate or graduate level. As we explained above, we tried to avoid the traps Peter Taylor mentions. The material developed here has already been used for teaching undergraduate and graduate students with little or no experience in computer algebra.

Secondly, you can use this book for a self-guided tour of Computational Commutative Algebra. We did our best to fill it with many examples, detailed

proofs, and generous hints for exercises and tutorials which should help to
pave your road. This does not necessarily mean that when you work your
way through the book, there will be no unexpected difficulties.

Probably you already know some of the topics we discuss. Or, maybe, you
think you know them. For instance, you may have previously encountered
the polynomial ring in a single indeterminate over a field such as $\mathbb{Q}$, $\mathbb{R}$,
or $\mathbb{C}$, and you may feel comfortable using such polynomials. But did you
know that there are polynomials whose square has fewer terms than the
polynomial itself? At first glance this seems unlikely, at second glance it may
look possible, and at third glance you will still not be able to decide, because
you find no example. By looking at the polynomial

$$f = x^{12} + \tfrac{2}{5}\,x^{11} - \tfrac{2}{25}\,x^{10} + \tfrac{4}{125}\,x^{9} - \tfrac{2}{125}\,x^{8} + \tfrac{2}{125}\,x^{7}$$
$$- \tfrac{3}{2750}\,x^{6} - \tfrac{1}{275}\,x^{5} + \tfrac{1}{1375}\,x^{4} - \tfrac{2}{6875}\,x^{3} + \tfrac{1}{6875}\,x^{2} - \tfrac{1}{6875}\,x - \tfrac{1}{13750}$$

whose square is

$$f^{2} = x^{24} + \tfrac{4}{5}\,x^{23} + \tfrac{44}{3125}\,x^{19} + \tfrac{2441}{171875}\,x^{18} - \tfrac{2016}{171875}\,x^{17} - \tfrac{16719}{37812500}\,x^{12}$$
$$+ \tfrac{141}{9453125}\,x^{11} - \tfrac{3}{859375}\,x^{7} + \tfrac{13}{8593750}\,x^{6} + \tfrac{1}{4296875}\,x^{5} + \tfrac{1}{47265625}\,x + \tfrac{1}{189062500}$$

you can convince yourself that such a phenomenon actually occurs. But what
is really surprising is that this is the *simplest* example possible, as we shall
see in Tutorial 42.

Thus we advise you to go through the book with an open and critical
mind. We have tried to fill it with a lot of hidden treasures, and we think that
even if you have some previous knowledge of Computational Commutative
Algebra, you will find something new or something that could change your
view of one topic or another.

Last, but not least, the book can also be used as a repository of explicit
algorithms, programming exercises, and CoCoA tricks. So, even if computers
and programming entice you more than algebraic theorems, you will find
plenty of things to learn and to do.

0.11 Some Final Words of Wisdom

Naturally, this introduction has to leave many important questions unan-
swered. What is the deeper meaning of Computational Commutative Algebra?
What is the relationship between doing computations and proving algebraic
theorems? Will this theory find widespread applications? What is the future
of Computational Commutative Algebra? Instead of elaborating on these
profound philosophical problems, let us end this introduction and send you
off into Chapter 1 with a few words of wisdom by Mark Green.

There is one change which has overtaken commutative algebra that is in my view revolutionary in character – the advent of symbolic computation. This is as yet an unfinished revolution. At present, many researchers routinely use Macaulay, Maple, Mathematica, and CoCoA to perform computer experiments, and as more people become adept at doing this, the list of theorems that have grown out of such experiments will enlarge. The next phase of this development, in which the questions that are considered interesting are influenced by computation and where these questions make contact with the real world, is just beginning to unfold. I suspect that ultimately there will be a sizable applied wing to commutative algebra, which now exists in embryonic form.

1. Foundations

Der Ball ist rund.
(Sepp Herberger)

In the introduction we have already discussed our battle plan and the main themes to be encountered, and now we are at the very start of the game. No book can be completely self-contained, and this one is no exception. In particular, we assume that the reader has some knowledge of basic algebra, but we think that she/he might feel more comfortable if we recall some fundamental definitions. Section 1.1 is specifically designed with this purpose in mind and also to present many examples. They serve as reminders of known facts for more experienced readers, and as training for beginners. The main notion recalled there is that of a polynomial, which plays a fundamental role throughout the book.

At the end of Section 1.1 we present, for the first time, a special feature of this book, namely the tutorials. Among other tasks, most tutorials require doing some programming using the computer algebra system CoCoA. As we said in the introduction, this book is not about computability, but rather about actual computations of objects related to polynomials. Therefore we are not going to discuss computability and related questions, but instead we shall develop the necessary background in Commutative Algebra and then show how you can work with it: go to your desk, turn on the computer, and work.

What are the most fundamental properties of polynomial rings over fields? One of them is certainly the unique factorization property. Section 1.2 is entirely devoted to this concept. In some sense this section can be considered as another link between very elementary notions in algebra and the themes of the book. However, the task of describing algorithms for factorizing polynomials is not taken up here. Only in a tutorial at the end of Section 1.2 do we give a guide to implementing Berlekamp's Algorithm which computes the factorization of univariate polynomials over finite fields.

After the first two sections, the reader should be sufficiently warmed up to enter the game for real, and Section 1.3 is intended to serve this purpose. In particular, Dickson's Lemma provides a fundamental finiteness result and gives us a first hint about how to compute with polynomial ideals and modules. Section 1.4 brings the reader into the realm of orderings. Term

orderings are an important tool for actually computing, since they enable us to write polynomials in a well-defined way which can then be implemented on a computer.

After ordering the terms in polynomials or tuples of polynomials completely, their leading terms can be singled out. Section 1.5 shows how to use those leading terms to build leading term ideals and modules. Conceptually, these are simpler objects to handle than the original ideals or modules. For instance, the main result of Section 1.5 is Macaulay's Basis Theorem which describes a basis of a quotient module in terms of a certain leading term module.

A drawback of Macaulay's Basis Theorem is that it neither says how to compute such a basis nor how to represent the residue classes. A first attempt to overcome these difficulties is made in Section 1.6 where the reader is instructed on how to perform a division with remainder for tuples of polynomials. This procedure is called the Division Algorithm and generalizes the well-known algorithm for univariate polynomials.

However, we shall see that the Division Algorithm fails to completely solve the problem of computing in residue class modules. New forces have to be brought into play. Section 1.7, the closing section of the first chapter, serves as a preparation for further advances. It is devoted to accumulating new knowledge and to enlarging the reader's background. More precisely, very general notions of gradings are described there. They can be used to overcome some of the difficulties encountered in Chapter 1. This goal will be the topic of subsequent chapters.

1.1 Polynomial Rings

> *Even the longest journey*
> *begins with the first step.*
> (Chinese Proverb)

As mentioned above, we think that the reader might feel more comfortable if we recall some fundamental definitions. Therefore the style of this section is slightly different from the rest of the book simply because we want to squeeze in several notions. Thus there will be more emphasis on examples than on theorems.

The main purpose of this section is to recall the notions of polynomials and polynomial rings. They are the most fundamental objects of Computational Commutative Algebra and play a central role throughout this book. It is important to clarify what we mean by a ring. Technically speaking, we mean an "associative, commutative ring with identity".

To be a little less blunt, we should say that rings are abundant in "nature" and the reader should have already met some, for instance the rings of integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$. One should remember that the rational numbers, the real numbers, and the complex numbers have the extra property that every non-zero element is invertible, and that they are called fields. Also all square matrices of a given size with entries in a ring form a ring with respect to the usual operations of componentwise sum and row-by-column product, but, in contrast to the previously mentioned rings, the property $A \cdot B = B \cdot A$ fails, i.e. they form a non-commutative ring.

Although we shall use matrices intensively, our basic objects are polynomial rings in a finite number of indeterminates over fields. Since they are commutative rings, let us first define these objects.

Recall that a **monoid** is a set S, together with an operation $S \times S \longrightarrow S$ which is associative and for which there exists an identity element, i.e. an element $1_S \in S$ such that $1_S \cdot s = s \cdot 1_S = s$ for all $s \in S$. When it is clear which monoid is considered, we simple write 1 instead of 1_S. Furthermore, a **group** is a monoid in which every element is invertible, i.e. such that for all $s \in S$ there exists an element $s' \in S$ which satisfies $s \cdot s' = s' \cdot s = 1_S$. A monoid is called **commutative** if $s \cdot s' = s' \cdot s$ for all $s, s' \in S$.

Definition 1.1.1. By a **ring** $(R, +, \cdot)$ (or simply R if no ambiguity can arise) we shall always mean a **commutative** ring with identity element, i.e. a set R together with two associative operations $+, \cdot : R \times R \to R$ such that $(R, +)$ is a commutative group with identity element 0, such that $(R, \cdot)$ is a commutative monoid with identity element 1_R, and such that the distributive laws are satisfied. If no ambiguity arises, we use 1 instead of 1_R. A **field** K is a ring such that $(K \backslash \{0\}, \cdot)$ is a group.

For the rest of this section, we let R be a ring. Some elements of a ring have special properties. For instance, if $r \in R$ satisfies $r^i = 0$ for some $i \geq 0$,

then r is called a **nilpotent element**, and if $rr' = 0$ implies $r' = 0$ for all $r' \in R$, then r is called a **non-zerodivisor**. A ring whose non-zero elements are non-zerodivisors is called an **integral domain**. For example, every field is an integral domain.

The following example is not central to the themes of this book, but it contributes to show the abundance of rings.

Example 1.1.2. Let $\mathcal{C}(\mathbb{R})$ be the set of continuous functions over the reals. If we define $f + g$ and $f \cdot g$ by the rules $(f + g)(a) = f(a) + g(a)$ and $(f \cdot g)(a) = f(a) \cdot g(a)$ for every $a \in \mathbb{R}$, then it is easy to see that $(\mathcal{C}(\mathbb{R}), +, \cdot)$ is a commutative ring.

Normally, when we define a new class of algebraic objects, we also want to know which maps between them respect their structure. Thus we now recall the concept of a ring homomorphism.

Definition 1.1.3. Let R, S, and T be rings.

a) A map $\varphi : R \to S$ is called a **ring homomorphism** if $\varphi(1_R) = 1_S$ and for all elements $r, r' \in R$ we have $\varphi(r + r') = \varphi(r) + \varphi(r')$ and $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$, i.e. if φ preserves the ring operations. In this case we also call S an R**-algebra** with **structural homomorphism** φ.

b) Given two R-algebras S and T whose structural homomorphisms are $\varphi : R \longrightarrow S$ and $\psi : R \longrightarrow T$, a ring homomorphism $\varrho : S \longrightarrow T$ is called an R**-algebra homomorphism** if we have $\varrho(\varphi(r) \cdot s) = \psi(r) \cdot \varrho(s)$ for all $r \in R$ and all $s \in S$.

For instance, going back to Example 1.1.2, we see that the inclusion of the constant functions into $\mathcal{C}(\mathbb{R})$ makes $\mathcal{C}(\mathbb{R})$ an $\mathbb{R}$-algebra, and that the map $\varphi : \mathcal{C}(\mathbb{R}) \longrightarrow \mathbb{R}$ defined by $\varphi(f) = f(0)$ is a ring homomorphism and also an $\mathbb{R}$-algebra homomorphism. For every ring R, there exists a unique ring homomorphism $\varphi : \mathbb{Z} \longrightarrow R$ which maps $1_{\mathbb{Z}}$ to 1_R. It is called the **characteristic homomorphism** of R.

Sometimes a field and a group are tied together by an operation of the field on the group to produce the very well known algebraic structure of a *vector space*. In this case the elements of the field are called *scalars*, the elements of the group are called *vectors*, and the operation is called *scalar multiplication*. Those concepts generalize in the following way.

Definition 1.1.4. An R**-module** M is a commutative group $(M, +)$ with an operation $\cdot : R \times M \to M$ (called **scalar multiplication**) such that $1 \cdot m = m$ for all $m \in M$, and such that the associative and distributive laws are satisfied. A commutative subgroup $N \subseteq M$ is called an R**-submodule** if we have $R \cdot N \subseteq N$. If $N \subset M$ then it is called a **proper** submodule. An R-submodule of the R-module R is called an **ideal** of R.

Given two R-modules M and N, a map $\varphi : M \longrightarrow N$ is called an R**-module homomorphism** or an R**-linear map** if $\varphi(m + m') = \varphi(m) + \varphi(m')$ and $\varphi(r \cdot m) = r \cdot \varphi(m)$ for all $r \in R$ and all $m, m' \in M$.

Using this terminology, we can say that an R-algebra is a ring with an extra structure of an R-module such that the two structures are compatible and the usual commutative and distributive laws are satisfied.

The definition of an ideal $I \subseteq R$ could also be rephrased by saying that a subset I of R is an ideal if it is an additive subgroup of R and $R \cdot I \subseteq I$. In a field K, the only two ideals are K itself and $\{0\}$. Given any ideal I in a ring R, we can form the residue class ring R/I. It is an R-module in the obvious way. It is even an R-algebra, since the canonical map $R \longrightarrow R/I$ is a ring homomorphism.

Some ideals of R have special properties. For instance, an ideal $I \subset R$ is called a **prime ideal** if $rr' \in I$ implies $r \in I$ or $r' \in I$ for all $r, r' \in R$, and it is called a **maximal ideal** of R if the only ideal properly containing I is R itself. It is easy to see that I is a prime ideal if and only if R/I is an integral domain, that I is a maximal ideal if and only if R/I is a field, and hence that maximal ideals are prime ideals.

Definition 1.1.5. Let M be an R-module.

a) A set $\{m_\lambda \mid \lambda \in \Lambda\}$ of elements of M is called a **system of generators** of M if every $m \in M$ has a representation $m = r_1 m_{\lambda_1} + \cdots + r_n m_{\lambda_n}$ such that $n \in \mathbb{N}$, $r_1, \ldots, r_n \in R$ and $\lambda_1, \ldots, \lambda_n \in \Lambda$. In this case we write $M = \langle m_\lambda \mid \lambda \in \Lambda \rangle$. The empty set is a system of generators of the zero module $\{0\}$.

b) The module M is called **finitely generated** if it has a finite system of generators. If M is generated by a single element, it is called **cyclic**. A cyclic ideal is called a **principal ideal**.

c) A system of generators $\{m_\lambda \mid \lambda \in \Lambda\}$ is called an R-**basis** of M if every element of M has a unique representation as above. If M has an R-basis, it is called a **free R-module**.

d) If M is a finitely generated free R-module and $\{m_1, \ldots, m_r\}$ is an R-basis of M, then r is called the **rank** of M and denoted by $\mathrm{rk}(M)$. We remind the reader that it is known that all bases of a finitely generated free module have the same length. Hence the rank of M is well-defined.

Example 1.1.6. Finitely generated and free modules arise in a number of situations.

a) The rings $\mathbb{Z}$ and $K[x]$ where K is a field have the property that all their ideals are principal. An integral domain with this property is called a **principal ideal domain**. For example, the ideal in $K[x]$ generated by $\{x - x^2, x^2\}$ is also generated by $\{x\}$.

b) The ideal $(2) \subseteq \mathbb{Z}$ is a free $\mathbb{Z}$-module of rank one, whereas the $\mathbb{Z}$-module $\mathbb{Z}/(2)$ is not free.

c) If K is a field and V is a K-vector space, then every K-submodule of V is free. This follows from the existence theorem for bases in vector spaces.

d) The ring R is a free R-module with basis $\{1\}$.

The following notion generalizes the vector space of n-tuples of elements in a field.

Definition 1.1.7. For $n \in \mathbb{N}$, the set $R^n = \{(r_1, \ldots, r_n) \mid r_1, \ldots, r_n \in R\}$ of all n-tuples is a free R-module with respect to componentwise addition and scalar multiplication. For $i = 1, \ldots, n$, let the tuple e_i be given by $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, with 1 occurring in the ith position. Then the set $\{e_1, \ldots, e_n\}$ is an R-basis of R^n. We call it the **canonical basis** of R^n.

Now we recall the notion of a univariate polynomial ring. Since we shall use it to define multivariate polynomial rings recursively, we start with an arbitrary ring R. We consider the set $R^{(\mathbb{N})}$ of all sequences $(r_0, r_1, \ldots)$ of elements $r_0, r_1, \ldots \in R$ such that we have $r_i \neq 0$ for only finitely many indices $i \geq 0$. Using componentwise addition and scalar multiplication, this set becomes a free R-module with R-basis $\{e_i \mid i \in \mathbb{N}\}$, where $e_i = (0, \ldots, 0, 1, 0, 0, \ldots)$ with 1 occurring in position $i + 1$. Every element of this set has a unique representation $(r_0, r_1, \ldots) = \sum_{i \in \mathbb{N}} r_i e_i$. Given two elements $\sum_{i \in \mathbb{N}} r_i e_i$ and $\sum_{i \in \mathbb{N}} s_i e_i$, we define

$$\left(\sum_{i \in \mathbb{N}} r_i e_i\right) \cdot \left(\sum_{i \in \mathbb{N}} s_i e_i\right) = \sum_{i \in \mathbb{N}} \left(\sum_{j=0}^{i} r_j s_{i-j}\right) e_i$$

Can you imagine where this strange rule comes from? (The answer to this question is given after the next definition.)

It is easy to check that the set $R^{(\mathbb{N})}$, together with componentwise addition and the product defined above, is a commutative ring with identity e_0, and that $e_i = e_1^i$ for all $i \in \mathbb{N}$. Furthermore, the map $R \to R^{(\mathbb{N})}$ given by $r \mapsto r \cdot e_0$ is an injective ring homomorphism.

Definition 1.1.8. We let R be a ring and equip $R^{(\mathbb{N})}$ with the ring structure defined above.

a) If we let $x = e_1$, the ring $R^{(\mathbb{N})}$ is called the **polynomial ring in the indeterminate x over** R and is denoted by $R[x]$. It is a commutative ring and every element of $R[x]$ has a unique representation $\sum_{i \in \mathbb{N}} r_i x^i$ with $r_i \in R$ and $r_i \neq 0$ for only finitely many indices $i \in \mathbb{N}$.

b) For $n \geq 1$, we recursively define $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ and call it the **polynomial ring in n indeterminates over** R.

c) The elements of a polynomial ring are called **polynomials**. Polynomials in one indeterminate are often called **univariate polynomials**, while polynomials in several indeterminates are called **multivariate polynomials**.

Notice that, given this definition, the multiplication of two univariate polynomials $\sum_{i \in \mathbb{N}} r_i x^i$ and $\sum_{i \in \mathbb{N}} s_i x^i$ comes out to be $\sum_{i \in \mathbb{N}} (\sum_{j=0}^{i} r_j s_{i-j}) x^i$, and this corresponds exactly to what we learn in high school. Many properties

of a ring are inherited by polynomial rings over it. Some instances of this general phenomenon are given by the following proposition.

Proposition 1.1.9. *Let R be an integral domain.*
a) *The units in $R[x_1, \ldots, x_n]$ are the units in R.*
b) *The polynomial ring $R[x_1, \ldots, x_n]$ is an integral domain.*

Proof. Since $R[x_1, \ldots, x_n]$ was defined recursively, it suffices to prove the claims for $n = 1$. Given two elements $f = \sum_{i \in \mathbb{N}} r_i x^i$ and $g = \sum_{j \in \mathbb{N}} r'_j x^j$ in $R[x] \setminus \{0\}$, we let $d = \max\{i \in \mathbb{N} \mid r_i \neq 0\}$ and $e = \max\{j \in \mathbb{N} \mid r'_j \neq 0\}$. Then the definition of the multiplication in $R[x]$ implies that one of the summands in the representation of the element fg is $r_d r'_e x^{d+e} \neq 0$. From this remark both claims follow immediately. □

Both statements of this proposition fail if R is not an integral domain. For instance, if $R = \mathbb{Z}/(4)$, then $(1 + 2x)(1 - 2x) = 1$ and $2x \cdot (2x^2 + 2) = 0$ in $R[x]$. Following the recursive definition, an example of a polynomial in three indeterminates over $\mathbb{Q}$ is

$$
\begin{aligned}
f(x_1, x_2, x_3) \;=\; & \left((\tfrac{2}{3} - x_1^3) + (x_1^4)x_2 \right) + \left((1 - x_1^5)x_2^4 - (\tfrac{3}{7}x_1 + 7x_1^3)x_2^5 \right. \\
& \left. + (x_1^{11})x_2^7 \right)x_3 + \left((\tfrac{1}{12}x_1 - 13x_1^2 + \tfrac{7}{67}x_1^3) + (x_1 - \tfrac{3}{22}x_1^3)x_2 + (4 - x_1)x_2^2 \right)x_3^2 \\
& + \left(x_2^2 + (4 - \tfrac{8}{13}x_1^9)x_2^3 \right)x_3^3
\end{aligned}
$$

Many parentheses have to be used to represent multivariate polynomials in this way. It sure looks ugly, doesn't it? But we can do much better. The associative and distributive laws provide us with a more compact representation. In fact, every polynomial $f \in R[x_1, \ldots, x_n]$ has a unique representation of the form

$$
f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha t_\alpha
$$

where $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $t_\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, and where only finitely many elements $c_\alpha \in R$ are different from zero. For instance, the polynomial above can be written as

$$
\begin{aligned}
f(x_1, x_2, x_3) \;=\; & x_1^{11}x_2^7 x_3 - \tfrac{8}{13}x_1^9 x_2^3 x_3^3 - x_1^5 x_2^4 x_3 - 7x_1^3 x_2^5 x_3 - \tfrac{3}{7}x_1 x_2^5 x_3 \\
& - \tfrac{3}{22}x_1^3 x_2 x_3^2 + x_1^4 x_2 + \tfrac{7}{67}x_1^3 x_3^2 - x_1 x_2^2 x_3^2 + x_2^2 x_3 + 5x_2^2 x_3^3 \\
& - 13x_1^2 x_3^2 + x_1 x_2 x_3^2 + 4x_2^2 x_3^2 - x_1^3 + \tfrac{1}{12}x_1 x_3^2 + \tfrac{2}{3}
\end{aligned}
$$

It is immediately clear that there are many different ways of writing down this polynomial depending on the ordering of the elements $x_1^{11}x_2^7 x_3$, $x_1^9 x_2^2 x_3^3$, $x_1^5 x_2^4 x_3$, etc.

More generally, let $r \geq 1$, and let $M = (R[x_1, \ldots, x_n])^r$ be the finitely generated free $R[x_1, \ldots, x_n]$-module with canonical basis $\{e_1, \ldots, e_r\}$ such that $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ as in Definition 1.1.7. Then every element $m \in M$ has a unique representation of the form

$$m = (f_1, \ldots, f_r) = \sum_{i=1}^{r} \sum_{\alpha \in \mathbb{N}^n} c_{\alpha,i} t_\alpha e_i$$

where $f_1, \ldots, f_r \in R[x_1, \ldots, x_n]$, and where only finitely many elements $c_{\alpha,i} \in R$ are different from zero.

In these representations, we used polynomials of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. Since such elements will occur frequently, we give them a name.

Definition 1.1.10. Let $n \geq 1$.

a) A polynomial $f \in R[x_1, \ldots, x_n]$ of the form $f = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ such that $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is called a **term** or **power product**. The set of all terms of $R[x_1, \ldots, x_n]$ is denoted by $\mathbb{T}^n$ or $\mathbb{T}(x_1, \ldots, x_n)$.

b) For a term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathbb{T}^n$, the number $\deg(t) = \alpha_1 + \cdots + \alpha_n$ is called the **degree** of t.

c) The map $\log : \mathbb{T}^n \to \mathbb{N}^n$ defined by $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mapsto (\alpha_1, \ldots, \alpha_n)$ is called the **logarithm**.

d) If $r \geq 1$ and $M = (R[x_1, \ldots, x_n])^r$ is the finitely generated free $R[x_1, \ldots, x_n]$-module with canonical basis $\{e_1, \ldots, e_r\}$, then a **term** of M is an element of the form te_i such that $t \in \mathbb{T}^n$ and $1 \leq i \leq r$. The set of all terms of M will be denoted by $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ or by $\mathbb{T}(x_1, \ldots, x_n) \langle e_1, \ldots, e_r \rangle$.

The set $\mathbb{T}^n$ is a commutative monoid. Its identity element is $1 = x_1^0 \cdots x_n^0$. The monoid $\mathbb{T}^n$ does not depend on the ring of coefficients R. The set $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ can be considered as the disjoint union of r copies of $\mathbb{T}^n$ where the symbols $e_1, \ldots, e_r$ simply indicate which copy of $\mathbb{T}^n$ we are considering.

Definition 1.1.11. Let $n \geq 1$, let $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha t_\alpha \in R[x_1, \ldots, x_n]$ be a polynomial, and let $m = \sum_{i=1}^{r} \sum_{\alpha \in \mathbb{N}^n} c_{\alpha,i} t_\alpha e_i \in M = (R[x_1, \ldots, x_n])^r$.

a) For every $\alpha \in \mathbb{N}^n, i \in \{1, \ldots, r\}$, the element $c_{\alpha,i} \in R$ is called the **coefficient** of the term $t_\alpha e_i$ in m.

b) The set $\{t_\alpha e_i \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle \mid c_{\alpha,i} \neq 0\}$ is called the **support** of m and denoted by $\mathrm{Supp}(m)$.

c) If $f \neq 0$, the number $\max\{\deg(t_\alpha) | t_\alpha \in \mathrm{Supp}(f)\}$ is called the **degree** of f and denoted by $\deg(f)$.

For example, the support of the polynomial $f \in \mathbb{Q}[x_1, x_2, x_3]$ above consists of 17 terms, and the sequence of their degrees is $19, 15, 10, 9, 7, 6, 5, 5, 5, 5, 5, 4, 4, 4, 3, 3, 0$. We have ordered the terms in $\mathrm{Supp}(f)$ by decreasing degree. However, this is not enough to order them completely since there are several terms with the same degree. Complete orderings on $\mathbb{T}^n$ and $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ will be examined in Section 1.4.

The polynomial ring can be used to define interesting ring homomorphisms. One of its fundamental properties, called the Universal Property,

says that ring homomorphisms starting from a polynomial ring are uniquely defined by the images of the indeterminates, and those images may be chosen freely.

Proposition 1.1.12. (Universal Property of the Polynomial Ring)
Let S be an R-algebra with structural homomorphism $\varphi : R \to S$, let $n \geq 1$, and let $s_1, \ldots, s_n$ be elements in S. Then there exists a unique ring homomorphism $\psi : R[x_1, \ldots, x_n] \to S$ such that $\psi|_R = \varphi$ and $\psi(x_i) = s_i$ for $i = 1, \ldots, n$.

Proof. By induction, it suffices to prove the claim for $n = 1$. For $d \geq 0$ and $c_0, \ldots, c_d \in R$, we let $\psi(\sum_{i=0}^{d} c_i x_1^i) = \sum_{i=0}^{d} \varphi(c_i) s_1^i$. It is easy to check that this defines a ring homomorphism having the required properties. On the other hand, since ψ has to be compatible with addition and multiplication, this definition is forced upon us and ψ is uniquely determined. $\square$

A ring homomorphism ψ defined in this way is also called an **evaluation homomorphism**, and the image of a polynomial f is called the **evaluation** $f(s_1, \ldots, s_n)$ of f at $(s_1, \ldots, s_n)$. In the special case when $S = R$, an evaluation homomorphism $\psi : R[x_1, \ldots, x_n] \longrightarrow R$ is also called a **substitution homomorphism**. Using evaluations, we can speak about generators of R-algebras in the following manner.

Definition 1.1.13. Let S be an R-algebra.
a) A set $\{s_\lambda \mid \lambda \in \Lambda\}$ of elements of S is called a **system of generators** of S if for every element $s \in S$ there is a finite subset $\{\lambda_1, \ldots, \lambda_t\}$ of Λ and a polynomial $f(x_1, \ldots, x_t) \in R[x_1, \ldots, x_t]$ such that $s = f(s_{\lambda_1}, \ldots, s_{\lambda_t})$.
b) The R-algebra S is called **finitely generated** if it has a finite system of generators.

Corollary 1.1.14. *An R-algebra S is finitely generated if and only if there exists a number $n \in \mathbb{N}$ and a surjective R-algebra homomorphism $\varphi : R[x_1, \ldots, x_n] \longrightarrow S$.*
In other words, every finitely generated R-algebra S is of the form $S \cong R[x_1, \ldots, x_n]/I$ where I is an ideal in $R[x_1, \ldots, x_n]$.

Proof. This follows from the fact that a set $\{s_1, \ldots, s_n\}$ of elements of S is a system of generators of S if and only if the R-algebra homomorphism $\varphi : R[x_1, \ldots, x_n] \longrightarrow S$ defined by $x_i \longmapsto s_i$ for $i = 1, \ldots, n$ is surjective. $\square$

For an R-algebra S which has a finite system of generators $\{s_1, \ldots, s_n\}$, the corresponding isomorphism $S \cong R[x_1, \ldots, x_n]/I$ is called a **presentation** of S by generators and relations, and the ideal I is called the ideal of **algebraic relations** among $\{s_1, \ldots, s_n\}$ with coefficients in R.

Exercise 1. Let $d \in \mathbb{Z}$ be a non-square number, and let $K = \mathbb{Q}[\sqrt{d}]$, where we use $\sqrt{d} = i \cdot \sqrt{-d}$ if $d < 0$. Prove that K is a field, and that every element $r \in K$ has a unique representation $r = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. The field K is called the **quadratic number field** generated by $\sqrt{d}$. After representing $r, s \in K$ by pairs of rationals, give formulae for $r + s$, $-r$, $r \cdot s$, and $\frac{1}{r}$ for $r \neq 0$.

Exercise 2. Show that, up to a unique isomorphism, the polynomial ring $R[x_1, \ldots, x_n]$ is the only R-algebra satisfying the universal property stated in Proposition 1.1.12. In other words, suppose that T is another R-algebra together with elements $t_1, \ldots, t_n \in T$, such that whenever you have an R-algebra S together with elements $s_1, \ldots, s_n \in S$, then there exists a unique R-algebra homomorphism $\psi : T \to S$ satisfying $\psi(t_i) = s_i$ for $i = 1, \ldots, n$. Then show that there is a unique R-algebra isomorphism $R[x_1, \ldots, x_n] \to T$ such that $x_i \mapsto t_i$ for $i = 1, \ldots, n$.

Exercise 3. Show that the map $\log : \mathbb{T}^n \longrightarrow \mathbb{N}^n$ is an isomorphism of monoids.

Exercise 4. Let $v_1 = (a_{11}, a_{21}, \ldots, a_{n1}), \ldots, v_n = (a_{1n}, a_{2n}, \ldots, a_{nn})$ be elements of $\mathbb{Z}^n$, and let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_n(\mathbb{Z})$ be the matrix whose columns are the coordinates of $v_1, \ldots, v_n$. Show that the set $\{v_1, \ldots, v_n\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}^n$ if and only if $\det(\mathcal{A}) \in \{1, -1\}$.

Exercise 5. Let S be the set of functions from $\mathbb{Z}$ to $\mathbb{Z}$.
  a) Show that S with the usual sum and product of functions is a $\mathbb{Z}$-algebra.
  b) Use considerations about the cardinality of S to show that S is not a finitely generated $\mathbb{Z}$-algebra.

Exercise 6. Let R be a ring and I a non-zero ideal of R. Prove that I is a free R-module if and only if it is a principal ideal generated by a non-zerodivisor.

Exercise 7. Let R be a ring. Show that the following conditions are equivalent.
  a) The ring R is a field.
  b) Every finitely generated R-module is free.
  c) Every cyclic R-module is free.

Exercise 8. Let K be a field, $P = K[x_1, x_2]$, and I be the ideal in P generated by $\{x_1, x_2\}$. Show that I is not a free P-module.

Tutorial 1: Polynomial Representation I

In what follows we work over the ring $K[x, y]$, where K is one of the fields defined in CoCoA. Using Definition 1.1.8, we see that we can represent every polynomial $f \in K[x, y]$ as a list of lists, where a univariate polynomial $a_0 + a_1 x + \cdots + a_d x^d$ such that $a_0, \ldots, a_d \in K$ and $a_d \neq 0$ is represented by the list $[a_0, \ldots, a_d]$.

The purpose of this tutorial is to program the transition from polynomials to lists (and back), and to see how addition and multiplication of polynomials can be carried out using their list representations. Thus this tutorial is mainly intended as an introduction to the kind of CoCoA programming we ask you to do in other tutorials.

There are solutions of parts of this tutorial in Appendix C.1. Since most programs require the use of lists, we suggest you read Appendices A.6 and B.5 before you start. A (long) list of CoCoA commands for dealing with lists can be generated by invoking the on-line manual with the command `H.Commands('list');`

a) Write a CoCoA program `ReprUniv(...)` which takes two arguments: the first argument should be a univariate polynomial over K, and the second one should be the indeterminate occurring in it. If the polynomial is $f = a_0 + a_1 x + \cdots + a_d x^d$, the program should return the list $[a_0, \ldots, a_d]$ representing this polynomial.
   Hint: There is a *pedestrian* solution involving a `For`-loop and the CoCoA function `CoeffOfTerm(...)` and an elegant one using the command `Coefficients(...)`.

b) Implement also a CoCoA function `ListToPoly(...)` which takes a list of numbers and constructs the corresponding univariate polynomial in the indeterminate x. Use this function and `ReprPoly(...)` to convert the polynomials $f_1 = x^4 + 3x^2 - x + 1$ and $f_2 = y^2 + 2y + 3$ to lists and back.
   Hint: A simple `For`-loop or the sum over an appropriately constructed list will do the trick.

c) Write CoCoA functions `AddUniv(...)` and `MultUniv(...)` which take two lists representing univariate polynomials and compute the lists representing their sum and product, respectively. Use the program `ListToPoly(...)` to check the correctness of both functions.
   Hint: When implementing the sum, you should switch the summands such that the first one has larger degree (i.e. a longer list). Then you can add the elements of the second list onto the first one.
   For the implementation of the product, you may want to consider the formula $(a_0 + \cdots + a_d x^d) \cdot (b_0 + \cdots + b_e x^e) = \sum_{i=0}^{d+e} (\sum_{j=0}^{i} a_j b_{i-j}) \cdot x^i$. It may be useful to bring both lists to the same length first (by appending zeros). The inner sum could be realized by a construction like `Sum(L)`, where `L` is the list of all $a_j b_{i-j}$.

d) Write a CoCoA program `ReprPoly(...)` which represents a polynomial $f \in K[x, y]$ as a list of lists of elements of K. The elements of the big list are lists representing univariate polynomials in $K[x]$, namely the coefficients of the different powers of y in the polynomial, considered as an element of $(K[x])[y]$ as in Definition 1.1.8.b. For instance, the polynomial $f_1 = x^2 + 2xy + 3y^2$ is represented by the list of lists $[[0, 0, 1], [0, 2], [3]]$.

Hint: The CoCoA command `Deg(F,x)` returns the degree of a polynomial F with respect to the indeterminate x. The function `Shorten(...)` in Appendix C.1 removes trailing zeros from a list. These facts and a double `For`-loop are good enough for a first solution. More elegantly, you can also use `Reversed(Coefficients(...))` and a clever list construction.

e) Write a CoCoA program `ListListToPoly(...)` which converts lists of lists back to polynomials in $K[x, y]$.

f) Apply the programs `ReprPoly(...)` and `ListListToPoly(...)` to the polynomials $f_1 = x^2 + 2xy + 3y^2$, $f_2 = y^2 - x^4$, and $f_3 = 1 + x + y + x^2 + y^2 + x^4 + y^4 + x^8 + y^8$.

g) Write CoCoA-programs `AddPoly(...)` and `MultPoly(...)` which take two lists L_1, L_2 representing polynomials in $K[x, y]$ and compute the lists representing their sum and product, respectively.

h) Check the correctness of your programs by converting $f_1 + f_2$, $f_1 \cdot f_2$ and $f_2 f_3 + f_1^3$ into lists in two ways.

i) *(For more advanced programmers)* Using recursive programming, redo parts d), e), and g) for polynomials in $K[x_1, \ldots, x_n]$. Try these functions in some concrete examples and show that they are correct.

Tutorial 2: The Extended Euclidean Algorithm

There is a well-known algorithm for computing the greatest common divisor of two positive integers called the **Euclidean Algorithm**. In this tutorial we shall extend it and use the extended version to show how to implement the basic operations of a field of type $\mathbb{F}_p = \mathbb{Z}/(p)$.

a) Let $a, b \in \mathbb{Z}$. Consider the following sequence of instructions.

1) If $a = b = 0$, return 0. If $a = 0$ and $b \neq 0$, return $|b|$. If $a \neq 0$ and $b = 0$, return $|a|$. Otherwise replace a and b by their absolute values and form the pair $(a, b) \in \mathbb{N}^2$.

2) If $a > b$, interchange a and b.

3) Compute a representation $b = qa + r$ with $q \in \mathbb{N}$ and a remainder $0 \leq r < a$. If $r = 0$, return a. If $r \neq 0$, replace (a, b) by (r, a) and repeat step 3).

Show that this is an algorithm which stops after finitely many steps and returns $\gcd(a, b)$, i.e. the greatest common divisor of a and b. (We use $\gcd(0, 0) = 0$.) It is called the **Euclidean Algorithm**.

b) Write a CoCoA function `Euclid(...)` which implements the algorithm of a).

c) Prove that, for $a, b \in \mathbb{Z}$, there exist $c, d \in \mathbb{Z}$ such that $ac + bd = \gcd(a, b)$.

d) Let $a, b \in \mathbb{Z}$. Consider the following sequence of instructions.

1) If $a = b = 0$, return the triple $(0, 0, 0)$. If $a = 0$ and $b \neq 0$, return the triple $(0, \frac{|b|}{b}, |b|)$. If $a \neq 0$ and $b = 0$, return the triple $(\frac{|a|}{a}, 0, |a|)$.

2) Form the triples $(c_0, d_0, e_0) = (\frac{|a|}{a}, 0, |a|)$ and $(c_1, d_1, e_1) = (0, \frac{|b|}{b}, |b|)$.

3) Check whether $e_1 \leq e_0$. If this is not the case, interchange (c_0, d_0, e_0) and (c_1, d_1, e_1).

4) Write e_0 in the form $e_0 = qe_1 + r$, where $q \in \mathbb{N}$ and $0 \leq r < e_1$. Then form $(c_2, d_2, e_2) = (c_0 - qc_1, d_0 - qd_1, r)$.

5) Replace (c_0, d_0, e_0) by (c_1, d_1, e_1) and (c_1, d_1, e_1) by (c_2, d_2, e_2).

6) Repeat steps 4) and 5) until $e_1 = 0$. Then return the triple (c_0, d_0, e_0) and stop.

Show that this is an algorithm, called the **Extended Euclidean Algorithm**, i.e. that it stops after finitely many steps, and that it computes a triple $(c, d, e) \in \mathbb{Z}^3$ such that $e = \gcd(a, b)$ and $ac + bd = e$.

e) Write a CoCoA function `ExtEuclid(...)` which implements the algorithm in d).

f) Explain how one can modify the Extended Euclidean Algorithm so that it applies to univariate polynomials over a field K. Write a CoCoA function `PolyExtEuclid(...)` which performs this computation.

Hint: Use the built-in CoCoA function `DivAlg(...)` to do the division with remainder.

g) Every element of $\mathbb{Z}/(p)$ can be uniquely represented by one of the integers in $\{0, 1, \ldots, p-1\}$. Write CoCoA functions `ZpAdd(...)`, `ZpMult(...)`, `ZpNeg(...)`, and `ZpInv(...)` which compute addition, multiplication, negatives, and inverses in $\mathbb{Z}/(p)$ using this representation. Do not use the built-in modular arithmetic of CoCoA, but find direct methods.

Tutorial 3: Finite Fields

In Tutorial 2 we showed how to perform actual computations in the finite fields of type $\mathbb{Z}/(p)$. The purpose of this tutorial is to build upon that knowledge and show how it is possible to compute in more general finite fields. Let $p > 1$ be a prime number.

(Note: Several parts require some basic knowledge of field theory.)

a) Let K be a finite field of characteristic p. Show that the number q of elements of K is a power of p, i.e. there is a number $e > 0$ such that $q = p^e$. (*Hint:* Note that K is a $\mathbb{Z}/(p)$-vector space.)

b) Let L be an algebraically closed field of characteristic p. Prove that there exists a unique subfield $\mathbb{F}_q$ of L which has q elements, and that it is the set of roots of the equation $x^q - x = 0$.

c) Show that every field K with q elements is isomorphic to $\mathbb{F}_q$, that there is an irreducible polynomial f of degree e in $\mathbb{Z}/(p)[x]$, and that there is an isomorphism $K \cong \mathbb{Z}/(p)[x]/(f)$.

Hint: For the second part, use the fact that the multiplicative group $K \backslash \{0\}$ is cyclic.

d) Implement a CoCoA function `IrredPoly(...)` which computes the list of all **monic** irreducible polynomials f of degree $d = \deg f \leq e$ in $\mathbb{Z}/(p)[x]$, i.e. whose coefficient of x^d is 1. Proceed degree by degree, starting with $[x, x - 1, \ldots, x - p + 1]$ and appending the list of all monic polynomials of degree d which are not divisible by one of the irreducible polynomials of degree $\leq d/2$.

e) Using $f = \texttt{Last(IrredPoly(...))}$, we can represent every element $r \in K$ as a list $r = [r_1, \ldots, r_e]$ of elements $r_1, \ldots, r_e \in \mathbb{Z}/(p)$ such that $r + (f) = r_1 + r_2 x + \cdots + r_e x^{e-1} + (f)$. Write CoCoA functions `FFAdd(...)`, `FFNeg(...)`, `FFMult(...)`, and `FFInv(...)` which compute the lists representing the sums, negatives, products, and inverses of elements of K, respectively. (*Hint:* Use the base ring `S::=Z/(P)[x]`.)

f) Compute a representation of the field $\mathbb{F}_{16}$ and its multiplication table.

1.2 Unique Factorization

Everything should be made
as simple as possible,
but not simpler.
(Albert Einstein)

In this section we discuss a fundamental property of polynomial rings over fields, namely the unique factorization property. One learns in school that for every integer n we may write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, where $p_1, \ldots, p_s$ are prime numbers. For instance, $504 = 2^3 \cdot 3^2 \cdot 7$. Moreover, such a factorization is unique up to sign changes and order, for instance $504 = (-2)^3 \cdot (-7) \cdot 3^2$. The main topic in this section is to prove that polynomial rings have the same property.

The spirit of the section is to give an account of the theory underlying this notion which is as simple as possible, but not simpler. Once it is known that polynomial rings over fields have the unique factorization property, the next question is how to compute factorizations of polynomials effectively. The treatment of that question goes beyond the scope of this book. However, in Tutorial 6 we give some hints on how to do it for univariate polynomials over $\mathbb{Z}/(p)$.

Other notions which everyone learns in school are the least common multiple and greatest common divisor of natural numbers. We show that factorial rings provide a suitable environment for defining such concepts (see Definition 1.2.6) and we prove some of their basic properties (see Proposition 1.2.8). Other subjects related to the unique factorization property will be considered in the exercises and tutorials.

Now, let us do first things first and introduce the notions of irreducible and prime elements in such a way that it is possible to speak about factorizations.

Definition 1.2.1. Let R be an integral domain and $r \in R \setminus \{0\}$ be a non-unit.

a) The element r is said to be **reducible**, if it can be expressed as the product of two elements neither of which is a unit. Otherwise it is called **irreducible**.

b) If $r = u \cdot r_1 \cdot r_2 \cdots r_s$ with a unit $u \in R$ and irreducible elements $r_1, \ldots, r_s$, then such an expression is called a **factorization** of r.

c) If r has the property that $r \mid r_1 \cdot r_2$ implies $r \mid r_1$ or $r \mid r_2$ for all $r_1, r_2 \in R$, then r is called a **prime** (or a **prime element**) of R.

For a unit $r \in R$, we shall call $r = r$ a factorization of r. We observe that the only divisors of an irreducible element are the units and the element itself.

Proposition 1.2.2. *In the polynomial ring $K[x]$ in one indeterminate over a field K, a non-zero non-unit element is a prime if and only if it is irreducible.*

Proof. The only non-trivial implication is to show that if f is irreducible, then it is a prime. We have already mentioned (see Example 1.1.6) that if K is a field, then every ideal in $K[x]$ is principal. Suppose f is irreducible, $f \mid ab$, and $f \nmid a$. Then $ab = gf$ for some $g \in K[x]$. Since the ideal (a, f) is generated by a divisor of f, we have $(a, f) = (1)$, and therefore $1 = ra + sf$ for some $r, s \in K[x]$. Thus we get $b = rab + sbf = rgf + sbf$ and $f \mid b$. □

In Exercise 9 we will see an element of an integral domain which is irreducible but not prime. The following example shows that the notion of irreducibility in a polynomial ring depends strongly on the field of coefficients.

Example 1.2.3. In the ring $\mathbb{R}[x]$ the element $x^2 + 1$ is irreducible. On the other hand, in the ring $\mathbb{C}[x]$, we have $x^2 + 1 = (x + i)(x - i)$, hence it is reducible. It is clear that other factorizations of $x^2 + 1$ are for instance $(i - x)(-i - x)$ and $(2x + 2i)(1/2x - 1/2i)$, but it is also clear that these factorizations are basically the same, i.e. they differ only by changing the factors by units.

This leads to the following definition.

Definition 1.2.4. Let R be an integral domain. Then R is said to be **factorial**, or a **factorial domain**, or a **unique factorization domain** if every non-unit in $R \setminus \{0\}$ has a unique factorization up to order and units.

For example, every field is trivially a factorial domain. In order to find less trivial examples, we want to study how this uniqueness of factorizations relates to the notions of irreducible and prime elements.

Proposition 1.2.5. *Let R be an integral domain with the property that every non-zero non-unit has a factorization. Then the following conditions are equivalent.*

a) The ring R is factorial.
b) Every irreducible element of R is a prime.

Proof. Let R be factorial, and let $r \in R$ be an irreducible element. Suppose $r \mid ab$. Hence we have an equation $ab = cr$ with non-units $a, b, c \in R \setminus \{0\}$. Then the irreducible factor r must show up either in the factorization of a or in that of b. Therefore we have either $r \mid a$ or $r \mid b$ which shows that r is a prime.

Conversely, let $a_1 a_2 \cdots a_s = b_1 b_2 \cdots b_t$ be factorizations of the same element. We see that $b_1 b_2 \cdots b_t \in (a_1)$, hence the assumption implies that one of the factors has to be in (a_1). Up to a permutation of the factors we may assume that $b_1 \in (a_1)$. Since both a_1 and b_1 are irreducible, they are equal up to a unit and can be cancelled in the equation $a_1 a_2 \cdots a_s = b_1 b_2 \cdots b_t$. Continuing in this way, we can see that the two factorizations are essentially the same. □

As with integers, it is possible to define greatest common divisors and least common multiples in a factorial domain.

Definition 1.2.6. Let R be a factorial domain. We say that two irreducible elements of R are **associated** if they differ only by multiplication with a unit of R. Let the set $\mathcal{P} \subseteq R$ be obtained by picking one element in each class of associated irreducible elements of R. Furthermore, let $m \geq 2$ and $f_1, \ldots, f_m \in R \setminus \{0\}$.

a) Let $f_1 = c_1 \prod_{p \in \mathcal{P}} p^{\alpha_p}$ and $f_2 = c_2 \prod_{p \in \mathcal{P}} p^{\beta_p}$ be factorizations of f_1 and f_2 with units $c_1, c_2 \in R$, with $\alpha_p, \beta_p \in \mathbb{N}$, and with $\alpha_p = \beta_p = 0$ for all but finitely many $p \in \mathcal{P}$. Then the element

$$\gcd(f_1, f_2) = \prod_{p \in \mathcal{P}} p^{\min\{\alpha_p, \beta_p\}}$$

is called a **greatest common divisor** of f_1 and f_2, and the element

$$\mathrm{lcm}(f_1, f_2) = \prod_{p \in \mathcal{P}} p^{\max\{\alpha_p, \beta_p\}}$$

is called a **least common multiple** of f_1 and f_2.

b) If $\gcd(f_1, f_2) = 1$, we say that f_1, f_2 are **coprime** or **relatively prime**.

c) For $m > 2$, we define a **greatest common divisor** and a **least common multiple** of $f_1, \ldots, f_m$ recursively by

$$\gcd(f_1, \ldots, f_m) = \gcd(\gcd(f_1, \ldots, f_{m-1}), f_m)$$

$$\mathrm{lcm}(f_1, \ldots, f_m) = \mathrm{lcm}(\mathrm{lcm}(f_1, \ldots, f_{m-1}), f_m)$$

d) Let $f = c \prod_{p \in \mathcal{P}} p^{\alpha_p}$ with a unit $c \in R$, with $\alpha_p \in \mathbb{N}$, and with $\alpha_p = 0$ for all but finitely many $p \in \mathcal{P}$ be the decomposition of an element $f \in R \setminus \{0\}$ into irreducible factors. Then the element

$$\mathrm{sqfree}(f) = \prod_{p \in \mathcal{P}} p^{\min\{1, \alpha_p\}}$$

is called a **squarefree part** of f.

It is clear that the definition of greatest common divisors and least common multiples does not depend on the order of the elements. It is also clear that greatest common divisors, least common multiples, and squarefree parts of elements $f_1, \ldots, f_m \in R \setminus \{0\}$ change only by a unit if we choose a different set of representatives $\mathcal{P}$ for the equivalence classes of irreducible elements. We shall therefore speak of **the** greatest common divisor and **the** least common multiple of $f_1, \ldots, f_m \in R \setminus \{0\}$, as well as **the** squarefree part of $f \in R \setminus \{0\}$, while always keeping in mind that they are unique only up to a unit.

In the following, we describe some connections between greatest common divisors, least common multiples, and ideal theory. First we characterize greatest common divisors and least common multiples by divisibility properties.

Proposition 1.2.7. (Characterization of gcd and lcm)
   Let R be a factorial domain, and let $f_1, \ldots, f_m \in R \setminus \{0\}$

   a) *An element $f \in R$ is the greatest common divisor of $f_1, \ldots, f_m$ if and only if $f \mid f_i$ for $i = 1, \ldots, m$ and every element $g \in R$ such that $g \mid f_i$ for $i = 1, \ldots, m$ satisfies $g \mid f$.*
   b) *An element $f \in R$ is the least common multiple of $f_1, \ldots, f_m$ if and only if $f_i \mid f$ for $i = 1, \ldots, m$ and every element $g \in R$ such that $f_i \mid g$ for $i = 1, \ldots, m$ satisfies $f \mid g$.*

Proof. First we prove a). For $i = 1, \ldots, m$, let $f_i = c_i \prod_{p \in \mathcal{P}} p^{\alpha_{pi}}$ be the factorization of f_i. Using the definition and induction on m, we see that $\gcd(f_1, \ldots, f_m) = \prod_{p \in \mathcal{P}} p^{\min\{\alpha_{p1}, \ldots, \alpha_{pm}\}}$. Thus it follows immediately that $\gcd(f_1, \ldots, f_m)$ divides f_i for $i = 1, \ldots, m$.

   Now let $g \in R$ be a common divisor of $f_1, \ldots, f_m$, and let $g = c \prod_{p \in \mathcal{P}} p^{\beta_p}$ be the factorization of g. For every $i \in \{1, \ldots, m\}$, the condition $g \mid f_i$ implies that $\beta_p \leq \alpha_{pi}$ for all $p \in \mathcal{P}$. Hence we get $\beta_p \leq \min\{\alpha_{p1}, \ldots, \alpha_{pm}\}$ for all $p \in \mathcal{P}$, and therefore $g \mid \gcd(f_1, \ldots, f_m)$.

   The proof of claim b) follows in exactly the same way.   □

Proposition 1.2.8. *Let R be a factorial domain and $f_1, \ldots, f_m \in R \setminus \{0\}$.*

   a) *The element $\mathrm{lcm}(f_1, \ldots, f_m)$ generates the ideal $(f_1) \cap \cdots \cap (f_m)$.*
   b) *We have $\gcd(f_1, f_2) = f_1 f_2 / \mathrm{lcm}(f_1, f_2)$.*
   c) *Suppose R is a principal ideal domain. Then $\gcd(f_1, \ldots, f_m)$ generates the ideal $(f_1, \ldots, f_m)$. In particular, we have $\gcd(f_1, \ldots, f_m) = 1$ if and only if there are elements $g_1, \ldots, g_m \in R$ such that $g_1 f_1 + \cdots + g_m f_m = 1$.*

Proof. Since least common multiples were defined recursively, it suffices to prove claim a) for $m = 2$. Let $f_1 = c_1 p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and $f_2 = c_2 p_1^{\beta_1} \cdots p_s^{\beta_s}$ be factorizations of f_1 and f_2, where $c_1, c_2 \in R$ are units, where $\alpha_i, \beta_j \geq 0$, and where $p_1, \ldots, p_s \in R$ are irreducible elements representing s different equivalence classes. Note that $\mathrm{lcm}(f_1, f_2) = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_s^{\max\{\alpha_s, \beta_s\}}$ is divisible by both f_1 and f_2, i.e. it is in $(f_1) \cap (f_2)$. Conversely, every element in $(f_1) \cap (f_2)$ is divisible by $p_i^{\alpha_i}$ and $p_i^{\beta_i}$ for $i = 1, \ldots, s$, and therefore by $p_i^{\max\{\alpha_i, \beta_i\}}$. Thus every element in $(f_1) \cap (f_2)$ is a multiple of $\mathrm{lcm}(f_1, f_2)$.

   The proof of b) follows from the fact that $\alpha_i + \beta_i = \min\{\alpha_i, \beta_i\} + \max\{\alpha_i, \beta_i\}$ for $i = 1, \ldots, s$. Finally, to show c), we note that any element of $(f_1, \ldots, f_m)$ is a multiple of $\gcd(f_1, \ldots, f_m)$. Conversely, let $h \in R$ be a generator of $(f_1, \ldots, f_m)$. Since $h \mid f_i$ for $i = 1, \ldots, m$, we have $h \mid \gcd(f_1, \ldots, f_m)$. Thus we get $\gcd(f_1, \ldots, f_m) \in (h) = (f_1, \ldots, f_m)$, as claimed.   □

   Now it is time to move directly to the heart of this section. We want to prove that polynomial rings over fields are factorial. The next lemma is the key to this proof.

Definition 1.2.9. Let R be a factorial domain and $f \in R[x] \setminus \{0\}$. A greatest common divisor of the coefficients of f is called a **content** of f. As before, we usually speak of **the** content of f and denote it by $\mathrm{cont}(f)$. If $\mathrm{cont}(f) = 1$, we say that f is **primitive**.

Lemma 1.2.10. (Gauß's Lemma)
Let R be a factorial domain, and let $f, g \in R[x]$ be non-zero polynomials.

a) We have $\mathrm{cont}(fg) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$.
b) If f, g are primitive, so is fg.

Proof. It is clear that a) follows from b), since every polynomial f is of the form $f = \mathrm{cont}(f) \cdot \tilde{f}$ for some primitive polynomial $\tilde{f}$. So, let us prove b). We write $f = \sum_{i \in \mathbb{N}} r_i x^i$ and $g = \sum_{i \in \mathbb{N}} s_i x^i$ with $r_i, s_i \in R$. Let p be an irreducible element of R. The hypothesis implies that the numbers $j = \min\{i \in \mathbb{N} \mid p \nmid r_i\}$ and $k = \min\{i \in \mathbb{N} \mid p \nmid s_i\}$ exist. Now R is factorial and p is irreducible, hence prime. As it does not divide r_j and s_k, it does not divide $r_j \cdot s_k$ either. The choice of j and k yields that p does not divide the coefficient of x^{j+k} in fg. Therefore it does not divide $\mathrm{cont}(fg)$, and we are done. $\qquad\square$

Lemma 1.2.11. *Let R be a factorial domain. Then every non-zero element of $R[x]$ has a factorization.*

Proof. Let $f \in R[x] \setminus \{0\}$ be a non-unit. Since f is of the form $f = \mathrm{cont}(f) \cdot g$ with a primitive polynomial g, and since $\mathrm{cont}(f)$ has a factorization by assumption, we may assume that f is primitive.

We proceed by induction on $d = \deg(f)$. If $d = 0$ then $f = \mathrm{cont}(f) = 1$ has a trivial factorization. If $d > 0$ and f is irreducible, there is nothing to prove. Otherwise, let $f = gh$ with non-units $g, h \in R[x] \setminus \{0\}$. If one of the two, say g, has degree zero, i.e. if $g \in R$, then $1 = \mathrm{cont}(f) = g \cdot \mathrm{cont}(h)$, contradicting the fact that g is not a unit. Thus the degrees of g and h are both strictly less than d, and an application of the inductive hypothesis finishes the proof. $\qquad\square$

Proposition 1.2.12. *Let R be a factorial domain. Then $R[x]$ is also a factorial domain.*

Proof. According to Proposition 1.2.5 and Lemma 1.2.11, we have to prove that every irreducible polynomial in $R[x]$ is prime. Let $Q(R)$ be the field of fractions of R. In order to prove the claim, we shall argue as follows: if f is an irreducible element of $R[x]$, we show that it is irreducible in $Q(R)[x]$, hence prime in $Q(R)[x]$. Finally, we infer from this that f is prime in $R[x]$.

Let f be an irreducible element in $R[x]$. Then it is clear that f is primitive. Suppose we have in $Q(R)[x]$ an equation $f = g_1 h_1$ with non-zero and non-invertible polynomials $g_1, h_1 \in Q(R)[x]$. Then g_1 and h_1 are of positive degree. By possibly clearing the denominators, we see that there exists an

element $r \in R$ such that $rf = g_2 h_2$ with $g_2, h_2 \in R[x]$. From Lemma 1.2.10 we know that $r = \mathrm{cont}(g_2) \cdot \mathrm{cont}(h_2)$. Thus we can simplify and get a new equation $f = g_3 h_3$ with primitive polynomials $g_3, h_3 \in R[x]$. Since the degrees of g_3 and h_3 are positive and R is an integral domain, neither is a unit, contradicting the irreducibility of f. Thus we have shown that f is irreducible in $Q(R)[x]$.

The ring $Q(R)[x]$ is a univariate polynomial ring over a field, hence in $Q(R)[x]$ every irreducible element is prime (see Proposition 1.2.2). Consequently, the polynomial f is prime in $Q(R)[x]$. It remains to show that f is prime as an element of $R[x]$. We start with an equation $ef = gh$, where $e, g, h \in R[x]$. If we read it in $Q(R)[x]$, we deduce that g or h must be a multiple of f in $Q(R)[x]$. Assume for instance that $g = qf$ with $q \in Q(R)[x]$. By clearing the denominators, we get $rg = pf$ for some $r \in R$ and $p \in R[x]$. Therefore we have $r \cdot \mathrm{cont}(g) = \mathrm{cont}(p)$, and after cancelling r we obtain $g \in (f)$, as was to be shown. $\square$

By repeatedly applying the previous proposition, we see that polynomial rings over fields are factorial domains. This is one of their fundamental properties and deserves to be the final theorem of the present section.

Theorem 1.2.13. *Let K be a field and $n \geq 1$. Then the polynomial ring $K[x_1, \ldots, x_n]$ is a factorial domain.*

Exercise 1. Prove that prime elements are irreducible.

Exercise 2. Let $p = 101$. Write a CoCoA program which checks whether a given polynomial $f \in \mathbb{Z}/(p)[x]$ of degree $\deg(f) \leq 3$ is irreducible. Prove the correctness of your method.

Exercise 3. Let p be a prime number and $\pi : \mathbb{Z}[x] \rightarrow \mathbb{Z}/(p)[x]$ the canonical homomorphism.
  a) Show that if $f \in \mathbb{Z}[x]$ is a monic polynomial and $\pi(f)$ is irreducible then f is irreducible.
  b) Prove that statement a) is, in general, false if f is not monic.
  c) Give a counterexample to the converse of a).

Exercise 4. Find a factorial domain $R \neq \mathbb{Z}$ which does not contain a field.

Exercise 5. Show that if R is a factorial domain and $\mathfrak{p}$ is minimal among the prime ideals different from (0), then $\mathfrak{p}$ is principal.

Exercise 6. Let R be an integral domain with the property that every non-zero non-unit has a factorization. Assume that, for all $a, b \in R \setminus \{0\}$, the ideal $(a) \cap (b)$ is principal.
  a) Prove that, given non-associated irreducible elements $a, b \in R \setminus \{0\}$, we have $(a) \cap (b) = (ab)$.
  Hint: Let $(a) \cap (b) = (c)$, let $ab = rc$, and let $c = sa$. Show that s cannot be a unit. Then deduce that r has to be a unit.

b) Use a) to prove that two factorizations of any element are the same up to order and units.
c) Conclude that R is a factorial domain.

Exercise 7. Consider the ring $R = \mathbb{Z}[\sqrt{-5}]$. Prove that the elements $f_1 = 2 + 2\sqrt{-5}$ and $f_2 = 6$ do not have a greatest common divisor in the sense of Proposition 1.2.7.a.
Hint: Show that both 2 and $1 + \sqrt{-5}$ are common divisors.

Exercise 8. Let R be a factorial domain and $a, b \in R \setminus \{0\}$ two co-prime elements. Prove that the polynomial $ax + b$ is an irreducible element of $R[x]$.

Exercise 9. Let K be a field, $P = K[x_1, x_2, x_3, x_4]$, and $\mathfrak{p}$ be the principal ideal generated by $f = x_1 x_4 - x_2 x_3$.

a) Show that the polynomial f is irreducible in P. Deduce that $P/\mathfrak{p}$ is an integral domain.
b) Prove that the residue class of x_1 modulo $\mathfrak{p}$ is irreducible in $P/\mathfrak{p}$, but not prime. Use this to infer that $P/\mathfrak{p}$ is not factorial.

Exercise 10. Let K be a field and $K(x)$ the field of fractions of $K[x]$. We consider the ring $R = K[x_1, x_2]/(x_1 x_2 - 1)$.

a) Show that R is isomorphic to a K-subalgebra of $K(x)$ which contains $K[x]$. (*Hint:* Try to map x_1 to x and x_2 to $\frac{1}{x}$. To show that only multiples of $x_1 x_2 - 1$ are in the kernel of this map, write polynomials in $K[x_1, x_2]$ as $\sum_{i>0} x_1^i \cdot f_i(x_1 x_2) + \sum_{i>0} x_2^i \cdot g_i(x_1 x_2) + c$ where $c \in K$.)
b) Using a), we may assume $K[x] \subset R \subset K(x)$. In this situation, show that x is a unit in R and every element $g \in R$ can be written as $g = x^r \cdot f$ where $r \in \mathbb{Z}$ and $f \in K[x]$.
c) Prove that R is a factorial domain. (*Hint:* Use the representation given in b) to show that every irreducible element is prime.)

Exercise 11. For a univariate polynomial f, we denote its **derivative** by f'. Let K be a field such that $\mathrm{char}(K) \neq 2, 3$.

a) Let $f(x) = x(x-a)(x-b)$ and assume that 2 and $a^2 + b^2 + (a-b)^2$ are squares in K. Then prove that $f'(x)$ splits as the product of two linear factors.
b) If 3 is a square in K, observe that $f = x^3 - 3ax^2 - 3b^2 x + 9ab^2$ is a product of three linear factors.
c) Use a) and b) to prove that the following conditions are equivalent.

   1) For all $a, b \in K$, there is an element $c \in K$ such that $a^2 + b^2 = c^2$.
   2) For every monic polynomial $f \in K[x]$ of degree 3 which is a product of three linear factors, f' is a product of two linear factors.

Tutorial 4: Euclidean Domains

In general, it is difficult to decide whether a given ring is factorial, and consequently there exists only a rather limited supply of examples of factorial domains. The purpose of this tutorial is to provide the reader with a tool for constructing or detecting a special kind of non-trivial factorial domains.

We say that (R, φ) (or simply R) is a **Euclidean domain** if R is a domain and φ is a function $\varphi : R \setminus \{0\} \to \mathbb{N}$ such that for all $a, b \in R \setminus \{0\}$ the following properties hold.

1) If $a \mid b$ then $\varphi(a) \leq \varphi(b)$.
2) There exist elements $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.

First of all, prove that in a Euclidean domain R the following additional rule holds.

3) Let $a, b \in R \setminus \{0\}$. If $b = ac$ for some non-unit $c \in R$, then $\varphi(a) < \varphi(b)$.
   Hint: Use 2) and write $a = qb + r$. Show that $r \neq 0$, hence $\varphi(r) < \varphi(b)$. Deduce $(1 - qc)a = r$, hence $\varphi(a) \leq \varphi(r)$.

Some rings, which should be familiar to the reader, are in fact Euclidean domains.

a) Show that the ring of integers $\mathbb{Z}$, together with the absolute value function, is a Euclidean domain.
b) Check that every univariate polynomial ring $K[x]$ over a field K, together with the degree function, is a Euclidean domain.

In the following, we let R be a Euclidean domain.

c) Show that if $m = \min\{\varphi(a) \mid a \in R \setminus \{0\}\}$, then $\{a \in R \setminus \{0\} \mid \varphi(a) = m\}$ is the set of units of R.
d) Use 1), and an argument similar to that given in Lemma 1.2.11, to prove that every non-unit in $R \setminus \{0\}$ has a factorization.
e) Use 2) to show that in R there is a notion of $\gcd(a, b)$ for $a, b \in R \setminus \{0\}$ in the sense of Proposition 1.2.7.a, and that $\gcd(a, b)$ can be expressed as $ra + sb$ with $r, s \in R$.
f) Use e) to prove that in R every irreducible element is prime. Conclude that R is factorial.
   Hint: Let p be irreducible and $ab = cp$. If p does not divide a, then $\gcd(a, p) = 1$. Hence $1 = ra + sp$, and therefore $b = \cdots$.
g) Consider the subring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. It is called the ring of **Gaußian numbers**.
   1) Let $\varphi : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}$ be defined by $\varphi(a + bi) = a^2 + b^2$. Show that φ makes $\mathbb{Z}[i]$ into a Euclidean domain.
      Hint: Let $z_1 = a + bi, z_2 = c + di$ and $z = \frac{z_1}{z_2} = \frac{(a+bi)(c-di)}{c^2+d^2} \in \mathbb{Q}[i]$. Choose for $q \in \mathbb{Z}[i]$ a "good" approximation of z and write $z_1 = qz_2 + r$.
   2) Find the set of units of $\mathbb{Z}[i]$.

3) Let $p \in \mathbb{N}$ be a prime number. Show that p is reducible in $\mathbb{Z}[i]$ if and only if there exist $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$.
   Hint: Prove that the map φ is compatible with multiplication.
4) Show that if $z \in \mathbb{Z}[i]$ is such that $\varphi(z)$ is a prime number in $\mathbb{Z}$, then z is prime in $\mathbb{Z}[i]$.
5) Representing elements of $\mathbb{Z}[i]$ as pairs of integers, implement two CoCoA functions `GaussGCD(...)` and `GaussLCM(...)` which compute the greatest common divisor and least common multiple of two Gaußian integers, respectively.
6) Using CoCoA, program a factorization algorithm `GaussFactor(...)` for elements $z \in \mathbb{Z}[i]$.
   Hint: Proceed as for integers, searching for divisors in the set of all elements $a + bi$ such that $a^2 + b^2$ divides $\varphi(z)$.

Tutorial 5: Squarefree Parts of Polynomials

In this tutorial we shall explore how one can effectively compute the square-free part of a univariate polynomial over certain fields. It will turn out that this seemingly innocent problem is in fact intrinsically related to the structure of the base field K.

a) Let K be a field of characteristic $p > 0$, and let $\varphi : K \to K$ be the map defined by $\varphi(a) = a^p$. The map φ is called the **Frobenius map**.

1) Show that the map φ is a ring homomorphism.
2) Show that φ is bijective if K is finite.
3) Deduce that if K is finite then every element has a unique p^{th} root.

If a field K has characteristic 0 or has characteristic $p > 0$ and, in addition, has the property that every element has a pth root, then K is called a **perfect field**. In the sequel, we let K be a perfect field and $f \in K[x]$ a non-zero polynomial. We use the convention $\gcd(f, 0) = f$ and denote the derivative of f by f'.

b) Let $\operatorname{char}(K) = p > 0$. Show that $f' = 0$ holds if and only if f is of the form $f = g^p$ for some $g \in K[x]$.
c) Suppose that $K = \mathbb{F}_q$, where $q = p^e$ and $e > 0$, is a finite field of characteristic $p > 0$ (see Tutorial 3), and let $f \in K[x]$ be a polynomial such that $f' = 0$. Explain how one can compute a polynomial $g \in K[x]$ such that $g^p = f$.
   Hint: Show that every term in the support of f is of the form $x^{\alpha p}$ and prove $(c^{p^{e-1}})^p = c$ for all $c \in K$.
d) Write a CoCoA function `PRoot(...)` which takes a polynomial $f \in \mathbb{F}_p[x]$ such that $f' = 0$ and computes a polynomial $g \in \mathbb{F}_p[x]$ such that $f = g^p$.
e) Show that if f is irreducible, then we have $\gcd(f, f') = 1$.
   Hint: Distinguish the cases $\operatorname{char}(K) = 0$ and $\operatorname{char}(K) = p > 0$.

f) Let $g \in K[x]$ be a polynomial such that $\gcd(f, g) = 1$. Prove the formula $\gcd(fg, (fg)') = \gcd(f, f') \gcd(g, g')$.

g) Let $\operatorname{char}(K) = 0$ and $f = c \prod_{i=1}^{s} p_i^{\alpha_i}$ be the factorization of f into distinct irreducible factors, where $c \in K \setminus \{0\}$. Show that $\gcd(f, f') = \prod_{i=1}^{s} p_i^{\alpha_i - 1}$ and deduce that $\operatorname{sqfree}(f)$ can be computed by using the formula

$$\operatorname{sqfree}(f) = f / \gcd(f, f')$$

h) Find an example which shows that g) is false if $\operatorname{char}(K) = p > 0$.

i) Now let K be a finite field of characteristic $p > 0$. In Proposition 3.7.12 we shall prove that $\operatorname{sqfree}(f)$ can be computed using the following algorithm.

   1) Compute $s_1 = \gcd(f, f')$. If $s_1 = 1$, then return f.
   2) Check whether we have $s_1' = 0$. In this case, use b) to conclude that $s_1 = g^p$ for some polynomial $g \in K[x]$. Compute g using $\texttt{PRoot}(\dots)$. Then replace f by $\frac{fg}{s_1} = \frac{f}{g^{p-1}}$, and continue with step 1).
   3) Compute $s_{i+1} = \gcd(s_i, s_i')$ for $i = 1, 2, \dots$ until $s_{i+1}' = 0$, i.e. until s_{i+1} is a pth power $s_{i+1} = g^p$ for some $g \in K[x]$. Then calculate g again, replace f by $\frac{fg}{s_1}$, and continue with step 1).

Write a CoCoA function $\texttt{SqFree}(\dots)$ which checks whether the base field is $\mathbb{Q}$ or $\mathbb{F}_p$ and computes the squarefree part of a given univariate polynomial.

Tutorial 6: Berlekamp's Algorithm

In the case of a finite field K, we shall explore a concrete algorithm which factors polynomials in $K[x]$. So, let p be a prime number, let e be a positive integer, let $q = p^e$, and let K be the field with q elements (see Tutorial 3). (If you are unfamiliar with finite fields, it is enough to concentrate on the case $q = p$, $K = \mathbb{Z}/(p)$.)

Our goal is to compute the factorization of a non-constant monic polynomial $f \in K[x]$ of degree $d = \deg(f)$.

a) Prove that the ring $R = K[x]/(f)$ is a d-dimensional K-vector space with basis $\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{d-1}\}$, where $\bar{x}$ is the residue class of x in R.

In what follows, let $Q = (q_{ij})$ be the $d \times d$-matrix over K whose i^{th} row consists of the coordinates of $\bar{x}^{q(i-1)}$ in the basis $\{1, \bar{x}, \dots, \bar{x}^{d-1}\}$ of R. Furthermore, we let $\bar{g} = \gamma_0 + \dots + \gamma_{d-1}\bar{x}^{d-1}$ with $\gamma_0, \dots, \gamma_{d-1} \in K$ be the representation of the residue class of a polynomial $g \in K[x]$ in this basis.

b) Show that $\bar{g}^q = (\gamma_0, \dots, \gamma_{d-1}) \cdot Q \cdot (1, \bar{x}, \dots, \bar{x}^{d-1})^{\text{tr}}$. Conclude that there is a 1-1 correspondence between elements $\bar{g} \in R$ such that $\bar{g}^q - \bar{g} = 0$ and vectors $(\gamma_0, \dots, \gamma_{d-1}) \in K^d$ such that $(\gamma_0, \dots, \gamma_{d-1}) \cdot (Q - I_d) = 0$, where I_d denotes the $d \times d$ identity matrix.

c) For any polynomial $g \in K[x]$ satisfying $\bar{g}^q - \bar{g} = 0$ in R, prove that we have $f = \prod_{\kappa \in K} \gcd(f, g - \kappa)$. (*Hint:* Find the factorization of $x^q - x$ and substitute g for x.)

d) Let $f = \prod_{i=1}^{r} p_i^{\alpha_i}$ be the factorization of f, where $\alpha_i > 0$ for $i = 1, \ldots, r$ and $p_1, \ldots, p_r$ are the different irreducible monic factors of f. Prove the following special case of the **Chinese Remainder Theorem**. The canonical map

$$\varepsilon : R \longrightarrow K[x]/(p_1^{\alpha_1}) \times \cdots \times K[x]/(p_r^{\alpha_r})$$

is an isomorphism of $K[x]$-algebras. (*Hint:* To show surjectivity, let $g_1, \ldots, g_r \in K[x]$, use $h_i = \prod_{j \neq i} p_j^{\alpha_j}$, get an equation $\sum_{i=1}^{r} a_i h_i = 1$, and consider $\varepsilon(\sum_{i=1}^{r} g_i a_i h_i + (f))$.)

Deduce that ε induces an isomorphism of K-vector spaces

$$\varphi : \{\bar{g} \in R \mid \bar{g}^q - \bar{g} = 0\} \longrightarrow K^r$$

e) Conclude from d) that the number of distinct irreducible factors of f is given by $r = \dim_K(\ker(Q - I_d))$. Write a CoCoA function `IsIrred(...)` which checks whether a given polynomial $f \in K[x]$ is irreducible. *Hint:* You may use the CoCoA function `Syz(...)` to compute the kernel of a linear map.

f) Consider the following sequence of instructions.

1) Compute the matrix Q and the number r defined above. Let $\{(v_{i1}, \ldots, v_{id}) \mid 1 \leq i \leq r\}$ be a K-basis of $\ker(Q - I_d)$ and $g_i = v_{i1} + v_{i2}x + \cdots + v_{id}x^{d-1} \in K[x]$ for $1 \leq i \leq r$. W.l.o.g. we can assume that $g_r = 1$ and $\deg(g_i) > 0$ for $1 \leq i < r$.

2) For all $\kappa \in K$, compute $\gcd(f, g_1 - \kappa)$ and obtain a representation $f = \prod_{\kappa \in K} \gcd(f, g_1 - \kappa)$. If this representation contains r different non-constant factors, return it as the result.

3) For $i = 1, 2, \ldots$, let $f = f_{i1} \cdots f_{i\mu_i}$ be the representation of f computed so far. For every $\kappa \in K$ and every $j \in \{1, \ldots, \mu_i\}$, compute $\gcd(f_{ij}, g_{i+1} - \kappa)$. Then check, if the representation

$$f = \prod_{j=1}^{\mu_i} \prod_{\kappa \in K} \gcd(f_{ij}, g_{i+1} - \kappa)$$

consists of r different non-constant factors. If not, increase i by one and repeat step 3), until it does. Then return this representation as the result.

Show that this is an algorithm which stops for some $i \leq r - 1$ and that it returns a representation of f as the product of powers of distinct irreducible monic polynomials. It is called **Berlekamp's Algorithm**. If we combine it with the algorithm for computing squarefree parts of polynomials in $K[x]$ described in Tutorial 5, we have a complete factorization algorithm for univariate polynomials over finite fields.

Hint: To show finiteness, use that the determinant of the matrix Φ of the map φ above is non-zero, and that the number of non-constant different factors in $f_{i1} \cdots f_{i\mu_i}$ is equal to the number of different entries in the ith column of Φ.

g) Implement Berlekamp's Algorithm for $K = \mathbb{Z}/(p)$. Then apply your function `Berlekamp(...)` and check it against the built-in routines of CoCoA in the following cases.

1) $f_1 = x^{100} - x^{200} \in \mathbb{Z}/(5)[x]$
2) $f_2 = 1 + x + x^2 + x^6 + x^7 + x^8 + x^{12} \in \mathbb{Z}/(2)[x]$
3) $f_3 = 1 - x^{100} \in \mathbb{Z}/(7)[x]$
4) $f_4 = 8 + 2x + 8x^2 + 10x^3 + 10x^4 + x^6 + x^8 \in \mathbb{Z}/(13)[x]$
5) $f_5 = 2 + x + x^2 + x^3 + x^4 + x^5 \in \mathbb{Z}/(31991)[x]$

1.3 Monomial Ideals and Monomial Modules

> *Mathematics is a game*
> *played according to certain simple rules*
> *with meaningless marks on paper.*
> (David Hilbert)

Let us start with a little game. Consider the monoid $\mathbb{T}^1 = \{1, x, x^2, x^3, \ldots\}$. Pick one element in $\mathbb{T}^1$, call it s_1, and delete it from $\mathbb{T}^1$. Then pick another element in $\mathbb{T}^1 \backslash \{s_1\}$, call it s_2, and delete it from $\mathbb{T}^1 \backslash \{s_1\}$. If s_2 is not divisible by s_1 you say that s_2 is a winner. Keep going on and construct a sequence $\{s_n\}$ of distinct elements of $\mathbb{T}^1$ and declare that s_n is a winner if it is not divisible by any of the preceding ones. It is immediately clear that, after the first choice has been made, only a finite number of potential winners are left. Therefore in your sequence from a certain point on all the elements are losers, i.e. multiples of some preceding element. In this case the explanation is easy, but a more important question arises: is a similar conclusion valid if you start with $\mathbb{T}^n$ instead?

One of the main purposes of this section is to answer that question, and the answer is Dickson's Lemma. Put in another way, we show that monomial ideals are finitely generated. The importance of this result will become more evident later, but of course it is already clear that statements about "finiteness" are crucial for actual computations. Towards the end of this section we also prove a powerful structure theorem for monomial modules.

Now we begin with the definition of two algebraic structures which help us translate our game into a solid mathematical result. We recall that a monoid is a set together with an associative operation on it such that there exists an identity. Since in all the cases considered in this book the operation will be commutative, we shall from now on use the term "monoid" to denote a commutative monoid.

Definition 1.3.1. Let $(\Gamma, \circ)$ be a monoid.
a) A non-empty subset $\Delta \subseteq \Gamma$ is called a **monoideal** (pronounced "mono-ideal") in Γ (or a **monoid ideal** in Γ) if we have $\Delta \circ \Gamma \subseteq \Delta$.
b) A subset B of a monoideal Δ in Γ is called a **system of generators of** Δ (or Δ is said to be **generated** by B) if Δ is the smallest monoideal in Γ containing B. In this case we have $\Delta = \{\beta \circ \gamma \mid \beta \in B, \gamma \in \Gamma\}$. If $B = \{\beta_1, \beta_2, \ldots\}$, we will also use the notation $\Delta = (\beta_1, \beta_2, \ldots)$.
c) A set Σ together with an operation $* : \Gamma \times \Sigma \to \Sigma$ given by $(\gamma, s) \mapsto \gamma * s$ is called a Γ-**monomodule** (or a **monoid module** over Γ) if for all $s \in \Sigma$ and all $\gamma_1, \gamma_2 \in \Gamma$ we have
  1) $1_\Gamma * s = s$,
  2) $(\gamma_1 \circ \gamma_2) * s = \gamma_1 * (\gamma_2 * s)$.
d) A non-empty subset $\Sigma' \subseteq \Sigma$ is called a Γ-**submonomodule** of Σ if $\Gamma * \Sigma' \subseteq \Sigma'$.

e) A subset B of a Γ-monomodule Σ is called a **system of generators of** Σ if $\Sigma = \{\gamma * s \mid \gamma \in \Gamma, s \in B\}$.

Later the symbols $\circ$ and $*$ will sometimes be omitted. Obviously, a monoideal in Γ is also a Γ-monomodule. In fact, it is a Γ-submonomodule of the Γ-monomodule Γ, just like for regular ideals and modules. The most important example of a monomodule for our purposes is the set of terms $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$ of a free module $R[x_1, \ldots, x_n]^r$ over some polynomial ring. It is a $\mathbb{T}^n$-monomodule generated by $\{e_1, \ldots, e_r\}$. Some monomodules require infinite systems of generators, as our next example shows.

Example 1.3.2. The set $\mathbb{Q}_{\geq 0}$ of non-negative rational numbers with the usual sum is a monoid. Then $\mathbb{Q}_{>0}$, the set of positive rational numbers, is a monoideal in $\mathbb{Q}_{\geq 0}$ which is generated by $\{\frac{1}{n} \mid n \geq 1\}$. It is easy to see that this monoideal is not finitely generated.

Now let $\mathbb{I} = \mathbb{R} \backslash \mathbb{Q}$ be the set of irrational numbers. Adding an element of $\mathbb{Q}_{\geq 0}$ to an element of $\mathbb{I}$ yields an element of $\mathbb{I}$. Since conditions 1) and 2) of Definition 1.3.1.c are satisfied, we have here an example of a $\mathbb{Q}_{\geq 0}$-monomodule. Again one can show that this monomodule is not finitely generated.

Definition 1.3.3. Let $(\Gamma, \circ)$ be a monoid and $(\Sigma, *)$ a Γ-monomodule.
 a) We say that the **cancellation law** holds in Γ, if $\gamma_1 \circ \gamma_3 = \gamma_2 \circ \gamma_3$ implies $\gamma_1 = \gamma_2$ for all $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$.
 b) We say that the **left-cancellation law** holds in Σ, if $\gamma * s_1 = \gamma * s_2$ implies $s_1 = s_2$ for all $\gamma \in \Gamma$, $s_1, s_2 \in \Sigma$.
 c) We say that the **right-cancellation law** holds in Σ, if $\gamma_1 * s = \gamma_2 * s$ implies $\gamma_1 = \gamma_2$ for all $\gamma_1, \gamma_2 \in \Gamma$, $s \in \Sigma$.

If we consider a monoid Γ as a Γ-monomodule in the obvious way, conditions b) and c) both agree with a) so that there is only one cancellation law in Γ. In Example 1.3.2, the cancellation law holds in $\mathbb{Q}_{\geq 0}$, and both the left-cancellation law and the right-cancellation law hold in the monomodule $\mathbb{I}$. Furthermore, for every $n \geq 1$, the cancellation law holds in the monoid of terms $\mathbb{T}^n$ introduced in Definition 1.1.10, and, for every $r \geq 1$, both the left-cancellation law and the right-cancellation law hold in the $\mathbb{T}^n$-monomodule $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$. The following concept provides an important finiteness condition for monoids.

Proposition 1.3.4. *For a monoid $(\Gamma, \circ)$ the following conditions are equivalent.*
 a) *Every monoideal in Γ is finitely generated.*
 b) *Every ascending chain $\Delta_1 \subseteq \Delta_2 \subseteq \cdots$ of monoideals in Γ is eventually stationary.*
 c) *Every non-empty set of monoideals in Γ has a maximal element with respect to inclusion.*

   If these conditions are satisfied, the monoid Γ is called **Noetherian**.

Proof. First we show $a) \Rightarrow b)$. Suppose we have a chain $\Delta_1 \subseteq \Delta_2 \subseteq \cdots$ of monoideals in Γ and a sequence $n_1 < n_2 < \cdots$ such that there exist elements $\gamma_i \in \Delta_{n_{i+1}} \setminus \Delta_{n_i}$ for all $i \geq 1$. Then we claim that the monoideal generated by $\{\gamma_1, \gamma_2, \ldots\}$ is not finitely generated. It is contained in the union $\cup_{i \geq 1} \Delta_i$, but not in one of the monoideals Δ_i. Now assume that it is generated by a finite set. Then such a finite set has to be contained in some Δ_i, a contradiction.

Now we prove $b) \Rightarrow c)$. Let S be a non-empty set of monoideals in Γ, and let $\Delta_1 \in S$. If Δ_1 is not maximal, there exists a monoideal $\Delta_2 \in S$ such that $\Delta_1 \subset \Delta_2$. Continuing in this way, we obtain a chain $\Delta_1 \subset \Delta_2 \subset \cdots$ which has to be finite by b). Then the last element of the chain is a maximal element of S.

To show the remaining implication $c) \Rightarrow a)$, we let $\Delta \subseteq \Gamma$ be a monoideal. The set of all monoideals in Γ which are generated by finite subsets of Δ contains a maximal element. By construction, this element has to be Δ itself. $\qquad\square$

Proposition 1.3.5. *For $n \geq 1$, the monoid $(\mathbb{N}^n, +)$ is Noetherian.*

Proof. We use induction on n. When $n = 1$, every monoideal is obviously of the form (a) with a fixed $a \in \mathbb{N}$. For $n > 1$, we let $\Delta_1 \subseteq \Delta_2 \subseteq \cdots$ be an ascending chain of monoideals in $\mathbb{N}^n$. Suppose there are indices $n_1 < n_2 < \cdots$ and elements $w_i \in \Delta_{n_{i+1}} \setminus \Delta_{n_i}$ for $i \geq 1$. Let $v_1 = w_{m_1} \in \{w_1, w_2, \ldots\}$ be a vector whose first component is minimal. Then we let $v_2 = w_{m_2} \in \{w_{m_1+1}, w_{m_1+2}, \ldots\}$ be a vector whose first component is minimal again, etc. In this way we construct a sequence $v_1, v_2, \ldots$ of vectors of $\mathbb{N}^n$ whose first components form a non-decreasing sequence.

For all $i \geq 1$, we let v_i' now be the vector in $\mathbb{N}^{n-1}$ which consists of the last $n-1$ components of v_i. By the induction hypothesis, the chain of monoideals $(v_1') \subseteq (v_1', v_2') \subseteq \cdots$ in $\mathbb{N}^{n-1}$ becomes eventually stationary. Then also the chain $(v_1) \subseteq (v_1, v_2) \subseteq \cdots$ of monoideals in $\mathbb{N}^n$ becomes eventually stationary, since the first components of $v_1, v_2, \ldots$ form an non-decreasing sequence. We arrive at a contradiction to the construction of $w_1, w_2, \ldots$, since we had $v_i = w_{m_i} \notin (w_1, \ldots, w_{m_i-1}) \supseteq (v_1, \ldots, v_{i-1})$ for all $i \geq 2$. $\qquad\square$

In the remaining part of this section we shall apply the above theory to the monoid of terms in a polynomial ring. The translation of the previous proposition provides us with an important finiteness condition for ideals in polynomial rings.

Corollary 1.3.6. (Dickson's Lemma)
Let $n \geq 1$, and let $t_1, t_2, \ldots$ be a sequence of terms in $\mathbb{T}^n$. Then there exists a number $N > 0$ such that for every $i > N$ the term t_i is a multiple of one of the terms $t_1, \ldots, t_N$, i.e. the monoideal $(t_1, t_2, \ldots) \subseteq \mathbb{T}^n$ is generated by $\{t_1, \ldots, t_N\}$.

In particular, for every ring R, the ideal $(t_1, t_2, \ldots) \subseteq R[x_1, \ldots, x_n]$ is finitely generated.

Proof. The map $\log : \mathbb{T}^n \to \mathbb{N}^n$ given by $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mapsto (\alpha_1, \ldots, \alpha_n)$ is clearly an isomorphism of monoids. The monoideal $(\log(t_1), \log(t_2), \ldots) \subseteq \mathbb{N}^n$ is finitely generated by the previous proposition. Thus there exists a number $N > 0$ such that this monoideal is generated by $\{\log(t_1), \ldots, \log(t_N)\}$. Consequently, the monoideal $(t_1, t_2, \ldots) \subseteq \mathbb{T}^n$ is generated by $\{t_1, \ldots, t_N\}$. $\quad\square$

As we shall see, ideals and modules generated by terms have many special properties. We begin our studies by giving them a special name. Let R be a ring, let $n \geq 1$, let $P = R[x_1, \ldots, x_n]$ be a polynomial ring, and let $r \geq 1$.

Definition 1.3.7. A P-submodule $M \subseteq P^r$ is called a **monomial module**, if it has a system of generators consisting of elements of $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. A monomial submodule of P is also called a **monomial ideal** of P.

Monomial ideals can be readily visualized, especially when there are just two or three indeterminates.

Remark 1.3.8. For monomial ideals $I \subseteq R[x_1, x_2]$, we can illustrate the set of terms in I as follows. A term $x_1^i x_2^j \in \mathbb{T}^2$ is represented by the point $(i, j) \in \mathbb{N}^2$. Then, for each term $x_1^i x_2^j \in I$, the quadrant $\{x_1^k x_2^l \mid k \geq i, l \geq j\}$ is contained in I. For instance, when $I = (x_1^5, x_1^3 x_2, x_1 x_2^2, x_2^4)$ we obtain the following picture.
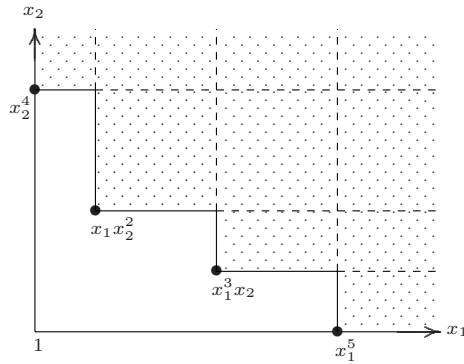
Dickson's Lemma can be generalized to monomial modules as follows.

Theorem 1.3.9. (Structure Theorem for Monomial Modules)
Let $M \subseteq P^r$ be a monomial module.

a) *The module M is finitely generated, i.e. there are finitely many terms $t_1, \ldots, t_s \in \mathbb{T}^n$ and numbers $\gamma_1, \ldots, \gamma_s \in \{1, \ldots, r\}$ such that we have $M = \langle t_1 e_{\gamma_1}, \ldots, t_s e_{\gamma_s} \rangle$.*

b) *There are monomial ideals $I_1, \ldots, I_r \subseteq P$ such that M is of the form $M \cong \oplus_{i=1}^r I_i e_i$.*

Proof. Let $B \subseteq \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ be a system of generators of M. For every number $i \in \{1, \ldots, r\}$ we define the set $B_i = \{t \in \mathbb{T}^n \mid te_i \in B\} \subseteq \mathbb{T}^n$. By Dickson's Lemma, the monomial ideals $I_i = (B_i)$ have finite systems of generators $G_i \subseteq B_i$. Obviously the P-module M is then generated by $G_1 e_1 \cup \cdots \cup G_r e_r \subseteq \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. This proves a) and the claim $M = \sum_{i=1}^r I_i e_i$ in b). The fact that this sum is direct follows from $M \subseteq \oplus_{i=1}^r P e_i$. $\qquad \square$

The first part of this theorem says in particular that the analogue of Proposition 1.3.4.a holds for monomial modules. Let us note that this implies that also the analogue of Proposition 1.3.4.b is true.

Corollary 1.3.10. *Every ascending chain of monomial submodules of P^r is eventually stationary.*

Proof. Suppose there exists a strictly ascending chain $M_1 \subset M_2 \subset \cdots$ of monomial submodules of P^r. Since each module is generated by terms, we can then find a term $t_i \in M_i \backslash M_{i-1}$ for every $i \geq 2$. Then we have $\langle t_2, \ldots, t_i \rangle \subseteq M_i$, and therefore $t_{i+1} \notin \langle t_2, \ldots, t_i \rangle$. Thus the monomial submodule $\langle t_2, t_3, \ldots \rangle$ of P^r is not finitely generated, in contradiction to the theorem. $\qquad \square$

Finally, we address the question of uniqueness for systems of generators of monomial modules.

Proposition 1.3.11. *Let $M \subseteq P^r$ be a monomial submodule.*

a) *For every system of generators $G = \{t_1, \ldots, t_s\}$ of M consisting of terms, and for every term $t \in M$, there exists a term $t_i \in G$ such that t is a multiple of t_i.*

b) *In the set of all systems of generators of M which consist entirely of terms there is a unique minimal element with respect to inclusion. We call it the* **minimal monomial system of generators** *of M.*

Proof. The first claim follows from the fact that if we write $t = \sum_{i=1}^s f_i t_i$ with polynomials $f_1, \ldots, f_s \in P$, then the term t must show up in the support of one of the elements $f_1 t_1, \ldots, f_s t_s$.

To show b), we prove existence first. By Theorem 1.3.9.a, there exists a finite system of generators of M consisting of terms. If we delete in this set all terms which are proper multiples of another element of that set, and if we also remove all repetitions of an element, we obtain a system of generators of M which cannot be shortened anymore.

To prove uniqueness, we suppose that there are two different minimal monomial systems of generators G_1 and G_2 of M. By symmetry, we may assume that there is a term $t \in G_1 \backslash G_2$. From a) we conclude that t is a multiple of an element $t' \in G_2$. Using a) again, we see that t', and therefore t, is a multiple of one of the elements of G_1. Since G_1 is minimal, that element is necessarily t itself, i.e. t and t' are multiples of each other. Thus $t = t' \in G_2$, a contradiction. $\qquad \square$

Exercise 1. Let Γ be a commutative group. Show that in it there is only one monoideal, namely Γ itself.

Exercise 2. Equip the set $\Gamma = \{0, \infty\}$ with the "natural" addition and show that $(\Gamma, +)$ is a commutative monoid in which the cancellation law does not hold.

Exercise 3. We consider the additive monoid $\mathbb{Q}_{\geq 0}$ (see Example 1.3.2). We let a be a non-negative real number and $\mathbb{Q}_{\geq a} = \{b \in \mathbb{Q}_{\geq 0} \mid b \geq a\}$.

a) Prove that if $a \in \mathbb{Q}$, then $\mathbb{Q}_{\geq a}$ is a principal monoideal, i.e. a monoideal generated by a single element.

b) Prove that if $a \notin \mathbb{Q}$, then $\mathbb{Q}_{\geq a}$ is a monoideal which is not finitely generated.

c) If $a \notin \mathbb{Q}$, find an infinite increasing sequence of monoideals in $\mathbb{Q}_{>0}$ whose union is $\mathbb{Q}_{\geq a}$.

d) Prove that the monomodule $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ is not finitely generated.

Exercise 4. Let us use the notation of Example 1.3.2 again.

a) Show that $\mathbb{Q}_{>0}$ with the usual multiplication is a monoid.

b) Show that this monoid has no non-trivial monoideal.

c) Show that $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ is a $\mathbb{Q}_{>0}$-monomodule.

Exercise 5. Let $(\Gamma, \circ)$ be a Noetherian monoid in which the cancellation law holds. Assuming that the only unit is 1_Γ, prove that every monoideal Δ has a unique minimal (i.e. shortest) set of generators.

Exercise 6. Let $(\Gamma, \circ)$ be a monoid, Δ a finitely generated monoideal in Γ, and let B be a system of generators of Δ. Prove that Δ can be generated by a finite subset of B.

Exercise 7. Let $n \geq 1$ and $r \geq 1$. Show that the set of terms $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ is a monomodule over $\mathbb{T}^n$.

Exercise 8. Let $B \subset \mathbb{T}^n$ be such that no element in B is divisible by another element in B. Prove that B is finite.

Exercise 9. Let $(\Gamma, \circ)$ be a monoid, and let Σ be a Γ-monomodule. We say that Σ is a **Noetherian** Γ-monomodule if every ascending chain of Γ-submonomodules $\Sigma_1 \subseteq \Sigma_2 \subseteq \cdots$ of Σ is eventually stationary.

a) For submonomodules of Σ, formulate and prove an analogue of Proposition 1.3.4.

b) Let Γ be a Noetherian monoid, and let Σ be a finitely generated Γ-monomodule. Then show that Σ is Noetherian.

c) Conclude that the $\mathbb{T}^n$-monomodule $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ is Noetherian.

Tutorial 7: Cogenerators

Let $(\Gamma, \circ)$ be a monoid, let Δ be a monoideal in Γ, let $\Lambda = \Gamma \backslash \Delta$ be the complement of Δ in Γ, and let $C \subseteq \Lambda$. We say that C **cogenerates** Δ if $\Lambda = \{\gamma \in \Gamma \mid \gamma \circ \gamma' \in C \text{ for some } \gamma' \in \Gamma\}$.
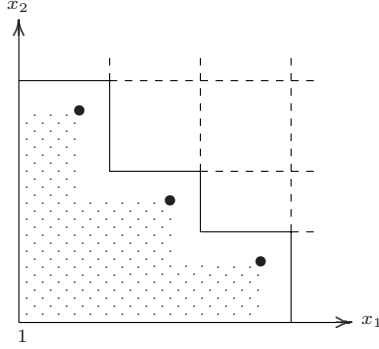
a) Show that the complement Λ of a monoideal in a monoid is characterized by the following property: if $\gamma \in \Lambda$ and $\gamma' \mid \gamma$, then $\gamma' \in \Lambda$.
b) Let $\Delta(I)$ be the monoideal in $\mathbb{T}^2$ consisting of the terms in the ideal $I = (x_1^5, x_1^3 x_2, x_1 x_2^2, x_2^4)$ introduced in Remark 1.3.8. Show that $\Delta(I)$ is finitely cogenerated and find a minimal set of cogenerators.
c) Now let $J = (x_1^5, x_1^3 x_2, x_1 x_2^2)$, and let $\Delta(J)$ be the associated monoideal in $\mathbb{T}^2$. Find a set of cogenerators and show that J is not finitely cogenerated.
d) Characterize the finitely cogenerated monoideals in $\mathbb{T}^2$. Show that they have a unique minimal set of cogenerators.
e) Let $m(\Delta)$ be the cardinality of a minimal set of generators and $c(\Delta)$ the cardinality of a minimal set of cogenerators of a finitely cogenerated monoideal $\Delta \subseteq \mathbb{T}^2$. Prove that $c(\Delta) = m(\Delta) - 1$.
f) Characterize monoideals in $\mathbb{T}^2$ cogenerated by a single element. Given such a monoideal $\Delta \subseteq \mathbb{T}^2$ and its cogenerator $\lambda \in \Lambda$, prove that we have $\Delta = \{t \in \mathbb{T}^2 \mid x_1 \cdot t \in \Delta, x_2 \cdot t \in \Delta\} \backslash \{\lambda\}$.
g) Write a CoCoA function `MinCogens(...)` which, given a finite list of terms, checks if the monoideal generated by them is finitely cogenerated and in that case computes the minimal set of cogenerators.

Tutorial 8: Basic Operations with Monomial Ideals and Modules

Let K be a field, let $n \geq 1$, let $P = K[x_1, \ldots, x_n]$, and let $r \geq 1$.

a) Show that a P-submodule $M \subseteq P^r$ is a monomial module if and only if for every $m \in M$ and every $t \in \mathrm{Supp}(m)$ we have $t \in M$.

b) Write a CoCoA function `Is_Monomial(...)` which, for a list of vectors generating a P-submodule $M \subseteq P^r$, checks if M is monomial and which returns `TRUE` or `FALSE`. (*Hint:* You may use the CoCoA operator `IsIn`.)

c) Implement a CoCoA function `MonComps(...)` which, for a list of terms generating a monomial P-submodule $M \subseteq P^r$, computes the list of monomial ideals $I_1, \ldots, I_r$ such that $M = I_1 e_1 \oplus \cdots \oplus I_r e_r$ as in Proposition 1.3.9.b.

d) Write a CoCoA program `MinMonomials(...)` which takes a list of terms generating a monomial P-submodule of P^r and computes the minimal monomial system of generators of that module. (*Hint:* Do the case of a monomial ideal first. Then apply the preceding program.)

In the sequel, we let $I \subseteq P$ be a monomial ideal and $M \subseteq P^r$ as well as $N \subseteq P^r$ monomial submodules, all given by lists of terms which generate them.

e) Prove that $M + N$ and $I \cdot M$ are monomial submodules of P^r. Write CoCoA functions `MonSum(...)` and `MonProd(...)` which compute those modules.

f) Show that $M \cap N$ is a monomial submodule of P^r by giving an explicit monomial system of generators. Then implement a CoCoA function `MonIntersection(...)` which computes this intersection. (*Hint:* Do the case $r = 1$ first. Then try to generalize your result.)

g) Prove that $M : N = \{f \in P \mid f \cdot N \subseteq M\}$ is a monomial ideal by giving an explicit monomial system of generators. Write a CoCoA function `MonColon(...)` which computes this **colon ideal**.

h) Let $1 \leq m < n$. Show that $M \cap K[x_1, \ldots, x_m]^r$ is a monomial $K[x_1, \ldots, x_m]$-submodule of $K[x_1, \ldots, x_m]^r$ by exhibiting an explicit monomial system of generators. Write a CoCoA function `MonElim(...)` which computes this **elimination module**.

i) Show that $\sqrt{I} = \{f \in P \mid f^i \in I \text{ for some } i \in \mathbb{N}\}$ is the monomial ideal generated by the squarefree parts of the generators of I. Write a CoCoA function `MonRadical(...)` which computes this **radical ideal**.

Hint: The hint given here anticipates some themes explained later, starting with the next section. Given two terms t_1, t_2, we let $t_1 > t_2$ if the first non-zero component of $\log(t_1) - \log(t_2)$ is positive. Show that, for $f \in P \setminus \{0\}$ and $i \in \mathbb{N}$, the largest term in $\mathrm{Supp}(f^i)$ is the ith power of the largest term in $\mathrm{Supp}(f)$. Now use a) and induction on the size of $\mathrm{Supp}(f)$ to prove that $f^i \in I$ implies $\mathrm{sqfree}(t) \in \sqrt{I}$ for all $t \in \mathrm{Supp}(f)$.

1.4 Term Orderings

Let us for a moment go back to Section 1.1 where we discussed the notion of polynomial rings in one and several indeterminates. A univariate polynomial with coefficients in a ring R is an expression of the type $f(x) = \sum r_i x^i$. One question is: in how many different ways can we write $f(x)$? We might agree that the coefficients should be written before the corresponding power product and also decide to be "nice" and avoid the $+$ sign before the first coefficient, but still we have to face the commutative property of the sum, which implies that for instance $1 + 2x - 3x^2$ can also be written as $1 - 3x^2 + 2x$. This may not be a relevant question for "pure" mathematicians, but it is fundamental if you wish to implement polynomials and use them in a computer program.

Clearly, what really matters is the order in which the terms 1, x, x^2, i.e. the elements in $\mathrm{Supp}(f)$, are written. Using the recursive definition of multivariate polynomials, we see that the way of writing them depends on how we write the univariate ones. And to do it, we see the necessity of knowing how to order $\mathbb{T}^1$. Look again at $f(x) = 1 + 2x - 3x^2$, whose support is $\{1, x, x^2\}$. There are six ways of ordering three elements, which then yield six representations of f, namely $1 + 2x - 3x^2$, $1 - 3x^2 + 2x$, $2x + 1 - 3x^2$, $2x - 3x^2 + 1$, $-3x^2 + 1 + 2x$, and $-3x^2 + 2x + 1$. However, we believe that you are going to "keep" only $1 + 2x - 3x^2$ and $-3x^2 + 2x + 1$.

Apart from aesthetic reasons, there is a technical one which validates this choice. Namely, suppose that you choose the rule "order by increasing degree", which yields the representation $1+2x-3x^2$, and suppose you want to multiply $f(x)$ by x^3, say. After termwise multiplication, the rule continues to hold and you do not have to reorder the result. This leads to an extra property that your ordering of terms should have, the property of being compatible with multiplication. Put in a more technical setting, you should require that the total ordering on $\mathbb{T}^1$ makes it into an *ordered monoid*. Then you see that the specification $1 < x$ implies $x < x^2 < x^3$ and so on, and finally you see that only two possible orderings are left, the one described by $1 < x$ and the one described by $x < 1$. This is the end of the story for univariate polynomials and also for multivariate ones, if a recursive representation is used.

But we have already seen that other properties of polynomials allow us to get rid of the parentheses and express them as sums of coefficients times elements in $\mathbb{T}^n$. So the question now is how to order $\mathbb{T}^n$. For the same reasons as before we need compatibility with its monoid structure. Let $f(x_1, x_2, x_3) = x_1 x_3 + x_2^2$; should we write it as $x_1 x_3 + x_2^2$ or rather as $x_2^2 + x_1 x_3$? There is no obvious answer to this question, and the purpose of this section is to shed some light on it.

In particular, we shall study total orderings on $\mathbb{T}^n$ and on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. If they have a certain additional property, they are called term orderings. This "fundamental property of module term orderings" is the key to showing finiteness for most algorithms we shall encounter later.

An attempt to classify all possible term orderings on $\mathbb{T}^n$, at least in some easy cases, is made in Tutorial 10. Although we avoid treating the general classification of term orderings, we do show that some orderings can be defined by matrices via scalar products (see Proposition 1.4.12), and that all the most important monoid orderings are of that type.

In the following, let $(\Gamma, \circ)$ be a monoid. Recall that for us this always means that Γ is commutative.

Definition 1.4.1. A **relation** σ on Γ is a subset of $\Gamma \times \Gamma$. If a pair (γ_1, γ_2) is in that subset, we shall write $\gamma_1 \geq_\sigma \gamma_2$. A relation σ on Γ is called **complete** if any two elements $\gamma_1, \gamma_2 \in \Gamma$ are comparable, i.e. if we have $\gamma_1 \geq_\sigma \gamma_2$ or $\gamma_2 \geq_\sigma \gamma_1$.

A complete relation σ on Γ is called a **monoid ordering** if the following conditions are satisfied for all $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$.

a) $\gamma_1 \geq_\sigma \gamma_1$ (reflexivity)
b) $\gamma_1 \geq_\sigma \gamma_2$ and $\gamma_2 \geq_\sigma \gamma_1$ imply $\gamma_1 = \gamma_2$ (antisymmetry)
c) $\gamma_1 \geq_\sigma \gamma_2$ and $\gamma_2 \geq_\sigma \gamma_3$ imply $\gamma_1 \geq_\sigma \gamma_3$ (transitivity)
d) $\gamma_1 \geq_\sigma \gamma_2$ implies $\gamma_1 \circ \gamma_3 \geq_\sigma \gamma_2 \circ \gamma_3$

If, in addition, we have

e) $\gamma \geq_\sigma 1_\Gamma$ for all $\gamma \in \Gamma$

then σ is called a **term ordering** on Γ.

If σ is a relation on Γ, and if $\gamma_1, \gamma_2 \in \Gamma$ are such that $\gamma_1 \geq_\sigma \gamma_2$, we also write $\gamma_2 \leq_\sigma \gamma_1$. Furthermore, if additionally $\gamma_1 \neq \gamma_2$, we write $\gamma_1 >_\sigma \gamma_2$ or $\gamma_2 <_\sigma \gamma_1$. If the cancellation law holds in Γ, condition 1.4.1.d can be reversed as follows.

Remark 1.4.2. Let σ be a monoid ordering on Γ.

a) Suppose that the cancellation law holds in Γ, and let $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$. Then an inequality $\gamma_1 \circ \gamma_3 \geq_\sigma \gamma_2 \circ \gamma_3$ implies $\gamma_1 \geq_\sigma \gamma_2$. This follows from the observation that $\gamma_2 >_\sigma \gamma_1$ implies $\gamma_2 \circ \gamma_3 \geq_\sigma \gamma_1 \circ \gamma_3$ by Definition 1.4.1.d, and equality is excluded by the cancellation law.
b) If $\Gamma \neq \{1_\Gamma\}$ and the cancellation law holds in Γ, then Γ is infinite. Namely, let $\gamma \neq 1_\Gamma$ be an element of Γ. Now let us consider the set $S = \{\gamma^i \mid i \in \mathbb{N}\}$. We have either $1_\Gamma >_\sigma \gamma$ or $\gamma >_\sigma 1_\Gamma$. In the first case $1_\Gamma >_\sigma \gamma >_\sigma \gamma^2 >_\sigma \cdots$ shows that S is infinite. In the second case we argue analogously.
c) By induction we can show that, for any $\gamma \in \Gamma$ and any $n > 0$, the condition $\gamma \geq_\sigma 1_\Gamma$ is equivalent to $\gamma^n \geq_\sigma 1_\Gamma$.

Under the isomorphism of monoids $\log : \mathbb{T}^n \to \mathbb{N}^n$, monoid orderings (resp. term orderings) on $\mathbb{T}^n$ correspond 1-1 to monoid orderings (resp. term orderings) on $\mathbb{N}^n$. Now we introduce some of the most important term orderings on $\mathbb{T}^n$.

Definition 1.4.3. For $t_1, t_2 \in \mathbb{T}^n$ we say $t_1 \geq_{\mathtt{Lex}} t_2$ if and only if the first non-zero component of $\log(t_1) - \log(t_2)$ is positive or $t_1 = t_2$. It is easy to check that this defines a term ordering on $\mathbb{T}^n$ — it is called the **lexicographic term ordering** and is denoted by $\mathtt{Lex}$.

Example 1.4.4. Using $\mathtt{Lex}$, the indeterminates are ordered decreasingly, i.e. by $x_1 >_{\mathtt{Lex}} x_2 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} x_n$. For instance, when $n = 3$, we have $x_1 x_2^2 >_{\mathtt{Lex}} x_2^3 x_3^4$, since $(1, 2, 0) - (0, 3, 4) = (1, -1, -4)$ has a positive first component. Similarly, we have $x_1^3 x_2^2 x_3^4 >_{\mathtt{Lex}} x_1^3 x_2^2 x_3$, since the first non-zero component of $(3, 2, 4) - (3, 2, 1) = (0, 0, 3)$ is positive. Also $x_1 x_3 >_{\mathtt{Lex}} x_2^2$, and we see how to use $\mathtt{Lex}$ to order the polynomial mentioned at the beginning of the section.

For $n = 26$, if one replaces x_{26} by A, x_{25} by B, etc., and one decides to write "smallest first", then the lexicographic ordering on the terms becomes similar to the usual ordering on words in a dictionary. We say similar and not equal because there is a fundamental difference between our words and the words in a dictionary. Our words (or terms) are commutative, so in our lexicon the two words *ape* and *pea* are the same. Although this book is entirely about commutative things, we must admit that non-commutative dictionaries have certain advantages.

Definition 1.4.5. For two terms $t_1, t_2 \in \mathbb{T}^n$ we say $t_1 \geq_{\mathtt{DegLex}} t_2$ if we have $\deg(t_1) > \deg(t_2)$, or if we have $\deg(t_1) = \deg(t_2)$ and $t_1 \geq_{\mathtt{Lex}} t_2$. It is easy to check that this, too, defines a term ordering on $\mathbb{T}^n$ — it is called the **degree-lexicographic term ordering** and is denoted by $\mathtt{DegLex}$.

Example 1.4.6. Using $\mathtt{DegLex}$, we see that $x_1 >_{\mathtt{DegLex}} \cdots >_{\mathtt{DegLex}} x_n$ holds again. For instance, when $n = 3$, we have $x_1 x_2^2 x_3^3 >_{\mathtt{DegLex}} x_1^2 x_2^2$, since $\deg(x_1 x_2^2 x_3^3) = 6 > 4 = \deg(x_1^2 x_2^2)$, and we have $x_1^2 x_2^2 x_3^2 >_{\mathtt{DegLex}} x_1 x_2^2 x_3^3$, since $\deg(x_1^2 x_2^2 x_3^2) = 6 = \deg(x_1 x_2^2 x_3^3)$ and $(2, 2, 2) - (1, 2, 3) = (1, 0, -1)$ has a positive first component.

Definition 1.4.7. For $t_1, t_2 \in \mathbb{T}^n$ we say $t_1 \geq_{\mathtt{DegRevLex}} t_2$ if we have $\deg(t_1) > \deg(t_2)$, or if we have $\deg(t_1) = \deg(t_2)$ and the last non-zero component of $\log(t_1) - \log(t_2)$ is negative, or if $t_1 = t_2$. It is easy to check that this defines a term ordering on $\mathbb{T}^n$ — it is called the **degree-reverse-lexicographic term ordering** and is denoted by $\mathtt{DegRevLex}$.

Example 1.4.8. Again, using $\mathtt{DegRevLex}$, the indeterminates are ordered by $x_1 >_{\mathtt{DegRevLex}} \cdots >_{\mathtt{DegRevLex}} x_n$. For instance, when $n = 3$, we have $x_1^4 x_2^7 x_3 >_{\mathtt{DegRevLex}} x_1^4 x_2^2 x_3^3$, since $\deg(x_1^4 x_2^7 x_3) = 12 > 9 = \deg(x_1^4 x_2^2 x_3^3)$, and we have $x_1 x_2^5 x_3^2 >_{\mathtt{DegRevLex}} x_1^4 x_2 x_3^3$, since both terms have degree 8 and

$(1, 5, 2) - (4, 1, 3) = (-3, 4, -1)$ has a negative last component. Similarly, we have $x_1^3 x_2^3 x_3^2 <_{\texttt{DegRevLex}} x_1^4 x_2^2 x_3^2$, since both terms have degree 8 and the last non-zero component of $(3, 3, 2) - (4, 2, 2) = (-1, 1, 0)$ is positive.

If we drop the first condition in the definition of $\texttt{DegRevLex}$, i.e. if we let $t_1 \geq_{\texttt{RevLex}} t_2$ if the last non-zero component of $\log(t_1) - \log(t_2)$ is negative or if $t_1 = t_2$, we obtain a monoid ordering on $\mathbb{T}^n$, called the **reverse-lexicographic ordering**, which is *not* a term ordering (see Exercise 3).

Definition 1.4.9. A monoid ordering σ on $\mathbb{T}^n$ is called **degree compatible** if $t_1 \geq_\sigma t_2$ for $t_1, t_2 \in \mathbb{T}^n$ implies $\deg(t_1) \geq \deg(t_2)$.

For instance, $\texttt{DegLex}$ and $\texttt{DegRevLex}$ are degree compatible term orderings.

Definition 1.4.10. Let $1 \leq j < n$, let $L = \{x_1, \ldots, x_j\}$, and let $t_1 = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $t_2 = x_1^{\beta_1} \cdots x_n^{\beta_n}$ be two terms in $\mathbb{T}^n$. We say $t_1 \geq_{\texttt{Elim}(L)} t_2$ if we have $\alpha_1 + \cdots + \alpha_j > \beta_1 + \cdots + \beta_j$, or if $\alpha_1 + \cdots + \alpha_j = \beta_1 + \cdots + \beta_j$ and $t_1 \geq_{\texttt{DegRevLex}} t_2$. It is easy to check that this defines a term ordering on $\mathbb{T}^n$ — it is called an **elimination ordering** for L and is denoted by $\texttt{Elim}(L)$.

The orderings $\texttt{Elim}(L)$ are members of a larger class of elimination orderings described in Section 3.4. Again the indeterminates are ordered by $x_1 >_{\texttt{Elim}(L)} \cdots >_{\texttt{Elim}(L)} x_n$.

Looking at these examples, we notice that they share a common property: the comparison of two terms is achieved by comparing their logarithms. Indeed, since the map $\log : \mathbb{T}^n \to \mathbb{N}^n$ is an isomorphism of monoids, one can use terms and their logarithms interchangeably. Thus in the above examples the comparison of terms is based on the comparison of the values of some linear functions on their logarithms.

For instance, if $t_1 = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $t_2 = x_1^{\beta_1} \cdots x_n^{\beta_n}$ and $(\gamma_1, \ldots, \gamma_n) = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$, then Definition 1.4.7 implies that $t_1 >_{\texttt{DegRevLex}} t_2$ if and only if the first non-zero component of $(\gamma_1 + \ldots + \gamma_n, -\gamma_n, \ldots, -\gamma_2)$ is positive. We see that the components of this vector are linear functions in the coordinates of $\log(t_1) - \log(t_2)$. This leads us to introduce the following construction.

Definition 1.4.11. Let $v_1, \ldots, v_n \in \mathbb{Z}^n$ be linearly independent vectors, and let V be the non-singular matrix whose i^{th} row is v_i for $i = 1, \ldots, n$. For $t_1, t_2 \in \mathbb{T}^n$, we say $t_1 \geq_{\texttt{Ord}(V)} t_2$ if $t_1 = t_2$ or if the first non-zero coordinate of the vector $V \cdot (\log(t_1) - \log(t_2))$ is positive, where $\cdot$ denotes the usual matrix-by-vector product and $(\log(t_1) - \log(t_2))$ has to be considered as a column vector. It is easy to check that this defines a monoid ordering $\texttt{Ord}(V)$ on $\mathbb{T}^n$. We call it the **ordering represented by** V.

Proposition 1.4.12. *Let V be the matrix whose rows are linearly indepen-dent vectors $v_1, \ldots, v_n \in \mathbb{Z}^n$. Then $\mathtt{Ord}(V)$ is a term ordering if and only if the first non-zero element in each column of V is positive.*

Proof. It is clear that a monoid ordering σ on $\mathbb{T}^n$ is a term ordering if and only if $x_i >_\sigma 1$ for $i = 1, \ldots, n$. Let a_i be the first non-zero element of the ith column of V. Then $V \cdot (\log(x_i) - \log(1)) = (0, \ldots, 0, a_i, \ldots)^{\text{tr}}$ shows that $x_i >_{\mathtt{Ord}(V)} 1$ is equivalent to $a_i > 0$. $\square$

For example, it is easy to see that $\mathtt{Lex}$ is the ordering represented by the identity matrix, and from the above description of $\mathtt{DegRevLex}$ it follows that it is represented by the matrix

$$V = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 0 & 0 & \ldots & 0 & -1 \\ 0 & 0 & \ldots & -1 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & -1 & 0 & \ldots & 0 \end{pmatrix}$$

Also for the other monoid orderings introduced above it is possible to see that they are represented by some matrix (see Exercise 6). There is a complete classification of monoid orderings on $\mathbb{T}^n$. It says that they essentially are all of type $\mathtt{Ord}(V)$, where V is a matrix with entries in $\mathbb{R}$ (see Exercise 7). For computational purposes, monoid orderings represented by integral matrices as above are good enough.

Our next two propositions deal with the question how term orderings behave under restrictions and extensions of the monoids on which they are defined.

Proposition 1.4.13. *Let σ be a monoid ordering on $\mathbb{T}^n$, and let $\mathbb{T}_i^{n-1}$ be the monoid of terms in the indeterminates $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$.*

a) *The restriction σ_i of σ to $\mathbb{T}_i^{n-1}$ is a monoid ordering.*
b) *If σ is a term ordering then also σ_i is a term ordering.*
c) *Suppose that σ is represented by a matrix V. Then σ_i is represented by the matrix V_i which is obtained from V by first deleting the ith column and then the first row which is linearly dependent on those above it.*

Proof. The first assertion is clear since $\mathbb{T}_i^{n-1}$ can be viewed as a submonoid of $\mathbb{T}^n$. The second one follows immediately from the definition of a term ordering. To prove c), we observe that if we disregard the ith indeterminate, we must delete the ith column from V. Then we are left with a matrix of shape $n \times (n-1)$ and rank $n-1$. We delete the first row which depends on those above it, because if for a vector all the previous scalar products vanish, then also the scalar product with the dependent row vanishes. Thus we get a matrix V_i of shape $(n-1) \times (n-1)$ and rank $n-1$. It represents σ_i, because for all $t_1, t_2 \in \mathbb{T}_i^{n-1}$ the vector $V_i \cdot (\log(t_1) - \log(t_2))$ agrees with $V \cdot (\log(t_1) - \log(t_2))$, except that we have to regard t_1 and t_2 as elements of $\mathbb{T}^n$ and to remove the entry corresponding to the deleted row. $\square$

Proposition 1.4.14. *Every monoid ordering σ on $\mathbb{N}^n$ has a unique extension to a monoid ordering σ' on $\mathbb{Z}^n$.*

Proof. For $v \in \mathbb{Z}^n$, there exist vectors $v_1, v_2 \in \mathbb{N}^n$ such that $v = v_1 - v_2$. We say $v \leq_{\sigma'} 0$ if and only if $v_1 \leq_\sigma v_2$. To see that this is well-defined, we take two representations $v = v_1 - v_2 = v_1' - v_2'$ with $v_1, v_2, v_1', v_2' \in \mathbb{N}^n$ and note that $v_1 \leq_\sigma v_2$ is equivalent to $v_1 + v_2' \leq_\sigma v_2 + v_2'$ by Remark 1.4.2.a. This in turn is equivalent to $v_1' + v_2 \leq_\sigma v_2 + v_2'$, and therefore to $v_1' \leq_\sigma v_2'$. If we now define $v \leq_{\sigma'} w \iff v - w \leq_{\sigma'} 0$ for $v, w \in \mathbb{Z}^n$, it is easy to check that Axioms a) – d) of Definition 1.4.1 are satisfied.

The uniqueness of σ' follows from the observation that, for $v, v' \in \mathbb{Z}^n$ such that $v = v_1 - v_2$ and $v' = v_1' - v_2'$ with $v_1, v_2, v_1', v_2' \in \mathbb{N}^n$, the condition $v \leq_{\sigma'} v'$ is equivalent to $v_1 + v_2' \leq_\sigma v_1' + v_2$.   □

In view of this proposition, and by extending $\mathtt{Lex}$ to $\mathbb{Z}^n$, we can rephrase Definition 1.4.11 as follows: $t_1 \geq_{\mathtt{Ord}(V)} t_2 \iff V \cdot (\log(t_1) - \log(t_2)) \geq_{\mathtt{Lex}} 0$ for $t_1, t_2 \in \mathbb{T}^n$.

The proposition also implies that studying monoid orderings on $\mathbb{T}^n$ is equivalent to studying monoid orderings on $\mathbb{Z}^n$. In particular, we shall use the same symbol for a monoid ordering on $\mathbb{T}^n$, its translation to $\mathbb{N}^n$, and its unique extension to $\mathbb{Z}^n$. In particular, we may apply this notational convention and say that for a monoid ordering σ on $\mathbb{T}^n$ and $t_1, t_1 \in \mathbb{T}^n$ we have $t_1 \geq_\sigma t_2 \iff \log(t_1) - \log(t_2) \geq_\sigma 0$.

The final part of this section treats the extension of the theory of monoid orderings to orderings on monomial modules. More precisely, for $n, r \geq 1$, we want to define suitable orderings on the set of terms $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ introduced in Definition 1.1.10.

Definition 1.4.15. Let $(\Gamma, \circ)$ be a monoid and $(\Sigma, *)$ a Γ-monomodule. A complete relation σ on Σ is called a **module ordering** if for all $s_1, s_2, s_3 \in \Sigma$ and all $\gamma \in \Gamma$ we have

a) $s_1 \geq_\sigma s_1$ (reflexivity)
b) $s_1 \geq_\sigma s_2$ and $s_2 \geq_\sigma s_1$ imply $s_1 = s_2$ (antisymmetry)
c) $s_1 \geq_\sigma s_2$ and $s_2 \geq_\sigma s_3$ imply $s_1 \geq_\sigma s_3$ (transitivity)
d) $s_1 \geq_\sigma s_2$ implies $\gamma * s_1 \geq_\sigma \gamma * s_2$

If, in addition, we have

e) $\gamma * s \geq_\sigma s$ for all $s \in \Sigma$ and all $\gamma \in \Gamma$

then σ is called a **module term ordering** on Σ.

For us, the most important case will be the case $\Gamma = \mathbb{T}^n$ and $\Sigma = \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. If $r = 1$, then module orderings are monoid orderings on $\mathbb{T}^n = \mathbb{T}^n \langle e_1 \rangle$ as introduced in Definition 1.4.1, and module term orderings are nothing but term orderings. We also note that it is easy to see that in this case condition e) is equivalent to $t e_i \geq_\sigma e_i$ for all $t \in \mathbb{T}^n$ and all $i = 1, \ldots, r$.

The most important module orderings for our purposes are constructed as follows.

Example 1.4.16. Let $\mathtt{To}$ be a term ordering on $\mathbb{T}^n$.

a) For $t_1 e_i, t_2 e_j \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ such that $t_1, t_2 \in \mathbb{T}^n$ and $i, j \in \{1, \ldots, r\}$, we let

$$t_1 e_i \geq_{\mathtt{ToPos}} t_2 e_j \qquad \Longleftrightarrow \qquad t_1 >_{\mathtt{To}} t_2 \quad \text{or} \quad (t_1 = t_2 \text{ and } i \leq j)$$

In this way we obtain a module term ordering $\mathtt{ToPos}$ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. The intuitive meaning of $\mathtt{ToPos}$ is that one first compares the two power products using $\mathtt{To}$ and then breaks ties by looking at their positions in the vector.

b) For $t_1 e_i, t_2 e_j \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ such that $t_1, t_2 \in \mathbb{T}^n$ and $i, j \in \{1, \ldots, r\}$, we let

$$t_1 e_i \geq_{\mathtt{PosTo}} t_2 e_j \qquad \Longleftrightarrow \qquad i < j \quad \text{or} \quad (i = j \text{ and } t_1 \geq_{\mathtt{To}} t_2)$$

Again we obtain a module term ordering $\mathtt{PosTo}$ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$.

Definition 1.4.17. Let $(\Gamma, \circ)$ be a monoid, let τ be a monoid ordering on Γ, and let $(\Sigma, *)$ be a Γ-monomodule. We say that a module ordering σ on Σ is **compatible** with τ if $\gamma_1 \geq_\tau \gamma_2$ implies $\gamma_1 * s \geq_\sigma \gamma_2 * s$ for all $\gamma_1, \gamma_2 \in \Gamma$ and all $s \in \Sigma$.

For instance, if $\mathtt{To}$ is a monoid ordering on $\mathbb{T}^n$, then both module orderings $\mathtt{ToPos}$ and $\mathtt{PosTo}$ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ are compatible with $\mathtt{To}$. We end this section by describing a fundamental property of term orderings.

Proposition 1.4.18. (Well-Orderings)
Let $(\Gamma, \circ)$ be a monoid, $(\Sigma, *)$ a Γ-monomodule, and σ a module ordering on Σ. Then the following conditions are equivalent.

a) Every non-empty subset of Σ has a minimal element with respect to σ.
b) Every descending chain $s_1 \geq_\sigma s_2 \geq_\sigma \cdots$ in Σ is eventually stationary.

*If these conditions are satisfied, the ordering σ is called a **well-ordering**. If the left-cancellation law holds in Σ, then every well-ordering is a module term ordering.*

Proof. The implication $a) \Rightarrow b)$ follows from the fact that the set of elements of a descending chain has a minimal element if and only if the chain is eventually stationary. Conversely, if there is a non-empty subset $\Sigma' \subseteq \Sigma$ having no minimal element with respect to σ, we can obviously construct an infinite, strictly descending chain of elements of Σ'.

To prove the additional claim, we observe that if $s >_\sigma \gamma * s$ for some $\gamma \in \Gamma$ and $s \in \Sigma$, then $s >_\sigma \gamma * s >_\sigma \gamma^2 * s >_\sigma \cdots$ is an infinite chain which is not eventually stationary. $\square$

Theorem 1.4.19. (Fundamental Property of Term Orderings)
For a module ordering σ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, the following conditions are equivalent.

a) *The relation σ is a module term ordering.*
b) *The relation σ is a well-ordering.*

Proof. In view of the previous proposition and the fact that the left-cancellation law holds in $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, it suffices to prove $a) \Rightarrow b)$. We suppose there is a chain $t_1 e_{\gamma_1} \geq_\sigma t_2 e_{\gamma_2} \geq_\sigma \cdots$ in $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ which is not eventually stationary, where $t_1, t_2, \ldots \in \mathbb{T}^n$ and $\gamma_1, \gamma_2, \ldots \in \{1, \ldots, r\}$. For some $i \in \{1, \ldots, r\}$, we then have a subchain $t_{\delta_1} e_i \geq_\sigma t_{\delta_2} e_i \geq_\sigma \cdots$ such that $1 \leq \delta_1 < \delta_2 < \cdots$ which is not eventually stationary. By Dickson's Lemma 1.3.6, the monoideal $(t_{\delta_1}, t_{\delta_2}, \ldots)$ is generated by finitely many terms $t_{\delta_1}, \ldots, t_{\delta_N}$ for some $N > 0$. Since σ is a module term ordering, it follows that for each $j > N$ there exists a number $k \in \{1, \ldots, N\}$ such that $t_{\delta_j} e_i \geq_\sigma t_{\delta_k} e_i$, a contradiction. $\qquad\square$

Exercise 1. Prove that the relations `Lex`, `DegLex`, `DegRevLex`, and `Elim(L)` on $\mathbb{T}^n$ are term orderings.

Exercise 2. For each of the term orderings `Lex`, `DegLex`, and `DegRevLex`, write down the 20 smallest terms of $\mathbb{T}^3$ in increasing order.

Exercise 3. Define a relation `RevLex` on $\mathbb{T}^n$ by $t_1 \geq_{\text{RevLex}} t_2$ if the last non-zero component of $\log(t_1) - \log(t_2)$ is negative, or if $t_1 = t_2$. Show that `RevLex` is a monoid ordering on $\mathbb{T}^n$ which is not a term ordering. How are the indeterminates ordered by `RevLex`?

Exercise 4. Go back to Example 1.4.4, replace x_1 by A, x_2 by B, etc., and decide to write "biggest first". What is the monoid ordering on $\mathbb{T}^n$ similar to the usual ordering on words in a dictionary?

Exercise 5. Let V be a matrix whose rows are linearly independent vectors $v_1, \ldots, v_n \in \mathbb{Z}^n$. Prove that the relation $\text{Ord}(V)$ is a monoid ordering on $\mathbb{T}^n$.

Exercise 6. For each of the term orderings `Lex`, `DegLex`, `DegRevLex`, and `Elim(L)`, give a non-singular matrix V such that they are represented by V.

Exercise 7. Let $u = (1, \sqrt{2})$ and let σ be the relation on $\mathbb{T}^2$ defined by $t_1 \geq_\sigma t_2$ if and only if $u \cdot (\log(t_1) - \log(t_2)) \geq 0$ for $t_1, t_2 \in \mathbb{T}^2$.
a) Show that σ is a term ordering on $\mathbb{T}^2$.
b) Show that σ cannot be represented by any matrix of integers.
  Hint: Prove that, for any term ordering τ represented by a matrix of integers, there exist terms $t, t' \in \mathbb{T}^2$ such that $t >_\sigma t'$ and $t <_\tau t'$.

Exercise 8. Prove that every monoid ordering σ on $\mathbb{Z}^n$ has a unique extension to a monoid ordering σ' on $\mathbb{Q}^n$.

Hint: A vector $v \in \mathbb{Q}^n$ can be represented in the form $v = \frac{1}{q} \cdot p$ with $q > 0$ and $p \in \mathbb{Z}^n$. Then define $v \geq_{\sigma'} 0$ if and only if $p \geq_\sigma 0$. To see that this is well-defined, take two representations $v = \frac{1}{q} \cdot p = \frac{1}{q'} \cdot p'$ with $q, q' > 0$ and $p, p' \in \mathbb{Z}^n$ and prove $p \geq_\sigma 0 \iff q'p \geq_\sigma 0$.

Exercise 9. Show that the relations `ToPos` and `PosTo` defined in Example 1.4.16 are module term orderings.

Exercise 10. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $e_1, \ldots, e_r$ be new indeterminates. Consider the P-linear map $\varphi : P^r \longrightarrow P[e_1, \ldots, e_r]$ defined by $\varphi((f_1, \ldots, f_r)) = f_1 e_1 + \cdots + f_r e_r$.

 a) Show that φ is an injective homomorphism of P-modules.

Using φ, we identify P^r with the corresponding submodule of $P[e_1, \ldots, e_r]$. Let ϑ be a monoid ordering on $\mathbb{T}^{n+r} = \mathbb{T}(x_1, \ldots, x_n, e_1, \ldots, e_r)$, let τ be the monoid ordering on $\mathbb{T}^n$ obtained by restriction of ϑ (see Proposition 1.4.13), and let σ be the ordering induced by ϑ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ via φ.

 b) Prove that σ is module ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$.
 c) Prove that σ is compatible with τ.

Exercise 11. Let σ be a module ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. View $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ as a disjoint union of r components, each of which is a copy of $\mathbb{T}^n$, and denote the restriction of σ to the ith component by σ_i.

 a) Prove that σ_i is a monoid ordering for every $i = 1, \ldots, r$.
 b) Let τ be a monoid ordering on $\mathbb{T}^n$ such that σ is compatible with τ. Prove that $\sigma_i = \tau$ for every $i = 1, \ldots, r$.

Tutorial 9: Monoid Orderings Represented by Matrices

Let $(v_1, \ldots, v_n)$, $(v'_1, \ldots, v'_n)$ be two n-tuples of linearly independent vectors in $\mathbb{Q}^n$, and let $V, V' \in \mathrm{Mat}_n(\mathbb{Q})$ be the matrices having those vectors as rows.

 a) Extend Definition 1.4.11 to orderings represented by rational matrices like $V \in \mathrm{Mat}_n(\mathbb{Q})$.
 b) Suppose there exists a lower triangular matrix $W \in \mathrm{Mat}_n(\mathbb{Q})$ whose entries in the diagonal are positive such that $V' = WV$. Prove that $\mathrm{Ord}(V) = \mathrm{Ord}(V')$.
 c) Prove that $\mathrm{Ord}(V)$ can be represented by a matrix in $\mathrm{Mat}_n(\mathbb{Z})$.
 d) Prove that if σ is a term ordering represented by a rational matrix V, then it can also be represented by a rational matrix V' whose entries are non-negative.
 e) Find such a representation for `DegRevLex`.
 f) Prove the following partial converse of b). If $\mathrm{Ord}(V) = \mathrm{Ord}(V')$, then there exists a rational number $\lambda > 0$ such that $v'_1 = \lambda v_1$.

g) Now we assume that $v_1' \neq \lambda v_1$ for all $\lambda > 0$. Write a CoCoA program `TODifference`(...) which computes two terms $t_1, t_2 \in \mathbb{T}^n$ such that $t_1 >_{\text{Ord}(V)} t_2$ and $t_1 <_{\text{Ord}(V')} t_2$.

h) Write a CoCoA program `CheckEquality`(...) which checks for a given number $d > 0$ if the term orderings represented by V and V' agree for all terms of degree $\leq d$ in $\mathbb{T}^n$.

i) *(This part is a much more elaborate project.)* Find criteria which characterize when V and V' represent the same monoid ordering.

Tutorial 10: Classification of Term Orderings

In this tutorial we want to get a good understanding of all possible term orderings on $\mathbb{T}^n$ for $n \leq 3$.

a) Prove that on $\mathbb{T}^1$ there is only one term ordering, namely `Deg`.

b) Show that on $\mathbb{T}^2$ there are precisely two degree compatible term orderings σ, τ which are characterized by $x_1 >_\sigma x_2$ and $x_2 >_\tau x_1$.

c) Classify all possible term orderings on $\mathbb{T}^2$ which satisfy $x_1 >_\sigma x_2$. To do that use the following scheme.

   1) Prove that there exists exactly one term ordering σ on $\mathbb{T}^2$ such that $x_1 >_\sigma x_2^i$ for all $i \geq 2$.

   2) Suppose that a term ordering σ on $\mathbb{T}^2$ satisfies $x_1 <_\sigma x_2^N$ for some $N \geq 2$, and let $q = \inf\{\frac{j}{i} \in \mathbb{Q}_+ \mid x_1^i <_\sigma x_2^j\}$. Prove that $1 \leq q \leq N$.

   3) Following 2), suppose that $q \in \mathbb{R}\backslash\mathbb{Q}$. Show that there exists exactly one term ordering σ with those properties and that it satisfies $x_1^{i_1} x_2^{i_2} \geq_\sigma x_1^{j_1} x_2^{j_2}$ if and only if $i_1 q + i_2 \geq j_1 q + j_2$.

   4) Following 2), suppose that $q \in \mathbb{Q}\backslash\{1\}$. Show that there exist exactly two term orderings with those properties. Prove that they are represented by matrices by exhibiting the matrices.

   5) Finally, if $q = 1$ in 2), show that there exists exactly one term ordering with those properties and that it is represented by a matrix.

d) For all terms of degree ≤ 2 in $\mathbb{T}^3$, find all orderings induced by degree compatible term orderings. You may assume that the indeterminates are numbered in such a way that $x_1 >_\sigma x_2 >_\sigma x_3$.

e) Repeat the previous part for all terms of degree ≤ 3 in $\mathbb{T}^3$.

f) Prove that there are infinitely many different degree compatible term orderings on $\mathbb{T}^3$.

g) Write a CoCoA program `TermOrderList`(...) which takes two numbers $i, d > 0$, defines a degree compatible term ordering TO_i on $\mathbb{T}^3$ which is different for each i, and returns the list of all terms of degree $\leq d$ ordered according to TO_i.

1.5 Leading Terms

The real leader has no need to lead.
He is content to point the way.
(Henry Miller)

In the last section we saw how to order terms. A first consequence is that, once a monoid ordering on $\mathbb{T}^n$ is chosen, we can sort the terms in the support of a polynomial, and therefore represent the polynomial in a unique way as a sum. This provides us with a new way of looking at polynomials.

In some sense, as soon as the ordering is given and the polynomial $f(x_1, x_2, x_3) = x_1x_3 - x_2^2 + x_1$ is written just as you see it (for instance if you are using `DegLex`), we can say that $-x_2^2 + x_1x_3 + x_1$ *is not allowed* anymore. If in the process of some computation $-x_2^2 + x_1x_3 + x_1$ shows up somewhere, it is automatically converted to $x_1x_3 - x_2^2 + x_1$. This does not violate the commutativity law, rather it conveys the idea that the equality $x_1x_3 - x_2^2 + x_1 = -x_2^2 + x_1x_3 + x_1$ should be interpreted in the following way. The polynomial $f(x_1, x_2, x_3)$, written correctly with the sequence of symbols $x_1x_3 - x_2^2 + x_1$, is equal to the polynomial $-x_2^2 + x_1x_3 + x_1$, because $-x_2^2 + x_1x_3 + x_1$ is automatically converted to $x_1x_3 - x_2^2 + x_1$, and this is the same sequence of symbols as before.

The hierarchy created among the terms in $\mathrm{Supp}(f)$ by the monoid ordering implies that x_1x_3 becomes "bigger" and "more important" than the other terms. Should it be called the "leader", the "initial", or the "head"? We call it the leading term of $f(x_1, x_2, x_3)$. Of course all of this can and will be extended to module orderings.

The first part of this section is devoted to explaining these concepts and to getting a better insight into their mathematical meaning. Then we address a very important problem. One of the main ideas in Computational Commutative Algebra is to study or detect properties of ideals and modules using the information coming from their associated leading term ideals and modules. The reason is that the latter objects, whose nature is purely combinatorial, are easier to deal with, and the first step in this direction is Macaulay's Basis Theorem.

Suppose we have an ideal I in a polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K. It is clear that the residue class ring P/I can be viewed as a K-vector space. Some natural questions arise. Is it possible to exhibit an explicit basis? Can we compute it? The second question will take much more effort, but with the aid of leading terms, Macaulay's Basis Theorem yields a beautiful answer to the first one. This theorem requires the assumption that the module ordering is a term ordering. Thus we see, for the first time, the theoretical importance of term orderings.

In the final part of this section we show how two fundamental term orderings, `Lex` and `DegRevLex`, can be characterized using the kind of leading terms they produce.

In what follows, we let R be a ring, $n \geq 1$, $P = R[x_1, \ldots, x_n]$ a polynomial ring, $r \geq 1$, and σ a module ordering on the set of terms $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ of P^r. The standard basis of P^r will be denoted by $\{e_1, \ldots, e_r\}$ as usual.

Remark 1.5.1. Every element $m \in P^r \setminus \{0\}$ has a unique representation as a linear combination of terms

$$m = \sum_{i=1}^s c_i t_i e_{\gamma_i}$$

where $c_1, \ldots, c_s \in R \setminus \{0\}$, $t_1, \ldots, t_s \in \mathbb{T}^n$, $\gamma_1, \ldots, \gamma_s \in \{1, \ldots, r\}$, and where $t_1 e_{\gamma_1} >_\sigma t_2 e_{\gamma_2} >_\sigma \cdots >_\sigma t_s e_{\gamma_s}$.

If we write $m = f_1 e_1 + \cdots + f_r e_r$, where $f_1, \ldots, f_r \in P$, then we have $\mathrm{Supp}(f_i) = \{t_j \mid \gamma_j = i\}$ for each $i \in \{1, \ldots, r\}$.

Definition 1.5.2. For a non-zero element $m \in P^r$, let $m = \sum_{i=1}^s c_i t_i e_{\gamma_i}$ be the representation according to Remark 1.5.1.

a) The term $\mathrm{LT}_\sigma(m) = t_1 e_{\gamma_1} \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ is called the **leading term** of m with respect to σ.

b) The element $\mathrm{LC}_\sigma(m) = c_1 \in R \setminus \{0\}$ is called the **leading coefficient** of m with respect to σ. If $\mathrm{LC}_\sigma(m) = 1$, we say that m is σ**-monic**, or simply **monic** if σ is clear from the context.

c) We let $\mathrm{LM}_\sigma(m) = \mathrm{LC}_\sigma(m) \cdot \mathrm{LT}_\sigma(m) = c_1 t_1 e_{\gamma_1}$.

For the zero vector $m = (0, \ldots, 0)$, we recall from Definition 1.1.11 that $\mathrm{Supp}(m) = \emptyset$. The leading term $\mathrm{LT}_\sigma(m)$ and the leading coefficient $\mathrm{LC}_\sigma(m)$ are not defined.

Note that the leading term of a vector $m \in P^r \setminus \{0\}$ really consists of two data: the term $t_1 \in \mathbb{T}^n$ which is sometimes also called the **leading power product** of m, and the position $\gamma_1 \in \{1, \ldots, r\}$ of this term which is sometimes called the **leading position** of m. In CoCoA, the leading power product of a vector can be obtained using the function `LPP(...)`, and the leading position is accessible via `LPos(...)`.

With respect to the usual operations such as addition and multiplication of polynomials, leading terms behave pretty much as one would expect: the leading term of a sum is the biggest leading term of one of the summands, except if some "cancellation" occurs, and the leading term of the product is the product of the leading terms, except for some pathological cases. Let us collect the precise rules.

Proposition 1.5.3. (Rules for Computing with Leading Terms)
As above, we let $P = R[x_1, \ldots, x_n]$ be a polynomial ring over a ring R and σ a module ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. Moreover, let $f, f_1, f_2 \in P$ be non-zero polynomials, and let $m, m_1, m_2 \in P^r$ be non-zero vectors of polynomials.

a) *We have* $\mathrm{Supp}(m_1 + m_2) \subseteq \mathrm{Supp}(m_1) \cup \mathrm{Supp}(m_2)$, *and if moreover* $m_1 + m_2 \neq 0$, *then* $\mathrm{LT}_\sigma(m_1 + m_2) \leq_\sigma \max_\sigma\{\mathrm{LT}_\sigma(m_1), \mathrm{LT}_\sigma(m_2)\}$.

b) *Suppose that* $m_1 + m_2 \neq 0$, *and suppose that* $\mathrm{LT}_\sigma(m_1) \neq \mathrm{LT}_\sigma(m_2)$ *or* $\mathrm{LC}_\sigma(m_1) + \mathrm{LC}_\sigma(m_2) \neq 0$. *Then we have*

$$\mathrm{LT}_\sigma(m_1 + m_2) = \max_\sigma\{\mathrm{LT}_\sigma(m_1), \mathrm{LT}_\sigma(m_2)\}$$

c) *For* $t \in \mathbb{T}^n$, *we have* $\mathrm{LT}_\sigma(tm) = t \cdot \mathrm{LT}_\sigma(m)$.

d) *If R is an integral domain, and if t is the term in* $\mathrm{Supp}(f)$ *for which* $t \cdot \mathrm{LT}_\sigma(m)$ *is maximal with respect to σ, then* $\mathrm{LT}_\sigma(fm) = t \cdot \mathrm{LT}_\sigma(m)$.

e) *If R is an integral domain, and if τ is a monoid ordering on* $\mathbb{T}^n$ *such that σ is compatible with τ, then we have*

$$\mathrm{LT}_\sigma(fm) = \mathrm{LT}_\tau(f) \cdot \mathrm{LT}_\sigma(m)$$

In particular, if R is an integral domain, then $\mathrm{LT}_\tau(f_1 f_2) = \mathrm{LT}_\tau(f_1) \cdot \mathrm{LT}_\tau(f_2)$.

Proof. To prove a), write $m_1 = \sum_{i=1}^{s} c_i t_i e_{\gamma_i}$ and $m_2 = \sum_{j=1}^{s'} c_j' t_j' e_{\gamma_j'}$ according to Remark 1.5.1. From the representation

$$m_1 + m_2 = \sum_{i=1}^{r} \sum_{t \in \mathbb{T}^n} \Big(\sum_{\{j \mid t_j = t, \gamma_j = i\}} c_j + \sum_{\{j \mid t_j' = t, \gamma_j' = i\}} c_j' \Big) t e_i$$

we conclude that $\mathrm{Supp}(m_1 + m_2) \subseteq \mathrm{Supp}(m_1) \cup \mathrm{Supp}(m_2)$ and also that $t e_i \leq_\sigma \max_\sigma\{t_1 e_{\gamma_1}, t_1' e_{\gamma_1'}\}$ for all $t e_i \in \mathrm{Supp}(m_1 + m_2)$.

For the proof of b), we represent m_1, m_2 and $m_1 + m_2$ as above. If we have $\mathrm{LT}_\sigma(m_1) = t_1 e_{\gamma_1} = t_1' e_{\gamma_1'} = \mathrm{LT}_\sigma(m_2)$, then $c_1 + c_1' \neq 0$ implies that $\mathrm{LT}_\sigma(m_1 + m_2) = t_1 e_{\gamma_1} = \max_\sigma\{t_1 e_{\gamma_1}, t_1' e_{\gamma_1'}\}$. When $t_1 e_{\gamma_1} <_\sigma t_1' e_{\gamma_1'}$ or $t_1 e_{\gamma_1} >_\sigma t_1' e_{\gamma_1'}$, the claim follows immediately from the above representation of $m_1 + m_2$.

In order to show claim c), we write $m = \sum_{i=1}^{s} c_i t_i e_{\gamma_i}$ as in Remark 1.5.1. Then $tm = \sum_{i=1}^{s} c_i (t t_i) e_{\gamma_i}$ is the representation of tm, since $t_i e_{\gamma_i} >_\sigma t_j e_{\gamma_j}$ for $1 \leq i < j \leq s$ implies $(t t_i) e_{\gamma_i} >_\sigma (t t_j) e_{\gamma_j}$. Thus we obtain $\mathrm{LT}_\sigma(tm) = t t_1 e_{\gamma_1} = t \cdot \mathrm{LT}_\sigma(m)$.

For the proof of d), we represent $f = \sum_{i=1}^{s} c_i t_i$ and $m = \sum_{j=1}^{s'} c_j' t_j' e_{\gamma_j}$ according to Remark 1.5.1. Then we have $t_i t_j' e_{\gamma_j} \leq_\sigma t_i \mathrm{LT}_\sigma(m) \leq_\sigma t \mathrm{LT}_\sigma(m)$ for $i = 1, \ldots, s$ and for $j = 1, \ldots, s'$. Let c_k be the coefficient of t in f. Now the claim follows from $fm = \sum_{i=1}^{s} \sum_{j=1}^{s'} (c_i c_j')(t_i t_j') e_{\gamma_j}$ and $c_k c_1' \neq 0$.

To prove e), we observe that if σ is compatible with τ, then the term $t = \mathrm{LT}_\tau(f)$ is the unique element of $\mathrm{Supp}(f)$ for which $t \cdot \mathrm{LT}_\sigma(m)$ is maximal with respect to σ. $\square$

Definition 1.5.4. Let $M \subseteq P^r$ be a P-submodule.

a) The module $\mathrm{LT}_\sigma(M) = \langle \mathrm{LT}_\sigma(m) \mid m \in M \backslash \{0\} \rangle$ is called the **leading term module** of M with respect to σ.

b) If $r = 1$, i.e. if $M \subseteq P$, then the ideal $\mathrm{LT}_\sigma(M) \subseteq P$ is also called the **leading term ideal** of M with respect to σ.
c) The monomodule $\{\mathrm{LT}_\sigma(m) \mid m \in M \backslash \{0\}\} \subseteq \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ will be denoted by $\mathrm{LT}_\sigma \{M\}$.

Notice that, for $M = \langle 0 \rangle$, we get $\mathrm{LT}_\sigma(M) = \langle 0 \rangle$ and $\mathrm{LT}_\sigma \{M\} = \emptyset$ using this definition. If $m_1, \ldots, m_s \in P^r$ are non-zero vectors, and if $M = \langle m_1, \ldots, m_s \rangle \subseteq P^r$ is the submodule generated by them, we have $\langle \mathrm{LT}_\sigma(m_1), \ldots, \mathrm{LT}_\sigma(m_s) \rangle \subseteq \mathrm{LT}_\sigma(M)$. The following example shows that this can be a proper inclusion.

Example 1.5.5. Let I be the ideal in $K[x, y]$ generated by $\{x^2 - 1, xy - 1\}$, and let $\sigma = \mathtt{DegLex}$. Then $f = y(x^2 - 1) - x(xy - 1) = x - y \in I$ implies $\mathrm{LT}_\sigma(f) = x \in \mathrm{LT}_\sigma(I)$, but x is not in the ideal generated by $\mathrm{LT}_\sigma(x^2 - 1) = x^2$ and $\mathrm{LT}_\sigma(xy - 1) = xy$.

Nevertheless, there are systems of elements of M whose leading terms generate $\mathrm{LT}_\sigma(M)$ as our next proposition shows.

Proposition 1.5.6. *Let $M \subseteq P^r$ be a non-zero P-submodule.*

a) *Every term $te_i \in \mathrm{LT}_\sigma(M)$ with $t \in \mathbb{T}^n$ and $1 \leq i \leq r$ is of the form $te_i = \mathrm{LT}_\sigma(m)$ for some $m \in M$.*
b) *There exist non-zero elements $m_1, \ldots, m_s \in M$ such that we have $\mathrm{LT}_\sigma(M) = \langle \mathrm{LT}_\sigma(m_1), \ldots, \mathrm{LT}_\sigma(m_s) \rangle$.*

Proof. The elements of the set $\mathrm{LT}_\sigma \{M\}$ generate the R-module $\mathrm{LT}_\sigma(M)$. By Proposition 1.3.11.a, every term in $\mathrm{LT}_\sigma(M)$ is then of the form $t \cdot \mathrm{LT}_\sigma(m)$ with $t \in \mathbb{T}^n$ and $m \in M$, and is therefore equal to $\mathrm{LT}_\sigma(tm)$. This proves a).

Theorem 1.3.9.a implies that $\mathrm{LT}_\sigma \{M\}$ is generated by finitely many terms as a monomodule over $\mathbb{T}^n$. Thus those terms generate the R-module $\mathrm{LT}_\sigma(M)$, and using a) we get claim b). $\square$

Now we are ready to prove the main result of this section. As we said before, Macaulay's Basis Theorem requires the assumption that the module ordering is a term ordering. Furthermore, we need to assume that our base ring is a field.

Theorem 1.5.7. (Macaulay's Basis Theorem)
Let K be a field, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over K, let $M \subseteq P^r$ be a P-submodule, and let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. We denote the set of all terms in $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle \backslash \mathrm{LT}_\sigma \{M\}$ by B. Then the residue classes of the elements of B form a basis of the K-vector space P^r / M.

Proof. First we prove that the elements $\bar{b} \in P^r / M$ such that $b \in B$ form a system of generators of P^r / M. In other words, we need to prove that the vector subspace $N = \sum_{b \in B} K \cdot b + M$ equals P^r. For a contradiction suppose

that $N \subset P^r$. Then the set $P^r \backslash N$ contains some non-zero elements. Hence Theorem 1.4.19 implies that there exists an element m of $P^r \backslash N$ having a minimal leading term with respect to σ. If now $\mathrm{LT}_\sigma(m) \in B$, then the element $m - \mathrm{LC}_\sigma(m)\,\mathrm{LT}_\sigma(m)$ is still in $P^r \backslash N$ and has a smaller leading term than m: a contradiction. Thus we need to have $\mathrm{LT}_\sigma(m) \in \mathrm{LT}_\sigma\{M\}$. So there exists an element $m' \in M$ such that $\mathrm{LT}_\sigma(m') = \mathrm{LT}_\sigma(m)$. Again the element $m - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(m')} m'$ lies in $P^r \backslash N$ and has a smaller leading term than m: a contradiction again.

Now we prove linear independence. Suppose there is a relation $m = \sum_{i=1}^{s} c_i m_i \in M$ such that $c_1, \ldots, c_s \in K \backslash \{0\}$ and $m_1, \ldots, m_s \in B$. Then we have $\mathrm{LT}_\sigma(m) \in \mathrm{LT}_\sigma\{M\}$, since $m \in M$. We also have $\mathrm{LT}_\sigma(m) \in \mathrm{Supp}(m) \subseteq \{m_1, \ldots, m_s\} \subseteq B$, because $m_1, \ldots, m_s$ are terms, and because of Proposition 1.5.3.a. Altogether we find $\mathrm{LT}_\sigma(m) \in \mathrm{LT}_\sigma\{M\} \cap B = \emptyset$ which is impossible. $\qquad \square$

To see how essential the assumption is that σ is a term ordering, consider the following example.

Example 1.5.8. Let $P = K[x]$, let $\sigma = \mathtt{Ord}(-1)$, and let I be the principal ideal generated by $x - x^2$. Then $\mathrm{LT}_\sigma(x - x^2) = x$, so that $\mathbb{T}^1 \backslash \mathrm{LT}_\sigma\{I\} = \{1\}$. However, the residue class of x cannot be a constant.

Remark 1.5.9. Macaulay's Basis Theorem gives us a first idea of how to compute effectively in P^r/M. First we would need to know $\mathrm{LT}_\sigma(M)$ for some module term ordering σ, and then we could represent every element uniquely as a finite linear combination of the residue classes of the elements of $B = \mathbb{T}^n \langle e_1, \ldots, e_r \rangle \backslash \mathrm{LT}_\sigma\{M\}$. Unfortunately, we do not yet know how to calculate $\mathrm{LT}_\sigma(M)$, and we cannot store the basis $\{\bar{b} \mid b \in B\}$ in a computer, since it is in general infinite. In the next chapter we shall see how to overcome these problems.

To conclude this section, we show how to characterize two of the most important term orderings on $\mathbb{T}^n$, namely $\mathtt{Lex}$ and $\mathtt{DegRevLex}$ in terms of their behaviour when they are used to order polynomials. So, for the rest of the section, let R be a ring, and let $P = R[x_1, \ldots, x_n]$.

Proposition 1.5.10. *Let σ be a monoid ordering on $\mathbb{T}^n$. Then the following conditions are equivalent.*

a) $\sigma = \mathtt{Lex}$

b) For $f \in P$ and $i \in \{1, \ldots, n\}$ such that $\mathrm{LT}_\sigma(f) \in R[x_i, \ldots, x_n]$, we have $f \in R[x_i, \ldots, x_n]$.

Proof. To prove a) $\Rightarrow$ b), let $f \in P$ be such that $\mathrm{LT}_{\mathtt{Lex}}(f) \in R[x_i, \ldots, x_n]$. If $t \in \mathrm{Supp}(f) \backslash \{\mathrm{LT}_{\mathtt{Lex}}(f)\}$, then by Definition 1.4.3 the first non-zero component of $\log(\mathrm{LT}_{\mathtt{Lex}}(f)) - \log(t)$ is positive. But since the first $i-1$ components of $\mathrm{LT}_{\mathtt{Lex}}(f)$ are zero, also the first $i-1$ components of $\log(t)$ have to be zero. Thus we get $t \in R[x_i, \ldots, x_n]$ for all $t \in \mathrm{Supp}(f)$.

Now we prove $b) \Rightarrow a)$. Let us consider two terms $t_1, t_2 \in \mathbb{T}^n$ such that $\log(t_1) - \log(t_2) = (0, \ldots, 0, c_{i-1}, \ldots, c_n)$, with $c_{i-1} > 0$. The first $i - 2$ coordinates of $\log(t_1)$ and $\log(t_2)$ are equal, so we can use property d) of Definition 1.4.1 and assume that they are zero. For the same reason we can also assume that the $(i-1)^{\mathrm{st}}$ coordinate of $\log(t_2)$ is zero, while the $(i-1)^{\mathrm{st}}$ coordinate of $\log(t_1)$ is different from zero. Next we consider the polynomial $f = t_1 + t_2$. Suppose for contradiction that $\mathrm{LT}_\sigma(f) = t_2$. Then $\mathrm{LT}_\sigma(f) \in R[x_i, \ldots, x_n]$, and b) implies that also $f \in R[x_i, \ldots, x_n]$. Consequently, we see that $t_1 = f - t_2 \in R[x_i, \ldots, x_n]$, in contradiction with the fact that the $(i-1)^{\mathrm{st}}$ coordinate of $\log(t_1)$ is different from zero. Therefore we have $\mathrm{LT}_\sigma(f) = t_1$, i.e. $t_1 >_\sigma t_2$.

Altogether, we have shown that $t_1 >_{\mathtt{Lex}} t_2$ implies $t_1 >_\sigma t_2$. By interchanging t_1 and t_2, we find that $t_1 >_{\mathtt{Lex}} t_2$ if and only if $t_1 >_\sigma t_2$. Therefore we have $\sigma = \mathtt{Lex}$. $\square$

Proposition 1.5.11. *Let σ be a monoid ordering on $\mathbb{T}^n$. Then the following conditions are equivalent.*

a) $\sigma = \mathtt{RevLex}$

b) *For $f \in P$ and $i \in \{1, \ldots, n\}$ such that $\mathrm{LT}_\sigma(f) \in (x_i, ..., x_n)$, we have $f \in (x_i, ..., x_n)$.*

Proof. To prove $a) \Rightarrow b)$, let $f \in P$ be such that $\mathrm{LT}_\sigma(f)$ is in the ideal $(x_i, \ldots, x_n)$. If $t \in \mathrm{Supp}(f) \setminus \{\mathrm{LT}_\sigma(f)\}$, then by the definition of $\mathtt{RevLex}$, the last non-zero component of $\log(\mathrm{LT}_\sigma(f)) - \log(t)$ is negative. But since the last non-zero component of $\log(\mathrm{LT}_\sigma(f))$ is in a position between i and n, also the last non-zero component of $\log(t)$ has to be in a position between i and n. This means that all the terms in $\mathrm{Supp}(f)$ have to be in the ideal $(x_i, \ldots, x_n)$.

Now we prove $b) \Rightarrow a)$. Let t_1, t_2 be two terms in $\mathbb{T}^n$ such that $\log(t_1) - \log(t_2) = (c_1, \ldots, c_i, 0, \ldots, 0)$, with $c_i < 0$. The last $n - i$ coordinates of $\log(t_1)$ and $\log(t_2)$ are equal, so we can use property d) of Definition 1.4.1 and assume that they are zero. For the same reason we can also assume that the ith coordinate of $\log(t_1)$ is zero while the ith coordinate of $\log(t_2)$ is different from zero. Let us consider the polynomial $f = t_1 + t_2$. Suppose for contradiction that $\mathrm{LT}_\sigma(f) = t_2$. Then $\mathrm{LT}_\sigma(f) \in (x_i, ..., x_n)$, and b) implies that also $f \in (x_i, ..., x_n)$. Consequently, we have $t_1 = f - t_2 \in (x_i, ..., x_n)$, in contradiction with the fact that the last $n - i$ coordinates of $\log(t_1)$ are zero. Therefore $\mathrm{LT}_\sigma(f) = t_1$, i.e. we have $t_1 >_\sigma t_2$, and we may conclude that $\sigma = \mathtt{RevLex}$. $\square$

Later on in this Chapter (see Section 1.7) and in the second volume we will study the concepts of gradings and homogeneity in great detail. However, for the moment it is enough to recall that a polynomial of degree d is said to be homogeneous if all the terms in its support have degree d. Also, we refer to Definition 1.4.9 for the notion of degree-compatible term orderings.

Then an easy modification of the proof of the preceding proposition yields the following characterization of the degree-reverse-lexicographic term ordering.

Corollary 1.5.12. *Let σ be a degree-compatible term ordering on $\mathbb{T}^n$. Then the following conditions are equivalent.*

a) $\sigma = \mathtt{DegRevLex}$

b) For every homogeneous polynomial $f \in P$ and every $i \in \{1, \ldots, n\}$ such that $\mathrm{LT}_\sigma(f) \in (x_i, \ldots, x_n)$, we have $f \in (x_i, \ldots, x_n)$.

Exercise 1. Let $f = x_1^2 + x_1 x_2 + x_2^2 \in P = K[x_1, x_2]$. Show that there is no monoid ordering σ on $\mathbb{T}^2$ such that $\mathrm{LT}_\sigma(f) = x_1 x_2$.

Exercise 2. For each of the following polynomials in $\mathbb{Q}[x_1, x_2, x_3]$, find a term ordering such that the given representation agrees with the one provided by Remark 1.5.1.

a) $f_1 = x_1 x_2^3 x_3 + 2 x_1 x_2^2 x_3^2 - x_1^2 x_3^3$

b) $f_2 = 4 x_1^4 x_2^5 x_3 + 2 x_1^3 x_2^2 x_3 + x_1 x_2^2 x_3^4$

c) $f_3 = -x_1^2 x_2^4 x_3 + 3 x_1 x_2^6 - 2 x_1^2 x_2^2$

Exercise 3. Do the leading terms of the polynomials $f_1 = x_1^4 x_2 - x_3^5$, $f_2 = x_1^3 x_2^3 - 1$, and $f_3 = x_1^2 x_2^4 - 2 x_3$ generate the leading term ideal with respect to $\mathtt{DegRevLex}$ of the ideal (f_1, f_2, f_3) in $\mathbb{Q}[x_1, x_2, x_3]$?

Exercise 4. Let K be a field. Try to use Macaulay's Basis Theorem to determine an explicit K-basis of the ring $K[x_1, x_2, x_3]/(x_1 - x_3^3, x_2 - x_3^4)$. *Hint:* Use the lexicographic term ordering.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $1 \le m < n$, and let $V \in \mathrm{Mat}_n(\mathbb{Z})$ be a matrix with $\det(V) \ne 0$ and of the following type

$$V = \begin{pmatrix} v \\ W \end{pmatrix}$$

where $v = (0, \ldots, 0, 1, \ldots, 1)$, the last 0 occurring in the mth position, and where $W \in \mathrm{Mat}_{n-1,n}(\mathbb{Z})$ is such that the first non-zero element in each of the first m columns is positive.

a) Show that the ordering $\mathtt{Ord}(V)$ on $\mathbb{T}^n$ is a term ordering.

b) Show that if $f \in P$ and $\mathrm{LT}_{\mathtt{Ord}(V)}(f) \in K[x_1, \ldots, x_m]$, then we have $f \in K[x_1, \ldots, x_m]$.

Exercise 6. Let K be a field, and let $V \in \mathrm{Mat}_n(\mathbb{Z})$ be a matrix with $\det(V) \ne 0$ which is of the following type

$$V = \begin{pmatrix} v \\ W \end{pmatrix}$$

where $v = (0, \ldots, 0, -1)$ and $W \in \mathrm{Mat}_{n-1,n}(\mathbb{Z})$.

a) Show that the ordering $\mathtt{Ord}(V)$ on $\mathbb{T}^n$ is not a term ordering.

b) Show that if $f \in K[x_1, \ldots, x_n]$ and $x_n \mid \mathrm{LT}_{\mathtt{Ord}(V)}(f)$, then $x_n \mid f$.

c) Can you modify V in such a way that b) holds for homogeneous polynomials, but not in general?

Tutorial 11: Polynomial Representation II

Using Remark 1.5.1, we have another possible way of representing polynomials from the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K in a computer program. We choose a term ordering σ on $\mathbb{T}^n$. For each $f \in P \backslash \{0\}$, we let

$$f = \sum_{i=1}^{s} c_i t_i$$

with $c_1, \ldots, c_s \in K \backslash \{0\}$ and with $t_1, \ldots, t_s \in \mathbb{T}^n$ such that $t_1 >_\sigma \cdots >_\sigma t_s$ be the representation according to Remark 1.5.1. Then we represent f in the computer program by the list of pairs

$$[[c_1, \log(t_1)], \ldots, [c_s, \log(t_s)]]$$

where $\log(t_1), \ldots, \log(t_s)$ are considered as vectors in $\mathbb{Z}^n$.

a) Write a CoCoA program `ReprPoly2(...)` which takes a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ and computes this representation.

b) Implement CoCoA functions `AddPoly2(...)` and `MultPoly2(...)` which calculate the lists corresponding to the sums and products of two polynomials represented in this way.

c) Check the correctness of your programs by applying them to the polynomials of Tutorial 1.f. Compute the lists representing $f_1 + f_2$, $f_1 \cdot f_2$, and $f_2 \cdot f_3 + f_1^3$ again in two ways.

Tutorial 12: Symmetric Polynomials

Let K be a field and $f \in P = K[x_1, \ldots, x_n]$ a polynomial. We call f **symmetric** if f is invariant under all permutations of the indeterminates $x_1, \ldots, x_n$. For $i = 1, \ldots, n$, the polynomials

$$s_i = \sum_{j_1 < \cdots < j_i} x_{j_1} \cdots x_{j_i}$$

are called the **elementary symmetric polynomials**. In this tutorial we intend to give an effective proof for the well-known theorem that every symmetric polynomial can be written as a polynomial in $s_1, \ldots, s_n$. To this end, we equip the polynomial ring P with the lexicographic term ordering `Lex`.

a) Show that the symmetric group $\mathfrak{S}_n$ (i.e. the group of all permutations of the variables $x_1, \ldots, x_n$) is generated by the transpositions $\langle x_1, x_2 \rangle, \ldots, \langle x_1, x_n \rangle$.

b) Write a CoCoA program `Is_Symmetric(...)` which checks if a given polynomial is symmetric and returns the corresponding Boolean value. (*Hint:* Show that it suffices to check invariance under a system of generators of $\mathfrak{S}_n$ and use the CoCoA command `Subst(...)`.)

c) Prove the recursive formula $s_i = \tilde{s}_i + x_n \tilde{s}_{i-1}$ for $n > 1$ and $i \in \mathbb{Z}$, where $\tilde{s}_1, \ldots, \tilde{s}_{n-1}$ are the elementary symmetric polynomials in the indeterminates $x_1, \ldots, x_{n-1}$, where we set $s_i = \tilde{s}_i = 0$ if $i < 0$ or $i > n$, and where $s_0 = \tilde{s}_0 = 1$.

d) Use c) to write a CoCoA program `ElSym(...)` which computes the ith elementary symmetric polynomial in n indeterminates.

e) Prove that the leading term $\mathrm{LT}_{\texttt{Lex}}(f) = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ of a symmetric polynomial $f \in P \backslash \{0\}$ satisfies $\alpha_1 \geq \cdots \geq \alpha_n$.

f) Show that one can subtract from f a suitable multiple of the polynomial $s_1^{\alpha_1 - \alpha_2} \cdots s_{n-1}^{\alpha_{n-1} - \alpha_n} \cdot s_n^{\alpha_n}$ such that the result is a symmetric polynomial with a smaller leading term with respect to `Lex`. Consequently, develop an algorithm for representing f as a polynomial in $s_1, \ldots, s_n$.

g) Implement the algorithm from f) in a CoCoA function `ReprSym(...)` which takes a polynomial $f \in P$ and returns a polynomial $g \in P$ such that $f = g(s_1, \ldots, s_n)$.

h) Apply `Is_Symmetric(...)` and `ReprSym(...)` to the following polynomials.
   1) $F_1 = x_1^3 x_2 + x_2^3 x_3 + x_1 x_2^3 + x_1 x_3^3 + x_1^3 x_3 + x_2 x_3^3 \in \mathbb{Q}[x_1, x_2, x_3]$
   2) $F_2 = \sum_{i \neq j} x_i^2 x_j \in \mathbb{Q}[x_1, \ldots, x_5]$
   3) $F_3 = x_1^5 + \cdots + x_5^5 \in \mathbb{Q}[x_1, \ldots, x_5]$

Tutorial 13: Newton Polytopes

Given a non-zero polynomial f in a polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K, we may wonder which terms in its support can be the leading term with respect to some term ordering. A partial answer to this question can be given using the **Newton polytope** of f which is the subject of this tutorial.

For $v_1, v_2 \in \mathbb{R}^n$, the set $\{\lambda_1 v_1 + \lambda_2 v_2 \mid \lambda_1, \lambda_2 \in \mathbb{R}_{\geq 0}, \lambda_1 + \lambda_2 = 1\}$ is called the **line segment** defined by v_1 and v_2 and is denoted by $[v_1 v_2]$. A subset $S \subseteq \mathbb{R}^n$ is called **convex** if for all $v_1, v_2 \in S$ the line segment $[v_1 v_2]$ is contained in S.

a) Let $S \subseteq \mathbb{R}^n$ be a non-empty subset. Show that there exists a unique convex subset of $\mathbb{R}^n$ containing S which is contained in every other convex set containing S. It is called the **convex hull** of S and denoted by $\mathrm{conv}(S)$.
   Hint: Consider the intersection of all convex sets containing S.

b) Let $S \subseteq \mathbb{R}^n$ be a convex set, and let $v \in \mathbb{R}^n \backslash S$. Prove the equality $\mathrm{conv}(S \cup \{v\}) = \{[vw] \mid w \in S\}$, but also give an example of a set $S' \subseteq \mathbb{R}^n$ such that $\{[vw] \mid v, w \in S'\}$ is not the convex hull of S'.

For a finite subset $S = \{v_1, \ldots, v_r\}$ of $\mathbb{R}^n$, its convex hull $\mathcal{P} = \mathrm{conv}(S)$ is also called a **polytope**. A **vertex** of $\mathcal{P}$ is an element $v \in \mathcal{P}$ such that $v \notin \mathrm{conv}(\mathcal{P} \backslash \{v\})$. The set of all vertices of $\mathcal{P}$ is denoted by $\mathrm{Vert}(\mathcal{P})$.

c) Show that $\mathcal{P} = \{\sum_{i=1}^r \lambda_i v_i \mid \lambda_1, \ldots, \lambda_r \in \mathbb{R}_{\geq 0}, \lambda_1 + \cdots + \lambda_r = 1\}$.
   Hint: Use induction on r, the fact that if we let $\alpha = \sum_{i=1}^{r-1} \lambda_i$, then $\sum_{i=1}^r \lambda_i v_i = \alpha(\sum_{i=1}^{r-1} \frac{\lambda_i}{\alpha} v_i) + \lambda_r v_r$, and apply b).

d) Show that $\mathrm{Vert}(\mathcal{P}) \subseteq S$.

e) Prove that the convex hull of $\mathrm{Vert}(\mathcal{P})$ is $\mathcal{P}$ and that, among all sets whose convex hull is $\mathcal{P}$, it is the unique minimal set with that property.

Now let us return to our non-zero polynomial $f \in P = K[x_1, \ldots, x_n]$. We let $S = \{\log(t) \mid t \in \mathrm{Supp}(f)\}$ and call $\mathrm{Newton}(f) = \mathrm{conv}(S)$ the **Newton polytope** of f. Further, we let $\mathrm{Vert}(f)$ be the subset of $\mathrm{Supp}(f)$ which corresponds to the set of vertices of $\mathrm{Newton}(f)$.

f) Prove that if $t \in \mathrm{Supp}(f) \backslash \mathrm{Vert}(f)$, then there is no monoid ordering σ such that $\mathrm{LT}_\sigma(f) = t$.
   Hint: Use the fact that if $S = \{v_1, \ldots, v_r\} \subseteq \mathbb{Q}^n$, then every element v of $\mathcal{P} \cap \mathbb{Q}^n$ has a representation $v = \sum_{i=1}^r \lambda_i v_i$ with $\lambda_1, \ldots, \lambda_r \in \mathbb{Q}_{\geq 0}$ and $\lambda_1 + \cdots + \lambda_r = 1$. (You do not have to prove this.) Now let $\mathrm{Vert}(f) = \{t_1, \ldots, t_s\}$. Find a relation $\log(t) = \sum_{i=1}^s \lambda_i \log(t_i)$ with $\lambda_i \in \mathbb{Q}_{\geq 0}$, and thus a relation $t^{a_0} = \prod_{i=1}^s t_i^{a_i}$ with $a_0, \ldots, a_s \in \mathbb{N}$ and $a_0 = a_1 + \cdots + a_s$.

g) Let $f = 3x^6 y^2 + 2x^3 y^3 - xy + 5x^3 y^5 \in K[x, y]$.
   1) Find a term ordering σ such that $\mathrm{LT}_\sigma(f) = x^6 y^2$.
   2) Find a term ordering σ such that $\mathrm{LT}_\sigma(f) = x^3 y^5$.
   3) Show that $\mathrm{LT}_\sigma(f) \neq xy$ for every term ordering σ.
   4) Show that $\mathrm{LT}_\sigma(f) \neq x^3 y^3$ for every monoid ordering σ.

1.6 The Division Algorithm

Divide et impera.
(Philip of Macedonia)

In Section 1.1 we introduced addition, subtraction and multiplication of polynomials. How about division? Can we divide and conquer polynomials? And why should we want to do that? As we mentioned in Remark 1.5.9, Macaulay's Basis Theorem is certainly the first step towards being able to compute in residue class modules P^r/M, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over a field. One gap still to be filled in is the lack of an algorithm which allows us to write a residue class as a linear combination of the residue classes of the terms contained in $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle \setminus \mathrm{LT}_\sigma \{M\}$.

Let us have a closer look at what happens for residue class rings of $K[x]$. In that case any given ideal is principal. Let $I \subseteq K[x]$ be a non-zero ideal and $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ a generator of I such that $a_d \neq 0$, i.e. such that $\deg(f) = d$. In Section 1.2 we have already mentioned division with remainder for univariate polynomials. By using this device, for any given polynomial g we get a representation $g = qf + p$, where p is either zero or a polynomial of degree less than d. This implies that every element in the ring $K[x]/(f)$ can be uniquely represented as a linear combination of the residue classes $1, \bar{x}, \ldots, \bar{x}^{d-1}$. The existence and uniqueness of this representation is a special instance of Macaulay's Basis Theorem, but the Division Algorithm for univariate polynomials allows us to effectively obtain it.

The topic of the present section is to conquer the multivariate case. As we shall see, there is no unique way to perform polynomial division in several indeterminates. Instead, the Division Algorithm tells us how much uniqueness we can expect and gives us an explicit way how to go about the computation. The result of dividing a vector $m \in P^r$ by a tuple of vectors $(g_1, \ldots, g_s)$ is a representation of the form $m = q_1 g_1 + \cdots + q_s g_s + p$ with $q_1, \ldots, q_s \in P$ and $p \in P^r$ having certain extra properties. The vector p is called the *normal remainder* of m with respect to $(g_1, \ldots, g_s)$. It has the drawback of depending both on the chosen module term ordering σ and the order of the elements in the tuple $(g_1, \ldots, g_s)$. Nevertheless, it will play a major role in Buchberger's Algorithm for computing Gröbner bases in Section 2.5.

In this section, we let K be a field, $n \geq 1$, $P = K[x_1, \ldots, x_n]$, $r \geq 1$, and σ a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$.

Example 1.6.1. In the case $K = \mathbb{Q}$, $n = r = 1$, and $P = K[x_1] = K[x]$, let us consider the polynomials $f = x^3 + 2x^2 + x + 1$ and $g = 2x + 1$. Then we can compute $\frac{f}{g}$ in the following way:

$$
\begin{array}{l}
x^3 \;+\; 2x^2 \;+\; x \;+\; 1 = g \cdot (\tfrac{1}{2}x^2 + \tfrac{3}{4}x + \tfrac{1}{8}) \ \text{ remainder } \ \tfrac{7}{8} \\
\underline{x^3 \;+\; \tfrac{1}{2}x^2} \\
\qquad \tfrac{3}{2}x^2 \;+\; x \;+\; 1
\end{array}
$$

$$\frac{\frac{3}{2}x^2 + \frac{3}{4}x}{\frac{1}{4}x + 1}$$
$$\frac{\frac{1}{4}x + \frac{1}{8}}{\frac{7}{8}}$$

In other words, we have $f = qg + p$ with $q = \frac{1}{2}x^2 + \frac{3}{4}x + \frac{1}{8}$ and $p = \frac{7}{8}$. The characteristic property of p is $\deg(p) < \deg(g)$.

When we are dealing with polynomials in two indeterminates, we can try to imitate this procedure and proceed as follows.

Example 1.6.2. Let $f = x_1^2 x_2 + x_1 x_2^2 + x_2^2$, $g_1 = x_1 x_2 - 1$, and $g_2 = x_2^2 - 1$ be three polynomials in $\mathbb{Q}[x_1, x_2]$. We are looking for polynomials q_1, q_2, and p such that $f = q_1 g_1 + q_2 g_2 + p$ and $\deg(p) < 2$. With that goal, we eliminate $\mathrm{LT}_{\mathtt{Lex}}(f)$ step by step as follows:

$$x_1^2 x_2 + x_1 x_2^2 + x_2^2 = \begin{cases} g_1 \cdot (x_1 + x_2) \\ g_2 \cdot (1) \end{cases} \qquad \text{remainder} \quad x_1 + x_2 + 1$$

$$\underline{x_1^2 x_2 - x_1}$$
$$x_1 x_2^2 + x_1 + x_2^2$$
$$\underline{x_1 x_2^2 - x_2}$$
$$x_1 + x_2^2 + x_2$$
$$\underline{x_2^2 - 1}$$
$$x_1 + x_2 + 1$$

Note that $\mathrm{LT}_{\mathtt{Lex}}(x_1 + x_2^2 + x_2) = x_1$ is not divisible by $\mathrm{LT}_{\mathtt{Lex}}(g_1)$ or $\mathrm{LT}_{\mathtt{Lex}}(g_2)$, so that it has to be added to the remainder. We obtain a representation $f = q_1 g_1 + q_2 g_2 + p$ such that $q_1 = x_1 + x_2$, $q_2 = 1$, and $p = x_1 + x_2 + 1$. Again we have $\deg(p) = 1 < 2 = \deg(g_1) = \deg(g_2)$.

Remark 1.6.3. The result of the procedure described in the previous example depends very much on the order of the elements g_1, g_2. For instance, if we let $g_1' = g_2$ and $g_2' = g_1$, we get a different result:

$$x_1^2 x_2 + x_1 x_2^2 + x_2^2 = \begin{cases} g_1' \cdot (x_1 + 1) \\ g_2' \cdot (x_1) \end{cases} \qquad \text{remainder} \quad 2x_1 + 1$$

$$\underline{x_1^2 x_2 - x_1}$$
$$x_1 x_2^2 + x_1 + x_2^2$$
$$\underline{x_1 x_2^2 - x_1}$$
$$2x_1 + x_2^2$$
$$\underline{x_2^2 - 1}$$
$$2x_1 + 1$$

In other words, we find a representation $f = q'_1 g'_1 + q'_2 g'_2 + p' = q'_2 g_1 + q'_1 g_2 + p'$ such that $q'_1 = x_1 + 1$, $q'_2 = x_1$, and $p' = 2x_1 + 1$.

The procedure described above can be extended to a very general situation. It provides us with the following algorithm. Note that whenever $t, t', t'' \in \mathbb{T}^n$ satisfy $t = t't''$, and for all $i \in \{1, \ldots, r\}$, we shall commit a slight abuse of notation and write $t'' = \frac{te_i}{t'e_i}$.

Theorem 1.6.4. (The Division Algorithm)
Let $s \geq 1$, and let $m, g_1, \ldots, g_s \in P^r \setminus \{0\}$. Consider the following sequence of instructions.

1) *Let $q_1 = \cdots = q_s = 0$, $p = 0$, and $v = m$.*
2) *Find the smallest $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(v)$ is a multiple of $\mathrm{LT}_\sigma(g_i)$. If such an i exists, replace q_i by $q_i + \frac{\mathrm{LM}_\sigma(v)}{\mathrm{LM}_\sigma(g_i)}$ and v by $v - \frac{\mathrm{LM}_\sigma(v)}{\mathrm{LM}_\sigma(g_i)} \cdot g_i$.*
3) *Repeat step 2) until there is no more $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(v)$ is a multiple of $\mathrm{LT}_\sigma(g_i)$. Then replace p by $p + \mathrm{LM}_\sigma(v)$ and v by $v - \mathrm{LM}_\sigma(v)$.*
4) *If now $v \neq 0$, start again with step 2). If $v = 0$, return the tuple $(q_1, \ldots, q_s) \in P^s$ and the vector $p \in P^r$.*

This is an algorithm which returns vectors $(q_1, \ldots, q_s) \in P^s$ and $p \in P^r$ such that
$$m = q_1 g_1 + \cdots + q_s g_s + p$$
and such that the following conditions are satisfied.

a) *No element of $\mathrm{Supp}(p)$ is contained in $\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle$.*
b) *If $q_i \neq 0$ for some $i \in \{1, \ldots, s\}$, then we have $\mathrm{LT}_\sigma(q_i g_i) \leq_\sigma \mathrm{LT}_\sigma(m)$.*
c) *For all indices $i = 1, \ldots, s$ and all terms t in the support of q_i, we have $t \cdot \mathrm{LT}_\sigma(g_i) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{i-1}) \rangle$.*

Moreover, the vectors $(q_1, \ldots, q_s) \in P^s$ and $p \in P^r$ satisfying the above conditions are uniquely determined by the tuple $(m, g_1, \ldots, g_s) \in (P^r)^{s+1}$.

Proof. First we observe that at each point in the Division Algorithm the equation
$$m = q_1 g_1 + \cdots + q_s g_s + p + v$$
holds, since in step 2) we have $q_i g_i + v = (q_i + \frac{\mathrm{LM}_\sigma(v)}{\mathrm{LM}_\sigma(g_i)})g_i + (v - \frac{\mathrm{LM}_\sigma(v)}{\mathrm{LM}_\sigma(g_i)}g_i)$, and in step 3) we have $p + v = (p + \mathrm{LM}_\sigma(v)) + (v - \mathrm{LM}_\sigma(v))$.

The algorithm stops after finitely many steps, because both in step 2) and in step 3) the leading term $\mathrm{LT}_\sigma(v)$ becomes strictly smaller with respect to σ. By Theorem 1.4.19, this can happen only finitely many times.

When the algorithm stops, we have $m = q_1 g_1 + \cdots + q_s g_s + p$. The vector p satisfies property a), since in step 3) a scalar multiple of a term is added to p only if that term is not a multiple of one of the terms $\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)$.

Now we prove by induction on the number of steps processed that we always have $\mathrm{LT}_\sigma(v) \leq_\sigma \mathrm{LT}_\sigma(m)$ and $\mathrm{LT}_\sigma(q_i g_i) \leq_\sigma \mathrm{LT}_\sigma(m)$ when $q_i \neq 0$.

This is obviously satisfied at the start of the algorithm. Every time step 2) is executed and the old and new values of q_i are not zero, we have the inequalities

$$\mathrm{LT}_\sigma\left((q_i + \tfrac{\mathrm{LM}_\sigma(v)}{\mathrm{LM}_\sigma(g_i)}) \cdot g_i\right) \leq_\sigma \max_\sigma\{\mathrm{LT}_\sigma(q_ig_i), \mathrm{LT}_\sigma(v)\} \leq_\sigma \mathrm{LT}_\sigma(m).$$

The same conclusion holds trivially if the old value of q_i was zero. Thus condition b) continues to hold throughout the algorithm.

Furthermore, condition c) is always satisfied, since in step 2) only scalar multiples of terms $t \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ are added to q_i for which $t \cdot \mathrm{LT}_\sigma(g_i)$ was not eliminated from v during an earlier execution of step 2), i.e. which are not a multiple of one of the terms $\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{i-1})$.

Finally, we show uniqueness. Suppose there are two representations $m = q_1g_1 + \cdots + q_sg_s + p = q_1'g_1 + \cdots + q_s'g_s + p'$ which satisfy conditions a), b), and c). Then we have

$$0 = (q_1 - q_1')g_1 + \cdots + (q_s - q_s')g_s + (p - p') \tag{$*$}$$

Condition a) implies that $\mathrm{LT}_\sigma(p - p') \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle$, and condition c) implies that $\mathrm{LT}_\sigma((q_i - q_i')g_i) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{i-1})\rangle$ for all $i \in \{1, \ldots, s\}$ with $q_i \neq q_i'$. Thus the leading terms of the summands in $(*)$ are pairwise different. In view of Rule 1.5.3.b, this is impossible unless $q_1 - q_1' = \cdots = q_s - q_s' = p - p' = 0$. □

Remark 1.6.5. Using the Division Algorithm, it is *not* always possible to decide whether the element $m \in P^r$ is contained in the submodule $\langle g_1, \ldots, g_s\rangle \subseteq P^r$. For instance, if $n = 2$, $r = 1$, $P = \mathbb{Q}[x_1, x_2]$, $m = x_1x_2^2 - x_1$, $g_1 = x_1x_2 + 1$, and $g_2 = x_2^2 - 1$, then we calculate with respect to `Lex` the following representation:

$$x_1x_2^2 - x_1 = \begin{cases} g_1 \cdot (x_2) \\ g_2 \cdot (0) \end{cases} \quad \text{remainder} \quad -x_1 - x_2$$

$$\underline{x_1x_2^2 + x_2}$$

$$-x_1 - x_2$$

Thus we find $m = q_1g_1 + q_2g_2 + p$ with $q_1 = x_2$, $q_2 = 0$, and $p = -x_1 - x_2 \neq 0$. But, in fact, the element $m = x_1 \cdot g_2$ is in the ideal $(g_1, g_2) \subseteq P$.

The Division Algorithm allows us to express the residue class of an element m modulo the submodule generated by $\{g_1, \ldots, g_s\}$ as a linear combination of those terms which are not multiples of any term in $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$. But the set of those terms is in general not the desired basis of P^r/M, as the following example shows.

Example 1.6.6. In the situation of Example 1.6.2, the Division Algorithm yields $f = (x_1 + x_2)g_1 + g_2 + (x_1 + x_2 + 1)$. If we use $g_1' = g_2$ and $g_2' = g_1$ as in Remark 1.6.3, we get $f = x_1 g_1 + (x_1 + 1)g_2 + (2x_1 + 1)$. Therefore we see that $x_1 - x_2 = (2x_1 + 1) - (x_1 + x_2 + 1)$ is an element of the ideal (g_1, g_2), i.e. that x_1 and x_2 have the same residue class in $P/(g_1, g_2)$.

But neither x_1 nor x_2 are multiples of any term in $\{\mathrm{LT}_\sigma(g_1), \mathrm{LT}_\sigma(g_2)\}$. Thus we cannot use $\mathbb{T}^2 \setminus (\mathrm{LT}_\sigma(g_1), \mathrm{LT}_\sigma(g_2))$ as a set of representatives of a K-basis of $P/(g_1, g_2)$.

We conclude this section with a definition which will be of fundamental importance when we discuss Buchberger's Algorithm (see Section 2.5).

Definition 1.6.7. Let $s \geq 1$, let $m, g_1, \ldots, g_s \in P^r \setminus \{0\}$, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$. We apply the Division Algorithm and obtain a representation $m = q_1 g_1 + \cdots + q_s g_s + p$ with $q_1, \ldots, q_s \in P$ and $p \in P^r$. Then the vector p is called the **normal remainder** of m with respect to $\mathcal{G}$ and is denoted by $\mathrm{NR}_{\sigma, \mathcal{G}}(m)$, or simply by $\mathrm{NR}_{\mathcal{G}}(m)$ if no confusion can arise. For $m = 0$, we let $\mathrm{NR}_{\mathcal{G}}(m) = 0$.

In other publications, the normal remainder of a vector is sometimes also called its **normal form** with respect to $\mathcal{G}$. However, we shall reserve the latter notion for a more special situation (see Section 2.4).

> **Exercise 1.** Let $n = 2$, let $P = K[x, y]$, and let $\sigma = \texttt{DegRevLex}$. Apply the Division Algorithm to divide f by (g_1, g_2) in the following cases.
> a) $f = x^2 + y^2$, $g_1 = xy - 1$, $g_2 = x^2 - xy$
> b) $f = x^7 - 1$, $g_1 = x^2 - y$, $g_2 = y^2 - x$
> c) $f = x^3 y^3 - x^3 - y^3$, $g_1 = xy^2 - x^2$, $g_2 = x^2 y - y^2$
>
> **Exercise 2.** Let $P = K[x_1, \ldots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, let $g \in P^r \setminus \{0\}$, and let $M = \langle g \rangle$ be the cyclic submodule of P^r generated by g.
> a) Prove that $\mathrm{LT}_\sigma(M) = \langle \mathrm{LT}_\sigma(g) \rangle$.
> b) Show that the residue classes of the terms contained in the set $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle \setminus \{t \cdot \mathrm{LT}_\sigma(g) \mid t \in \mathbb{T}^n\}$ form a K-basis of P^r/M.
> c) Conclude that $\dim_K(P^r/M) = \infty$ if $r > 1$.
> d) Show that, for every $m \in P^r$, the Division Algorithm yields the unique representation of the residue class of m modulo M in terms of the basis in b).
>
> **Exercise 3.** Let $f, g_1, g_2 \in P = K[x_1, x_2]$ be polynomials such that $g_1 \in K[x_1]$ and $g_2 \in K[x_2]$. Then show that $\mathrm{NR}_{(g_1, g_2)}(f) = \mathrm{NR}_{(g_2, g_1)}(f)$.
>
> **Exercise 4.** Give an example of four polynomials $f, g_1, g_2, g_3 \in \mathbb{Q}[x, y, z]$ and a term ordering σ such that the normal remainder of f with respect to $\mathcal{G} = (g_1, g_2, g_3)$ never has a degree $< \deg(f)$, no matter how $\mathcal{G}$ is ordered.
>
> **Exercise 5.** Let $f = y^2 z^2 - x^3 - x$, $g_1 = y^3 - x^2 - 1$, and $g_2 = xy - z^2$ be polynomials in $\mathbb{Q}[x, y, z]$, and let $\mathcal{G} = (g_1, g_2)$. Give an example of a term ordering σ on $\mathbb{T}^3$ such that $\mathrm{NR}_{\sigma, \mathcal{G}}(f) = 0$ and an example of a term ordering τ on $\mathbb{T}^3$ such that $\mathrm{NR}_{\tau, \mathcal{G}}(f) \neq 0$.

Tutorial 14: Implementation of the Division Algorithm

In this tutorial we consider several possibilities to implement versions of the Division Algorithm. As above, let K be a field, let $n \geq 1$, let $P = K[x_1, \ldots, x_n]$, let $r \geq 1$, let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, let $s \geq 1$, and let $g_1, \ldots, g_s \in P^r \setminus \{0\}$.

a) Program a CoCoA function $\texttt{Division}(\ldots)$ which takes a non-zero vector $m \in P^r$ and a list of non-zero vectors $G = [g_1, \ldots, g_s]$, performs the Division Algorithm, and computes a list $[[q_1, \ldots, q_s], p]$ corresponding to the representation $m = q_1 g_1 + \cdots + q_s g_s + p$ and having properties a), b), and c) of Theorem 1.6.4.

   Hint: For implementing step 2), you may want to use the CoCoA functions $\texttt{LPP}(\ldots)$ and $\texttt{LPos}(\ldots)$.

b) In the following cases, use $\texttt{Division}(\ldots)$ to compute representations as above. In all cases, use both $\texttt{PosLex}$ and $\texttt{DegRevLexPos}$. Check your answers by applying the built-in CoCoA function $\texttt{DivAlg}(\ldots)$.

   1) $n = 3$, $r = 2$, $m = (x_1^2 + x_2^2 + x_3^2, x_1 x_2 x_3)$, $g_1 = (x_1, x_2)$, $g_2 = (x_2, x_3)$, $g_3 = (x_3, x_1)$
   2) $n = r = 4$, $m = (x_1^4, x_2^4, x_3^4, x_4^4)$, $g_1 = (x_1 + 1, 0, 0, 0)$, $g_2 = (0, x_2 + 1, 0, 0)$, $g_3 = (0, 0, x_3 + 1, 0)$, $g_4 = (0, 0, 0, x_4 + 1)$
   3) $n = 2$, $r = 5$, $m = (x_1^4, x_1^3 x_2, x_1^2 x_2^2, x_1 x_2^3, x_2^4)$, $g_1 = (x_1^4, x_1^3, x_1^2, x_1, 1)$, $g_2 = (1, x_2, x_2^2, x_2^3, x_2^4)$

c) Given $m, g_1, \ldots, g_s \in P^r \setminus \{0\}$, consider the following sequence of instructions.

   1) Let $i = 1$ and $q_1 = \cdots = q_s = 0$.
   2) Find the largest term $t \in \text{Supp}(m)$ which is of the form $t = t' \, \text{LT}_\sigma(g_i)$ for some $t' \in \mathbb{T}^n$. If there exists such a term, let $c \in K \setminus \{0\}$ be its coefficient in m, replace m by $m - \frac{c}{\text{LC}_\sigma(g_i)} t' \, g_i$, and add $\frac{c}{\text{LC}_\sigma(g_i)} t'$ to q_i.
   3) Repeat step 2) as often as possible. When finally the intersection $\text{Supp}(m) \cap (\text{LT}_\sigma(g_i))$ is empty, increase i by one.
   4) If $i \leq s$, continue with step 2). Otherwise set $p = m$ and return the list $[q_1, \ldots, q_s, p]$.

   Show that this is an algorithm, i.e. that it stops after finitely many steps, and that it returns a list $[[q_1, \ldots, q_s], p]$ such that $q_1, \ldots, q_s \in P$, $p \in P^r$, and $m = q_1 g_1 + \cdots + q_s g_s + p$.

d) Give an example in which the representation calculated in c) does not have the properties required in Theorem 1.6.4.

e) Show that, if one repeats the algorithm of c) often enough (i.e. if one applies it to the element p instead of m, etc.), the representations of m one gets become eventually stable. Give an example in which this stable representation still does not agree with the representation calculated by the Division Algorithm.

f) Implement the algorithm of c) and the procedure described in e) in a CoCoA function `Division2(...)` and compare its efficiency with the function `Division(...)` by applying it to the test cases of b).

Tutorial 15: Normal Remainders

If we are only interested in the normal remainder of an element $m \in P^r$ with respect to a tuple of vectors $\mathcal{G}$, we can use a simplified version of the Division Algorithm which we want to examine in this tutorial.

Let K be a field, $P = K[x_1, \ldots, x_n]$ a polynomial ring over K, σ a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, and $\mathcal{G} = (g_1, \ldots, g_s) \in (P^r)^s$. To each vector $m \in P^r$, we can apply the **Normal Remainder Algorithm**.

1) Choose the largest term $t \in \mathrm{Supp}(m)$ with respect to σ which is divisible by one of the leading terms $\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)$. If no such term exists, return m and stop.
2) Find the minimal $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(g_i)$ divides t and write $t = t' \, \mathrm{LT}_\sigma(g_i)$ with $t' \in \mathbb{T}^n$.
3) Let $c \in K \setminus \{0\}$ be the coefficient of t in m. Replace m by $m - \frac{ct'}{\mathrm{LC}_\sigma(g_i)} g_i$ and continue with step 1).

As we shall see, for the purposes of Section 2.5, it will suffice to implement and use this algorithm.

a) Prove that the Normal Remainder Algorithm is an algorithm, i.e. that it stops after finitely many steps. Then compare it to the Division Algorithm and show that it returns $\mathrm{NR}_\mathcal{G}(m)$.
b) Write a CoCoA program `NormalRemainder(...)` which computes the normal remainder of an element $m \in P^r$ with respect to the list of vectors G using the above algorithm. Do not use the built-in function `NR(...)` of CoCoA.
c) Apply the program `NormalRemainder(...)` in the following cases, where $K = \mathbb{Q}$ and $\sigma = \mathtt{PosLex}$.
   1) $m = x_1^4 x_2 + x_2^4 x_3 + x_3^4 x_1 \in \mathbb{Q}[x_1, x_2, x_3]$, $g_1 = x_1^2 x_2$, $g_2 = x_2^2 x_3$, $g_3 = x_3^2 x_1$
   2) $m = (x_1^3 + 1, x_2^3 + 1, x_3^3 + 1) \in \mathbb{Q}[x_1, x_2, x_3]^3$, $g_1 = (x_1, x_2, x_3)$, $g_2 = (0, x_2, x_1)$
   3) $m = (x_1 x_2 + x_3 x_4, x_1 x_2 x_3 x_4) \in \mathbb{Q}[x_1, x_2, x_3, x_4]^2$, $g_1 = (x_1, 0)$, $g_2 = (x_2, 0)$, $g_3 = (0, x_3)$, $g_4 = (0, x_4)$
d) Give an example which shows that the normal remainder of an element $m \in P^r$ depends on the ordering of the elements in $\mathcal{G} = (g_1, \ldots, g_s)$.
e) Give an example of an element $m \in \langle g_1, \ldots, g_s \rangle \subseteq P^r$ such that $\mathrm{NR}_\mathcal{G}(m) \neq 0$. Show that if an element $m \in P^r$ does satisfy $\mathrm{NR}_\mathcal{G}(m) = 0$, then it is contained in the submodule $\langle g_1, \ldots, g_s \rangle \subseteq P^r$.

1.7 Gradings

> *The writer saw that some mathematicians*
> *call this lemma "Nakayama's lemma"*
> *and therefore the writer asked Nakayama, [...]*
> *what would be the best name for this lemma?*
> *Then, Nakayama kindly answered the writer*
> *that the name of Krull-Azumaya [...]*
> *would be the best name for the lemma.*
> (Masayoshi Nagata)

This section starts slowly and then tapers off. It mainly serves as a link between the first chapter and the subsequent ones. In the previous section we studied the Division Algorithm and tried to use it to effectively compute both a basis of a quotient module P^r/M and the representation of every residue class in terms of such a basis. We found that it does not solve the problem completely. How can we go on?

As happens many times in mathematics, new tools are needed. In particular, it will turn out to be important to have general notions of graded rings and modules available. So, in this section we introduce and study quite general kinds of gradings, namely rings graded over monoids and modules graded over monomodules. Two main results are that we characterize homogeneous ideals and graded submodules by the property that they have homogeneous sets of generators (see Proposition 1.7.10) and that it is possible to represent homogeneous elements in terms of those generators using homogeneous coefficients of complementary degree (see Corollary 1.7.11).

In the last part of the section, we prove two useful results about rings graded over monoids carrying a monoid ordering. We characterize homogeneous prime ideals (see Proposition 1.7.12), and we prove a graded version of a result which we call Nakayama's Lemma (see Proposition 1.7.15), following mathematical tradition and ignoring the wishes of its inventor. Although not all results in this section are given in their greatest generality, they will be general enough for our later applications, and Nakayama's Lemma will become one of the cornerstones of the second volume.

Recall that in this book all monoids and rings are assumed to be commutative. Throughout this section, let R be a ring and M an R-module.

Definition 1.7.1. Let $(\Gamma, +)$ be a monoid.

a) The ring R is called a Γ**-graded ring** (or a (R, Γ)**-graded ring**, or **graded over** Γ) if there exists a family of additive subgroups $\{R_\gamma\}_{\gamma \in \Gamma}$ such that

  1) $R = \oplus_{\gamma \in \Gamma} R_\gamma$,
  2) $R_\gamma \cdot R_{\gamma'} \subseteq R_{\gamma + \gamma'}$ for all $\gamma, \gamma' \in \Gamma$.

b) The elements of R_γ are called **homogeneous of degree** γ. For $r \in R_\gamma$ we write $\deg(r) = \gamma$.

c) If $r \in R$ and $r = \sum_{\gamma \in \Gamma} r_\gamma$ is the decomposition of r according to a.1), where $r_\gamma \in R_\gamma$, then r_γ is called the **homogeneous component** of degree γ of r.

If R is a Γ-graded ring, then 0 is a homogeneous element of R of every degree. Moreover, the decomposition of every element into its homogeneous components is unique, since in Definition 1.7.1.a we have a direct sum. If the cancellation law holds in Γ, then the set R_0 is a subring of R, and for every $\gamma \in \Gamma$ the set R_γ is an R_0-module.

The following two examples constitute the most important situations in which we shall meet Γ-graded rings.

Example 1.7.2. Let S be a ring, let $n \geq 1$, and let $P = S[x_1, \ldots, x_n]$ be a polynomial ring over S. If we let

$$P_d = \{f \in P \mid \deg(t) = d \text{ for all } t \in \text{Supp}(f)\}$$

for $d \geq 0$, we make P into an $\mathbb{N}$-graded ring. This grading is called the **standard grading** of P. It satisfies $\deg(x_1) = \cdots = \deg(x_n) = 1$. For $d \geq 0$, the elements of P_d are called **homogeneous polynomials** (or **forms**) of degree d.

Example 1.7.3. Let S be a ring, let $n \geq 1$, and let $P = S[x_1, \ldots, x_n]$ be a polynomial ring over S. For each $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, we let $P_{(\alpha_1, \ldots, \alpha_n)} = S \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. It is clear that in this way $P = \oplus_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n} P_{(\alpha_1, \ldots, \alpha_n)}$ becomes an $\mathbb{N}^n$-graded ring. We can also view P as a $\mathbb{Z}^n$-graded ring if we define $P_{(\alpha_1, \ldots, \alpha_n)} = 0$ for every $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ such that $\alpha_i < 0$ for some $i \in \{1, \ldots, n\}$.

A natural way to extend Definition 1.7.1 to cover R-modules would be to use the monoid Γ again as the set of possible degrees. As we shall see in Section 2.3, this is not sufficiently general, so that we have to resort to the following notion.

Definition 1.7.4. Let $(\Gamma, +)$ be a monoid, let R be a Γ-graded ring, let $(\Sigma, *)$ be a Γ-monomodule, and let M be an R-module. We say that M is a Σ-**graded** R-**module** (or a Σ-**graded** (R, Γ)-**module**, or simply a Γ-**graded** R-**module** if $\Sigma = \Gamma$) if there is a family of subgroups $\{M_s\}_{s \in \Sigma}$ such that

1) $M = \oplus_{s \in \Sigma} M_s$,
2) $R_\gamma \cdot M_s \subseteq M_{\gamma * s}$ for all $\gamma \in \Gamma$ and all $s \in \Sigma$.

For the remainder of this section, we let $(\Gamma, +)$ be a monoid in which the cancellation law holds, R a Γ-graded ring, $(\Sigma, *)$ a Γ-monomodule, and M a Σ-graded R-module. Then the set M_s is an R_0-module for every $s \in \Sigma$. Let us have a look at the quintessential example of a Σ-graded R-module.

Example 1.7.5. Let S be a ring, let $n \geq 1$, and let $P = S[x_1, \ldots, x_n]$ be a polynomial ring over S equipped with the $\mathbb{N}^n$-grading defined in Example 1.7.3. Via the isomorphism $\log : \mathbb{T}^n \longrightarrow \mathbb{N}^n$, we shall view this as a $\mathbb{T}^n$-grading. For $r \geq 1$, the set of terms $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ of the P-module P^r is a $\mathbb{T}^n$-monomodule. Now we let $(P^r)_{te_i} = Ste_i$ for $t \in \mathbb{T}^n$ and $1 \leq i \leq r$, i.e. for $te_i \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. It is easy to check that this makes P^r into a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded P-module.

Given a Σ-graded R-module, there exists a cheap way of making more Σ-graded R-modules called *shifting degrees*. Modules obtained by shifting degrees in R itself are the basic building blocks in the construction of graded free resolutions in Volume 2.

Definition 1.7.6. Let $\gamma \in \Gamma$ be a fixed element such that the multiplication map $\mu_\gamma : \Sigma \longrightarrow \Sigma$ defined by $s \mapsto \gamma * s$ is injective. For instance, if the left-cancellation law holds in Σ, this assumption is satisfied for all $\gamma \in \Gamma$.

a) For every $s \in \Sigma$, we define $M(\gamma)_s = M_{\gamma * s}$. Then we let $M(\gamma) = \oplus_{s \in \Sigma} M(\gamma)_s$. It is easy to check that in this way we get a Σ-graded R-module $M(\gamma)$. We call it the module obtained by **shifting degrees** by γ. If the map $\mu_\gamma : \Sigma \longrightarrow \Sigma$ is bijective, the set underlying $M(\gamma)$ agrees with M.

b) Modules of the form $\oplus_{i \in I} R(\gamma_i)$, where I is a set and $\gamma_i \in \Gamma$ for all $i \in I$, will be called Γ-**graded free** R-modules. Here we let $(\oplus_{i \in I} R(\gamma_i))_\gamma = \oplus_{i \in I} R(\gamma_i)_\gamma$ for all $\gamma \in \Gamma$.

Having defined Γ-graded rings and Σ-graded R-modules, we also need the appropriate sets of homomorphisms between those objects.

Definition 1.7.7. Let S be another ring which is graded over a monoid $(\Gamma', +)$, and let N be another Σ-graded R-module.

a) For a ring homomorphism $\varphi : R \to S$ and a homomorphism of monoids $\psi : \Gamma \to \Gamma'$, we call (φ, ψ) (or simply φ) a **homomorphism of graded rings** if $\varphi(R_\gamma) \subseteq S_{\psi(\gamma)}$ for every $\gamma \in \Gamma$.

b) An R-linear map $\lambda : M \to N$ is called a **homomorphism of Σ-graded R-modules** or a **homogeneous R-linear map** if $\lambda(M_s) \subseteq N_s$ for all $s \in \Sigma$.

For instance, let $\gamma \in \Gamma$ be an invertible element, and let $r \in R_\gamma$. Then the R-linear map $\mu_r : R(-\gamma) \to R$ defined by $r' \mapsto rr'$ is a homomorphism of graded R-modules.

Next we want to introduce the "correct" kind of subobjects of graded rings and modules. Note that if we equip $P = K[x]$ with the standard grading and let $I = (x - 1) \subseteq P$, then it is clear that $I \cap P_d = (0)$ for every $d \in \mathbb{N}$. Somehow this suggests that I does not "inherit" the grading of P. In other words, what we really need is that the canonical injective map $I \hookrightarrow P$ is a homomorphism of graded R-modules. Spelling this out in concrete terms, we arrive at the following definition.

Definition 1.7.8. An R-submodule N of the Σ-graded R-module M is called a Σ**-graded R-submodule** of M if we have $N = \oplus_{s \in \Sigma}(N \cap M_s)$.

A Γ-graded submodule of R is also called a Γ**-homogeneous ideal** of R, or simply a **homogeneous ideal** of R if Γ is clear from the context.

Remark 1.7.9. Let $N \subseteq M$ be a Σ-graded R-submodule. We can equip the residue class module M/N with the structure of a Σ-graded R-module by defining $(M/N)_s = M_s/N_s$ for every $s \in \Sigma$. Thus the canonical homomorphism $M \longrightarrow M/N$ becomes a homomorphism of Σ-graded R-modules. In particular, the residue class ring R/I of R by a homogeneous ideal is again a Γ-graded ring.

For practical purposes, the following proposition and its corollary are most useful. They allow us to quickly prove that some submodule is Σ-graded by exhibiting a homogeneous system of generators, and to use this fact to get "nice" representations of arbitrary homogeneous elements in terms of those homogeneous generators.

Proposition 1.7.10. *Let $N \subseteq M$ be an R-submodule, and let $N_s = N \cap M_s$ for all $s \in \Sigma$. Then the following conditions are equivalent.*

a) $N = \oplus_{s \in \Sigma} N_s$

b) *If $n \in N$ and $n = \sum_{s \in \Sigma} n_s$ is the decomposition of n into its homogeneous components, then $n_s \in N$ for all $s \in \Sigma$.*

c) *There is a system of generators of N which consists of homogeneous elements.*

Proof. First we show $a) \Rightarrow b)$. Choose an element $n \in N$ and let $n = \sum_{s \in \Sigma} n_s$ be its decomposition according to a), where $n_s \in N_s$ for all $s \in \Sigma$. Since $n_s \in N_s \subseteq M_s$ and $M = \oplus_{s \in \Sigma} M_s$, this is also the decomposition of n into its homogeneous components in M. Thus the homogeneous components of n lie in N.

Implication $b) \Rightarrow c)$ follows by taking all homogeneous components of a system of generators of N. Now we show $c) \Rightarrow a)$. Let $\{n_\beta \mid \beta \in B\}$ be a homogeneous system of generators of N and let $n \in N$. We write $n = \sum_{\beta \in B} r_\beta n_\beta$ with elements $r_\beta \in R$. For each $\beta \in B$ we decompose $r_\beta = \sum_{\gamma \in \Gamma} r_{\beta,\gamma}$ into its homogeneous components. Then

$$n = \sum_{\beta \in B} \sum_{\gamma \in \Gamma} r_{\beta,\gamma} n_\beta = \sum_{s \in \Sigma} \left(\sum_{\{(\beta,\gamma) \mid \gamma * \deg(n_\beta) = s\}} r_{\beta,\gamma} n_\beta \right) \in \sum_{s \in \Sigma} N_s$$

shows $N = \sum_{s \in \Sigma} N_s$, and from $M = \oplus_{s \in \Sigma} M_s$ we get that this sum is direct. $\square$

Corollary 1.7.11. *Suppose that the right-cancellation law holds in Σ. Let $N \subseteq M$ be a Σ-graded R-submodule, let $\{n_\beta \mid \beta \in B\}$ be a set of homogeneous generators of N, and let $s \in \Sigma$. Every element $n \in N_s$ has a representation $n = \sum_{\beta \in B} r_\beta n_\beta$ with homogeneous elements $r_\beta \in R$ such that $\deg(r_\beta) * \deg(n_\beta) = s$ for every $\beta \in B$.*

Proof. Let $n = \sum_{\beta \in B} a_\beta n_\beta$ with $a_\beta \in R$ for $\beta \in B$. We decompose a_β as the sum of its homogeneous components and group them by writing $a_\beta = a'_\beta + a''_\beta$, where a'_β is the unique homogeneous component of a_β such that $\deg(a'_\beta) * \deg(n_\beta) = s$. We get $n = \sum_{\beta \in B} a'_\beta n_\beta + \sum_{\beta \in B} a''_\beta n_\beta$. Equivalently, we have $0 = (\sum_{\beta \in B} a'_\beta n_\beta - n) + \sum_{\beta \in B} a''_\beta n_\beta$. By construction, the element $\sum_{\beta \in B} a'_\beta n_\beta - n$ is a homogeneous component of this sum, i.e. it has to be zero. $\qquad\square$

In the preceding proof we used the assumption that the right-cancellation law holds in Σ in order to have a'_β uniquely singled out by the relation $\deg(a'_\beta) * \deg(n_\beta) = s$. We leave the generalization to the reader (see Exercise 9).

For the remainder of this section, we shall assume that we are also given a monoid ordering τ on Γ. By Remark 1.4.2.b, this implies that the monoid Γ is infinite. We can characterize homogeneous prime ideals by the usual property applied to homogeneous elements only.

Proposition 1.7.12. *Let $\mathfrak{p}$ be a homogeneous proper ideal in R. Then the following conditions are equivalent.*

a) The ideal $\mathfrak{p}$ is a prime ideal.

b) If $fg \in \mathfrak{p}$ for homogeneous elements $f, g \in R$, then $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$.

Proof. It suffices to show that b) implies a). Let $f, g \in R$ be two elements such that $fg \in \mathfrak{p}$. We decompose them into their homogeneous components. If we allow some components to be zero, we may assume that the two sets of degrees are identical, i.e. that we have $f = f_{\gamma_1} + \cdots + f_{\gamma_s}$ and $g = g_{\gamma_1} + \cdots + g_{\gamma_s}$, where $\gamma_1 <_\tau \cdots <_\tau \gamma_s$. For a contradiction, we assume that the numbers $i = \min\{k \in \mathbb{N} \mid f_{\gamma_k} \notin \mathfrak{p}\}$ and $j = \min\{k \in \mathbb{N} \mid g_{\gamma_k} \notin \mathfrak{p}\}$ exist. Now we look at the homogeneous component of degree $\gamma_i + \gamma_j$ of fg. It is given by the formula

$$f_{\gamma_i} g_{\gamma_j} \; + \sum_{\{(k,l) \neq (i,j) \,\mid\, \gamma_k + \gamma_l = \gamma_i + \gamma_j\}} f_{\gamma_k} g_{\gamma_l}$$

Since $\gamma_k <_\tau \gamma_i$ or $\gamma_l <_\tau \gamma_j$ for every summand above, we have $k < i$ or $l < j$, and therefore $f_{\gamma_k} g_{\gamma_l} \in \mathfrak{p}$. Hence also $f_{\gamma_i} g_{\gamma_j}$ belongs to $\mathfrak{p}$, and the hypothesis implies $f_{\gamma_i} \in \mathfrak{p}$ or $g_{\gamma_j} \in \mathfrak{p}$, a contradiction. $\qquad\square$

Although neither of the two equivalent conditions in the previous proposition contains any reference to τ, the existence of such a monoid ordering is instrumental for the claim to hold, as our next example shows.

Example 1.7.13. Let $R = \mathbb{Z}[i]$ be the ring of Gaußian numbers (see Tutorial 4), i.e. the $\mathbb{Z}$-subalgebra of $\mathbb{C}$ generated by $\{i\}$. If we use the group $\Gamma = \mathbb{Z}/(2)$, we see that R is a Γ-graded ring with $R_0 = \mathbb{Z}$ and $R_1 = \mathbb{Z}i$. Let us consider the ideal $I = (2)$ in R. It is not a prime ideal, since

$(1-i)(1+i) = 2$ and neither $1-i$ nor $1+i$ is in I. However, if $f, g \in R$ are homogeneous elements such that $fg \in I$, then $f \in I$ or $g \in I$. In all four cases $f \in R_i$, $g \in R_j$ with $i, j \in \{1, 2\}$, this follows from the fact that 2 is a prime number.

Our last goal in this section is to prove a version of Nakayama's famous lemma adapted to graded modules. First, we need the following result.

Lemma 1.7.14. *If τ is a term ordering on Γ, then $R_+ = \oplus_{\gamma >_\tau 0} R_\gamma$ is a homogeneous ideal of R.*

Proof. It suffices to show $R \cdot R_+ \subseteq R_+$. This follows from the fact that every element is a finite sum of homogeneous elements, and for homogeneous elements $f \in R_\gamma$, $g \in R_{\gamma'}$ with $\gamma, \gamma' \in \Gamma$ and $\gamma' >_\tau 0$ we have $fg \in R_{\gamma + \gamma'}$ with $\gamma + \gamma' >_\tau \gamma \geq_\tau 0$ by Definition 1.4.1. $\square$

Proposition 1.7.15. (Graded Version of Nakayama's Lemma)
Let τ be a term ordering on Γ and σ a well-ordering on Σ which is compatible with τ. Suppose that the right-cancellation law holds in Σ. Let M_1, M_2 be two Σ-graded R-submodules of M such that $M_1 \subseteq M_2 \subseteq M_1 + R_+ \cdot M_2$. Then $M_1 = M_2$.

Proof. It suffices to show $M_2 \subseteq M_1$. Suppose that this is not the case. By Proposition 1.4.18, there exists a homogeneous element $m \in M_2 \setminus M_1$ of minimum degree with respect to σ. Using the hypothesis and Corollary 1.7.11, we see that there exist homogeneous elements $m' \in M_1$, $g_1, \ldots, g_s \in M_2$, and $f_1, \ldots, f_s \in R_+$ such that $m = m' + \sum_{i=1}^{s} f_i g_i$ and such that $\deg(f_i) * \deg(g_i) = \deg(m)$ for $i = 1, \ldots, s$. Since $\deg(f_i) >_\tau 0$ for $i = 1, \ldots, s$, the degrees of the elements $g_1, \ldots, g_s$ are less than the degree of m. The choice of m then implies $g_1, \ldots, g_s \in M_1$. Consequently, we get $m \in M_1$, a contradiction. $\square$

Corollary 1.7.16. *Let τ be a term ordering on Γ and σ a well-ordering on Σ which is compatible with τ. Suppose that the right-cancellation law holds in Σ.*

a) *A set of homogeneous elements $m_1, \ldots, m_s \in M$ generates the R-module M if and only if their residue classes $\overline{m}_1, \ldots, \overline{m}_s$ in $M/(R_+ \cdot M)$ generate this residue class module.*

b) *If R_0 is a field, every homogeneous system of generators of M contains a minimal one.*

Proof. To prove a), it suffices to show the implication "$\Leftarrow$". Let N be the graded submodule of M generated by $\{m_1, \ldots, m_s\}$. By assumption we have $M \subseteq N + R_+ \cdot M$. Therefore Nakayama's Lemma yields $M = N$.

The proof of b) follows from a), from $R/R_+ \cong R_0$, and from the fact that every system of generators of the R_0-module $M/(R_+ \cdot M)$ contains a basis. $\square$

Exercise 1. Let Γ be a monoid in which the cancellation law holds, and let R be a Γ-graded ring. Prove that $1 \in R_0$.
Hint: Write $1 = \sum_{\gamma \in \Gamma} r_\gamma$ and show that $r_0 = 1$.

Exercise 2. Let $\Gamma = \{0, \infty\}$ be the monoid defined in Exercise 2 of Section 1.3, and let R be a ring.

a) Define $\deg(r) = \infty$ for all $r \in R$. Show that this makes R into a Γ-graded ring in which the element 1 is homogeneous of some non-zero degree.

b) Equip $S = R \oplus R$ with componentwise addition and multiplication, and let $S_0 = R \oplus 0$ as well as $S_\infty = 0 \oplus R$. Show that this makes S into a Γ-graded ring in which the element $1 = (1, 1)$ is *not* homogeneous.

Exercise 3. Let R be a ring, let $P = R[x_1, \ldots, x_n]$, and let $r \geq 1$. Check that the definition $P_t = R \cdot t$ for $t \in \mathbb{T}^n$ makes P into a $\mathbb{T}^n$-graded ring, and that P^r together with the grading defined in Example 1.7.5 is a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded P-module.

Exercise 4. Let K be a field, let $R = K[x]$, let $\Gamma = \mathbb{N}$, and let $R_\gamma = \{c(x-1)^\gamma \mid c \in K\}$ for all $\gamma \in \Gamma$.

a) Show that R is a Γ-graded ring.

b) Prove that $I = (x)$ is not a homogeneous ideal of R.

c) Give an example of a homogeneous ideal of R.

Exercise 5. Check that the set $M(\gamma) = \oplus_{s \in \Sigma} M(\gamma)_s$, as introduced in Definition 1.7.6, is indeed a Σ-graded R-module. Then consider an element $r \in R_\gamma$ and the map $M \longrightarrow M(\gamma)$ defined by $m \mapsto rm$, and show that it is a homomorphism of Σ-graded R-modules.

Exercise 6. Let K be a field, let $R = K[x_1, x_2]$, let $\Gamma = \mathbb{N}^2$, and let $R_{(\alpha_1, \alpha_2)} = \{cx_1^{\alpha_1} x_2^{\alpha_2} \mid c \in K\}$ for $(\alpha_1, \alpha_2) \in \mathbb{N}^2$ as in Example 1.7.3. Furthermore, let $\Gamma' = \mathbb{N}$ and let $R_{\gamma'}$ be the K-vector space generated by $\{x_1^{\alpha_1} x_2^{\alpha_2} \mid \alpha_1 + \alpha_2 = \gamma'\}$ for $\gamma' \in \Gamma'$. In this way, R becomes both a Γ- and a Γ'-graded ring. Finally, let $\varphi : R \to R$ be the identity map and $\psi : \Gamma \to \Gamma'$ the map defined by $\psi((\alpha_1, \alpha_2)) = \alpha_1 + \alpha_2$. Show that (φ, ψ) is a homomorphism of graded rings.

Exercise 7. Let R be a Γ-graded ring and $S \subseteq R$ a subring. Discuss whether and how one can equip S with a Γ-grading in such a way that the inclusion $S \hookrightarrow R$ becomes a homomorphism of graded rings.

Exercise 8. Let Γ be a monoid in which the cancellation law holds. A Γ-graded ring $R = \oplus_{\gamma \in \Gamma} R_\gamma$ is called a Γ-**graded field** if every homogeneous element of $R \setminus \{0\}$ is a unit. Let R be a Γ-graded field.

a) Prove that R_0 is a field, and that for every $\gamma \in \Gamma$ the R_0-vector space R_γ has dimension ≤ 1. (*Hint:* Use Exercise 1.)

b) Give an example of a Γ-graded field which is not a field. (*Hint:* Consider the ring $K[x, x^{-1}]$.)

c) Show that $\{\gamma \in \Gamma \mid R_\gamma \neq 0\}$ is a group.

d) Let M be a finitely generated Γ-graded R-module. Prove that M has an R-basis consisting of homogeneous elements. (*Hint:* Start with a minimal homogeneous system of generators and show that it is a basis.)

Exercise 9. Modify the statement of Corollary 1.7.11 to generalize it to the case of a monomodule Σ in which the right-cancellation law does not necessarily hold.

Exercise 10. Give an example of a ring R graded over a monoid $(\Gamma, +)$ such that there exists a monoid order σ on Γ, but $R_+ = \oplus_{\gamma >_\sigma 0} R_\gamma$ is not an ideal of R.

Tutorial 16: Homogeneous Polynomials

Recall that the standard grading on the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K was defined by $P_d = \{f \in P \mid \deg(t) = d \text{ for all } t \in \text{Supp}(f)\}$ for $d \in \mathbb{N}$ in Example 1.7.2, and that the elements of P_d are called homogeneous polynomials of degree d.

In this tutorial we want to get a better understanding of the space P_d of homogeneous polynomials of degree d. We want to know its dimension and to characterize its elements.

a) Show that P_d is a K-vector space of dimension $\binom{n+d-1}{d}$ for all $d \in \mathbb{N}$.
b) Find and prove a formula which computes the dimension of the quotient vector space of P_d/V, where V is the subspace of polynomials which are divisible by x_1.
c) Let K be an infinite field. Suppose that $f \in P$ satisfies $f(a_1, \ldots, a_n) = 0$ for every $(a_1, \ldots, a_n) \in K^n$. Then show that $f = 0$.
d) Produce an example which shows that the above statement is false if K is finite.
e) Prove that if $f \in P$ is a non-zero homogeneous polynomial of degree d, then $f(\lambda a_1, \ldots, \lambda a_n) = \lambda^d \cdot f(a_1, \ldots, a_n)$ holds for all $\lambda \in K$ and all $(a_1, \ldots, a_n) \in K^n$.
f) Prove that the converse of e) holds if K has at least $\max\{\deg(f), d\} + 1$ elements.

Now consider the following non-standard grading on $P = K[x_1, x_2]$. We declare x_1 to be homogeneous of degree 2 and x_2 to be homogeneous of degree 1. Then we let $P_d = \{f \in P \mid 2\alpha_1 + \alpha_2 = d \text{ for all } x_1^{\alpha_1} x_2^{\alpha_2} \in \text{Supp}(f)\} \cup \{0\}$ for all $d \in \mathbb{N}$.

g) Prove this definition makes P into a $\mathbb{N}$-graded ring.
h) Explicitly describe the function from $\mathbb{N}$ to $\mathbb{N}$ which maps d to $\dim_K(P_d)$, i.e. find a formula for $\dim_K(P_d)$.
i) Modify e) above to fit this case.

2. Gröbner Bases

Towards the end of Chapter 1 we encountered Macaulay's Basis Theorem. It says that, given a polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K and a P-submodule M of P^r, one can attack the problem of computing a K-basis of the quotient module P^r/M if one knows $\mathrm{LT}_\sigma(M)$ for some term ordering σ. But we saw that the leading terms of a set of generators of M do not necessarily generate $\mathrm{LT}_\sigma(M)$.

Thus the opening sections of this chapter are variations on the theme that *not all systems of generators of a module are equal. Some are more special than others.* In Section 2.1 we find that the leading terms of a system of non-zero generators $\{g_1, \ldots, g_s\}$ of M generate $\mathrm{LT}_\sigma(M)$ if and only if it is special in the following sense: for every $m \in M \setminus \{0\}$ there exists a representation $m = \sum_{i=1}^s f_i g_i$ with $f_1, \ldots, f_s \in P$ such that $\mathrm{LT}_\sigma(m) \geq_\sigma \mathrm{LT}_\sigma(f_i g_i)$ for all $i = 1, \ldots, s$ such that $f_i \neq 0$.

Then we change our strategy and attack systems of generators from another side. Given a term ordering σ on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$, every element $g \in P^r \setminus \{0\}$ can be split as $g = \mathrm{LM}_\sigma(g) - g'$. By looking at this equation modulo $\langle g \rangle$, we can view g as a *rewrite rule*, namely the rule which substitutes $\mathrm{LM}_\sigma(g)$ with the element g' which represents the same residue class. If we have a bunch of non-zero vectors $\{g_1, \ldots, g_s\}$, we get a bunch of rewrite rules. What kind of game can we play with those rules?

Suppose a vector $m \in P^r$ contains a term in its support which is a multiple of $\mathrm{LT}_\sigma(g_i)$ for some $i \in \{1, \ldots, s\}$. Then we can use the rule associated to g_i and rewrite m. The element obtained in this way is congruent to m modulo M. The procedure of moving from one representative of this residue class to another resembles the division algorithm. However, at each point we may have several moves available, and a different order of those moves could lead to a different result. A generating set $\{g_1, \ldots, g_s\}$ of M is special if, no matter which order you choose, you always arrive at the same result. In Section 2.2, we treat rewrite rules and prove the surprising fact that this new kind of specialty is equivalent to the ones described before.

However, the most fundamental motive for looking at special systems of generators is still missing. The notion of a syzygy of a tuple $(g_1, \ldots, g_s)$ is

one of the decisive ideas for successful applications of Computational Commutative Algebra. Using the theory of gradings developed in Section 1.7, we show that every syzygy of $(\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s))$ can be lifted to a syzygy of $(g_1, \ldots, g_s)$ if and only if $\{g_1, \ldots, g_s\}$ has the special properties discussed earlier.

After threatening to do it for a long time, we finally combine all those ideas and introduce Gröbner bases. A Gröbner basis of a submodule M of P^r is a set of generators which is special in one (and therefore all) of the above ways. In Section 2.4 we launch an investigation into their properties and uses by showing that their existence can be viewed as a consequence of Dickson's Lemma. Most applications of Gröbner bases will be treated in Chapter 3 and Volume 2, but some rewards for our careful preparations can be reaped immediately, for instance a proof of Hilbert's Basis Theorem, the notion of normal forms, the submodule membership test, and a new version of Macaulay's Basis Theorem.

Next we put a great emphasis on the derived notion of a reduced Gröbner basis. It has the astonishing property that, given a submodule M of P^r and a term ordering σ, it is a unique system of generators of M satisfying certain natural conditions. We believe that this is one of the most ubiquitous theoretical tools in Computational Commutative Algebra. Just to give the flavour of its importance, we show how one can use it to deduce a seemingly unrelated result about the existence and uniqueness of the field of definition of submodules of P^r.

After all this theory, it is time to explain how one can actually step into action and compute a Gröbner basis of M from a given finite set of generators. The power of our study of syzygies enables us to capture the spirit of Buchberger's Algorithm in Section 2.5. Not only shall we prove and improve its basic procedure, but we shall also finally achieve our goal of effectively computing in residue class modules via Macaulay's Basis Theorem and normal forms.

As sometimes happens in real life, including science, the discovery of a tool which enables us to solve one problem opens the door to many other discoveries. Gröbner bases are certainly one of those tools, but before delving into the realm of their applications, we close the chapter with another one, namely Hilbert's Nullstellensatz. This theorem is one of the milestones in the process of translating algebra into geometry and geometry into algebra and forms the background for many applications in algebraic geometry. Section 2.6 is entirely devoted to its proof, which also uses some pieces of Gröbner basis theory. It highlights the importance of switching from one ground field to a field extension, so that the geometric notion of an affine variety gets its proper perspective.

Once more the chapter closes with an *opening theme*. Besides being a metaphor of life, this end of one struggle already lays the groundwork for successful applications in subsequent chapters.

2.1 Special Generation

> *All animals are equal.*
> *But some animals are more equal than others.*
> (George Orwell)

Let f be a non-zero polynomial and g a non-zero polynomial in the principal ideal generated by f, i.e. let $g = hf$ for a suitable polynomial h. If σ is a monoid ordering on $\mathbb{T}^n$, then $\mathrm{LT}_\sigma(g) = \mathrm{LT}_\sigma(hf) = \mathrm{LT}_\sigma(h)\,\mathrm{LT}_\sigma(f)$. In other words, the leading term of every element in the principal ideal generated by f is in the ideal generated by $\mathrm{LT}_\sigma(f)$.

On the other hand, let us go back for a moment to Example 1.5.5. We saw that for $f = y(x^2 - 1) - x(xy - 1) = x - y$ and $\sigma = \texttt{DegLex}$ the leading monomials of the two summands cancel out, so that x, the leading term of the result, is smaller than the leading terms of the summands. This shows that some generators have a special behaviour with respect to the leading terms of the elements they generate. More precisely, we see that $x = \mathrm{LT}_\sigma(f) \notin (\mathrm{LT}_\sigma(x^2 - 1), \mathrm{LT}_\sigma(xy - 1)) = (x^2, xy)$. However, if we add in this example the elements guaranteed by Proposition 1.5.6.b, we get another set of generators of the ideal $(x^2 - 1, xy - 1)$ whose leading terms generate the leading term ideal.

This is the prototypical case of the phenomenon that *not all systems of generators of an ideal or module are equal* alluded to in the introduction of this chapter. Some systems of generators have special properties which we want to describe in this and the following sections. Later it will become clear that all of those properties are incarnations of the same concept, namely the concept of Gröbner bases.

As usual, we let K be a field, $n \geq 1$, $P = K[x_1, \ldots, x_n]$ a polynomial ring, $r \geq 1$, and σ a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$.

Proposition 2.1.1. (Special Generation of Submodules)
Let $M \subseteq P^r$ be a P-submodule, and let $g_1, \ldots, g_s \in P^r \setminus \{0\}$. Then the following conditions are equivalent.

A_1) *For every element $m \in M \setminus \{0\}$, there are $f_1, \ldots, f_s \in P$ such that $m = \sum_{i=1}^s f_i g_i$ and $\mathrm{LT}_\sigma(m) \geq_\sigma \mathrm{LT}_\sigma(f_i g_i)$ for all $i = 1, \ldots, s$ such that $f_i g_i \neq 0$.*

A_2) *For every element $m \in M \setminus \{0\}$, there are $f_1, \ldots, f_s \in P$ such that $m = \sum_{i=1}^s f_i g_i$ and $\mathrm{LT}_\sigma(m) = \max_\sigma\{\mathrm{LT}_\sigma(f_i g_i) \mid i \in \{1, \ldots, s\}, f_i g_i \neq 0\}$.*

Proof. Since Condition A_2) obviously implies A_1), it suffices to prove the reverse direction. The inequality "$\geq_\sigma$" in A_2) follows immediately from A_1). The inequality "$\leq_\sigma$" in A_2) follows from Proposition 1.5.3.a. $\qquad \square$

If $M \subseteq P^r$ is a P-submodule and $g_1, \ldots, g_s \in M \setminus \{0\}$, then Conditions A_1) and A_2) say that $\{g_1, \ldots, g_s\}$ is a special system of generators of M. Using the example mentioned above, we see that it is not true that

Conditions A_1) and A_2) hold for every system of generators of M, because $\mathrm{LT}_\sigma(f) <_\sigma \max_\sigma\{x^2, xy\} \leq_\sigma \max_\sigma\{\mathrm{LT}_\sigma(f_1(x^2-1)), \mathrm{LT}_\sigma(f_2(xy-1))\}$, independent of which elements $f_1, f_2 \in P \setminus \{0\}$ we choose.

It is also interesting to observe that if τ is a term ordering on $\mathbb{T}^n$ and σ is a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ which is compatible with τ, then we can expand $\mathrm{LT}_\sigma(f_i g_i) = \mathrm{LT}_\tau(f_i)\,\mathrm{LT}_\sigma(g_i)$ in the above statements.

The intuitive meaning of Conditions A_1) and A_2) is that every element $m \in M \setminus \{0\}$ should have a representation $m = \sum_{i=1}^s f_i g_i$ such that the highest term which occurs in the computation of the right-hand side does not cancel. Consequently, the leading term of m is a multiple of one of the terms $\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)$. Now we examine this last property more closely.

Proposition 2.1.2. (Generation of Leading Term Modules)
Let $M \subseteq P^r$ be a P-submodule and $g_1, \ldots, g_s \in M \setminus \{0\}$. Then the following conditions are equivalent.

B_1) *The set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ generates the $\mathbb{T}^n$-monomodule $\mathrm{LT}_\sigma\{M\}$.*
B_2) *The set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ generates the P-submodule $\mathrm{LT}_\sigma(M)$ of P^r.*

Proof. Since B_1) implies B_2) by definition, it suffices to show the reverse direction. Let $m \in M \setminus \{0\}$, and let $\mathrm{LT}_\sigma(m) = f_1\,\mathrm{LT}_\sigma(g_1) + \cdots + f_s\,\mathrm{LT}_\sigma(g_s)$ for some polynomials $f_1, \ldots, f_s \in P$. By Proposition 1.5.3.a, the term $\mathrm{LT}_\sigma(m)$ is in the support of one of the vectors $f_1\,\mathrm{LT}_\sigma(g_1), \ldots, f_s\,\mathrm{LT}_\sigma(g_s)$. Thus there is an index $i \in \{1, \ldots, s\}$ and a term $t \in \mathrm{Supp}(f_i)$ such that $\mathrm{LT}_\sigma(m) = t \cdot \mathrm{LT}_\sigma(g_i)$. $\square$

Finally, we show the first important link between the two properties of special systems of generators which we have described so far.

Proposition 2.1.3. *Let $M \subseteq P^r$ be a P-submodule, and let $g_1, \ldots, g_s$ be non-zero elements of M. Then Conditions A_1), A_2) of Proposition 2.1.1 and Conditions B_1), B_2) of Proposition 2.1.2 are equivalent.*

Proof. Condition A_2) implies B_1) by Proposition 1.5.3.d. Thus we show $B_1) \Rightarrow A_1$). Suppose there exists an element $m \in M \setminus \{0\}$ which cannot be represented in the desired way. By Theorem 1.4.19, there exists such an element m with minimal leading term with respect to σ. By B_1), we have $\mathrm{LT}_\sigma(m) = t \cdot \mathrm{LT}_\sigma(g_i)$ for some $i \in \{1, \ldots, s\}$ and some $t \in \mathbb{T}^n$. Clearly, we have $m - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_i)} t g_i \neq 0$, since $m = \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_i)} t g_i$ would be a representation satisfying A_1). Therefore we find $\mathrm{LT}_\sigma(m - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_i)} t g_i) <_\sigma \mathrm{LT}_\sigma(m)$, and the element $m - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_i)} t g_i \in M \setminus \{0\}$ can be represented as required in A_1). But then also m can be represented as required in A_1), in contradiction with our assumption. $\square$

Exercise 1. Give an example of a term ordering σ, a module $M \subseteq P^r$, and a set of elements $\{g_1, \ldots, g_s\} \subseteq P^r \setminus M$ which satisfies Conditions A_1) and A_2).

Exercise 2. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, let $g_1, g_2 \in P$ be two K-linearly independent linear polynomials, and let $i_1, i_2 \in \{1, \ldots, n\}$ be such that $x_{i_1} = \mathrm{LT}_\sigma(g_1)$ and $x_{i_2} = \mathrm{LT}_\sigma(g_2)$. Prove that the following conditions are equivalent.

  a) Conditions A_1) and A_2) hold for g_1, g_2.
  b) $x_{i_1} \neq x_{i_2}$

Exercise 3. Prove that for $r = 1$ and $\sigma = \mathtt{RevLex}$, Conditions B_1) and B_2) are strictly weaker than A_1) and A_2).

Exercise 4. Let $r = 1$ and $\sigma = \mathtt{DegLex}$. Show that the polynomials $g_1 = x_1 x_2 - x_2$ and $g_2 = x_1^2 - x_2$ do not have properties B_1) and B_2). Find $\mathrm{LT}_{\mathtt{DegLex}}((g_1, g_2))$ and a third polynomial $g_3 \in (g_1, g_2)$ such that $\{g_1, g_2, g_3\}$ satisfies B_1) and B_2).

Exercise 5. Let σ be a term ordering on $\mathbb{T}^2$, and let $g_1 = x^3 - 1$ and $g_2 = y^3 - y$. Prove that $\{g_1, g_2\}$ satisfies B_1) and B_2). Represent $f = x^3 y + xy^3 - x^3 - xy - y + 1$ as a combination of g_1 and g_2 according to Condition A_1).

Tutorial 17: Minimal Polynomials of Algebraic Numbers

In this tutorial we let K be a field and $L = K[x]/(f)$ a finite extension field of K, where $f \in K[x]$ is an irreducible polynomial of degree d. We represent an element $\ell \in L$ as the residue class of a polynomial $g \in K[x]$ and ask the following question.

     How can one compute the minimal polynomial of ℓ over K?

   Below we shall develop two elementary approaches to this question. In Section 3.6, we shall see a more general method for determining the minimal polynomial of an element in an arbitrary finitely generated K-algebra.

  a) Let $\bar{x}$ be the residue class of x in L. Show that $\{1, \bar{x}, \ldots, \bar{x}^{d-1}\}$ is a K-basis of L and conclude that the minimal polynomial of ℓ over K has degree $\leq d$.
  b) For $i = 0, \ldots, d$, let $a_i \in K$ be the coefficient of x^i in the minimal polynomial of ℓ over K and $h_i \in K[x]$ the remainder of the division of g^i by f. Prove $a_0 + a_1 h_1 + \cdots + a_d h_d = 0$ and show that this yields a system of d linear equations for $a_0, \ldots, a_d$. Explain how we can use its solution space to answer our question.
  c) Implement the method developed in b) in a CoCoA function `LinAlgMP(...)` which takes f and g and computes the minimal polynomial of ℓ over K. *Hint:* You may use the CoCoA function `Syz(...)` to find the solution space of a system of linear equations.

d) Apply your function `LinAlgMP(...)` to compute the minimal polynomials over $\mathbb{Q}$ of the following algebraic numbers.
   1) $\frac{1}{2} + \frac{i}{2}\sqrt{3}$
   2) $\sqrt[4]{2} + \sqrt{2} + 2$
   3) $(\bar{x}^3 + \bar{x} - 1)/\bar{x}$, where $f = x^5 - x - 2$. (*Hint:* Notice that $\frac{1}{\bar{x}} = \frac{1}{2}\bar{x}^4 - \frac{1}{2}$.)

e) Now we consider the ideal $I = (x_2 - g(x_1), f(x_1)) \subseteq K[x_1, x_2]$. Prove that a polynomial $h \in K[x_2]$ satisfies $h(\ell) = 0$ if and only if $h \in I$. Conclude that the minimal polynomial of ℓ over K is an element of minimal degree in the principal ideal $I \cap K[x_2]$. (*Hint:* Show that $K[x_1, x_2]/I \cong L$.)

f) Prove that $\mathrm{LT}_{\mathtt{Lex}}(I)$ contains a power of x_2. Conclude that, in order to find the minimal polynomial of ℓ over K, it suffices to compute a system of generators of I which satisfies Conditions $B_1)$ and $B_2)$ with respect to `Lex`.

g) Write a CoCoA function `LexMP(...)` which takes f and g and computes the minimal polynomial of ℓ over K using the method developed in f). (*Hint:* You may assume that the base ring is $\mathbb{Q}[\mathtt{x[1]}, \mathtt{x[2]}]$, `Lex` and apply the CoCoA function `LT(I)`.) Use your function `LexMP(...)` to check your results in d).

h) Compute the minimal polynomial of $(\bar{x}^3 + \bar{x} - 1)/\bar{x}^5$ over $\mathbb{Q}$ in the case $f = x^7 - x - 1$ using both `LinAlgMP(...)` and `LexMP(...)`. Write down the two polynomials whose leading terms generate $\mathrm{LT}_{\mathtt{Lex}}(I) = (x_1, x_2^7)$. Which of the two methods is in general more efficient? Why?

i) Develop different methods for computing the representation of ℓ^{-1} in the K-basis $\{1, \bar{x}, \ldots, \bar{x}^{d-1}\}$ of L using the following ideas.
   1) Linear Algebra
   2) The Extended Euclidean Algorithm

   Prove the correctness of your methods. Then write two CoCoA functions `LinAlgInv(...)` and `ExtEucInv(...)`, and compare the results in the cases of d).

2.2 Rewrite Rules

All roads lead to Rome.
(Roman Proverb)
All roads do not lead to Rome.
(Slovenian Proverb)

Let us go back to the Division Algorithm discussed in Section 1.6 and try to understand its working more deeply. What is its essence? If we look at Theorem 1.6.4, we see that the event which triggers steps 2) and 3) is the detection of a term in the support of m which is a multiple of one of the leading terms $LT_\sigma(g_1), \ldots, LT_\sigma(g_s)$. Once such a term is found, the basic operation is to replace it by smaller terms.

A closer look at what happens is provided by the following example. Let $f = x^2 y$, $g_1 = x^2 - x + 1$, $g_2 = xy - x - y + 3$, and let $\sigma = \mathtt{DegLex}$. Since $x^2 y$ is a multiple of $LT_\sigma(g_1)$, the first step of the Division Algorithm applied to f and (g_1, g_2) yields $f = y \cdot g_1 + 0 \cdot g_2 + (f - yg_1)$, and we find $f - yg_1 = y(x - 1)$. In this first step we have replaced f by $f - yg_1$. The core of this operation is to take g_1, write it as $x^2 - (x - 1)$, and replace x^2 by $x - 1$. Thus we use g_1 as a rule for replacing its *head*, namely x^2, by its *tail*, namely $x - 1$. Clearly, if a polynomial g_1 is written as $a - b$, we have $a = b \bmod (g_1)$, but here we emphasize the fact that $a = b \bmod (g_1)$ can be viewed as a rule for replacing a by b. In other words, we orient the equality by destroying its symmetry in order to use a polynomial as a *rewrite rule*.

Now we continue with the Division Algorithm. First we observe that $LT_\sigma(xy - y) = xy$ is a multiple of $LT_\sigma(g_2)$. So the second step yields $f = y \cdot g_1 + 1 \cdot g_2 + (f - yg_1 - g_2)$ and $f - yg_1 - g_2 = x - 3$. Again we stress the point that the core of this operation is to use g_2 as a rewrite rule in the sense that its leading term xy is replaced by its tail $x + y - 3$. Here the Division Algorithm stops.

Suppose instead that we perform the Division Algorithm with respect to f and (g_2, g_1). Then we get $f = (x+1) \cdot g_2 + 1 \cdot g_1 + (f - (x+1)g_2 - g_1)$, and we see that $f - (x + 1)g_2 - g_1 = -x + y - 4$. The algorithm stops and returns an output which is not the same as before.

Summarizing, we can say that the core of the Division Algorithm is to use the elements $g_1, \ldots, g_s$ as rewrite rules. To use g_i as a rewrite rule means to replace the leading term of g_i by the remaining part of it, with the obvious adjustment if g_i is not monic. Of course we should be allowed to use the rewrite rules repeatedly. But in the Division Algorithm the rewrite rules have a well defined hierarchy, i.e. the application of the first rewrite rule is preferred to the second one, and so on. If we have the possibility of using several rewrite rules at a certain point, the Division Algorithm forces us to use the first one in the hierarchy.

What happens if we destroy this hierarchy? Then we are allowed to use at each step any applicable rewrite rule, but the drawback is immediately clear. A look at the previous example convinces us that different possible paths

may lead to different results. So the natural question is whether there are sets of rewrite rules such that all possible paths can be continued until they reach the same result. "Confluence" is the name of this game and the essence of this section, a modern version of the motto *"all roads lead to Rome"*.

And there is a final surprising result. We will discover that for a set of polynomials or vectors of polynomials, being special in the sense of confluence is equivalent to being special in the sense of Conditions A) and B) described in Section 2.1. Thus rewrite rules provide a different aspect of the same phenomenon. Although it is beyond the scope of this book, it turns out that this view is most suitable for generalizations in a number of directions, e.g. to the non-commutative case.

Now it is time to study these ideas in a more technical manner. Let K be a field, $n \neq 1$, $P = K[x_1, \ldots, x_n]$ a polynomial ring, $r \geq 1$, and σ a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$.

Definition 2.2.1. Let $g_1, \ldots, g_s \in P^r \setminus \{0\}$ and $G = \{g_1, \ldots, g_s\}$.

a) Let $m_1, m_2 \in P^r$, and suppose there exist a constant $c \in K$, a term $t \in \mathbb{T}^n$, and an index $i \in \{1, \ldots, s\}$ such that $m_2 = m_1 - c\, t g_i$ and $t \cdot \mathrm{LT}_\sigma(g_i) \notin \mathrm{Supp}(m_2)$. Then we say that m_1 **reduces to** m_2 **in one step** using the **rewrite rule** defined by g_i (or simply that m_1 reduces to m_2 in one step using g_i), and we write $m_1 \xrightarrow{g_i} m_2$. The passage from m_1 to m_2 is also called a **reduction step**.

b) The transitive closure of the relations $\xrightarrow{g_1}, \ldots, \xrightarrow{g_s}$ is called the **rewrite relation** defined by G and is denoted by $\xrightarrow{G}$. In other words, for $m_1, m_2 \in P^r$, we let $m_1 \xrightarrow{G} m_2$ if and only if there exist indices $i_1, \ldots, i_t \in \{1, \ldots, s\}$ and elements $m'_0, \ldots, m'_t \in P^r$ such that

$$m_1 = m'_0 \xrightarrow{g_{i_1}} m'_1 \xrightarrow{g_{i_2}} \cdots \xrightarrow{g_{i_t}} m'_t = m_2$$

c) An element $m_1 \in P^r$ with the property that there is no $i \in \{1, \ldots, s\}$ and no $m_2 \in P^r \setminus \{m_1\}$ such that $m_1 \xrightarrow{g_i} m_2$ is called **irreducible** with respect to $\xrightarrow{G}$.

d) The equivalence relation defined by $\xrightarrow{G}$ will be denoted by $\xleftrightarrow{G}$.

In part a) of this definition, we can choose $c = 0$ and $t \in \mathbb{T}^n$ such that $t \cdot \mathrm{LT}_\sigma(g_i) \notin \mathrm{Supp}(m_1)$. This is called a **trivial reduction**. By using it we see that $m_1 \xrightarrow{g_i} m_1$. In the example mentioned in the introduction, we have for instance $f \xrightarrow{g_1} xy - y$ and $xy - y \xrightarrow{g_2} x - 3$. Thus $f \xrightarrow{G} x - 3$ and $x - 3 \xleftrightarrow{G} f$ hold, while $x - 3 \xrightarrow{G} f$ is not true, because the leading term of f is larger than x.

Proposition 2.2.2. (Properties of Rewrite Relations)
Let $g_1, \ldots, g_s \in P^r \setminus \{0\}$, and let $G = \{g_1, \ldots, g_s\}$.

a) If $m_1, m_2 \in P^r$ satisfy $m_1 \xrightarrow{G} m_2$ and $m_2 \xrightarrow{G} m_1$, then $m_1 = m_2$.

b) If $m_1, m_2 \in P^r$ satisfy $m_1 \xrightarrow{G} m_2$, and if $t \in \mathbb{T}^n$, then we have $tm_1 \xrightarrow{G} tm_2$.

c) Every chain $m_1 \xrightarrow{G} m_2 \xrightarrow{G} \cdots$ such that $m_1, m_2, \ldots \in P^r$ becomes eventually stationary.

d) If $m_1, m_2 \in P^r$ satisfy $m_1 \xrightarrow{g_i} m_2$ for $i \in \{1, \ldots, s\}$, and if $m_3 \in P^r$, then there exists an element $m_4 \in P^r$ such that $m_1 + m_3 \xrightarrow{G} m_4$ and $m_2 + m_3 \xrightarrow{G} m_4$.

e) If $m_1, m_2, m_3, m_4 \in P^r$ satisfy $m_1 \xleftrightarrow{G} m_2$ and $m_3 \xleftrightarrow{G} m_4$, then we have $m_1 + m_3 \xleftrightarrow{G} m_2 + m_4$.

f) If $m_1, m_2 \in P^r$ satisfy $m_1 \xleftrightarrow{G} m_2$, and if $f \in P$, then we have $fm_1 \xleftrightarrow{G} fm_2$.

g) For $m \in P^r$, we have $m \xleftrightarrow{G} 0$ if and only if $m \in \langle g_1, \ldots, g_s \rangle$.

h) For $m_1, m_2 \in P^r$, we have $m_1 \xleftrightarrow{G} m_2$ if and only if $m_1 - m_2 \in \langle g_1, \ldots, g_s \rangle$.

Proof. To show claim a), we consider a chain of reduction steps which represents $m_1 \xrightarrow{G} m_2 \xrightarrow{G} m_1$, i.e. a chain $m_1 = m_0' \xrightarrow{g_{i_1}} \cdots \xrightarrow{g_{i_t}} m_t' = m_1$ such that $i_1, \ldots, i_t \in \{1, \ldots, s\}$ and $m_j' = m_2$ for some $j \in \{1, \ldots, t-1\}$. The effect of a reduction step is that a term is replaced by other terms, all of which are smaller with respect to σ. So let te_k with $t \in \mathbb{T}^n$ and $k \in \{1, \ldots, s\}$ be the largest term with respect to σ which is reduced in this chain. This term is not contained in the support of the result anymore, unless each reduction step is trivial, i.e. unless $m_1 = m_2$.

Claim b) holds, since it holds at each reduction step. Thus we prove c) now. Suppose there exist $i_1, i_2, \ldots \in \{1, \ldots, s\}$ and $m_1, m_2, \ldots \in P^r$ such that we have a chain of reduction steps $m_1 \xrightarrow{g_{i_1}} m_2 \xrightarrow{g_{i_2}} \cdots$ which does not become stationary. The first claim is that each m_i must have a term in its support which reduces eventually. Indeed we observe that if this does not happen, it means that starting from m_i the sequence of reductions is actually a sequence of equalities. Therefore there exists a term t_i in $\text{Supp}(m_i)$ which is the largest term with respect to σ which is reduced later in the chain. Then we have $t_1 \geq_\sigma t_2 \geq_\sigma \cdots$, and since every term t_i is reduced eventually, this chain does not become stationary either, in contradiction with Theorem 1.4.19.

For the proof of d), we let $c \in K$, $t \in \mathbb{T}^n$, and $i \in \{1, \ldots, s\}$ be such that $m_2 = m_1 - ctg_i$ and $t\,\text{LT}_\sigma(g_i) \notin \text{Supp}(m_2)$. Clearly we may assume $c \neq 0$. We let c' be the coefficient of $t\,\text{LT}_\sigma(g_i)$ in m_3 and distinguish two cases. When $c' = -c$, we have $m_1 + m_3 = m_2 + m_3 + ctg_i = m_2 + m_3 - c'tg_i$. Since the coefficient of $t\,\text{LT}_\sigma(g_i)$ in $m_2 + m_3 - c'tg_i$ vanishes, we get

$m_2 + m_3 \xrightarrow{g_i} m_1 + m_3$, and we can choose $m_4 = m_1 + m_3$. When $c' \neq -c$ we define m_4 by

$$m_4 = m_1 + m_3 - (c + c')t g_i = m_2 + m_3 - c't g_i$$

and obtain the claim, because the coefficient of $t\,\mathrm{LT}_\sigma(g_i)$ vanishes in m_4.

Next, claim e) follows from d), and f) follows from b) and e) by representing f as a sum of monomials. Since h) is an immediate consequence of e) and g), it remains to show g). If $m \xrightarrow{G} 0$, we collect the terms used in the various reduction steps and get a representation $m = f_1 g_1 + \cdots + f_s g_s$ with $f_1, \ldots, f_s \in P$. Conversely, given an element $m \in P^r$ with such a representation, it suffices by e) to prove $f_i g_i \xrightarrow{G} 0$ for $i = 1, \ldots, s$. This follows from $g_i \xrightarrow{G} 0$ and f). $\qquad\square$

Unfortunately, it is not clear how we could use part g) of the above proposition to check whether a given element $m \in P^r$ is contained in the submodule $\langle g_1, \ldots, g_s \rangle$, because we do not know the direction of the reduction steps used in $m \xrightarrow{G} 0$. In other words, if we use only reduction steps $m = m_0 \xrightarrow{g_{i_1}} m_1 \xrightarrow{g_{i_2}} \cdots$, we might get stuck at some point with an irreducible element with respect to $\xrightarrow{G}$. The next example shows that this can really happen.

Example 2.2.3. Let $n = 3$, $r = 1$, $G = \{g_1, g_2\}$ with $g_1 = x_1^2 - x_2$ and $g_2 = x_1 x_2 - x_3$, and let σ be the term ordering `DegRevLex`. Then the polynomial $f = x_1^2 x_2 - x_1 x_3$ is contained in the ideal (g_1, g_2), since $f = x_1 g_2$. But if we use the reduction step $f \xrightarrow{g_1} x_2^2 - x_1 x_3$, we arrive at an irreducible element with respect to $\xrightarrow{G}$.

It is also important to notice that if σ is not a term ordering, then claim c) of Proposition 2.2.2 may fail to hold, as the following example shows.

Example 2.2.4. Let $n = 2$, let $r = 1$, let $G = \{g\}$ with $g = x - xy$, and let $\sigma = $ `RevLex`. Then the chain $x \xrightarrow{g} xy \xrightarrow{g} xy^2 \xrightarrow{g} \cdots$ does not become stationary.

After seeing the main properties of rewrite relations, we want to investigate the property of confluence which, as we said before, is crucial for later applications.

Proposition 2.2.5. *Let $g_1, \ldots, g_s \in P^r \setminus \{0\}$, let $G = \{g_1, \ldots, g_s\}$, and let $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$. Then the following conditions are equivalent.*

C_1) *For an element $m \in P^r$, we have $m \xrightarrow{G} 0$ if and only if $m \in M$.*

C_2) *If $m \in M$ is irreducible with respect to $\xrightarrow{G}$, then we have $m = 0$.*

C_3) *For every element $m_1 \in P^r$, there is a unique element $m_2 \in P^r$ such that $m_1 \xrightarrow{G} m_2$ and m_2 is irreducible with respect to $\xrightarrow{G}$.*

C_4) *If* $m_1, m_2, m_3 \in P^r$ *satisfy* $m_1 \xrightarrow{G} m_2$ *and* $m_1 \xrightarrow{G} m_3$, *then there exists an element* $m_4 \in P^r$ *such that* $m_2 \xrightarrow{G} m_4$ *and* $m_3 \xrightarrow{G} m_4$. *(A relation* $\xrightarrow{G}$ *with this property is called* **confluent**.*)*
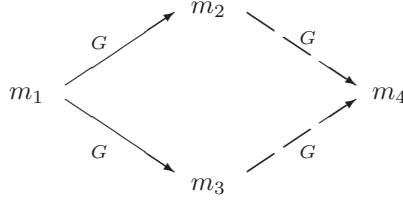
Proof. For the proof of C_1) $\Rightarrow$ C_2), we note that if $m \in M$, then C_1) implies $m \xrightarrow{G} 0$. Thus if m is irreducible with respect to $\xrightarrow{G}$, we get $m = 0$. Next we show that C_2) implies C_3). By Proposition 2.2.2.c, there is an element $m_2 \in P^r$ which is irreducible with respect to $\xrightarrow{G}$ and which satisfies $m_1 \xrightarrow{G} m_2$. Suppose $m_2' \in P^r$ is another element with those properties. Then we have $m_2 - m_2' \in M$, since $m_1 \xrightarrow{G} m_2$ and $m_1 \xrightarrow{G} m_2'$. Furthermore, the element $m_2 - m_2'$ is irreducible with respect to $\xrightarrow{G}$, since no term in $\mathrm{Supp}(m_2) \cup \mathrm{Supp}(m_2')$ is a multiple of one of the terms $\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)$. By C_2), we conclude $m_2 = m_2'$.

Now we prove C_3) $\Rightarrow$ C_4). By Proposition 2.2.2.c, there are elements $m_2', m_3' \in P^r$ which are irreducible with respect to $\xrightarrow{G}$ and which satisfy $m_2 \xrightarrow{G} m_2'$ as well as $m_3 \xrightarrow{G} m_3'$. From $m_1 \xrightarrow{G} m_2'$, $m_1 \xrightarrow{G} m_3'$, and C_3), we conclude $m_2' = m_3'$. Then the claim follows for $m_4 = m_2' = m_3'$.

Finally, to show C_4) $\Rightarrow$ C_1), it suffices, by Proposition 2.2.2.g, to prove $m \xrightarrow{G} 0$ for $m \in M$, where we already know $m \xleftarrow{G} 0$. Let $m_1, \ldots, m_t \in P^r$ be such that $m_1 = m$, $m_t = 0$, and for all $i = 1, \ldots, t-1$ we either have $m_i \xrightarrow{G} m_{i+1}$ or $m_{i+1} \xrightarrow{G} m_i$. Let $\ell \in \{1, \ldots, t-2\}$ be the largest index such that $m_{\ell+1} \xrightarrow{G} m_\ell$. Then we have $m_{\ell+1} \xrightarrow{G} 0$ and $m_{\ell+1} \xrightarrow{G} m_\ell$, and C_4) yields $m_\ell \xrightarrow{G} 0$. If we replace the sequence $m = m_1, \ldots, m_t = 0$ by the shorter sequence $m = m_1, \ldots, m_\ell, 0$, we see that the claim follows by induction. $\qquad\square$

The remainder of this section deals with connections between confluent rewrite relations and the previous section. First we prove a useful technical result.

Lemma 2.2.6. *Let* $g_1, \ldots, g_s \in P^r \setminus \{0\}$, *let* $G = \{g_1, \ldots, g_s\}$, *and let* $M = \langle g_1, \ldots, g_s \rangle$. *Assume that an element* $m \in M \setminus \{0\}$ *satisfies* $m \xrightarrow{G} 0$.

a) *There exist an index* $\alpha \in \{1, \ldots, s\}$ *and a term* $t \in \mathbb{T}^n$ *such that* $\mathrm{LT}_\sigma(m) = t \cdot \mathrm{LT}_\sigma(g_\alpha)$.

b) *By collecting all reduction steps in* $m \xrightarrow{G} 0$, *we get* $f'_1, \ldots, f'_s \in P$ *such that* $m - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_\alpha)} t\, g_\alpha = \sum_{i=1}^s f'_i g_i$ *and such that* $\mathrm{LT}_\sigma(m) >_\sigma \mathrm{LT}_\sigma(f'_i g_i)$ *for* $i = 1, \ldots, s$ *with* $f'_i g_i \neq 0$.

c) *If we put* $f_i = f'_i$ *for* $i \in \{1, \ldots, s\} \setminus \{\alpha\}$ *and* $f_\alpha = f'_\alpha + \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_\alpha)} t$, *then we obtain an element* $m = \sum_{i=1}^s f_i g_i$ *whose leading term satisfies* $\mathrm{LT}_\sigma(m) = \max_\sigma \{\mathrm{LT}_\sigma(f_i g_i) \mid i \in \{1, \ldots, s\}, \ f_i g_i \neq 0\}$.

Proof. Claim a) follows immediately from the fact that $\mathrm{LT}_\sigma(m)$ has to be eliminated at one of the reduction steps.

Now we prove b). Let $m_1, \ldots, m_t \in P^r$ be such that $m_1 = m$, $m_t = 0$, and for all $i = 1, \ldots, t-1$ we have $m_i \xrightarrow{G} m_{i+1}$ using one reduction step. By a), there exists a reduction step where the leading term of m is reduced. This step is unique, since it substitutes $\mathrm{LT}_\sigma(m)$ with smaller terms. So, let $\ell \in \{1, \ldots, t-1\}$ be such that $m_{\ell+1} = m_\ell - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_\alpha)} t\, g_\alpha$. Then

$$m - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_\alpha)} t\, g_\alpha = m - (m_\ell - m_{\ell+1}) = \sum_{i=1}^{\ell-1}(m_i - m_{i+1}) + \sum_{i=\ell+1}^{t-1}(m_i - m_{i+1})$$

is of the form $\sum_{i=1}^s f'_i g_i$. Here the polynomials f'_i are obtained by collecting the elements of type $c\,t$ appearing in the two sums, where each difference $m_i - m_{i+1}$ is of the form $m_i - m_{i+1} = c\,t\,g_\beta$ for some $c \in K$, $t \in \mathbb{T}^n$, and $\beta \in \{1, \ldots, s\}$. To conclude the proof it suffices to observe that when we write $m_i - m_{i+1} = c\,t\,g_\beta$, we get $t\,\mathrm{LT}_\sigma(g_\beta) \leq_\sigma \mathrm{LT}_\sigma(m_i)$ by the definition of a reduction step.

Finally, we see that c) is an immediate consequence of b).   □

Let us examine the claims of this lemma in a concrete case.

Example 2.2.7. Let $g_1 = x^2 - xy$, $g_2 = xy - x - z$, and $g_3 = xy + xz$ be polynomials in $\mathbb{Q}[x, y, z]$, let $G = \{g_1, g_2, g_3\}$, and let $\sigma = \mathtt{DegLex}$. Suppose we want to reduce the polynomial x^3 with respect to the rewrite relation $\xrightarrow{G}$.

One possibility is to apply the following chain of reduction steps.

$$x^3 \xrightarrow{g_1} x^2 y \xrightarrow{g_2} x^2 + xz \xrightarrow{g_1} xy + xz \xrightarrow{g_3} 0$$

As predicted by part a) of the lemma, we find $x^3 = \mathrm{LT}_\sigma(x^3) = x\,\mathrm{LT}_\sigma(g_1)$. Furthermore, by collecting the reduction steps, we get $x^3 - xg_1 = xg_2 + g_1 + g_3$, where $x^3 = \mathrm{LT}_\sigma(x^3)$ is strictly bigger than $x^2 y = \mathrm{LT}_\sigma(xg_2)$, $x^2 = \mathrm{LT}_\sigma(g_1)$, and $xy = \mathrm{LT}_\sigma(g_3)$ with respect to σ.

Finally, to check part c) of the lemma, we also bring xg_1 to the other side and write

$$x^3 = (x+1)g_1 + xg_2 + g_3$$

Here we have $x^3 = \max_\sigma \{\mathrm{LT}_\sigma((x+1)g_1), \mathrm{LT}_\sigma(xg_2), \mathrm{LT}_\sigma(g_3)\}$, as claimed.

Unfortunately, the lemma requires that the element reduces to zero. In our case, we could have followed a different sequence of reduction steps, for instance

$$x^3 \xrightarrow{g_1} x^2 y \xrightarrow{g_1} xy^2 \xrightarrow{g_2} xy + yz \xrightarrow{g_2} yz + x + z$$

Here we end up with an element which cannot be reduced further and which is non-zero. By looking at this sequence of instruction steps, we cannot decide whether x^3 satisfies the hypothesis of the lemma.

Both in the introduction to this section and in the previous example we have seen that the property of being confluent is not shared by all rewrite relations. Is there a better way of understanding it? The following proposition gives a somehow unexpected answer.

Proposition 2.2.8. *Let* $g_1, \ldots, g_s \in P^r \setminus \{0\}$, *let* $G = \{g_1, \ldots, g_s\}$, *and let* $M = \langle g_1, \ldots, g_s \rangle$. *Then Conditions* $A_1)$, $A_2)$ *of Proposition 2.1.1 are equivalent with Conditions* $C_1)$, $C_2)$, $C_3)$, *and* $C_4)$ *of Proposition 2.2.5.*

Proof. To prove $A_2) \Rightarrow C_2)$ by contradiction, we suppose that there is an element $m \in M \setminus \{0\}$ which is irreducible with respect to $\xrightarrow{G}$. By Condition $A_2)$, the element m has a representation $m = \sum_{i=1}^{s} f_i g_i$ such that $f_1, \ldots, f_s \in P$ and $\mathrm{LT}_\sigma(m) = \max_\sigma \{\mathrm{LT}_\sigma(f_i g_i) \mid i \in \{1, \ldots, s\}, \ f_i g_i \neq 0\}$. Let $t \mathrm{LT}_\sigma(g_i)$ be the term which achieves this maximum. Then the element $m' = m - \frac{\mathrm{LC}_\sigma(m)}{\mathrm{LC}_\sigma(g_i)} t g_i$ satisfies $m \xrightarrow{G} m'$ and $m' \neq m$, a contradiction.

Conversely, $C_1) \Rightarrow A_2)$ follows directly from Lemma 2.2.6. □

Exercise 1. Let σ be a module term ordering, let $g \in P^r \setminus \{0\}$, and let $G = \{g\}$. Show that the rewrite relation $\xrightarrow{G}$ is confluent.

Exercise 2. Let σ be a module term ordering, and let G be a finite set of terms in P^r. Show that Conditions $C)$ of Proposition 2.2.5 hold for the rewrite relation $\xrightarrow{G}$.

Exercise 3. Give an example of a rewrite relation $\xrightarrow{G}$ which is not confluent.

Exercise 4. Let σ be a monoid ordering on $\mathbb{T}^n$, let $t_1, t_2 \in \mathbb{T}^n$ be terms with $t_1 >_\sigma t_2$, and let $g = t_1 - t_2$. Consider the rewrite relation defined by $G = \{g\}$. (Observe that here we do not assume that σ is a term ordering.) Prove that the following conditions are equivalent.

a) $t_1 \nmid t_2$

b) Every chain $f_1 \xrightarrow{G} f_2 \xrightarrow{G} \cdots$ such that $f_1, f_2, \ldots \in P$ becomes eventually stationary.

Tutorial 18: Algebraic Numbers

In this tutorial, we want to use CoCoA to give some hints about how one can effectively compute in the field $\overline{\mathbb{Q}}$ of algebraic numbers, i.e. the algebraic closure of $\mathbb{Q}$. We shall compute only up to conjugates, i.e. we shall represent an algebraic number by its minimal polynomial over $\mathbb{Q}$. To distinguish between conjugate algebraic numbers, we would also have to provide reasonably good approximations in $\mathbb{Q}[i]$. Furthermore, we shall be content to find *some* polynomial which has a certain algebraic number as one of its zeros. After factoring this polynomial using the CoCoA function $\texttt{Factor}(\ldots)$ one could then try to use methods of numerical analysis to find the factor which is the minimal polynomial of the desired algebraic number.

   Let $a_1, a_2 \in \overline{\mathbb{Q}}$ be two algebraic numbers represented by irreducible polynomials $g_1, g_2 \in \mathbb{Q}[x]$ of degrees d_1, d_2, respectively.

a) Use Macaulay's Basis Theorem 1.5.7 to show that the residue classes of $\{x_1^i x_2^j \mid 0 \le i < d_1,\ 0 \le j < d_2\}$ form a $\mathbb{Q}$-basis of the $\mathbb{Q}$-algebra $\mathbb{Q}[x_1, x_2]/(g_1(x_1), g_2(x_2))$.

b) Show that one can find a polynomial having $a_1 + a_2$ as one of its zeros in the following way.

   1) Represent the residue classes of the powers $1, x_1 + x_2, (x_1 + x_2)^2, \ldots$ in the basis given in a). Use the rewrite relation $\xrightarrow{G}$ corresponding to $G = \{g_1(x_1), g_2(x_2)\}$ to find such representations.

   2) Continue with step 1) until there is a linear relation between the representations of $1, x_1 + x_2, \ldots, (x_1 + x_2)^d$ for some $d \ge 0$. Then there is a polynomial of degree d which vanishes at $a_1 + a_2$.

c) Write a CoCoA program $\texttt{AlgSum}(\ldots)$ which takes the pair (g_1, g_2) and computes a polynomial which vanishes at $a_1 + a_2$ using the algorithm developed in b).

d) Repeat parts b) and c) for the product $a_1 a_2$. In particular, write a CoCoA program $\texttt{AlgMult}(\ldots)$ which finds a polynomial which vanishes at $a_1 a_2$.

e) Given an algebraic number $a \in \overline{\mathbb{Q}}$ represented by an irreducible polynomial $g \in \mathbb{Q}[x]$, what is the minimal polynomial of $-a$? Write a CoCoA program $\texttt{AlgNeg}(\ldots)$ which takes g and computes the minimal polynomial of $-a$.

f) Given a non-zero algebraic number $a \in \overline{\mathbb{Q}}$ represented by an irreducible polynomial $g \in \mathbb{Q}[x]$, what is the minimal polynomial of $\frac{1}{a}$? Write a CoCoA program $\texttt{AlgInv}(\ldots)$ which takes g and computes the minimal polynomial of $\frac{1}{a}$.

g) Apply your CoCoA programs $\texttt{AlgSum}(\ldots)$, $\texttt{AlgMult}(\ldots)$, $\texttt{AlgNeg}(\ldots)$, and $\texttt{AlgInv}(\ldots)$ in the following cases. (You'll have to find g_1, g_2 first!)

   1) $a_1 = \sqrt{2}$, $a_2 = \sqrt{3}$
   2) $a_1 = \sqrt[3]{3}$, $a_2 = \frac{1}{2} + \frac{i}{2}\sqrt{3}$
   3) $a_1 = \sqrt{2} + \sqrt{3}$, $a_2 = -i$

2.3 Syzygies

Not in the beauty of the words
lies the persuasion of an explanation,
but in their combination ($\sigma\upsilon\zeta\upsilon\gamma\acute{\iota}\alpha$, syzygía).
(Dionysius Halicarnassensis)

In the previous two sections we saw a number of conditions satisfied by certain *special* systems of generators of an ideal or module, but not by all of them. Although Proposition 1.5.6 says that such special systems of generators exist always, we do not yet know how to replace a given system of generators with another one having those additional properties.

In this section we change our point of view once more and look at these phenomena from the perspective of syzygies. Despite the exotic name, a syzygy is a very simple object to define. Namely, given a ring R and a tuple of elements $(g_1, \ldots, g_s)$ of an R-module, every tuple $(f_1, \ldots, f_s)$ of elements of R such that $f_1 g_1 + \cdots + f_s g_s = 0$ is called a *syzygy* of $(g_1, \ldots, g_s)$. The introduction of syzygies will eventually achieve several goals. First of all, we see in this section that the failure of Conditions $A)$, $B)$, $C)$ can be better understood in terms of syzygies. Even more important is the fact that in subsequent sections we shall use syzygies to find an algorithmic way to replace a given set of generators, which does not satisfy the conditions, with another one, which does.

What we have said so far suggests the importance of syzygies, and in fact they turn out to be one of the most fundamental algebraic objects. Consequently, the computation of a system of generators for the module of syzygies of a given tuple is one of the central problems in Computational Commutative Algebra. It is also the key to many applications studied in Chapter 3.

But for the moment, let us get down to earth and start digging for the hidden treasures in the land of syzygies. To find the set of all syzygies of a given tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of non-zero polynomial vectors $g_1, \ldots, g_s \in P^r$, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over a field K, we use the same strategy which brought us rich rewards before: reduce questions about polynomials or vectors of polynomials to questions about their leading terms. Thus we start out by connecting the defining exact sequence of the module of syzygies $\mathrm{Syz}(\mathcal{G})$ of $\mathcal{G}$ and the defining exact sequence of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, the syzygy module of $\mathrm{LM}_\sigma(\mathcal{G}) = (\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))$, via a *fundamental diagram*.

Then we compute an explicit system of generators for $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, and finally we try to *lift* those syzygies to syzygies of $\mathcal{G}$. This means that we try to find syzygies of $\mathcal{G}$ whose highest homogeneous components (in some sense) are the syzygies generating $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. When we try to lift the treasures of syzygies in this way, we encounter another unexpected gem: A system of generators of a module has the property that the syzygies of their leading

terms can be lifted if and only if the set of generators satisfies Conditions $A)$, $B)$, and $C)$!

Definition 2.3.1. Let R be a ring, M an R-module, and $\mathcal{G} = (g_1, \ldots, g_s)$ a tuple of elements of M.

a) A **syzygy** of $\mathcal{G}$ is a tuple $(f_1, \ldots, f_s) \in R^s$ such that $f_1 g_1 + \cdots + f_s g_s = 0$.

b) The set of all syzygies of $\mathcal{G}$ forms an R-module which we call the **(first) syzygy module** of $\mathcal{G}$ and which we denote by $\mathrm{Syz}_R(\mathcal{G})$ or by $\mathrm{Syz}_R(g_1, \ldots, g_s)$. If no confusion can arise, we shall also write $\mathrm{Syz}(\mathcal{G})$ or $\mathrm{Syz}(g_1, \ldots, g_s)$.

As in the previous sections, we let K be a field, $n \geq 1$, $P = K[x_1, \ldots, x_n]$ a polynomial ring, $r \geq 1$, and σ a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. Furthermore, we let $g_1, \ldots, g_s \in P^r \setminus \{0\}$, we let $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$, and we denote the s-tuple $(g_1, \ldots, g_s)$ by $\mathcal{G}$. Then we consider the P-module P^s with canonical basis $\{\varepsilon_1, \ldots, \varepsilon_s\}$ and the homomorphism $\lambda : P^s \longrightarrow M$ given by $\varepsilon_j \mapsto g_j$ for $j = 1, \ldots, s$. In this situation we can also describe the syzygy module of $\mathcal{G}$ by $\mathrm{Syz}_P(\mathcal{G}) = \ker(\lambda)$.

The nature of many facts explained in this section is not elementary, so the inexperienced reader might have some difficulties. For instance, it is clear that even if we start with an ideal, given by a set of polynomial generators, the set of their syzygies is a module. So the theory is described in the framework of modules. Moreover, we shall need to introduce a fine grading on the module of syzygies in order to detect the correct "highest homogeneous component" when we follow the above approach.

Since we do not want any reader running away from this book at this point, we decided to use a didactic tool: *a running example*. This is an example which we will revisit several times during the section, and which we will use to make all definitions and constructions as lucid as possible. Let us start our running example by introducing its basic objects.

Example 2.3.2. Let $n = 3$, let $r = 1$, and let us equip $P = \mathbb{Q}[x, y, z]$ with the degree-lexicographic term ordering σ. Then we consider the ideal $M = \langle g_1, g_2 \rangle$ generated by $g_1 = x^2 - y^2 - x$ and $g_2 = xy^2 - z^3$, and the pair $\mathcal{G} = (g_1, g_2)$. Of course the reason why we call this ideal M (and not I) is to have a better way of comparing the example with the general theory.

The syzygy module of $\mathcal{G}$ is the submodule $\mathrm{Syz}(\mathcal{G}) = \{(f_1, f_2) \in P^2 \mid f_1 g_1 + f_2 g_2 = 0\} = \{(f_1, f_2) \in P^2 \mid f_1(x^2 - y^2 - x) + f_2(xy^2 - z^3) = 0\}$ of P^2. Some syzygies of $\mathcal{G}$ are obviously given by $(g_2, -g_1)$ and its multiples, but are there others?

When we combine the exact sequence $0 \longrightarrow M \longrightarrow P^r \longrightarrow P^r/M \longrightarrow 0$ with the description of $\mathrm{Syz}(\mathcal{G})$ as the kernel of λ, we obtain a long exact sequence

$$0 \longrightarrow \mathrm{Syz}(\mathcal{G}) \longrightarrow P^s \overset{\lambda}{\longrightarrow} P^r \longrightarrow P^r/M \longrightarrow 0$$

Now let $N \subseteq P^r$ be the P-submodule of P^r generated by the vectors $\{\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s)\}$, let $\mathrm{LM}_\sigma(\mathcal{G})$ be the tuple $(\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))$, and let $\Lambda : P^s \longrightarrow N$ denote the homomorphism given by $\varepsilon_j \mapsto \mathrm{LM}_\sigma(g_j)$ for $j = 1, \ldots, s$. Then $\mathrm{Ker}(\Lambda)$ is the syzygy module of $\mathrm{LM}_\sigma(\mathcal{G})$. Consequently, it will be denoted by $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. We obtain another long exact sequence

$$0 \longrightarrow \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) \longrightarrow P^s \overset{\Lambda}{\longrightarrow} P^r \longrightarrow P^r/N \longrightarrow 0$$

Recall from Example 1.7.5 that P^r carries a natural structure of a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded module over the $\mathbb{T}^n$-graded ring P. More precisely, we have $(P^r)_{te_i} = K \cdot te_i$ and $P_t = K \cdot t$ for $t \in \mathbb{T}^n$ and $i = 1, \ldots, r$. If we look at the definition of Λ, we see that $\Lambda(\sum_{j=1}^s f_j \varepsilon_j) = \sum_{j=1}^s f_j \mathrm{LM}_\sigma(g_j)$. This fact suggests that we should try to equip the P-module P^s with a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-grading which is somehow compatible with Λ. By using this approach we find, in the next proposition, that the second sequence carries more structure than the first one.

Proposition 2.3.3. *In the above situation we define*

$$(P^s)_{te_i} = \{\sum_{j=1}^s c_j t_j \varepsilon_j \in P^s \mid c_j = 0 \ \ \text{or} \ \ t_j \mathrm{LT}_\sigma(g_j) = te_i \ \text{ for } j = 1, \ldots, s\}$$

for all $te_i \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$.

a) *We have $P^s = \oplus_{te_i \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle}(P^s)_{te_i}$. In this way, P^s becomes a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded module over the $\mathbb{T}^n$-graded ring P.*

b) *The map Λ is a homomorphism of $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded P-modules. In fact, the sequence $0 \longrightarrow \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) \longrightarrow P^s \overset{\Lambda}{\longrightarrow} P^r \longrightarrow P^r/N \longrightarrow 0$ consists of homomorphisms of $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded modules.*

Proof. In order to show a), we first observe that $(P^s)_{te_i}$ is a group for every $t \in \mathbb{T}^n$ and every $i \in \{1, \ldots, r\}$. Then we verify $P^s = \oplus_{te_i \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle}(P^s)_{te_i}$. Every element $\sum_{j=1}^s f_j \varepsilon_j \in P^s$ is a sum of elements of the form $ct' \varepsilon_j$ with $c \in K \setminus \{0\}$ and $t' \in \mathbb{T}^n$. By definition, we have $ct' \varepsilon_j \in (P^s)_{t' \mathrm{LT}_\sigma(g_j)}$, so that it remains to show that the sum is a direct sum.

To this end we notice that, for each $j \in \{1, \ldots, s\}$, there exists at most one term t' in the support of f_j such that $t' \mathrm{LT}_\sigma(g_j) = te_i$. Therefore every term in the support of $\sum_{j=1}^s f_j \varepsilon_j$ is contained precisely in one summand $(P^s)_{te_i}$. Finally, we observe that $t \cdot (P^s)_{t'e_i} \subseteq (P^s)_{tt'e_i}$ shows that our definition actually yields a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded module over the $\mathbb{T}^n$-graded ring P.

Now we prove b). For every $te_i \in \mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ and every element $\sum_{j=1}^s c_j t_j \varepsilon_j \in (P^s)_{te_i}$ we have $\Lambda(\sum_{j=1}^s c_j t_j \varepsilon_j) = \sum_{j=1}^s c_j t_j \mathrm{LM}_\sigma(g_j) = (\sum_{j=1}^s c_j \mathrm{LC}_\sigma(g_j))te_i \in (P^r)_{te_i}$. Therefore the map Λ is a homomorphism of $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded modules, and $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) = \mathrm{ker}(\Lambda)$ inherits the structure of a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded module. Since N is a monomial submodule of P^r, it is a $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded submodule by Proposition 1.7.10,

and the canonical homomorphism $P^r \longrightarrow P^r/N$ is a homomorphism of $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-graded P-modules by Remark 1.7.9. Thus the whole sequence consists of homomorphisms of $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-graded modules.   □

Example 2.3.2 (continued) In our example we have $\mathrm{LM}_\sigma(\mathcal{G}) = (x^2, xy^2)$. Then for instance $(P^2)_{x^2y^2} = \{(c_1t_1, c_2t_2) \in P^2 \mid c_1t_1x^2, c_2t_2xy^2 \in \mathbb{Q}\cdot x^2y^2\}$. Examples of elements which belong to $(P^2)_{x^2y^2}$ are $(y^2, 0)$, $(-y^2, x)$, and $(\frac{1}{2}y^2, -4x)$.

The intrinsic meaning of the new concepts which we are now going to introduce will be discussed more thoroughly in Volume 2. For the time being, they are only defined with the purpose of better dealing with the $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-gradings described above.

Definition 2.3.4. Let m be a non-zero element of a $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-graded module, and let $m = \sum_{\mu \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle} m_\mu$ be the decomposition of m into its homogeneous components. The term $\max_\sigma\{\mu \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle \mid m_\mu \neq 0\}$ is called the σ**-degree** of m, and the homogeneous component of m of this degree is called the σ**-leading form** of m.

In the case of the $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-grading on P^s defined in Proposition 2.3.3, we denote the σ-degree of an element $m \in P^s\setminus\{0\}$ by $\deg_{\sigma,\mathcal{G}}(m)$, and its σ-leading form by $\mathrm{LF}_{\sigma,\mathcal{G}}(m)$. In the next proposition we show how to determine $\deg_{\sigma,\mathcal{G}}(m)$ and $\mathrm{LF}_{\sigma,\mathcal{G}}(m)$ for a non-zero element $m \in P^s$.

Proposition 2.3.5. *Let the module P^s be equipped with the $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-grading defined above, let $f_1, \ldots, f_s \in P$, and let $m = \sum_{j=1}^s f_j\varepsilon_j \in P^s\setminus\{0\}$.*

a) *We have $\deg_{\sigma,\mathcal{G}}(m) = \max_\sigma\{\mathrm{LT}_\sigma(f_jg_j) \mid j \in \{1, \ldots, s\},\ f_jg_j \neq 0\}$.*

b) *We have $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \sum_{j=1}^s \bar{f}_j\varepsilon_j$, where*

$$\bar{f}_j = \begin{cases} 0 & \text{if } f_j = 0 \text{ or } \mathrm{LT}_\sigma(f_jg_j) <_\sigma \deg_{\sigma,\mathcal{G}}(m) \\ c_jt_j & \text{if } \mathrm{LT}_\sigma(f_jg_j) = \deg_{\sigma,\mathcal{G}}(m) \text{ and } c_j \in K,\ t_j \in \mathrm{Supp}(f_j) \\ & \text{are such that } \mathrm{LM}_\sigma(f_jg_j) = c_jt_j\,\mathrm{LM}_\sigma(g_j) \end{cases}$$

Proof. Claim a) follows from Proposition 1.5.3 and Definition 2.3.4. To show b), we use that $\deg_{\sigma,\mathcal{G}}(m) = \max_\sigma\{t\,\mathrm{LT}_\sigma(g_j) \mid 1 \leq j \leq s,\ t \in \mathrm{Supp}(f_j)\}$ by a), and this maximum is achieved precisely for the terms described in the formula.   □

Sometimes we are dealing with the case $r = 1$, or we can pick a monoid ordering τ on $\mathbb{T}^n$ such that σ is compatible with τ. In this case, we have $\bar{f}_j = c_jt_j = \mathrm{LM}_\tau(f_j)$ in part b) of this proposition.

Example 2.3.2 (continued) Let us compute both the σ-degree and the σ-leading form of some elements of P^s in our running example. For instance, if we consider the pair $(\frac{1}{2}y^2z, -4xz)$, we have $\deg_{\sigma,\mathcal{G}}(\frac{1}{2}y^2z, -4xz) = x^2y^2z$ and $\mathrm{LF}_{\sigma,\mathcal{G}}(\frac{1}{2}y^2z, -4xz) = (\frac{1}{2}y^2z, -4xz)$. Alternatively, if we start with the pair $(y^2z - x, -4x^2 - y - 3) \in P^2$, we get $\deg_{\sigma,\mathcal{G}}(y^2z - x, -4x^2 - y - 3) = x^3y^2$ and $\mathrm{LF}_{\sigma,\mathcal{G}}(y^2z - x, -4x^2 - y - 3) = (0, -4x^2)$.

Our next goal is to connect the two long exact sequences constructed above. We define a map LM : $P^r \longrightarrow P^r$, which sends 0 to 0 and m to $\mathrm{LM}_\sigma(m)$ if $m \neq 0$. Analogously we define a map LF : $P^s \longrightarrow P^s$ which sends 0 to 0 and m to $\mathrm{LF}_{\sigma,\mathcal{G}}(m)$ if $m \neq 0$. In this way we get the following **fundamental diagram**.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Syz}(\mathcal{G}) & \longrightarrow & P^s & \xrightarrow{\lambda} & P^r & \longrightarrow & P^r/M & \longrightarrow & 0 \\
& & & & \downarrow{\scriptstyle \mathrm{LF}} & & \downarrow{\scriptstyle \mathrm{LM}} & & & & \\
0 & \longrightarrow & \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) & \longrightarrow & P^s & \xrightarrow{\Lambda} & P^r & \longrightarrow & P^r/N & \longrightarrow & 0
\end{array}
$$

This diagram suggests natural questions, for instance whether the vertical maps are homomorphisms (clearly they aren't), and whether the diagram commutes (it doesn't). A more precise answer to the second question is provided by our next proposition.

Proposition 2.3.6. *In the situation described above, let $m \in P^s \setminus \mathrm{Syz}(\mathcal{G})$.*

a) *We have $\mathrm{LT}_\sigma(\lambda(m)) \leq_\sigma \deg_{\sigma,\mathcal{G}}(m)$.*
b) *We have $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ if and only if $\mathrm{LT}_\sigma(\lambda(m)) <_\sigma \deg_{\sigma,\mathcal{G}}(m)$.*
c) *We have $\Lambda(\mathrm{LF}(m)) = \mathrm{LM}(\lambda(m))$ if and only if $\mathrm{LT}_\sigma(\lambda(m)) = \deg_{\sigma,\mathcal{G}}(m)$.*

Now, let $m \in \mathrm{Syz}(\mathcal{G})$ instead.

d) *We have $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Therefore the map LF induces a map*

$$
\mathrm{LF}\,|_{\mathrm{Syz}(\mathcal{G})} : \mathrm{Syz}(\mathcal{G}) \longrightarrow \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))
$$

which we denote by LF again.

Proof. Claim a) follows from the rules for computing with leading terms (see Proposition 1.5.3) and from Proposition 2.3.5.a. Namely, for the element $m = \sum_{j=1}^{s} f_j \varepsilon_j \in P^s \setminus \{0\}$ we calculate

$$
\mathrm{LT}_\sigma(\lambda(m)) = \mathrm{LT}_\sigma(\sum_{j=1}^{s} f_j g_j) \leq_\sigma \max_\sigma\{\mathrm{LT}_\sigma(f_j g_j) \mid j \in \{1,\ldots,s\},\ f_j g_j \neq 0\}
$$
$$
= \deg_{\sigma,\mathcal{G}}(m)
$$

To prove b), we write $m = \sum_{j=1}^{s} f_j \varepsilon_j \in P^s \setminus \{0\}$ and $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \sum_{j=1}^{s} \bar{f}_j \varepsilon_j$ as in Proposition 2.3.5. Then $\Lambda(\mathrm{LF}(m)) = \sum_{j=1}^{s} \bar{f}_j \,\mathrm{LM}_\sigma(g_j) = 0$ is equivalent to the vanishing of the coefficient of $\deg_{\sigma,\mathcal{G}}(m)$ in $\sum_{j=1}^{s} f_j g_j$, i.e. it is equivalent to $\mathrm{LT}_\sigma(\lambda(m)) <_\sigma \deg_{\sigma,\mathcal{G}}(m)$.

To prove c), we note that $\mathrm{LT}_\sigma(\lambda(m)) \neq \deg_{\sigma,\mathcal{G}}(m)$ implies by a) and b) that we have $\Lambda(\mathrm{LF}(m)) = 0$. Since $\lambda(m) \neq 0$, we then get $\mathrm{LM}(\lambda(m)) = \mathrm{LM}_\sigma(\lambda(m)) \neq 0 = \Lambda(\mathrm{LF}(m))$. Conversely, if $\mathrm{LT}_\sigma(\lambda(m)) = \deg_{\sigma,\mathcal{G}}(m)$, then $\mathrm{LM}(\lambda(m)) = \mathrm{LM}_\sigma(\sum_{j=1}^{s} f_j g_j) = \sum_{\{j \mid \bar{f}_j \neq 0\}} \mathrm{LM}_\sigma(f_j g_j) = \sum_{j=1}^{s} \bar{f}_j \,\mathrm{LM}_\sigma(g_j) = \Lambda(\mathrm{LF}(m))$.

Finally we show claim d). Let $m = \sum_{j=1}^{s} f_j \varepsilon_j \in \mathrm{Syz}(\mathcal{G}) \setminus \{0\}$. Starting with $\lambda(m) = 0$, we get that the coefficient of $\deg_{\sigma,\mathcal{G}}(m)$ in $\sum_{j=1}^{s} f_j g_j$ vanishes, and hence $\sum_{\{j \mid \bar{f}_j \neq 0\}} \mathrm{LM}_\sigma(f_j g_j) = \sum_{j=1}^{s} \bar{f}_j \, \mathrm{LM}_\sigma(g_j) = \Lambda(\mathrm{LF}(m)) = 0$.
$\hfill\square$

Let us check the claims of this proposition in our running example.

Example 2.3.2 (continued) Recall that $M = \langle g_1, g_2 \rangle$ is the ideal generated by $g_1 = x^2 - y^2 - x$ and $g_2 = xy^2 - z^3$, and that $\sigma = \mathtt{DegLex}$.

a) The element $m = (y^2, -x)$ of P^2 satisfies $\lambda(m) = y^2 g_1 - x g_2 = -y^4 - xy^2 + xz^3$, and thus $\deg_{\sigma,\mathcal{G}}(m) = x^2 y^2$ is not a scalar multiple of $\mathrm{LM}(\lambda(m)) = \mathrm{LM}_\sigma(\lambda(m)) = xz^3$. Going the other way in the fundamental diagram, we calculate $\mathrm{LF}(m) = (y^2, -x)$ and $\Lambda(\mathrm{LF}(m)) = y^2 \, \mathrm{LM}_\sigma(g_1) - x \, \mathrm{LM}_\sigma(g_2) = 0$. In particular $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Here we have a case where $\mathrm{LT}_\sigma(\lambda(m)) <_\sigma \deg_{\sigma,\mathcal{G}}(m)$ and where $\mathrm{LM}(\lambda(m)) \neq \Lambda(\mathrm{LF}(m))$.

b) The element $m = (x, y)$ of P^2 satisfies $\lambda(m) = xg_1 + yg_2 = x^3 - xy^2 - x^2 + xy^3 - yz^3$, and thus $\deg_{\sigma,\mathcal{G}}(m) = xy^3$ as well as $\mathrm{LM}(\lambda(m)) = xy^3$. On the other hand, we calculate $\mathrm{LF}(m) = (0, y)$ and $\Lambda(\mathrm{LF}(m)) = y \, \mathrm{LM}_\sigma(g_2) = xy^3$. Here we have a case where $\mathrm{LT}_\sigma(\lambda(m)) = \deg_{\sigma,\mathcal{G}}(m)$ and $\mathrm{LM}(\lambda(m)) = \Lambda(\mathrm{LF}(m))$.

In this example the element $m = (y^2, -x)$ satisfies $m \notin \mathrm{Syz}(\mathcal{G})$, whereas $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. The fact that $\mathrm{LF}(m)$ is a syzygy of $\mathrm{LM}_\sigma(\mathcal{G})$ may be considered as a sort of first step in the construction of a syzygy of $\mathcal{G}$. Thus a possible approach to our problem of computing a system of generators for $\mathrm{Syz}(\mathcal{G})$ could be to find elements which generate $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ and to "lift" them to elements of $\mathrm{Syz}(\mathcal{G})$ in some way. The remainder of this section is devoted to studying the feasibility of such an approach. As a first step we see how to obtain an explicit finite set of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

Theorem 2.3.7. (Syzygies of Elements of Monomial Modules)
For $j = 1, \ldots, s$, we write $\mathrm{LM}_\sigma(g_j)$ in the form $\mathrm{LM}_\sigma(g_j) = c_j t_j e_{\gamma_j}$ with $c_j \in K$, $t_j \in \mathbb{T}^n$, and $\gamma_j \in \{1, \ldots, r\}$. For all $i, j \in \{1, \ldots, s\}$, we define $t_{ij} = \frac{\mathrm{lcm}(t_i, t_j)}{t_i}$.

a) *For all $i, j \in \{1, \ldots, s\}$ such that $i < j$ and $\gamma_i = \gamma_j$, the element $\sigma_{ij} = \frac{1}{c_i} t_{ij} \varepsilon_i - \frac{1}{c_j} t_{ji} \varepsilon_j \in P^s$ is a syzygy of $\mathrm{LM}_\sigma(\mathcal{G})$, called a **fundamental syzygy**, and is homogeneous of σ-degree $\deg_{\sigma,\mathcal{G}}(\sigma_{ij}) = \mathrm{lcm}(t_i, t_j) e_{\gamma_i}$.*

b) *We have*
$$\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) = \langle \sigma_{ij} \mid 1 \leq i < j \leq s, \; \gamma_i = \gamma_j \rangle$$

In particular, $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ is a finitely generated $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-graded submodule of P^s.

Proof. To prove a), we note that $\Lambda(\sigma_{ij}) = 0$ and that

$$\deg_{\sigma,\mathcal{G}}(t_{ij} \varepsilon_i) = \frac{\mathrm{lcm}(t_i, t_j)}{t_i} \, \mathrm{LT}_\sigma(g_i) = \mathrm{lcm}(t_i, t_j) e_{\gamma_i}$$

$$=\operatorname{lcm}(t_i, t_j)e_{\gamma_j} \;=\; \tfrac{\operatorname{lcm}(t_i,t_j)}{t_j}\operatorname{LT}_\sigma(g_j) \;=\; \deg_{\sigma,\mathcal{G}}(t_{ji}\varepsilon_j)$$

Now we prove b). In view of a), it is clear that $\operatorname{Syz}(\operatorname{LM}_\sigma(\mathcal{G})) \neq 0$ if and only if there exist $i, j \in \{1, \ldots, s\}$ such that $i < j$ and $\gamma_i = \gamma_j$. Since Λ is a homomorphism of $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-graded P-modules, its kernel is a $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-graded submodule of P^s and has a homogeneous system of generators. Let us consider one of those homogeneous generators and write it as $m = \sum_{j=1}^s a_j \bar{t}_j \varepsilon_j \in P^s \setminus \{0\}$ with $a_j \in K$ and $\bar{t}_j \in \mathbb{T}^n$. There are an index $\mu \in \{1, \ldots, s\}$ and a term $t \in \mathbb{T}^n$ such that $\bar{t}_j \operatorname{LT}_\sigma(g_j) = te_\mu$ whenever $a_j \neq 0$, which is another way of saying that m is homogeneous and $\deg_{\sigma,\mathcal{G}}(m) = te_\mu$. Next, let $\operatorname{size}(m)$ denote the cardinality of the set $\{i \in \{1, \ldots, s\} \mid a_i \neq 0\}$. Since $\Lambda(m) = 0$, we have $\sum_{j=1}^s a_j c_j = 0$, and since $m \neq 0$, it follows that $\operatorname{size}(m) \geq 2$. Hence there are at least two indices α, β such that $a_\alpha \neq 0$ and $a_\beta \neq 0$. From $t = \bar{t}_\alpha t_\alpha = \bar{t}_\beta t_\beta$ we see that t is a multiple of $\operatorname{lcm}(t_\alpha, t_\beta)$, hence

$$\bar{t}_\alpha = \tfrac{t}{t_\alpha} = \tfrac{t}{\operatorname{lcm}(t_\alpha, t_\beta)} t_{\alpha\beta} \quad \text{and} \quad \bar{t}_\beta = \tfrac{t}{t_\beta} = \tfrac{t}{\operatorname{lcm}(t_\alpha, t_\beta)} t_{\beta\alpha}$$

We deduce that the syzygy $\tfrac{t}{\operatorname{lcm}(t_\alpha, t_\beta)}\sigma_{\alpha\beta}$ has the same σ-degree as m. Moreover we see that if $m' = m - a_\alpha c_\alpha \tfrac{t}{\operatorname{lcm}(t_\alpha, t_\beta)}\sigma_{\alpha\beta}$, then $\operatorname{size}(m') < \operatorname{size}(m)$. An obvious inductive argument concludes the proof. $\qquad\square$

As an immediate consequence of the above theorem, it follows that there are no non-zero syzygies if $\gamma_i \neq \gamma_j$ for all $1 \leq i < j \leq s$. This observation is amplified in Exercise 7. Clearly, the proof of the theorem can be used as an algorithm for computing the representation of an element of $\operatorname{Syz}(\operatorname{LM}(\mathcal{G}))$ in terms of the generators σ_{ij}.

Example 2.3.8. Let $n = 3$, let $r = 1$, and let us equip $P = \mathbb{Q}[x, y, z]$ with the term ordering $\sigma = \mathtt{DegRevLex}$. We consider the vector $\mathcal{G} = (g_1, g_2, g_3)$, where $g_1 = 4x^2y - x$, $g_2 = 3xy^3$, and $g_3 = yz - x - 1$. Then we have $\operatorname{LM}_\sigma(\mathcal{G}) = (4x^2y, 3xy^3, yz)$.

The module element $m = (y^2z, -2xz, 2x^2y^2) = y^2z\varepsilon_1 - 2xz\varepsilon_2 + 2x^2y^2\varepsilon_3$ is contained in $\operatorname{Syz}(\operatorname{LM}_\sigma(\mathcal{G}))$, since $y^2z \cdot 4x^2y - 2xz \cdot 3xy^3 + 2x^2y^2 \cdot yz = 0$. Moreover, the element m is homogeneous of σ-degree $\deg_{\sigma,\mathcal{G}}(m) = x^2y^3z$, and we have $\operatorname{size}(m) = 3$.

According to Theorem 2.3.7, we should be able to express m as a combination of σ_{12}, σ_{13}, and σ_{23}. Using the notation of the proof of the theorem, we see that a_1, a_2, a_3 are different from zero. So, let $\alpha = 1$ and $\beta = 2$. We get $\operatorname{lcm}(t_1, t_2) = x^2y^3$, and therefore $\tfrac{x^2y^3z}{\operatorname{lcm}(t_1, t_2)} = \tfrac{x^2y^3z}{x^2y^3} = z$. Thus we form the element $m' = m - a_1 c_1 \tfrac{x^2y^3z}{\operatorname{lcm}(t_1, t_2)}\sigma_{12} = m - 4z\sigma_{12}$. Now we compute $\sigma_{12} = \tfrac{1}{4}y^2\varepsilon_1 - \tfrac{1}{3}x\varepsilon_2 = (\tfrac{1}{4}y^2, -\tfrac{1}{3}x, 0)$ and get $m' = (y^2z, -2xz, 2x^2y^2) - 4z(\tfrac{1}{4}y^2, -\tfrac{1}{3}x, 0) = (0, -\tfrac{2}{3}xz, 2x^2y^2)$. Finally, we determine $\sigma_{23} = \tfrac{1}{3}z\varepsilon_2 - xy^2\varepsilon_3 = (0, \tfrac{1}{3}z, -xy^2)$. It is clear that $(0, -\tfrac{2}{3}xz, 2x^2y^2) = -2x\sigma_{23}$. In conclusion, we find the desired representation $m = 4z\sigma_{12} - 2x\sigma_{23}$.

The next steps in our program are to give a meaning to the process of "lifting" a syzygy of $\mathrm{LM}_\sigma(\mathcal{G})$ to a syzygy of $\mathcal{G}$, and then to study whether such liftings can always be found.

Definition 2.3.9. An element $m \in P^s$ is called a **lifting** of an element $\overline{m} \in P^s$ if we have $\mathrm{LF}(m) = \overline{m}$.

Proposition 2.3.10. *The following conditions are equivalent.*

D_1) *Every homogeneous element of* $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ *has a lifting in* $\mathrm{Syz}(\mathcal{G})$.

D_2) *There exists a homogeneous system of generators of* $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ *consisting entirely of elements which have a lifting in* $\mathrm{Syz}(\mathcal{G})$.

D_3) *There exists a finite homogeneous system of generators of* $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ *consisting entirely of elements which have a lifting in* $\mathrm{Syz}(\mathcal{G})$.

Proof. Since $D_1) \Rightarrow D_3)$ as an immediate consequence of Theorem 2.3.7, and since $D_3) \Rightarrow D_2)$ holds trivially, it suffices to prove that $D_1)$ follows from $D_2)$. Let I be a set, let $\{\overline{m}_i\}_{i \in I}$ be a homogeneous system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ indexed over I, and let $m_i \in \mathrm{Syz}(\mathcal{G})$ be a lifting of $\overline{m}_i$ for every $i \in I$. Given a homogeneous element $\overline{m} \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) \setminus \{0\}$, there exists a natural number h such that we have $\overline{m} = \sum_{j=1}^{h} c_j t_j \overline{m}_{i_j}$ with $c_j \in K \setminus \{0\}$, with $t_j \in \mathbb{T}^n$, and with $i_j \in I$ for $j = 1, \ldots, h$. Clearly, we may assume $\deg_{\sigma,\mathcal{G}}(t_j \overline{m}_{i_j}) = \deg_{\sigma,\mathcal{G}}(\overline{m})$ for $j = 1, \ldots, h$. From the fact that $\mathrm{LF}(t_j m_{i_j}) = t_j \overline{m}_{i_j}$ we conclude $\deg_{\sigma,\mathcal{G}}(t_j m_{i_j}) = \deg_{\sigma,\mathcal{G}}(\overline{m})$. This, in turn, implies $\mathrm{LF}(\sum_{j=1}^{h} c_j t_j m_{i_j}) = \sum_{j=1}^{h} c_j t_j \overline{m}_{i_j} = \overline{m}$, which concludes the proof. $\square$

If we want to find all elements of $\mathrm{Syz}(\mathcal{G})$ using this process of lifting, we need to ascertain that there exists a system of generators of $\mathrm{Syz}(\mathcal{G})$ consisting of liftings. This is achieved by the following proposition whose proof demonstrates once more the power of term orderings.

Proposition 2.3.11. *Let* $\{\overline{m}_1, \ldots, \overline{m}_t\}$ *be a homogeneous system of generators of the module* $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, *and let* $m_1, \ldots, m_t \in \mathrm{Syz}(\mathcal{G})$ *be elements such that* $\mathrm{LF}(m_i) = \overline{m}_i$ *for* $i = 1, \ldots, t$. *Then* $\{m_1, \ldots, m_t\}$ *is a system of generators of* $\mathrm{Syz}(\mathcal{G})$.

Proof. For contradiction we assume that the subset S of $\mathrm{Syz}(\mathcal{G})$ of syzygies which are not generated by $\{m_1, \ldots, m_t\}$ is not empty. By the fundamental property of term orderings (see Theorem 1.4.19), there exists $m \in S$ with minimal $\deg_{\sigma,\mathcal{G}}$. Then there exists a natural number h such that we have $\mathrm{LF}(m) = \sum_{j=1}^{h} c_j t_j \overline{m}_{i_j}$ with $c_j \in K \setminus \{0\}$, with $t_j \in \mathbb{T}^n$, and with $i_j \in \{1, \ldots, t\}$ for $j = 1, \ldots, h$. The element $m' = m - \sum_{i=1}^{h} c_i t_i m_{i_j}$ satisfies either $m' = 0$ or $\deg_{\sigma,\mathcal{G}}(m') <_\sigma \deg_{\sigma,\mathcal{G}}(m)$. In both cases we get a contradiction, and the proof is complete. $\square$

The final proposition in this section is the gem we promised in the introduction.

Proposition 2.3.12. *Let $g_1, \ldots, g_s \in P^r \setminus \{0\}$ and $M = \langle g_1, \ldots, g_s \rangle$. Then Conditions A_1), A_2) of Proposition 2.1.1 and Conditions D_1), D_2), D_3) of Proposition 2.3.10 are equivalent.*

Proof. First we show that Condition A_2) implies D_1). Let $m = \sum_{j=1}^{s} f_j \varepsilon_j$ be a non-zero homogeneous element of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. We may suppose that $\lambda(m) \neq 0$, since in case $\lambda(m) = 0$ we have $m \in \mathrm{Syz}(\mathcal{G})$ and $\mathrm{LF}(m) = m$, i.e. the element m is a lifting of itself. By Condition A_2), the element $\lambda(m)$ has a representation $\lambda(m) = \sum_{i=1}^{s} h_i g_i$ with polynomials $h_1, \ldots, h_s \in P$ such that $\mathrm{LT}_\sigma(\lambda(m)) = \max_\sigma \{\mathrm{LT}_\sigma(h_i g_i) \mid i \in \{1, \ldots, s\}, \ h_i g_i \neq 0\}$. Now we consider the element $h = \sum_{j=1}^{s} h_j \varepsilon_j \in P^s$. We have $m - h \in \mathrm{Syz}(\mathcal{G})$ and $\mathrm{LT}_\sigma(\lambda(m)) = \mathrm{LT}_\sigma(\lambda(h)) = \deg_{\sigma, \mathcal{G}}(h)$. On the other hand, since $\mathrm{LF}(m) = m$ and $\Lambda(\mathrm{LF}(m)) = 0$, Proposition 2.3.6.b yields $\mathrm{LT}_\sigma(\lambda(m)) <_\sigma \deg_{\sigma, \mathcal{G}}(m)$. Altogether, we get $\deg_{\sigma, \mathcal{G}}(m) >_\sigma \deg_{\sigma, \mathcal{G}}(h)$ and $\mathrm{LF}(m - h) = \mathrm{LF}(m) = m$. Thus the element $m - h$ is a lifting of m.

Now let us show the reverse implication. We assume for contradiction that there exists an element $v \in M \setminus \{0\}$ which cannot be represented as requested by Condition A_2). We observe that if $v = \sum_{i=1}^{s} f_i g_i$ for some polynomials $f_1, \ldots, f_s \in P$ and if $m = \sum_{j=1}^{s} f_j \varepsilon_j$, then we have $v = \lambda(m)$. In other words, the element m is a preimage of v under λ. By the fundamental property of term orderings (see Theorem 1.4.19), we know that among all preimages of v under λ, there exists one preimage m with minimal $\deg_{\sigma, \mathcal{G}}(m)$. We cannot have $\deg_{\sigma, \mathcal{G}}(m) = \mathrm{LT}_\sigma(v)$, because otherwise the representation $v = \sum_{i=1}^{s} f_i g_i$ is already of the form required by Condition A_2). Therefore Proposition 2.3.6.a shows that we must have $\mathrm{LT}_\sigma(v) <_\sigma \deg_{\sigma, \mathcal{G}}(m)$. Next, Proposition 2.3.6.b yields $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Thus Condition D_1) gives us an element $m' = \sum_{j=1}^{s} f_j' \varepsilon_j \in \mathrm{Syz}(\mathcal{G})$ such that $\mathrm{LF}(m') = \mathrm{LF}(m)$. In particular, this means that $\deg_{\sigma, \mathcal{G}}(m - m') <_\sigma \deg_{\sigma, \mathcal{G}}(m)$ and $\lambda(m - m') = \lambda(m) = v$, which contradicts the minimality of the σ-degree of m. $\qquad\square$

Exercise 1. Find a term ordering σ and elements $g_1, \ldots, g_s \in P^r \setminus \{0\}$ which generate a submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$ such that Conditions D_1), D_2), and D_3) are not satisfied.

Exercise 2. Find a 2×3-matrix over $P = K[x, y, z]$ whose associated ideal of 2×2-minors is generated by $\{x^2 - y, xy - z, y^2 - xz\}$. By adding suitable rows to this matrix, show how one can produce non-trivial syzygies of the triple $\mathcal{G} = (x^2 - y, xy - z, y^2 - xz)$.

Exercise 3. In the case $n = 2$, $P = \mathbb{Q}[x, y]$, $r = 2$, compute a system of generators of the syzygy module of the tuple $\mathcal{G} = ((xy + y, x), (x - y, y), (x, x + y), (-x, y))$ by hand.

Exercise 4. Let $P = K[x, y, z]$ be a polynomial ring over a field K, let $r = 1$, and let $\mathcal{G} = (x, y, z)$. Compute the syzygy module of a set of generators of $\mathrm{Syz}_P(\mathcal{G})$.

Exercise 5. Give a direct proof for the fact that Condition D_1) of Proposition 2.3.10 implies Condition B_2) of Proposition 2.1.2.
Hint: If $m \in M \setminus \{0\}$ has a leading term outside N, pick a preimage of m under λ of smallest σ-degree and look at the fundamental diagram.

Exercise 6. Let $g_1, \ldots, g_s \in P^r \setminus \{0\}$, let $M = \langle g_1, \ldots, g_s \rangle$, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$.
   a) Prove that $\mathrm{Syz}(\mathcal{G}) = 0$ if and only if M is a free P-module with basis $\{g_1, \ldots, g_s\}$.
   b) Let $s = 3$, let $n = 3$, let $r = 2$, let $g_1 = (x^2, x - y)$, let $g_2 = (0, y)$, and let $g_3 = (xy, z)$. Then show that $\mathrm{Syz}(\mathcal{G}) \neq 0$.

Exercise 7. Let $g_1, \ldots, g_s \in P^r \setminus \{0\}$, let $M = \langle g_1, \ldots, g_s \rangle$, let $\mathcal{G}$ be the s-tuple $(g_1, \ldots, g_s)$, let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, and let $\mathrm{LT}_\sigma(g_i) = t_i e_{\gamma_i}$ with $t_i \in \mathbb{T}^n$ and $\gamma_i \in \{1, \ldots, r\}$ for $i = 1, \ldots, s$.
   a) Prove that M is a free P-module if $\gamma_i \neq \gamma_j$ for all $i \neq j$.
   b) Deduce that the submodule of P^3 generated by the set of vectors $\{(x, y - z, x), (z, y^2 - x, x), (z^2 - y + 1, y^2 - x, x - 3)\}$ is free.

Tutorial 19: Syzygies of Elements of Monomial Modules

Let K be a field, $n \geq 1$, $P = K[x_1, \ldots, x_n]$, $r \geq 1$, and $M \subseteq P^r$ a monomial submodule generated by $\{t_1 e_{\gamma_1}, \ldots, t_s e_{\gamma_s}\}$, where $t_1, \ldots, t_s \in \mathbb{T}^n$ and $\gamma_1, \ldots, \gamma_s \in \{1, \ldots, r\}$.

   a) Use Theorem 2.3.7 to give an explicit system of generators of the syzygy module of $(t_1 e_{\gamma_1}, \ldots, t_s e_{\gamma_s})$. Write a CoCoA function $\mathtt{MonomialSyz}(\ldots)$ which takes a system of generators of a monomial module M as above and computes its first syzygy module.
   b) Show by example that the system of generators of the syzygy module given in a) is in general not minimal, even if $\{t_1 e_{\gamma_1}, \ldots, t_s e_{\gamma_s}\}$ is minimal.
   c) Apply your function $\mathtt{MonomialSyz}(\ldots)$ to compute the syzygy modules of the following tuples.
      1) $(x^{34} y^7, x^{23} y^{19}) \in \mathbb{Q}[x, y]^2$
      2) $(x, y, z) \in \mathbb{Q}[x, y, z]^3$
      3) $(xy, yz, xz) \in \mathbb{Q}[x, y, z]^3$
      4) $(x e_1, y e_1, y e_2, z e_2, x e_3, z e_3) \in (\mathbb{Q}[x, y, z]^3)^6$
   d) Show that if $r = 1$, $1 \leq i < j < k \leq s$, and t_k divides $\mathrm{lcm}(t_i, t_j)$, then the fundamental syzygy σ_{ij} (as defined in Theorem 2.3.7) is in the module generated by σ_{ik} and σ_{jk}.
   e) Write an improved version $\mathtt{MonomialIdealSyz}(\ldots)$ of your program from a) which works for systems of generators of monomial ideals and takes the optimization of part d) into account.
   f) Apply the function $\mathtt{MonomialIdealSyz}(\ldots)$ in the appropriate cases of c). Each time, try to determine whether the computed system of generators of the syzygy module is minimal.

Tutorial 20: Lifting of Syzygies

In this tutorial we shall try to program the lifting of syzygies discussed in the last part of the current section. As usual, let K be a field, let $n \geq 1$, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring, let $r \geq 1$, let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, let $\mathcal{G} = (g_1, \ldots, g_s) \in (P^r)^s$ be a tuple of non-zero vectors, and let $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$. We assume that Conditions D_1), D_2), and D_3) are satisfied. For $i = 1, \ldots, s$, we write $\mathrm{LT}_\sigma(g_i) = t_i e_{\gamma_i}$ with $t_i \in \mathbb{T}^n$ and $1 \leq \gamma_i \leq r$, and, for $i, j \in \{1, \ldots, s\}$ such that $\gamma_i = \gamma_j$, we let $t_{ij} = \mathrm{lcm}(t_i, t_j)/t_i = t_j/\gcd(t_i, t_j)$.

a) Show that, for $1 \leq i < j \leq s$ such that $\gamma_i = \gamma_j$, there are representations

$$\mathrm{LC}_\sigma(g_i)^{-1} t_{ij} g_i - \mathrm{LC}_\sigma(g_j)^{-1} t_{ji} g_j = \sum_{k=1}^{s} f_{ijk} g_k$$

where $f_{ij1}, \ldots, f_{ijs} \in P$, and where $\mathrm{LT}_\sigma(f_{ijk} g_k) <_\sigma \mathrm{LT}_\sigma(t_{ij} g_i)$ for all $k \in \{1, \ldots, s\}$ such that $f_{ijk} \neq 0$.

b) Let $\{\sigma_{ij} \mid 1 \leq i < j \leq s, \ \gamma_i = \gamma_j\}$ be the system of generators of the kernel of the map $\Lambda : P^s \longrightarrow P^r$, $e_i \longmapsto \mathrm{LM}_\sigma(g_i)$ introduced in Theorem 2.3.7. Prove that the elements $s_{ij} = \sigma_{ij} - \sum_{k=1}^{s} f_{ijk} \varepsilon_k$ are liftings of σ_{ij} for all i, j as above.

c) Conclude that the set $\{s_{ij} \mid 1 \leq i < j \leq s, \ \gamma_i = \gamma_j\}$ is a system of generators of the syzygy module $\mathrm{Syz}(\mathcal{G})$.

d) Using the program `Division(...)` from Tutorial 14 as a subfunction, write a CoCoA program `StdRepr(...)` which takes the tuple $\mathcal{G}$ and indices i, j as above and computes a list of polynomials $[f_{ij1}, \ldots, f_{ijs}]$ corresponding to the representation in a).

e) Using the program `MonomialSyz(...)` from Tutorial 19 and `StdRepr(...)` as subfunctions, write a CoCoA program `LiftSyz(...)` which takes the tuple $\mathcal{G}$ and computes the list of all syzygies s_{ij} as in b).

f) Using the module term ordering `DegRevLexPos`, compute the lists of all syzygies σ_{ij} and all s_{ij} in the following cases.

   1) $\mathcal{G} = (x_1^2 - x_2, x_2^2 - x_3, x_3^2 - x_1) \in \mathbb{Q}[x_1, x_2, x_3]^3$
   2) $\mathcal{G} = (x_1 e_1, x_2 e_1, x_3 e_2, x_1 e_3) \in (\mathbb{Q}[x_1, x_2, x_3]^3)^4$
   3) $\mathcal{G} = (x_1 x_4 - x_2 x_3, x_1 x_3^2 - x_2^2 x_4, x_1^2 x_3 - x_2^3, x_2 x_4^2 - x_3^3) \in \mathbb{Q}[x_1, x_2, x_3, x_4]^4$

2.4 Gröbner Bases of Ideals and Modules

> *The motifs of a combination, in themselves simple,*
> *are often interwoven with each other. [...]*
> *The idea which links the motifs is artistic,*
> *it creates something that had never before been there.*
> (Emanuel Lasker)

In the previous three sections we saw many conditions arising from a number of different motifs, and all of them turned out to be equivalent. Whenever such a phenomenon shows up, it is clear that something very important is going on: there must be some fundamental idea behind the scene which needs to be brought to center stage. In our case it is the notion of a *Gröbner basis*. It is one of those rare notions in the history of modern mathematics which was able to deviate the main stream of events. It became a fundamental tool, both for its theoretical and practical consequences.

The section opens by linking the different motifs studied before through the idea of a Gröbner basis. The natural search for the existence of such objects leads to a fairly easy positive answer (see Proposition 2.4.3). Part of this existence result is Hilbert's Basis Theorem 2.4.6 for finitely generated modules over finitely generated K-algebras. Of course it is not necessary to develop the theory of Gröbner bases to achieve that result, but we decided to include it here as an application in order to highlight the theoretical power of Gröbner bases.

Then we become more ambitious and try to solve the problem of computing in residue class modules. Using a Gröbner basis, we define the *normal form* of an element with respect to a submodule and show that it is independent of the Gröbner basis chosen. It agrees with the normal remainder given by the Division Algorithm 1.6.4. Thus it is a unique representative of the residue class of the given element which can be computed by performing the Division Algorithm with respect to any Gröbner basis of the submodule. Consequently, we get a *submodule membership test*, also called *ideal membership test* when $r = 1$, and a new formulation of Macaulay's Basis Theorem.

But what is really striking is another form of uniqueness. In our opinion, it is one of the most important theoretical results of this theory. Given a Gröbner basis of a submodule M of P^r, we can modify its elements in such a way that we get another Gröbner basis with the extra properties of being monic, minimal, and interreduced. Surprisingly, this *reduced Gröbner basis* of M depends only on the module and the chosen term ordering. As we shall see, the possibility of representing a submodule by a unique system of generators has numerous theoretical and practical applications. To give a first support to this claim, we devote the last part of this section to the proof of the existence and uniqueness of the *field of definition* of a given submodule M, i.e. a minimal subfield of K which contains the coefficients of some system of generators of M.

Now we start the main part of this section by recalling that, as usual, we let K be a field, $n \geq 1$, $P = K[x_1, \ldots, x_n]$ a polynomial ring, $r \geq 1$, and σ a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. In the following theorem we collect all the conditions studied in the previous sections.

Theorem 2.4.1. (Characterization of Gröbner Bases)
For a set of elements $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ which generates a submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$, let $\xrightarrow{G}$ be the rewrite rule defined by G, let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$, let λ be the map $\lambda : P^s \longrightarrow P^r$ defined by $\varepsilon_i \mapsto g_i$, and let $\Lambda : P^s \longrightarrow P^r$ be the map defined by $\varepsilon_i \mapsto \mathrm{LM}_\sigma(g_i)$. Then the following conditions are equivalent.

A_1) *For every element $m \in M \setminus \{0\}$, there are $f_1, \ldots, f_s \in P$ such that $m = \sum_{i=1}^s f_i g_i$ and $\mathrm{LT}_\sigma(m) \geq_\sigma \mathrm{LT}_\sigma(f_i g_i)$ for all $i = 1, \ldots, s$ such that $f_i g_i \neq 0$, i.e. such that $\mathrm{LT}_\sigma(m) \geq_\sigma \deg_{\sigma, \mathcal{G}}(\sum_{i=1}^s f_i \varepsilon_i)$.*

A_2) *For every element $m \in M \setminus \{0\}$, there are $f_1, \ldots, f_s \in P$ such that $m = \sum_{i=1}^s f_i g_i$ and $\mathrm{LT}_\sigma(m) = \max_\sigma \{\mathrm{LT}_\sigma(f_i g_i) \mid i \in \{1, \ldots, s\}, f_i g_i \neq 0\}$, i.e. such that $\mathrm{LT}_\sigma(m) = \deg_{\sigma, \mathcal{G}}(\sum_{i=1}^s f_i \varepsilon_i)$.*

B_1) *The set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ generates the $\mathbb{T}^n$-monomodule $\mathrm{LT}_\sigma\{M\}$.*

B_2) *The set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ generates the P-submodule $\mathrm{LT}_\sigma(M)$ of P^r.*

C_1) *For an element $m \in P^r$, we have $m \xrightarrow{G} 0$ if and only if $m \in M$.*

C_2) *If $m \in M$ is irreducible with respect to $\xrightarrow{G}$, then we have $m = 0$.*

C_3) *For every element $m_1 \in P^r$, there is a unique element $m_2 \in P^r$ such that $m_1 \xrightarrow{G} m_2$ and m_2 is irreducible with respect to $\xrightarrow{G}$.*

C_4) *If $m_1, m_2, m_3 \in P^r$ satisfy $m_1 \xrightarrow{G} m_2$ and $m_1 \xrightarrow{G} m_3$, then there exists an element $m_4 \in P^r$ such that $m_2 \xrightarrow{G} m_4$ and $m_3 \xrightarrow{G} m_4$.*

D_1) *Every homogeneous element of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ has a lifting in $\mathrm{Syz}(\mathcal{G})$.*

D_2) *There exists a homogeneous system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ consisting entirely of elements which have a lifting in $\mathrm{Syz}(\mathcal{G})$.*

D_3) *There exists a finite homogeneous system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ consisting entirely of elements which have a lifting in $\mathrm{Syz}(\mathcal{G})$.*

Proof. This follows from Propositions 2.1.3, 2.2.8, and 2.3.12. $\qquad \square$

Definition 2.4.2. Let $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ be a set of elements which generates a submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$. If the conditions of Theorem 2.4.1 are satisfied, then G is called a **Gröbner basis** of M with respect to σ or a σ-**Gröbner basis** of M. In the case $M = \langle 0 \rangle$, we shall say that $G = \emptyset$ is a σ-Gröbner basis of M.

2.4.A   Existence of Gröbner Bases

Our first task is to show the existence of Gröbner bases. If we recall Proposition 1.5.6.b, it is clear that there are elements $g_1, \ldots, g_s \in M$ satisfying Condition B_2). But do they generate M? Our next proposition answers this question affirmatively.

Proposition 2.4.3. (Existence of a σ-Gröbner Basis)
Let M be a non-zero P-submodule of P^r.

a) *Given $g_1, \ldots, g_s \in M \setminus \{0\}$ such that $\mathrm{LT}_\sigma(M) = \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle$, we have $M = \langle g_1, \ldots, g_s \rangle$, and the set $G = \{g_1, \ldots, g_s\}$ is a σ-Gröbner basis of M.*

b) *The module M has a σ-Gröbner basis $G = \{g_1, \ldots, g_s\} \subseteq M \setminus \{0\}$.*

Proof. First we show claim a) by contradiction. Suppose $\langle g_1, \ldots, g_s \rangle \subset M$. By Theorem 1.4.19, there exists an element $m \in M \setminus \langle g_1, \ldots, g_s \rangle$ whose leading term $\mathrm{LT}_\sigma(m)$ is minimal with respect to σ among all elements of that set. Since we have $\mathrm{LT}_\sigma(m) \in \mathrm{LT}_\sigma(M) = \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle$, there are $c \in K \setminus \{0\}$, $t \in \mathbb{T}^n$, and $i \in \{1, \ldots, s\}$ such that $\mathrm{LM}_\sigma(m) = c\, t\, \mathrm{LM}_\sigma(g_i)$. Thus we get $\mathrm{LT}_\sigma(m - c\, t\, g_i) <_\sigma \mathrm{LT}_\sigma(m)$, and hence $m - c\, t\, g_i \in \langle g_1, \ldots, g_s \rangle$, contradicting $m \notin \langle g_1, \ldots, g_s \rangle$.

Claim b) follows from a) using Proposition 1.5.6.b. $\square$

The existence of Gröbner bases implies one of the most important properties of polynomial rings over fields. In Section 1.3 we described the property of being Noetherian in the case of monoideals. Using a similar formulation, we extend it to ideals and modules.

Definition 2.4.4. A ring (resp. module) is called **Noetherian** if every ascending chain of ideals (resp. submodules) becomes eventually stationary.

The following characterizations of Noetherian modules are in complete analogy with the case of Noetherian monoids and can be shown exactly as Proposition 1.3.4.

Proposition 2.4.5. *Let R be a ring and M an R-module. The following conditions are equivalent.*

a) *Every submodule of M is finitely generated.*

b) *Every ascending chain $N_1 \subseteq N_2 \subseteq \cdots$ of submodules of M is eventually stationary.*

c) *Every non-empty set of submodules of M has a maximal element (with respect to inclusion).*

As a consequence of Proposition 2.4.3, we obtain a version of Hilbert's Basis Theorem for finitely generated modules over finitely generated K-algebras.

Theorem 2.4.6. (Hilbert's Basis Theorem)
Every finitely generated module over a finitely generated K-algebra is Noetherian. In particular, $P = K[x_1, \ldots, x_n]$ is a Noetherian ring.

Proof. If we represent the K-algebra in the form P/I with a polynomial ring $P = K[x_1, \ldots, x_n]$ and an ideal $I \subseteq P$, we can view the module M as a finitely generated P-module via the canonical map $P \longrightarrow P/I$. Obviously it suffices to show that every P-submodule of M is finitely generated. Since M is finitely generated, we can represent M in the form $M = P^r/U$ with $r \geq 1$ and a submodule $U \subseteq P^r$. Since every submodule of M is of the form N/U with a submodule $N \subseteq P^r$, it suffices to show that every P-submodule of P^r is finitely generated, and this is an immediate consequence of Proposition 2.4.3.   □

2.4.B   Normal Forms

Our next application of Gröbner bases is to show how they help us to perform effective calculations in a residue class module P^r/M. Several attempts to solve this question have failed so far, because we were not able to find a unique representative in P^r for a residue class in P^r/M. Using a Gröbner basis, we now find that all those attempts lead to the same unique answer.

Let $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ be a σ-Gröbner basis of $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$, and let $m \in P^r$. By Condition C_3), there exists a unique element $m_G \in P^r$ such that $m \xrightarrow{G} m_G$ and such that m_G is irreducible with respect to $\xrightarrow{G}$. A priori this element seems to depend on the Gröbner basis chosen, but indeed it does not, as the following proposition shows.

Proposition 2.4.7. *In the above situation, m_G is the unique element of P^r with the properties that $m - m_G \in M$ and $\operatorname{Supp}(m_G) \cap \operatorname{LT}_\sigma\{M\} = \emptyset$. In particular, it does not depend on the particular σ-Gröbner basis chosen.*

Proof. We know that $m - m_G \in M$ and that the support of m_G does not intersect $\operatorname{LT}_\sigma\{M\}$. Uniqueness follows from the observation that, for two such elements m_G and m_H, the support of $m_G - m_H \in M$ does not intersect $\operatorname{LT}_\sigma\{M\}$, and this is, by Condition C_2), only possible if $m_G - m_H = 0$.   □

Definition 2.4.8. Let $M \subseteq P^r$ be a non-zero module, and let $m \in P^r$. The element $m_G \in P^r$ described above is called the **normal form** of m with respect to σ. It is denoted by $\operatorname{NF}_{\sigma,M}(m)$, or simply by $\operatorname{NF}_\sigma(m)$ if it is clear which submodule is considered.

Below we collect some properties of normal forms. In particular, we see that the Division Algorithm with respect to a Gröbner basis provides an effective method for computing normal forms.

Corollary 2.4.9. *In the above situation, let* $\mathcal{G} = (g_1, \ldots, g_s)$.

   a) *If* $m \in P^r$, *then* $\mathrm{NR}_{\sigma,\mathcal{G}}(m)$ *agrees with* $\mathrm{NF}_\sigma(m)$. *In particular, the nor-mal remainder does not depend on the order of the elements* $g_1, \ldots, g_s$.

   b) *For* $m_1, m_2 \in P^r$, *we have* $\mathrm{NF}_\sigma(m_1 - m_2) = \mathrm{NF}_\sigma(m_1) - \mathrm{NF}_\sigma(m_2)$.

   c) *For* $m \in P^r$, *we have* $\mathrm{NF}_\sigma(\mathrm{NF}_\sigma(m)) = \mathrm{NF}_\sigma(m)$.

Proof. Claim a) follows from $m - \mathrm{NR}_{\sigma,\mathcal{G}}(m) \in M$ and from the fact that the support of $\mathrm{NR}_{\sigma,\mathcal{G}}(m)$ does not meet $\mathrm{LT}_\sigma\{M\}$. Next we show b). We have $m_1 - m_2 - (\mathrm{NF}_\sigma(m_1) - \mathrm{NF}_\sigma(m_2)) = (m_1 - \mathrm{NF}_\sigma(m_1)) - (m_2 - \mathrm{NF}_\sigma(m_2)) \in M$ and $\mathrm{NF}_\sigma(m_1) - \mathrm{NF}_\sigma(m_2)$ is irreducible with respect to $\xrightarrow{G}$. The uniqueness of such an element yields the conclusion. Claim c) follows similarly, because $\mathrm{NF}_\sigma(m) - \mathrm{NF}_\sigma(m) = 0 \in M$ and $\mathrm{NF}_\sigma(m)$ is irreducible with respect to $\xrightarrow{G}$. $\qquad\square$

For the purposes of actual computations, one of the most useful appli-cations of normal forms is the possibility to check whether an element is contained in a submodule or whether one submodule is contained in another.

Proposition 2.4.10. (Submodule Membership Test)
Let $\{g_1, \ldots, g_s\} \subseteq P^r$ *generate a* P*-submodule* $M = \langle g_1, \ldots, g_s \rangle$ *of* P^r, *and let* $\{h_1, \ldots, h_t\} \subseteq P^r$ *generate a* P*-submodule* $N = \langle h_1, \ldots, h_t \rangle \subseteq P^r$.

   a) *For* $m_1, m_2 \in P^r$, *we have* $m_1 - m_2 \in M$ *if and only if* $\mathrm{NF}_{\sigma,M}(m_1) = \mathrm{NF}_{\sigma,M}(m_2)$. *In particular, an element* $m \in P^r$ *satisfies* $m \in M$ *if and only if* $\mathrm{NF}_{\sigma,M}(m) = 0$.

   b) *We have* $N \subseteq M$ *if and only if* $\mathrm{NF}_{\sigma,M}(h_i) = 0$ *for* $i = 1, \ldots, t$.

   c) *The condition* $M = N$ *is equivalent to* $\mathrm{NF}_{\sigma,N}(g_i) = \mathrm{NF}_{\sigma,M}(h_j) = 0$ *for* $i = 1, \ldots, s$ *and* $j = 1, \ldots, t$.

   d) *If* $N \subseteq M$ *and* $\mathrm{LT}_\sigma\{M\} \subseteq \mathrm{LT}_\sigma\{N\}$, *then* $M = N$.

Proof. To show the first claim, let $m_1, m_2 \in P^r$ such that $m_1 - m_2 \in M$. Then $0 = \mathrm{NF}_{\sigma,M}(m_1 - m_2) = \mathrm{NF}_{\sigma,M}(m_1) - \mathrm{NF}_{\sigma,M}(m_2)$ by Corollary 2.4.9.b. Conversely, let $\mathrm{NF}_{\sigma,M}(m_1) = \mathrm{NF}_{\sigma,M}(m_2)$. In this case, the claim follows from $m_1 - m_2 = (m_1 - \mathrm{NF}_{\sigma,M}(m_1)) - (m_2 - \mathrm{NF}_{\sigma,M}(m_2)) \in M$.

Clearly, claim b) is a consequence of a), and claim c) follows from b). Thus it remains to prove claim d). Since we have $N \subseteq M$, it is clear that $\mathrm{LT}_\sigma\{N\} \subseteq \mathrm{LT}_\sigma\{M\}$. Thus the hypothesis that we have the other inclusion $\mathrm{LT}_\sigma\{M\} \subseteq \mathrm{LT}_\sigma\{N\}$ implies equality $\mathrm{LT}_\sigma\{N\} = \mathrm{LT}_\sigma\{M\}$. Now take an element $m \in M$. We have $\mathrm{Supp}(\mathrm{NF}_{\sigma,N}(m)) \cap \mathrm{LT}_\sigma\{N\} = \emptyset$, and therefore $\mathrm{Supp}(\mathrm{NF}_{\sigma,N}(m)) \cap \mathrm{LT}_\sigma\{M\} = \emptyset$. The uniqueness in Proposition 2.4.7 shows that $\mathrm{NF}_{\sigma,N}(m) = 0$, i.e. we get $m \in N$. $\qquad\square$

As an important application of the notion of Gröbner basis, we get a new version of Macaulay's Basis Theorem 1.5.7.

Corollary 2.4.11. (New Version of Macaulay's Basis Theorem)
Let $M \subseteq P^r$ be a P-submodule, let $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ be a σ-Gröbner basis of M, and let B be the set of all terms in $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ which are not a multiple of any term in the set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$. Then the residue classes of the elements of B form a K-basis of P^r/M.

Proof. The fact that G is a σ-Gröbner basis of M implies that $\mathrm{LT}_\sigma\{M\}$ is generated by $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ by Condition $B_1)$ of Theorem 2.4.1. So the statement follows immediately from Theorem 1.5.7. $\square$

2.4.C   Reduced Gröbner Bases

In the last part of this section we address the question of uniqueness of Gröbner bases and provide an application of it. Given a module term ordering σ, a submodule $M \subseteq P^r$ has many σ-Gröbner bases. For instance, we can add arbitrary elements of M to a σ-Gröbner basis and it remains a σ-Gröbner basis of M. However, there is a unique one which satisfies the following additional conditions.

Definition 2.4.12. Let $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ and $M = \langle g_1, \ldots, g_s \rangle$. We say that G is a **reduced σ-Gröbner basis** of M if the following conditions are satisfied.
a) For $i = 1, \ldots, s$, we have $\mathrm{LC}_\sigma(g_i) = 1$.
b) The set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ is a minimal system of generators of $\mathrm{LT}_\sigma(M)$.
c) For $i = 1, \ldots, s$, we have $\mathrm{Supp}(g_i - \mathrm{LT}_\sigma(g_i)) \cap \mathrm{LT}_\sigma\{M\} = \emptyset$.

Theorem 2.4.13. (Existence and Uniqueness of Reduced Gröbner Bases)
For every P-submodule $M \subseteq P^r$, there exists a unique reduced σ-Gröbner basis.

Proof. We start by proving existence. Let $G = \{g_1, \ldots, g_s\}$ be any σ-Gröbner basis of M. If we replace g_i by $\mathrm{LC}_\sigma(g_i)^{-1} g_i$ for $i = 1, \ldots, s$, we obtain a Gröbner basis with property a). By Condition $B_2)$ of Theorem 2.4.1, the monomial module $\mathrm{LT}_\sigma(M)$ is generated by $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$. Then we use Proposition 1.3.11.b to get from this set the unique minimal system of generators of $\mathrm{LT}_\sigma(M)$. After possibly renumbering the vectors we may assume that this minimal system of generators is $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_t)\}$, where $t \leq s$. And using again Condition $B_2)$ and Proposition 2.4.3.a, we see that the set $G' = \{g_1, \ldots, g_t\}$ is a σ-Gröbner basis of M which satisfies conditions a) and b) of the definition.

   Now we write $g_i = \mathrm{LT}_\sigma(g_i) + h_i$, and if we let $g_i' = \mathrm{LT}_\sigma(g_i) + \mathrm{NF}_\sigma(h_i)$ for $i = 1, \ldots, t$, we can form the set $G'' = \{g_1', \ldots, g_t'\}$. We claim that G'' is a reduced σ-Gröbner basis of M. Since $g_i' = g_i - (h_i - \mathrm{NF}_\sigma(h_i))$, we use

Proposition 2.4.7 and get $g_i' \in M$ for $i = 1, \ldots, t$. By Condition B_2), the set G'' is a σ-Gröbner basis of M. Since it clearly satisfies conditions a) and b) of the definition, it remains to prove that it also satisfies condition c). Indeed, for every $i \in \{1, \ldots, t\}$, no term in $\mathrm{Supp}(\mathrm{NF}_\sigma(h_i))$ lies in $\mathrm{LT}_\sigma\{M\}$, because $\mathrm{NF}_\sigma(h_i)$ is irreducible with respect to $\xrightarrow{G'}$.

Finally, to show uniqueness, we assume that $G = \{g_1, \ldots, g_s\}$ and $H = \{h_1, \ldots, h_t\}$ are two reduced σ-Gröbner bases of M. From the fact that the minimal monomial system of generators of a monomial module is unique (see Proposition 1.3.11.b), we conclude $s = t$ and that we can renumber the elements of H such that $\mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(h_i)$ for $i = 1, \ldots, s$. Moreover, for $i = 1, \ldots, s$, we have $g_i - h_i \in M$, and $g_i - h_i$ is, by condition c) of the definition, irreducible with respect to $\xrightarrow{G}$. Thus property C_2) of Theorem 2.4.1 proves $g_i = h_i$ for $i = 1, \ldots, s$.   □

As an application of the existence and uniqueness of reduced σ-Gröbner bases we can show the existence and uniqueness of a field of definition for submodules of P^r.

Definition 2.4.14. Let K be a field, $P = K[x_1, \ldots, x_n]$ a polynomial ring, and $M \subseteq P^r$ a P-submodule.

a) Let $k \subseteq K$ be a subfield. We say that M is **defined over** k if there exist elements in $k[x_1, \ldots, x_n]^r$ which generate M as a P-module.

b) A subfield $k \subseteq K$ is called a **field of definition** of M if M is defined over k and there exists no proper subfield $k' \subset k$ such that M is defined over k'.

It is clear that if a field of definition of a P-submodule $M \subseteq P^r$ exists, it has to contain the prime field of K. Let us look at a concrete example.

Example 2.4.15. Let $I \subseteq \mathbb{C}[x_1, x_2, x_3]$ be the ideal generated by the set $\{x_1^2 - \sqrt{5}x_1x_2 + 3x_1x_3 + 2\sqrt{5}x_3^2, \ x_1x_2 - \sqrt{2}x_3^2, \ 2x_1x_2 + \sqrt{3}x_3^2\}$. Obviously, the ideal I is defined over $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$.

But it is also easy to check that $I = (x_1^2 + 3x_1x_3, \ x_1x_2, \ x_3^2)$. Therefore, the ideal I is defined over the prime field $\mathbb{Q}$ of $\mathbb{C}$, and the unique field of definition of I is $\mathbb{Q}$.

The following lemma captures one important aspect of the proof of the existence and uniqueness of the field of definition.

Lemma 2.4.16. *Let $K' \subseteq K$ be a field extension, let $P' = K'[x_1, \ldots, x_n]$, let $M' \subseteq (P')^r$ be a P'-submodule of $(P')^r$, and let M be the P-submodule of P^r generated by the elements of M'.*

a) *A σ-Gröbner basis of M' is also a σ-Gröbner basis of M. In particular, we have $\mathrm{LT}_\sigma\{M'\} = \mathrm{LT}_\sigma\{M\}$.*

b) *The reduced σ-Gröbner basis of M' is also the reduced σ-Gröbner basis of M.*

Proof. Let $G = \{g_1, \ldots, g_s\} \subseteq (P')^r \setminus \{0\}$ be a σ-Gröbner basis of M'. Since the set G generates the P'-module M' and the set M' generates the P-module M, the set G generates the P-module M.

Let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$. Using Theorem 2.3.7, we see that $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) = \langle \sigma_{ij} \mid 1 \leq i < j \leq s, \gamma_i = \gamma_j \rangle$, where $\sigma_{ij} \in (P')^s$ is given by $\sigma_{ij} = \frac{1}{c_i} t_{ij} \varepsilon_i - \frac{1}{c_j} t_{ji} \varepsilon_j$. By Condition D_1) of Theorem 2.4.1, the elements σ_{ij} have liftings in $(P')^s$. These liftings are also liftings in P^s of the elements σ_{ij} if we consider those as elements of P^s. Using Condition D_3) of Theorem 2.4.1, we deduce that G is in fact a σ-Gröbner basis of M. This proves a).

To prove b), we observe that the extra conditions required in Definition 2.4.12 are independent of the base field. $\qquad\square$

Theorem 2.4.17. (Existence and Uniqueness of the Field of Definition)
Let M be a non-zero P-submodule of P^r.

a) *There exists a unique field of definition of M.*
b) *Given any module term ordering σ, let G be the corresponding reduced σ-Gröbner basis of M. Then the field of definition of M is the field generated over the prime field of K by the coefficients of the terms in the support of the vectors in G.*

Proof. Let σ be a module term ordering, and let G be the reduced σ-Gröbner basis of M. Moreover, let k be the field generated over the prime field of K by the coefficients of the elements of G. Since the set G generates M, the module M is defined over k.

Suppose now that $K' \subseteq K$ is a subfield over which M is defined, i.e. suppose there exists a system of generators $\{m_1, \ldots, m_t\}$ of the P-module M which is contained in $K'[x_1, \ldots, x_n]^r \setminus \{0\}$. Let $G' = \{g'_1, \ldots, g'_s\} \subseteq K'[x_1, \ldots, x_n]^r$ be the reduced σ-Gröbner basis of the $K'[x_1, \ldots, x_n]$-module $\langle m_1, \ldots, m_t \rangle \subseteq K'[x_1, \ldots, x_n]^r$. Since the reduced σ-Gröbner basis of a module is unique, Lemma 2.4.16.b implies $G = G'$. From this we infer that $k \subseteq K'$.

The facts that M is defined over k, and that every other field over which M is defined contains k, together imply both claims of the theorem. $\qquad\square$

Exercise 1. Let $I = (g)$ with $g \in P \setminus \{0\}$ be a principal ideal in P. Show that $G = \{g\}$ is a Gröbner basis of I with respect to every term ordering.

Exercise 2. Let $m_1, \ldots, m_s \in P^r$ be terms, and let $M = \langle m_1, \ldots, m_s \rangle$. Show that $\{m_1, \ldots, m_s\}$ is a Gröbner basis of M with respect to every term ordering.

Exercise 3. Let $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ be a σ-Gröbner basis of the P-module $M = \langle g_1, \ldots, g_s \rangle$, and let $m \in M$. Show that $G \cup \{m\}$ is a σ-Gröbner basis of M.

Exercise 4. Let $g_1 = x_2 - x_1^2$ and $g_2 = x_3 - x_1^3$ be polynomials in $K[x_1, x_2, x_3]$. Find a term ordering σ on $\mathbb{T}^3$ such that $G = \{g_1, g_2\}$ is a σ-Gröbner basis of the ideal $I = (g_1, g_2)$, and a term ordering τ such that it is not.

Exercise 5. Let $P = K[x_1, \ldots, x_n]$, let $m \leq n$, let $G = \{f_1, f_2, \ldots, f_m\}$, where $f_i \in K[x_i]$ for $i = 1, \ldots, m$, and let $I \subseteq P$ be the ideal generated by G.

a) Use Condition C_3) of Theorem 2.4.1 to show that G is a σ-Gröbner basis of I with respect to every term ordering σ.

b) If, moreover, the polynomials f_i are monic, show that G is the reduced σ-Gröbner basis of I with respect to every term ordering σ.

Exercise 6. Let R be a Noetherian integral domain. Show that the following conditions are equivalent.

a) For all $a, b \in R \setminus \{0\}$, the ideal $(a) \cap (b)$ is principal.

b) The ring R is factorial.

Hint: Use Exercise 6 in Section 1.2.

Exercise 7. Using Corollary 2.4.11 and CoCoA, find a set of terms whose residue classes form a basis of $\mathbb{Z}/(5)[x, y, z]/(x^2 - yz, y^3 + z^3, z^5 - x^2 y^2)$ as a $\mathbb{Z}/(5)$-vector space. (*Hint:* You may use the CoCoA function `GBasis(...)`.)

Exercise 8. A system of generators $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ of a P-module $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$ is called a **minimal σ-Gröbner basis** of M if $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ is a minimal system of generators of $\mathrm{LT}_\sigma(M)$.

a) Prove that any two minimal σ-Gröbner bases of M have the same number of elements.

b) Give an example of a module M which has two different minimal σ-Gröbner bases, all of whose elements g_i have leading coefficients $\mathrm{LC}_\sigma(g_i) = 1$.

Exercise 9. Let σ be a term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. We set $\mathrm{LT}_\sigma(0) = \infty$. In particular, we are assuming $\mathrm{LT}_\sigma(g) <_\sigma \mathrm{LT}_\sigma(0)$ for every $g \in P^r$. Given a tuple $(g_1, \ldots, g_s) \in (P^r)^s$, we identify it with the tuple $(g_1, \ldots, g_s, 0) \in (P^r)^{s+1}$, hence with $(g_1, \ldots, g_s, 0, 0) \in (P^r)^{s+2}$, and so on.

For two tuples $\mathcal{G} = (g_1, \ldots, g_s) \in (P^r)^s$ and $\mathcal{G}' = (g_1', \ldots, g_{s'}') \in (P^r)^{s'}$, we define $\mathcal{G} \preceq \mathcal{G}'$ if and only if $\mathrm{LT}_\sigma(\mathcal{G}) \leq_{\mathrm{Lex}} \mathrm{LT}_\sigma(\mathcal{G}')$. This means that either there exists an index $i \geq 1$ such that $\mathrm{LT}_\sigma(g_i) <_\sigma \mathrm{LT}_\sigma(g_i')$ and $\mathrm{LT}_\sigma(g_j) = \mathrm{LT}_\sigma(g_j')$ for $1 \leq j < i$, or we have $\mathcal{G} = \mathcal{G}'$.

A tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of elements in P^r is said to be **increasingly ordered** with respect to σ if $\mathrm{LT}_\sigma(g_1) \leq_\sigma \cdots \leq_\sigma \mathrm{LT}_\sigma(g_s)$. It is said to be **interreduced** if $g_i \neq 0$ for $i = 1, \ldots, s$ and $\mathrm{LT}_\sigma(g_i)$ does not divide any term in $\mathrm{Supp}(g_j)$ for $i, j \in \{1, \ldots, s\}$ such that $i \neq j$. Finally, the tuple $\mathcal{G}$ it is called **monic** if all its components are monic.

a) For $g_1, \ldots, g_s, g_{s+1}, \ldots, g_t \in P^r$, show $(g_1, \ldots, g_s, g_{s+1}, \ldots, g_t) \preceq (g_1, \ldots, g_s)$.

b) Prove that the relation $\preceq$ is reflexive and transitive, but not a total ordering on the set of the increasingly ordered tuples of elements of P^r.

c) Let M be a non-zero submodule of P^r, and let $\mathcal{G}$ be an increasingly ordered, interreduced tuple of elements of M. Show that the following conditions are equivalent.

  1) With respect to $\preceq$, the tuple $\mathcal{G}$ is minimal among all increasingly ordered, interreduced, monic tuples of elements of M.

  2) The tuple $\mathcal{G}$ is obtained by increasingly ordering the reduced σ-Gröbner basis of M.

Exercise 10. Let I be an ideal of $P = K[x_1, \ldots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, and let Γ be a group of K-algebra automorphisms of P. Show by example that if I is Γ-stable (i.e. if $\gamma(I) \subseteq I$ for all $\gamma \in \Gamma$), then the reduced σ-Gröbner basis of I need not be Γ-stable.

Tutorial 21: Linear Algebra

The purpose of this tutorial is to show how Gaußian Elimination in Linear Algebra relates to the theory of Gröbner bases. Let K be a field, let $m, n > 0$, and let $\mathcal{A} = (a_{ij})$ be an $m \times n$-matrix with coefficients in K. We equip the ring $P = K[x_1, \ldots, x_n]$ with the lexicographic term ordering Lex.

a) Write a CoCoA program RowReduce(...) which uses row operations to bring the matrix $\mathcal{A}$ into row echelon form and then returns the matrix $\mathcal{B} = (b_{ij})$ obtained in this way.

b) For $i = 1, \ldots, m$, let $f_i = a_{i1}x_1 + \cdots + a_{in}x_n$ and $g_i = b_{i1}x_1 + \cdots + b_{in}x_n$. Show that $G = \{g_i \mid 1 \leq i \leq m, \ g_i \neq 0\}$ is a Lex-Gröbner basis of the ideal $I = (f_1, \ldots, f_m)$.

c) Find and prove an algorithm which computes the Lex-Gröbner basis of an ideal I of P which is generated by polynomials of degree ≤ 1.

d) Implement your algorithm in a CoCoA function LinearGB(...) which takes a list of polynomials of degree ≤ 1 generating I and returns the Lex-Gröbner basis of I.

e) Use LinearGB(...) to compute the Lex-Gröbner bases of the following ideals.

  1) $I_1 = (3x_1 - 6x_2 - 2x_3, 2x_1 - 4x_2 + 4x_4, x_1 - 2x_2 - x_3 - x_4) \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]$

  2) $I_2 = (x_1 + x_2 + x_3, x_1 - x_2, x_1 - x_3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$

  3) $I_3 = (x_1 + 1, x_2 + x_3 + 1, x_4 + x_5 + 1, x_1 + x_4 - 1) \subseteq \mathbb{Q}[x_1, \ldots, x_5]$

Tutorial 22: Reduced Gröbner Bases

In this tutorial we shall implement an algorithm to find the reduced Gröbner basis from an arbitrary one, and we shall study various particular cases of reduced Gröbner bases. So let K be a field, $n \geq 1$, $P = K[x_1, \ldots, x_n]$, $r \geq 1$, σ a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, and $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ a σ-Gröbner basis of the P-submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$.

a) Implement the method described in the proof of Theorem 2.4.13. Write a CoCoA function `ReduceGB(...)` which takes any σ-Gröbner basis of M and computes the reduced σ-Gröbner basis from it.

b) Apply your function `ReduceGB(...)` in the following cases, assuming each time that the given sets are `Lex`-Gröbner bases of the ideals they generate.

  1) $G_1 = \{x^2 + y^2 + 1, \ x^2y + 2xy + x, \ -2xy - x + y^3 + y, \ -y^5 - 2y^4 + y^2 + y - 2\} \subseteq \mathbb{Z}/(5)[x, y]$.
  2) $G_2 = \{xz^3 - x - 3y^6 - 18y^4 - 12y^3 - 18y^2 - 12y - 3, \ 15x - y^6 - 12y^5 - 79y^3 - 24y^2 - 67y + z^3 - 26, \ y^6 + 6y^4 + 4y^3 + 6y^2 + 4y - z^3 + 2, \ z^3 - 1\} \subseteq \mathbb{Q}[x, y, z]$.
  3) $G_3 = \{x^2 + y - 1, \ xy - 2y^2 + 2y, \ 4y^3 - 7y^2 + 3y, \ 1/2x^2 + 1/2xy - y^2 + 3/2y - 1/2\} \subseteq \mathbb{Q}[x, y]$.

c) Now we equip the polynomial ring P with its standard grading (see Example 1.7.2). Prove that an ideal $I \subseteq P$ is homogeneous if and only if its reduced σ-Gröbner basis consists of homogeneous polynomials.
   Hint: First show that any homogeneous ideal has a σ-Gröbner basis consisting of homogeneous polynomials.

d) Let $m \geq 1$, let $\mathcal{A} = (a_{ij})$ be an $m \times n$-matrix with coefficients in K, and let $f_i = a_{i1}x_1 + \cdots + a_{in}x_n$ for $i = 1, \ldots, m$. Using row operations only, we bring $\mathcal{A}$ to reduced row echelon form $\mathcal{B} = (b_{ij})$, i.e. in the row echelon form we clear out everything starting from the bottom. For the non-zero rows numbered $i = 1, \ldots, t$ of $\mathcal{B}$, we form the linear polynomials $g_i = b_{i1}x_1 + \cdots + b_{in}x_n$. Prove that $\{g_1/\mathrm{LC}_{\mathtt{Lex}}(g_1), \ldots, g_t/\mathrm{LC}_{\mathtt{Lex}}(g_t)\}$ is the reduced `Lex`-Gröbner basis of the ideal $I = (f_1, \ldots, f_m)$ of P.

e) Write a CoCoA program `LinRedGB(...)` which computes the reduced `Lex`-Gröbner basis of an ideal $I = (f_1, \ldots, f_m)$ as in d) using the method described there.

f) Apply your function `LinRedGB(...)` to the ideals I_1 and I_2 of Tutorial 21.e. Check your results by comparing them to the results of `LinearGB(...)` and `ReduceGB(...)`.

g) Suppose that $\{m_1, \ldots, m_t\} \subseteq P^r \setminus \{0\}$ is any system of generators of the P-module M, and that $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$ is the reduced σ-Gröbner basis of M. Then there are matrices $\mathcal{A} = (a_{ij})$ and $\mathcal{B} = (b_{ij})$ with coefficients in P such that $m_i = a_{i1}g_1 + \cdots + a_{is}g_s$ for $i = 1, \ldots, t$ and $g_j = b_{j1}m_1 + \cdots + b_{jt}m_t$ for $j = 1, \ldots, s$. Give an example in which $\mathcal{A}\mathcal{B}$ is not the identity matrix.

2.5 Buchberger's Algorithm

> *Knowing $+$ and $\times$ is good enough,*
> *understanding their interaction is* ideal.
> (Bruno Buchberger)

In the last section we saw some theoretical applications of Gröbner bases, especially of reduced Gröbner bases. But Gröbner bases would be hardly more than a small side subject in commutative algebra if we did not have the possibility of computing them. The key to almost all applications of Gröbner bases in Computational Commutative Algebra, and therefore to the remainder of these volumes, is the algorithm developed by Bruno Buchberger in his doctoral thesis [Bu65].

Knowing that every ideal has a unique reduced Gröbner basis is good enough, but actually computing it is *ideal*. This computation is based on the characterization of Gröbner bases via lifting of syzygies. The idea is that we need to check whether the set of generators satisfies Condition D_3). If a syzygy of the leading terms is found which does not lift to a syzygy of the generators, we can find an element of the module which has a *new* leading term. By adding it to the set of generators, we can achieve the desired lifting. Then the termination of the algorithm is guaranteed by Dickson's Lemma (more precisely, by Corollary 1.3.10), and its correctness follows from the fact that lifting of syzygies characterizes Gröbner bases (see Theorem 2.4.1).

Since Buchberger's Algorithm is the basic tool underlying most calculations in Computational Commutative Algebra, it is very important to study possibilities for optimizing it. First indications on how to avoid some unnecessary steps in the execution of the algorithm are given in Remark 2.5.6 and Proposition 2.5.8. Some additional possibilities are contained in Tutorial 25. For the case of systems of generators consisting of homogeneous polynomials or vectors of polynomials, an efficient version of Buchberger's Algorithm will be explained in Volume 2.

At the end of this section we discuss the Extended Buchberger Algorithm. Besides a Gröbner basis, it also yields the change of basis matrix from the given system of generators to the Gröbner basis (see Proposition 2.5.11).

As usual, let K be a field, let $n \geq 1$, let $P = K[x_1, \dots, x_n]$ be a polynomial ring, let $r \geq 1$, and let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \dots, e_r \rangle$. Our goal is to compute a σ-Gröbner basis of a P-submodule $M \subseteq P^r$ which is explicitly given by a system of generators $G = \{g_1, \dots, g_s\} \subseteq P^r \setminus \{0\}$. Let $\mathcal{G}$ be the tuple $(g_1, \dots, g_s)$. We start by writing $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ with $c_i \in K \setminus \{0\}$, $t_i \in \mathbb{T}^n$, and $\gamma_i \in \{1, \dots, r\}$ for $i = 1, \dots, s$, and by recalling the fundamental diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Syz}(\mathcal{G}) & \longrightarrow & P^s & \xrightarrow{\lambda} & P^r & \longrightarrow & P^r/M & \longrightarrow & 0 \\
& & & & \big\downarrow{\scriptstyle \mathrm{LF}} & & \big\downarrow{\scriptstyle \mathrm{LM}} & & & & \\
0 & \longrightarrow & \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) & \longrightarrow & P^s & \xrightarrow{\Lambda} & P^r & \longrightarrow & P^r/N & \longrightarrow & 0
\end{array}
$$

studied in Section 2.3. Then we introduce or recall the following abbreviations.

Definition 2.5.1. Let $\mathbb{B}$ be the set $\mathbb{B} = \{(i, j) \mid 1 \leq i < j \leq s, \gamma_i = \gamma_j\}$. The elements of $\mathbb{B}$ are called the **critical pairs** of $\mathcal{G}$. Moreover, we let $t_{ij} = \frac{\mathrm{lcm}(t_i, t_j)}{t_i} = \frac{t_j}{\gcd(t_i, t_j)} \in \mathbb{T}^n$ and $\sigma_{ij} = \frac{1}{c_i} t_{ij} \varepsilon_i - \frac{1}{c_j} t_{ji} \varepsilon_j \in P^s$ for all $i, j \in \{1, \ldots, s\}$. For every critical pair $(i, j) \in \mathbb{B}$, we call

$$S_{ij} = \lambda(\sigma_{ij}) = \frac{1}{c_i} t_{ij} \, g_i - \frac{1}{c_j} t_{ji} \, g_j \in M$$

the **S-vector** of g_i and g_j. If $r = 1$, we call $S_{ij} \in P$ also the **S-polynomial** of g_i and g_j.

We can rephrase Theorem 2.3.7 by saying that if $(i, j) \in \mathbb{B}$ is a critical pair, then the fundamental syzygy σ_{ij} is a homogeneous element of P^s with $\deg_{\sigma, G}(\sigma_{ij}) = \mathrm{lcm}(t_i, t_j) e_{\gamma_i}$ and that the set $\Sigma = \{\sigma_{ij} \mid (i, j) \in \mathbb{B}\}$ is a homogeneous system of generators of the P-module $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Furthermore, we know by Theorem 2.4.1 that G is a σ-Gröbner basis of M if and only if all fundamental syzygies σ_{ij} have liftings in $\mathrm{Syz}(\mathcal{G})$. For some of them, this is always the case.

Proposition 2.5.2. Let $(i, j) \in \mathbb{B}$ be such that $S_{ij} \xrightarrow{G} 0$. Then σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$.

Proof. If $S_{ij} = 0$, there is nothing to show, since σ_{ij} is a lifting of itself. Thus we may assume $S_{ij} \neq 0$. In view of Lemma 2.2.6, we can use $S_{ij} \xrightarrow{G} 0$ to obtain a representation $S_{ij} = \sum_{k=1}^{s} f_k g_k$ with $f_1, \ldots, f_s \in P$ such that $\mathrm{LT}_\sigma(S_{ij}) = \max_\sigma \{\mathrm{LT}_\sigma(f_k g_k) \mid 1 \leq k \leq s, \ f_k g_k \neq 0\}$. Since σ_{ij} is homogeneous, we have $\Lambda(\mathrm{LF}(\sigma_{ij})) = \Lambda(\sigma_{ij}) = 0$, and Proposition 2.3.6.b yields $\deg_{\sigma, G}(\sigma_{ij}) >_\sigma \mathrm{LT}_\sigma(S_{ij})$. Now we consider the element $\tau_{ij} = \sigma_{ij} - \sum_{k=1}^{s} f_k \varepsilon_k \in P^s$. From $\deg_{\sigma, G}(\sum_{k=1}^{s} f_k \varepsilon_k) = \mathrm{LT}_\sigma(S_{ij}) <_\sigma \deg_{\sigma, G}(\sigma_{ij})$ we deduce that $\mathrm{LF}_{\sigma, G}(\tau_{ij}) = \sigma_{ij}$. From $\lambda(\tau_{ij}) = \lambda(\sigma_{ij}) - S_{ij} = 0$ and $\mathrm{LF}(\tau_{ij}) = \sigma_{ij}$ we conclude that τ_{ij} is a lifting of σ_{ij} in $\mathrm{Syz}(\mathcal{G})$. $\qquad\square$

Corollary 2.5.3. (Buchberger's Criterion)
Let $M \subseteq P^r$ be a P-submodule generated by $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$, and let $\mathcal{G} = (g_1, \ldots, g_s)$. Then the following conditions are equivalent.

a) *The set G is a σ-Gröbner basis of M.*
b) *For all critical pairs $(i, j) \in \mathbb{B}$, we have $\mathrm{NR}_{\sigma, \mathcal{G}}(S_{ij}) = 0$.*

Proof. If G is a σ-Gröbner basis of M, then $S_{ij} \in M$ yields $\mathrm{NR}_{\sigma, \mathcal{G}}(S_{ij}) = 0$ by Corollary 2.4.9.a and Proposition 2.4.10.a. Conversely, if condition b) holds, then $S_{ij} \xrightarrow{G} 0$. Using Proposition 2.5.2 we see that, for every pair $(i, j) \in \mathbb{B}$, the element σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$. Thus Condition D_3) of Theorem 2.4.1 holds. $\qquad\square$

Let us see how this criterion applies in practice. The following example also shows that *the leading term ideal of the square of an ideal is, in general,* NOT *the square of the leading term ideal.*

Example 2.5.4. Let $P = \mathbb{Q}[x, y, z]$, let $\sigma = \text{DegRevLex}$, and let I be the ideal of P generated by $g_1 = x^2 - y^2$, $g_2 = xy^2 - z^3$, and $g_3 = y^4 - xz^3 = -y^2 g_1 + x g_2$. Successively, we compute

$$S_{12} = y^2 g_1 - x g_2 = -y^4 + xz^3 \xrightarrow{g_3} 0$$
$$S_{13} = y^4 g_1 - x^2 g_3 = -y^6 + x^3 z^3 \xrightarrow{g_3} x^3 z^3 - xy^2 z^3 \xrightarrow{g_1} 0$$
$$S_{23} = y^2 g_2 - x g_3 = -y^2 z^3 + x^2 z^3 \xrightarrow{g_1} 0$$

Thus Buchberger's Criterion applies and says that $\{g_1, g_2, g_3\}$ is a σ-Gröbner basis of I. In particular, the leading term ideal of I is $\text{LT}_\sigma(I) = (x^2, xy^2, y^4)$.

By the way, in this example the obvious inclusion $\text{LT}_\sigma(I)^2 \subseteq \text{LT}_\sigma(I^2)$ is a strict one, disproving a claim in [CLS92], p. 443. More precisely, the element $f = g_2^2 - g_1 g_3 = y^6 + x^3 z^3 - 3xy^2 z^3 + z^6 \in I^2$ has a leading term $\text{LT}_\sigma(f) = y^6$ which is not in $\text{LT}_\sigma(I)^2$.

The idea of Buchberger's Algorithm is to enlarge G in such a way that eventually all elements σ_{ij} with $(i, j) \in \mathbb{B}$ have a lifting in $\text{Syz}(\mathcal{G})$. By Theorem 2.4.1, this ensures that the enlarged set is a σ-Gröbner basis of M.

Theorem 2.5.5. (Buchberger's Algorithm)
Let $(g_1, \ldots, g_s) \in (P^r)^s$ be a tuple of non-zero elements which generate a submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$. For $i = 1, \ldots, s$, let $\text{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ with $c_i \in K \setminus \{0\}$, $t_i \in \mathbb{T}^n$, and $\gamma_i \in \{1, \ldots, r\}$. Consider the following sequence of instructions.

1) *Let $\mathcal{G} = (g_1, \ldots, g_s)$, $s' = s$ and $B = \{(i, j) \mid 1 \le i < j \le s', \gamma_i = \gamma_j\}$.*
2) *If $B = \emptyset$, return the result $\mathcal{G}$. Otherwise, choose a critical pair $(i, j) \in B$ and delete it from B.*
3) *Compute $S_{ij} = \dfrac{t_j}{c_i \gcd(t_i, t_j)} g_i - \dfrac{t_i}{c_j \gcd(t_i, t_j)} g_j$ and $\text{NR}_{\sigma, \mathcal{G}}(S_{ij})$. If the result is $\text{NR}_{\sigma, \mathcal{G}}(S_{ij}) = 0$, continue with step 2).*
4) *Increase s' by one. Append $g_{s'} = \text{NR}_{\sigma, \mathcal{G}}(S_{ij})$ to $\mathcal{G}$ and the set of critical pairs $\{(i, s') \mid 1 \le i < s', \gamma_i = \gamma_{s'}\}$ to B. Then continue with step 2).*

This is an algorithm, i.e. it stops after finitely many steps. It returns a tuple $\mathcal{G}$ of vectors which form a σ-Gröbner basis of M.

Proof. Every time step 2) is executed, one critical pair is cancelled from B. The set B is enlarged only in step 4). When this happens, an element is appended to $\mathcal{G}$ which has a leading term with respect to σ which is not in the monomodule generated by the leading terms of the previous elements of $\mathcal{G}$. Corollary 1.3.10 shows that P^r cannot contain an infinite chain

$$\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle \subset \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s+1}) \rangle \subset \cdots$$

Therefore step 4) can be executed only a finite number of times, i.e. the procedure stops after finitely many steps.

It remains to show that when the algorithm stops, the vectors in the resulting tuple $\mathcal{G}$ form a σ-Gröbner basis of M. Let s'' be the number of elements of the resulting tuple $\mathcal{G}$. During the execution of the procedure all pairs (i, j) such that $1 \leq i < j \leq s''$ and $\gamma_i = \gamma_j$ are considered, since whenever s' is increased in step 4), all necessary new pairs (i, s') are added to B. By Corollary 2.5.3, it suffices to show that, for every such pair (i, j), we have $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$. If at a certain step $S_{ij} = 0$ or $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$, there is nothing to prove. If at a certain step $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) \neq 0$, then $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ is added to the tuple $\mathcal{G}$. Hence $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ reduces to 0 via the rewrite rule defined by the vectors in the new tuple. $\qquad \square$

A closer look at this proof shows that a number of variants and optimizations of Buchberger's Algorithm are possible. Some of the most effective ones will be discussed in Tutorial 25 and in Volume 2. Here we limit ourselves to pointing out some obvious opportunities for improvement.

Remark 2.5.6. (First Optimizations of Buchberger's Algorithm)

a) In Buchberger's Algorithm, one can substitute the computation of the normal remainder $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ by any procedure producing an element $m \in P^r$ which satisfies $S_{ij} \xrightarrow{\mathcal{G}} m$, and $\mathrm{LT}_\sigma(m) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s'}) \rangle$ if $m \neq 0$.

b) If $\mathbb{B}' \subseteq \mathbb{B}$ is a subset with the property that also the set $\{\sigma_{ij} \mid (i, j) \in \mathbb{B}'\}$ generates $\mathrm{Syz}(\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))$, it suffices to start with $B = \mathbb{B}'$ in step 1) of Buchberger's Algorithm. This follows from Proposition 2.3.11.

c) In step 2) of the theorem we did not specify which critical pair $(i, j) \in B$ we should choose. One possibility is to take the pair (i, j) for which $\mathrm{lcm}(t_i, t_j)$ is minimal with respect to σ. This is called the **normal selection strategy**. It works well in practice if the term ordering σ is degree-compatible. Another possibility which avoids sorting the terms $\mathrm{lcm}(t_i, t_j)$ with respect to σ is to take any pair (i, j) for which the degree of $\mathrm{lcm}(t_i, t_j)$ is minimal.

To help the reader understand Theorem 2.5.5 better, we now apply Buchberger's Algorithm in a concrete case.

Example 2.5.7. Let $n = 2$, let $r = 1$, let $M \subseteq P = K[x, y]$ be the ideal generated by $g_1 = x^2$ and $g_2 = xy + y^2$. We compute a Gröbner basis of M with respect to $\sigma = \mathtt{Lex}$ and follow the steps of Buchberger's Algorithm.

1) Let $\mathcal{G} = (g_1, g_2)$, $s' = 2$ and $B = \{(1, 2)\}$.
2) Choose $(1, 2) \in B$ and set $B = \emptyset$.
3) We compute $S_{12} = yg_1 - xg_2 = -xy^2 \xrightarrow{g_2} y^3 = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{12}) \neq 0$.

4) Let $s' = 3$, let $\mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = y^3$, and let $B = \{(1,3), (2,3)\}$. Then return to step 2).

2) Choose $(1,3) \in B$ and set $B = \{(2,3)\}$.

3) We compute $S_{13} = y^3 g_1 - x^2 g_3 = 0$ and return to step 2).

2) Choose $(2,3) \in B$ and set $B = \emptyset$.

3) We compute $S_{23} = y^2 g_2 - x g_3 = y^4$. Then we calculate $S_{23} \xrightarrow{g_3} 0 = \mathrm{NR}_{\sigma, \mathcal{G}}(S_{23})$ and return to step 2).

2) Since $B = \emptyset$, we return the result $\mathcal{G} = (g_1, g_2, g_3)$.

If $r = 1$, i.e. if M is an ideal in P, there is another optimization of Buchberger's Algorithm which turns out to be useful in practise.

Proposition 2.5.8. *Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero polynomials, let $I = (g_1, \ldots, g_s) \subseteq P$, and let $t_i = \mathrm{LT}_\sigma(g_i)$ for $i = 1, \ldots, s$. Suppose that $\gcd(t_i, t_j) = 1$ for some pair $(i, j) \in \mathbb{B}$. Then σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$.*

Proof. This follows from the observations that $\sigma_{ij} = \frac{1}{c_i} t_j \varepsilon_i - \frac{1}{c_j} t_i \varepsilon_j$ and that $\tau_{ij} = \frac{1}{c_i c_j} g_j \varepsilon_i - \frac{1}{c_i c_j} g_i \varepsilon_j$ is a lifting of σ_{ij} in $\mathrm{Syz}(\mathcal{G})$. $\qquad\square$

Remark 2.5.9. For $f, g \in P$, the pair $(-g, f)$ is called the **trivial syzygy** of (f, g). Therefore Proposition 2.5.8 can be rephrased by saying that if $\gcd(t_i, t_j) = 1$, then the trivial syzygy of $(\mathrm{LM}_\sigma(g_i), \mathrm{LM}_\sigma(g_j))$ can be lifted to the trivial syzygy of (g_i, g_j).

The above result can be used to detect some special Gröbner bases.

Corollary 2.5.10. *Let $G = \{g_1, \ldots, g_s\} \subseteq P \setminus \{0\}$, and let $I = (g_1, \ldots, g_s)$. Assume that the leading terms of the elements $g_1, \ldots, g_s$ are pairwise coprime. Then G is a σ-Gröbner basis of I.*

Proof. Let $\mathcal{G} = (g_1, \ldots, g_s)$. By Proposition 2.5.8, every element σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$. Thus G satisfies Condition D_3) of Theorem 2.4.1. $\qquad\square$

Finally, we can extend Buchberger's Algorithm in such a way that it not only computes a Gröbner basis of a submodule $M \subseteq P^r$, but also a matrix of polynomials which describes how the Gröbner basis can be expressed in terms of the original system of generators of M.

Proposition 2.5.11. (The Extended Buchberger Algorithm)
Let $(g_1, \ldots, g_s) \in (P^r)^s$ be a tuple of non-zero vectors in P^r which generate a submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$. We write $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ with $c_i \in K \setminus \{0\}$, $t_i \in \mathbb{T}^n$, and $\gamma_i \in \{1, \ldots, r\}$ for $i = 1, \ldots, s$. Consider the following sequence of instructions.

1) *Let $\mathcal{G} = (g_1, \ldots, g_s)$, let $s' = s$, let $\mathcal{A}$ be the $s \times s$ identity matrix, and let $B = \{(i, j) \mid 1 \le i < j \le s, \gamma_i = \gamma_j\}$.*

2) *If $B = \emptyset$, return the result $(\mathcal{G}, \mathcal{A})$. Otherwise, choose a critical pair $(i, j) \in B$ and delete it from B.*

3) *Using the Division Algorithm, find $q_1, \ldots, q_{s'} \in P$ and $p \in P^r$ such that $S_{ij} = q_1 g_1 + \cdots + q_{s'} g_{s'} + p$ and the conditions of Theorem 1.6.4 hold. If $p = 0$, continue with step 2).*

4) *If $p \neq 0$ in step 3), then increase s' by one, append $g_{s'} = p$ to $\mathcal{G}$, add $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ to B, and append the column vector $\frac{t_j}{c_i \gcd(t_i, t_j)} a_i - \frac{t_i}{c_j \gcd(t_i, t_j)} a_j - q_1 a_1 - \cdots - q_{s'-1} a_{s'-1}$ to $\mathcal{A}$, where $a_1, \ldots, a_{s'-1}$ denote the previous columns of $\mathcal{A}$. Continue with step 2).*

This is an algorithm, i.e. it stops after finitely many steps. It returns a tuple $\mathcal{G} = (g_1, \ldots, g_{s'})$ of vectors which form a σ-Gröbner basis of M, where $s' \geq s$, together with an $s \times s'$-matrix $\mathcal{A} = (a_{ij})$ of polynomials such that $g_j = a_{1j} g_1 + \cdots + a_{sj} g_s$ for $j = 1, \ldots, s'$.

Proof. In view of Theorem 2.5.5, it suffices to prove the last claim. Each time a new column is appended to $\mathcal{A}$ in step 4), we have $g_j = a_{1j} g_1 + \cdots + a_{sj} g_s$ for $j < s'$, where s' is the current number of columns of $\mathcal{A}$. Now the calculation

$$
\begin{aligned}
g_{s'} = p &= S_{ij} - q_1 g_1 - \cdots - q_{s'-1} g_{s'-1} \\
&= \tfrac{t_{ij}}{c_i}(a_{1i} g_1 + \cdots + a_{si} g_s) - \tfrac{t_{ji}}{c_j}(a_{1j} g_1 + \cdots + a_{sj} g_s) \\
&\quad - \sum_{k=1}^{s'-1} q_k (a_{1k} g_1 + \cdots + a_{sk} g_s) \\
&= (g_1, \ldots, g_s) \cdot \left(\tfrac{t_j}{c_i \gcd(t_i, t_j)} a_i - \tfrac{t_i}{c_j \gcd(t_i, t_j)} a_j - q_1 a_1 - \cdots - q_{s'-1} a_{s'-1} \right) \\
&= (g_1, \ldots, g_s) \cdot (a_{1s'}, \ldots, a_{ss'})^{\mathrm{tr}} = a_{1s'} g_1 + \cdots + a_{ss'} g_s
\end{aligned}
$$

finishes the proof. $\square$

To show how this extended algorithm works in practice, let us apply it in the situation of Example 2.5.7.

Example 2.5.12. Let $n = 2$, let $r = 1$, let $M \subseteq P = K[x, y]$ be the ideal generated by $g_1 = x^2$ and $g_2 = xy + y^2$. As in Example 2.5.7, we follow the steps of the Buchberger Algorithm, except that we now use the extended version above.

1) Let $\mathcal{G} = (g_1, g_2)$, let $s' = 2$, let $\mathcal{A} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$, and let $B = \{(1,2)\}$.

2) Choose $(1,2) \in B$ and set $B = \emptyset$.

3) We compute $S_{12} = -xy^2 = 0 \cdot g_1 + (-y) \cdot g_2 + y^3$ and let $q_1 = 0$, $q_2 = -y$, and $p = y^3$.

4) Let $s' = 3$, let $\mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = y^3$, and let $B = \{(1,3), (2,3)\}$. We append the column vector $y a_1 - x a_2 - 0 \cdot a_1 + y a_2$ to the matrix $\mathcal{A}$ and get $\mathcal{A} = \left(\begin{smallmatrix} 1 & 0 & y \\ 0 & 1 & -x+y \end{smallmatrix} \right)$. Then we return to step 2).

2) Choose $(1,3) \in B$ and set $B = \{(2,3)\}$.

3) We compute $S_{13} = y^3 g_1 - x^2 g_3 = 0$ and return to step 2).

2) Choose $(2,3) \in B$ and set $B = \emptyset$.

3) We compute $S_{23} = y^4 = 0 \cdot g_1 + 0 \cdot g_2 + y g_3$. Then we return to step 2).

2) Since $B = \emptyset$, we return the result $(\mathcal{G}, \mathcal{A})$, where $\mathcal{G} = (g_1, g_2, g_3)$ and $\mathcal{A} = \left(\begin{smallmatrix} 1 & 0 & y \\ 0 & 1 & -x+y \end{smallmatrix} \right)$.

Exercise 1. Let $P = K[x, y, z]$, let $\mathcal{F} = (x^2 - y, xy - z) \in P^2$, and let $\sigma = \texttt{DegRevLex}$. Perform all steps of Buchberger's Algorithm applied to $\mathcal{F}$. Then find a term ordering σ such that $\mathcal{F}$ is a σ-Gröbner basis of the ideal $(x^2 - y, xy - z)$.

Exercise 2. Apply Buchberger's Algorithm as in Example 2.5.7 to compute a $\texttt{DegLexPos}$-Gröbner basis of the submodule $M = \langle g_1, g_2, g_3, g_4 \rangle$ of $\mathbb{Q}[x, y]^3$ in the following cases.

a) $g_1 = (x^2, xy, y^2)$, $g_2 = (y, 0, x)$, $g_3 = (0, x, y)$, $g_4 = (y, 1, 0)$
b) $g_1 = (y - x, y, y)$, $g_2 = (xy, x, x)$, $g_3 = (x, y, y)$, $g_4 = (x, y, 0)$
c) $g_1 = (0, y, x)$, $g_2 = (0, x, xy - x)$, $g_3 = (y, x, 0)$, $g_4 = (y^2, y, 0)$

Exercise 3. In the cases of Exercise 2, determine representatives for a K-basis of $\mathbb{Q}[x, y]^3 / M$.

Exercise 4. Find out which module $M \subseteq \mathbb{Q}[x, y]^3$ in Exercise 2 contains the vector

$$m = (x^2 y - y^2 + xy^2, \; xy^2 - y^2 + x^2 + 2xy - x - y, \; x^2 y + xy^2 - 3xy + x)$$

Exercise 5. A polynomial $f \in P = K[x_1, \ldots, x_n]$ is called a **binomial** if it is of the form $f = at + a't'$ with $a, a' \in K \setminus \{0\}$ and $t, t' \in \mathbb{T}^n$. Let σ be a term ordering on $\mathbb{T}^n$ and I a **binomial ideal**, i.e. an ideal generated by binomials.

a) Prove that every element of the reduced σ-Gröbner basis of I is a binomial or a monomial.
b) Given a term $t \in \mathbb{T}^n$, show that $\mathrm{NF}_{\sigma, I}(t)$ is a scalar multiple of a term.

Exercise 6. Consider the polynomial ring $P = \mathbb{Q}[x, y]$, the P-submodule $M = \langle g_1, g_2, g_3, g_4 \rangle \subseteq P^3$ such that $g_1 = (xy, x, y)$, $g_2 = (y^2 + y, x + y^2, x)$, $g_3 = (-x, y, x)$, $g_4 = (y^2, y, x)$, and the module term ordering $\sigma = \texttt{LexPos}$.

a) Using the algorithm given in Proposition 2.5.11, compute a σ-Gröbner basis $\{g_1, \ldots, g_{s'}\}$ of M, where $s' \geq 4$, and a matrix $\mathcal{A}$ such that $(g_1, \ldots, g_{s'}) = (g_1, \ldots, g_4) \cdot \mathcal{A}$.
b) Now use the method described in the proof of Proposition 2.4.13 to compute the reduced σ-Gröbner basis $\{g_1', \ldots, g_6'\}$ of M. Then find a matrix $\mathcal{A}'$ such that $(g_1', \ldots, g_6') = (g_1, \ldots, g_4) \cdot \mathcal{A}'$.
c) For the following elements of P^3, check whether they lie in M, and if they do, find their representations in terms of both $\{g_1', \ldots, g_6'\}$ and $\{g_1, \ldots, g_4\}$.
   1) $m_1 = (-2y, y - 1, xy + y)$
   2) $m_2 = (xy^5 - xy + y, xy^4 + x + 2y^2 - y, y^5 + xy)$
d) For the following pairs of elements of P^3, check whether $m_1 + M$ agrees with $m_2 + M$ in the residue class module P^3 / M.
   1) $m_1 = (2y, x^2 y + x^2 + xy + 2x - 3y, -x + y)$, $m_2 = (-x^2 + y - x, x^3 + 2x^2, x^2 - y)$
   2) $m_1 = (x^3 + x^2 + y - x, x^2 + x, x + y)$, $m_2 = (y, x^3 + 2x^2 - xy - y, 0)$

Tutorial 23: Buchberger's Criterion

In this tutorial we shall implement Buchberger's Criterion 2.5.3 and use it to decide whether certain sets of polynomials are Gröbner bases of the ideals they generate. As in the whole section, we let K be a field, we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over K, we let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, where $r \geq 1$, we let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero vectors, and we let $M \subseteq P^r$ be the P-submodule generated by the vectors in $\mathcal{G}$.

a) Write a CoCoA function `CheckGB(...)` which takes $\mathcal{G}$ and uses Buchberger's Criterion 2.5.3 to check whether it forms a σ-Gröbner basis of M. (*Hint:* You may want to use the function `NormalRemainder(...)` from Tutorial 15 or the built-in CoCoA function `NR(...)`.)

b) Let $G = \{x_2 - x_1^2, x_3 - x_1^3\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$. Use the function `CheckGB(...)` to check whether G is a σ-Gröbner basis of the ideal it generates, where σ is one of the following term orderings: `Lex`, `DegLex`, `Ord(V)` where $V = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ or $V = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

c) Use the function `CheckGB(...)` to determine which of the following systems of generators are Gröbner bases with respect to the stated term orderings of the ideals and modules they generate. In the first three cases, try to find a term ordering and a system of generators containing G such that Corollary 2.5.10 can be applied.

1) $G = \{x_1 x_2^2 - x_1 x_3 + x_2, x_1 x_2 - x_3^2, x_1 - x_2 x_3^4\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `Lex`

2) $G = \{x_1^4 x_2^2 - x_3^5, x_1^3 x_2^3 - 1, x_1^2 x_2^4 - 2x_3\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `DegLex`

3) $G = \{x_1 x_3 - x_2^2, x_1 x_4 - x_2 x_3, x_2 x_4 - x_3^2\} \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]$ with respect to `DegRevLex`

4) $G = \{(x_1^2 - x_2 x_3)(e_1 + e_2), (x_1 x_3 - x_2 x_4)(e_1 - e_2), (x_3^2 - x_1 x_4)e_1, (x_3^2 - x_1 x_4)e_2\} \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]^2$ with respect to `PosDegRevLex` and `DegRevLexPos`

5) $G = \{(x_1 - x_2^2)e_1, (x_1 - x_3^3)e_1, (x_2 - x_1^2)e_2, (x_2 - x_3^3)e_2, (x_3 - x_1^2)e_3, (x_3 - x_2^3)e_3\} \subseteq \mathbb{Q}[x_1, x_2, x_3]^3$ with respect to `PosDegRevLex` and `DegRevLexPos`

d) Let $n > 1$, and let σ be the lexicographic term ordering on $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ such that $x_1 >_\sigma \cdots >_\sigma x_n >_\sigma y_1 >_\sigma \cdots >_\sigma y_n$. Moreover, for $i = 1, \ldots, n$, let $s_i = \sum_{1 \leq j_1 < \cdots < j_i \leq n} x_{j_1} \cdots x_{j_i}$ be the ith elementary symmetric polynomial in $x_1, \ldots, x_n$ (see also Tutorial 12), and let $h_{i,j} = \sum_{\alpha_j + \cdots + \alpha_n = i} x_j^{\alpha_j} \cdots x_n^{\alpha_n}$ for $i, j = 1, \ldots, n$. Use Buchberger's Criterion to prove that the polynomials

$$g_i = (-1)^i (y_i - s_i) + \sum_{j=1}^{i-1} (-1)^j h_{i-j,i} (y_j - s_j)$$

such that $i = 1, \ldots, n$ form a σ-Gröbner basis of the polynomial ideal $I = (y_1 - s_1, \ldots, y_n - s_n)$.

e) Verify the result of d) for $n = 1, \ldots, 5$ by applying your function `CheckGB(...)`. Can you compute this for larger n? How far can you go?

Tutorial 24: Computing Some Gröbner Bases

The purpose of this tutorial is to implement a first version of Buchberger's Algorithm in the case of polynomial ideals, and to use it to study some particular examples. For instance, we will see that the elements of the reduced Gröbner basis of an ideal can have very high degree, even if the generators of the ideals have low degrees.

Then, for the specific ideal $I = (yz - z^2, xz - z^2, xy - z^2)$, you will be guided to find *all* possible reduced Gröbner bases of I, and to give a meaning to the picture on the cover of this book. As usual, we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K.

a) Write a CoCoA function `SPoly(...)` which takes a tuple of non-zero polynomials $(g_1, \ldots, g_s)$ and indices $i, j \in \{1, \ldots, s\}$ with $i \neq j$ as arguments and returns the S-polynomial S_{ij} of g_i and g_j with respect to the current term ordering.

b) Implement Buchberger's Algorithm 2.5.5 in the case of polynomial ideals. To this end, write a CoCoA program `FirstGB(...)` which takes a tuple of non-zero polynomials generating the ideal and computes a Gröbner basis with respect to the current term ordering. (*Hint:* For step 3), use the built-in function `NR(...)` or `NormalRemainder(...)` of Tutorial 15.)

c) Using `FirstGB(...)`, calculate the Gröbner bases of the following ideals with respect to the stated term orderings.

1) $I = (x_2^2, \, x_1 x_2 x_3 + x_3^3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `DegRevLex`

2) $I = (x_1^2 x_2 - 1, \, x_1 x_2^2 - x_1) \subseteq \mathbb{Q}[x_1, x_2]$ with respect to `Lex` and `DegLex`

3) $I = (x_1 - x_3^4, \, x_2 - x_3^5) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `Lex` and `DegRevLex`

d) Prove that for every number $m \geq 1$, the reduced Gröbner basis of

$$I_m = (x_1^{m+1} - x_2 x_3^{m-1} x_4, \, x_1 x_2^{m-1} - x_3^m, \, x_1^m x_3 - x_2^m x_4) \subseteq K[x_1, x_2, x_3, x_4]$$

with respect to `DegRevLex` contains $f_m = x_3^{m^2+1} - x_2^{m^2} x_4$. Note that the degree $m^2 + 1$ of this polynomial is much higher than the degrees of the generators of I_m. Can you write down the whole reduced Gröbner basis of I_m with respect to `DegRevLex`? (Guess it or prove it!)

e) If you couldn't do the second part of d), calculate the reduced Gröbner basis of the ideal I_m with respect to `DegRevLex` using `FirstGB(...)` for $m = 1, \ldots, 100$ and determine its length.

f) Prove that the ideal I_3 of part d) has (up to sign) the same reduced Gröbner bases with respect to `Lex` and `DegRevLex`. Does this hold for all $m \geq 1$?

In the remainder of this tutorial, we want to study the polynomial ideal $I = (xy - z^2, xz - z^2, yz - z^2)$ in $P = K[x, y, z]$. Although we are not going to use it, we mention that I is the ideal of all polynomials which vanish at three lines in $\mathbb{A}_K^3$ passing through the origin, or, equivalently, at three points in $\mathbb{P}_K^2$ (see Tutorials 27 and 35).

g) Let σ be any term ordering such that $x >_\sigma z$ and $y >_\sigma z$. Show that the reduced σ-Gröbner basis of I is $\{xz - z^2, yz - z^2, xy - z^2\}$.

h) Let σ be any term ordering such that $x >_\sigma z$ and $z >_\sigma y$. Show that the reduced σ-Gröbner basis of I is $\{xy - yz, xz - yz, z^2 - yz\}$.

i) Let σ be any term ordering such that $y >_\sigma z$ and $z >_\sigma x$. Show that the reduced σ-Gröbner basis of I is $\{z^2 - xz, yz - xz, xy - xz\}$.

j) Consider the situation where σ is a term ordering such that $z >_\sigma x$ and $z >_\sigma y$. Show that there are only two possible reduced Gröbner bases of I, according as $x >_\sigma y$ or $y >_\sigma x$. Observe that in both cases the number of elements in the reduced Gröbner basis is four.

k) Prove there are exactly five reduced Gröbner bases of I.

l) Group the term orderings in five classes, depending on the inequalities considered before. Then find five term orderings which give rise to the five reduced Gröbner bases you found above.

m) Prove that for each of the five reduced Gröbner bases, there is an infinite set of term orderings σ such that it is the reduced σ-Gröbner basis of I.

n) Consider the description of term orderings by matrices explained in Section 1.4. Try to use it to interpret the following picture.
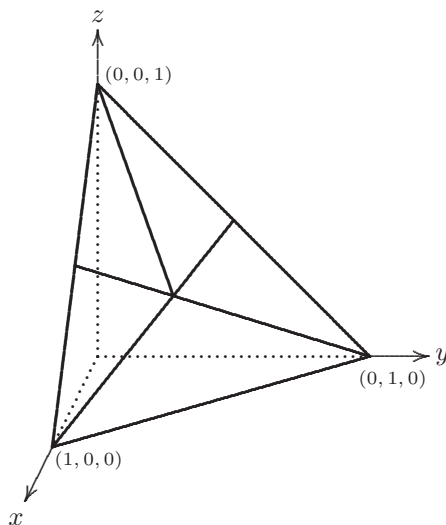
Tutorial 25: Some Optimizations of Buchberger's Algorithm

The purpose of this tutorial is to find and to implement optimized versions of Buchberger's Algorithm in the case of polynomial ideals. The amount of time consumed by a certain Gröbner basis computation depends largely on the number of critical pairs which have to be dealt with, and on the number of reduction steps which have to be performed in order to treat each critical pair. Therefore we will ask you to implement *counters* in your programs which measure these quantities, and we will judge our progress towards our goal of optimizing Buchberger's Algorithm by looking at the numbers returned by those counters.

Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $I \subseteq P$ be an ideal, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero polynomials which generate I. Furthermore, let σ be a term ordering, and let the elements $t_i, t_{ij} \in \mathbb{T}^n$, $\sigma_{ij} \in P^s$, and $S_{ij} \in P$ be defined as at the beginning of this section.

a) Update your CoCoA function `FirstGB(...)` from Tutorial 24 such that it returns not only a σ-Gröbner basis of I, but also the number of critical pairs (i, j) such that $S_{ij} \neq 0$, i.e. such that the normal remainder had to be computed, and the total number of reduction steps which were necessary to compute all those normal remainders.
   Hint: You will have to modify the function `NormalRemainder(...)` from Tutorial 15 suitably.

b) Apply your new function `FirstGB(...)` in the following five cases. Each time, compute a Gröbner basis with respect to `DegRevLex` and one with respect to `Lex`.

   1) $I = (x_1^2 - 2x_2^2 + 3x_1,\ x_1^3 - 2x_1x_2)$ in $\mathbb{Q}[x_1, x_2]$
   2) $I = (x_1 - 2x_3^4,\ x_2 - 3x_3^5)$ in $\mathbb{Q}[x_1, x_2, x_3]$
   3) $I = (x_1^2 - 2x_2^2,\ x_1^3 - 3x_3^3,\ x_1^4 - x_4^4)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$
   4) $I = (x_1^3 - 4x_2^3,\ x_1^5 - 7x_3^5,\ x_1^7 - 11x_4^7)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$
   5) $I = (x_1^2 + x_2^2 + x_3^3 - 1,\ x_1^3 + x_2^4 + x_3^5 - 1)$ in $\mathbb{Q}[x_1, x_2, x_3]$

c) Implement a CoCoA function `SecondGB(...)` which takes the list $\mathcal{G}$ and computes a σ-Gröbner basis of I via Buchberger's Algorithm 2.5.5, where the pair $(i, j) \in B$ is chosen in step 2) according to the normal selection strategy (see Remark 2.5.6.c), and where the optimization which follows from Proposition 2.5.8 is used.

d) Apply your function `SecondGB(...)` in the cases of b) and compare the results of your counters with those returned by the function `FirstGB(...)`.

e) Given $1 \leq i < j < k \leq s$, find three terms $t, t', t'' \in \mathbb{T}^n$ such that $t\sigma_{ij} + t'\sigma_{jk} - t''\sigma_{ik} = 0$. Prove that one can choose $t = 1$ if and only if t_k divides $\mathrm{lcm}(t_i, t_j)$. Give similar criteria for $t' = 1$ and $t'' = 1$. The triple (i, j, k) is called a **Buchberger triple** if one can choose $t = 1$ or $t' = 1$ or $t'' = 1$.

f) Prove that one can drop a critical pair (i, j) in the execution of Buchberger's Algorithm if it is contained in a Buchberger triple and if the other two pairs have been treated already. Write a CoCoA function `ThirdGB`(...) which is based on `SecondGB`(...) and adds this new optimization. To make sure that you do not drop more than one pair from a Buchberger triple, implement a list T which keeps track of the pairs which have been treated already.

g) Apply your function `ThirdGB`(...) in the cases of b) and determine the improvement which has been achieved.

h) Start again with your implementation `SecondGB`(...) of Buchberger's Algorithm, and replace step 4) by the following sequence of instructions.

4a) Increase s' by one. Append $g_i = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ to $\mathcal{G}$, and form the set $C = \{(i, s') \mid 1 \le i < s',\ \gamma_i = \gamma_{s'}\}$.

4b) Delete in C all pairs (j, s') such that there exists an index i in $\{1, \ldots, s'-1\}$ with the properties that $i < j$ and $t_{s'i}$ divides $t_{s'j}$.

4c) Delete in C all pairs (i, s') such that there exists an index j in $\{1, \ldots, s'-1\}$ with the properties that $i < j$ and $t_{s'j}$ properly divides $t_{s'i}$.

4d) Delete in B all pairs (i, j) such that no divisibility occurs between $t_{s'i}$ and $t_{s'j}$ (hence both (i, s') and (j, s') survived the preceding two steps) and we have $\gcd(t_{is'}, t_{js'}) = 1$.

4e) Replace B by $B \cup C$ and continue with step 2).

The fact that this modified algorithm still computes a σ-Gröbner basis of M in finitely many steps will be studied in Volume 2. Implement it in a CoCoA function `GoodGB`(...), apply this function in the cases of b), and compare the values returned by your counters with the earlier results.

2.6 Hilbert's Nullstellensatz

> *The art of doing mathematics*
> *consists in finding that special case*
> *which contains all the germs of generality.*
> (David Hilbert)

As in the first chapter, this closing section deviates from the main line of development. It is both a bridge to many applications of Computational Commutative Algebra and a foundation for numerous theoretical advances in later chapters. In the introduction of this book we mentioned that one of the most common areas where Computational Commutative Algebra is applied is algebraic geometry. The fundamental tool to translate statements from algebraic geometry into the language of commutative algebra and back is Hilbert's Nullstellensatz.

So, what is the relation between geometry and polynomials? Polynomial rings were introduced right at the beginning of this book. Since then, we kept trying to extract information from their intrinsic algebraic structure. But there is another way of looking at polynomials: they can be seen as *functions*. More precisely, given a polynomial f in the polynomial ring $K[x_1, \ldots, x_n]$ over a field K and an extension field $L \supseteq K$, we can evaluate f at each point of L^n and obtain a function from L^n to L.

Of special importance is then the set of *zeros* of f, i.e. the set of points $(a_1, \ldots, a_n) \in L^n$ such that $f(a_1, \ldots, a_n) = 0$. More generally, we can extend the setting to many polynomial equations and look for their common zeros. These are the geometric counterparts of polynomial ideals, and Hilbert's Nullstellensatz, in its different versions, provides the connection between both kinds of objects.

Since we are trying to be as self-contained as possible, we present a proof of Hilbert's Nullstellensatz in the current section. At several key points the theory of Gröbner bases will prove very useful. On the way, we shall also obtain a clearer picture of how the set of solutions of a system of polynomial equations depends on the field over which those equations are defined, and on the field where we look for the coordinates of the solution points. For instance, the polynomial $x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ has no zeros in $\mathbb{R}$, but the two zeros i and $-i$ in $\mathbb{C}$. As we shall see, this simple special case already contains the germ of many more general phenomena.

The section begins with the proofs of some algebraic facts which lead to the field theoretic version of Hilbert's Nullstellensatz (see Theorem 2.6.6). This theorem can also be viewed as a structure theorem for maximal ideals in polynomial rings over algebraically closed fields (see Corollary 2.6.9). As a consequence, we are able to interpret the zeros of an ideal I in such a polynomial ring as the set of maximal ideals containing I (see Proposition 2.6.11). For instance, the zeros of $x^4 + 2x^2 + 1 \in \mathbb{C}[x]$ correspond to the maximal ideals $(x + i)$ and $(x - i)$ containing this polynomial.

Given a field extension $K \subset L$, an important result is proved about the behaviour of ideals under extension from $K[x_1, \ldots, x_n]$ to $L[x_1, \ldots, x_n]$. This result is the key to the weak form of Hilbert's Nullstellensatz (see Theorem 2.6.13) which provides us with an effective way to check whether a given polynomial ideal has zeros in $\overline{K}^n$, where $\overline{K}$ is the algebraic closure of K. For our ideal $(x^4 + 2x^2 + 1) \subseteq \mathbb{R}[x]$, the easy observation $1 \notin (x^4 + 2x^2 + 1)$ suffices to conclude that it has zeros in the algebraic closure $\mathbb{C}$ of $\mathbb{R}$.

Finally, we prove the Nullstellensatz in its full generality (see Theorem 2.6.16). It says that the operation of forming the vanishing ideal of a subset of $\overline{K}^n$ is an inverse to the operation of taking the set of zeros of a polynomial ideal if one considers radical ideals only. This highlights the importance of the ideal theoretic operation of forming the radical of an ideal. In the case of the principal ideal $(x^4 + 2x^2 + 1)$ in $\mathbb{C}[x]$, it says that the vanishing ideal of its set of zeros $\{i, -i\}$ is its radical ideal $(x^2 + 1)$.

2.6.A   The Field-Theoretic Version

Let K be an arbitrary field. Many algebraic geometers use the following terminology.

Definition 2.6.1. A finitely generated K-algebra is also called an **affine K-algebra**.

According to Corollary 1.1.14, such algebras are of the form P/I for some polynomial ring $P = K[x_1, \ldots, x_n]$ and some ideal $I \subseteq P$. Now we present three lemmas leading up to the first theorem of this section which is also called the field-theoretic version of Hilbert's Nullstellensatz. Recall that the field of fractions of a polynomial ring $P = K[x_1, \ldots, x_n]$ is usually denoted by $Q(P) = K(x_1, \ldots, x_n)$.

Lemma 2.6.2. *Let x be an indeterminate over our field K. Then $K(x)$ is not an affine K-algebra.*

Proof. Suppose $K(x) = K[\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}]$ for some $f_1, \ldots, f_s, g_1, \ldots, g_s \in K[x]$ such that $g_1 \cdot g_2 \cdots g_s \neq 0$. Since $\frac{1}{x} \notin K[x]$, we may assume $g_1 \cdot g_2 \cdots g_s \notin K$. Then the fraction $\frac{1}{1+g_1 \cdot g_2 \cdots g_s}$ can be written as a polynomial expression in $\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}$. Clearing denominators, we get $(g_1 \cdot g_2 \cdots g_s)^i = (1 + g_1 \cdot g_2 \cdots g_s) \cdot h$ for suitable $i > 0$ and $h \in K[x]$. Now $K[x]$ is a factorial domain (see Theorem 1.2.13), but clearly no irreducible factor of the non-constant polynomial $1 + g_1 \cdot g_2 \cdots g_s$ can divide one of the polynomials $g_1, \ldots, g_s$. This contradiction finishes the proof. $\square$

Lemma 2.6.3. *Let $A \subseteq B \subseteq C$ be three rings.*

 a) If B is a finitely generated A-module, then it is also a finitely generated A-algebra.

b) *If B is a finitely generated A-algebra and if C is a finitely generated B-algebra, then C is a finitely generated A-algebra.*

Proof. Let $\{b_1, \ldots, b_s\}$ be a set of generators of B as an A-module. Then $B = Ab_1 + \cdots + Ab_s \subseteq A[b_1, \ldots, b_s] \subseteq B$ implies claim a). For the proof of b), we use Corollary 1.1.14 to write $B = A[x_1, \ldots, x_n]/I$ with an ideal $I \subseteq A[x_1, \ldots, x_n]$ and $C = B[y_1, \ldots, y_m]/J$ with an ideal $J \subseteq B[y_1, \ldots, y_m]$. Then the claim follows from

$$C \cong A[x_1, \ldots, x_n, y_1, \ldots, y_m]/\big(I \cdot A[x_1, \ldots, x_n, y_1, \ldots, y_m] + \pi^{-1}(J)\big)$$

where $\pi : A[x_1, \ldots, x_n, y_1, \ldots, y_m] \longrightarrow B[y_1, \ldots, y_m]$ is the canonical homomorphism. $\qquad\square$

The next result is deeper. We want to show that under certain circumstances a K-subalgebra of an affine K-algebra is an affine K-algebra. The following example shows that this is not always the case.

Example 2.6.4. The K-subalgebra $K[x, xy, xy^2, xy^3, \ldots]$ of $K[x, y]$ is not finitely generated. Namely, for every finite set of elements of this subalgebra, the finitely many terms in the support of those polynomials can be written as polynomials in finitely many terms $x, xy, \ldots, xy^i$. But since we have $xy^i \notin K[x, xy, \ldots, xy^{i-1}]$ for $i \geq 2$, those polynomials do not generate the subalgebra.

Lemma 2.6.5. *Let A and B be two K-algebras such that $A \subseteq B$. Assume that B is an affine K-algebra and a finitely generated A-module. Then A is an affine K-algebra.*

Proof. Let $\{b_1, \ldots, b_s\}$ be a set of generators of B as a K-algebra and $\{\beta_1, \ldots, \beta_t\}$ a set of generators of B as an A-module. Then there are elements $a_{ij}, a'_{ijk} \in A$ such that we have expressions

$$b_i = \sum_{j=1}^{t} a_{ij}\beta_j \text{ for } i = 1, \ldots, s \quad \text{and} \quad \beta_i\beta_j = \sum_{k=1}^{t} a'_{ijk}\beta_k \text{ for } i, j = 1, \ldots, t.$$

Let A_0 be the K-subalgebra of A generated by all elements a_{ij} and a'_{ijk}. It is an affine K-algebra, hence Noetherian by Theorem 2.4.6. Assume for a moment that we know that B is a finitely generated A_0-module. Then B is a Noetherian A_0-module by Theorem 2.4.6 again. Thus A, an A_0-submodule of B, is a finitely generated A_0-module. Therefore A is a finitely generated A_0-algebra by Lemma 2.6.3.a. Since A_0 is an affine K-algebra, also A is an affine K-algebra by Lemma 2.6.3.b.

Consequently, to finish the proof it suffices to show that B is a finitely generated A_0-module. To this end we observe that every element of B is a polynomial expression in $\beta_1, \ldots, \beta_t$ with coefficients in A_0 because of the first set of expressions above. Using the second set of expressions, we can replace

every product $\beta_i\beta_j$ by an element of $A_0\beta_1 + \cdots + A_0\beta_t$. If we iterate those substitutions, we see that every element of B is in $A_0\beta_1 + \cdots + A_0\beta_t + A_0$, i.e. the A_0-module B is generated by $\{1, \beta_1, \ldots, \beta_t\}$. $\square$

Theorem 2.6.6. (Field-Theoretic Version of Hilbert's Nullstellensatz)
Let $P = K[x_1, \ldots, x_n]$ and $\mathfrak{m}$ a maximal ideal of P.

a) For every $i \in \{1, \ldots, n\}$, the intersection $\mathfrak{m} \cap K[x_i]$ is a non-zero ideal.

b) The affine K-algebra $P/\mathfrak{m}$ is a finitely generated K-vector space.

Proof. First we show that a) implies b). By assumption, for $i = 1, \ldots, n$, the intersection $\mathfrak{m} \cap K[x_i]$ is a non-zero principal ideal generated by some non-constant polynomial $f_i \in K[x_i]$. Then the ideal $\mathfrak{n} = (f_1, \ldots, f_n) \subseteq P$ is contained in $\mathfrak{m}$ and we have a surjective homomorphism $P/\mathfrak{n} \longrightarrow P/\mathfrak{m}$. Therefore it suffices to show that $P/\mathfrak{n}$ is a finitely generated K-vector space. Now $\{f_1, \ldots, f_n\}$ is a Gröbner basis of $\mathfrak{n}$ with respect to every term ordering σ by Corollary 2.5.10. If we write $\mathrm{LT}_\sigma(f_i) = x_i^{d_i}$ with $d_i \geq 1$ for $i = 1, \ldots, n$, we may deduce from Corollary 2.4.11 that a K-vector space basis of $P/\mathfrak{n}$ is given by the finite set of residue classes of the terms $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ such that $0 \leq \alpha_i < d_i$ for $i = 1, \ldots, n$.

Now we prove a) by induction on n. If $n = 1$, the ideal $\mathfrak{m}$ is a principal ideal generated by an irreducible polynomial, and the claim holds. If $n > 1$, we denote the affine K-algebra $P/\mathfrak{m}$ by B. Let $i \in \{1, \ldots, n\}$, let $\overline{x}_i$ be the residue class of x_i in B, and let A be the field of fractions of the integral domain $K[\overline{x}_i]$ contained in the field B. Clearly, considered as an A-algebra, B is generated by $\{\overline{x}_1, \ldots, \overline{x}_{i-1}, \overline{x}_{i+1}, \ldots, \overline{x}_n\}$. Hence B is isomorphic to $A[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]/\mathfrak{n}$ for some maximal ideal $\mathfrak{n}$. By induction and the implication shown above, B is a finitely generated A-vector space. Therefore, by Lemma 2.6.5, the field A is a finitely generated K-algebra. Then $\overline{x}_i$ is not an indeterminate over K by Lemma 2.6.2, and hence $\mathfrak{m} \cap K[x_i]$ is different from (0). $\square$

Condition a) of the above theorem does not hold for more general rings, as the following example shows. (In this example we shall use some facts about power series and Laurent series rings which will be discussed more thoroughly in Chapter V. The inexperienced reader may safely skip it.)

Example 2.6.7. Let $R = K[[x]][y]$ be the polynomial ring in the indeterminate y over the univariate power series ring $K[[x]]$ over a field K. Then the principal ideal $\mathfrak{m} = (xy - 1)$ is maximal, because $R/(xy - 1) \cong K[[x]]_x$ is a field. But we have $\mathfrak{m} \cap K[y] = (0)$.

Definition 2.6.8. A field K is called **algebraically closed** if every irreducible polynomial in $K[x]$ is linear. This implies that every polynomial $f \in K[x]$ of degree d can be written as

$$f(x) = c\,(x - a_1)^{\alpha_1}(x - a_2)^{\alpha_2}\cdots(x - a_s)^{\alpha_s}$$

where $c, a_1, \ldots, a_s \in K$ and $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$ are such that $a_1, \ldots, a_s$ are pairwise distinct and $\alpha_1 + \cdots + \alpha_s = d$.

For instance, the **Fundamental Theorem of Algebra** says that the field of complex numbers $\mathbb{C}$ is algebraically closed. The fields $\mathbb{R}$ and $\mathbb{Q}$ are not algebraically closed, since the quadratic polynomial $x^2 + 1$ is irreducible over them.

An important result which you should know is that, for every field K, there exists an algebraic extension field $\overline{K}$ which is an algebraically closed field. (And if you do not know it, you can look for instance at [La70], Ch. 7.) The field $\overline{K}$ is unique up to a K-algebra isomorphism and is called the **algebraic closure** of K. For example, the field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, since it is algebraically closed and an algebraic extension of $\mathbb{R}$. The algebraic closure of $\mathbb{Q}$ is the field of algebraic numbers $\overline{\mathbb{Q}}$ discussed in Tutorial 18.

The field-theoretic version of Hilbert's Nullstellensatz can also be interpreted as a structure theorem for maximal ideals in polynomial rings over algebraically closed fields.

Corollary 2.6.9. *Let K be an algebraically closed field, and let $\mathfrak{m}$ be a maximal ideal in $K[x_1, \ldots, x_n]$. Then there exist elements $a_1, \ldots, a_n$ in K such that*

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$$

Proof. Theorem 2.6.6 yields non-zero polynomials $f_1, \ldots, f_n \in \mathfrak{m}$ such that $f_i \in K[x_i]$ for $i = 1, \ldots, n$. Every polynomial f_i factorizes completely into linear factors, since K is algebraically closed. Moreover, the ideal $\mathfrak{m}$ is maximal, hence prime. This implies that it contains one of the linear factors of each polynomial f_i, say $x_i - a_i$. Then $\mathfrak{m}$ contains the ideal $(x_1 - a_1, \ldots, x_n - a_n)$ which, on the other hand, is a maximal ideal. Thus they must be equal and the proof is complete. $\square$

2.6.B The Geometric Version

In the remainder of this section we want to explain the geometric versions of Hilbert's Nullstellensatz. The German word "Nullstellensatz" literally means "zero-places-proposition". Let us define what this refers to.

Definition 2.6.10. Let $K \subseteq L$ be a field extension, let $\overline{K}$ be the algebraic closure of K, and let $P = K[x_1, \ldots, x_n]$.

a) An element $(a_1, \ldots, a_n) \in L^n$ (which we shall also call a **point** of L^n) is said to be a **zero** of a polynomial $f \in P$ in L^n if $f(a_1, \ldots, a_n) = 0$, i.e. if the evaluation of f at the point $(a_1, \ldots, a_n)$ is zero. The set of all zeros of f in L^n will be denoted by $\mathcal{Z}_L(f)$. If we simply say that $(a_1, \ldots, a_n)$ is a zero of f, we mean $(a_1, \ldots, a_n) \in \overline{K}^n$ and $f(a_1, \ldots, a_n) = 0$.

b) For an ideal $I \subseteq P$, the **set of zeros** of I in L^n is defined as

$$\mathcal{Z}_L(I) = \{(a_1, \ldots, a_n) \in L^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

Again we call the set of zeros of I in $\overline{K}^n$ simply the set of zeros of I and denote it by $\mathcal{Z}(I)$. Later we shall also call $\mathcal{Z}(I)$ the **affine variety** defined by I.

It is easy to see that the set of zeros $\mathcal{Z}_L(f)$ of a polynomial $f \in P$ in L^n agrees with the set of zeros $\mathcal{Z}_L((f))$ of the principal ideal it generates. Moreover, if an ideal $I \subseteq P$ is generated by a set of polynomials $\{f_1, \ldots, f_s\}$, then we have $\mathcal{Z}_L(I) = \cap_{i=1}^s \mathcal{Z}_L(f_i)$.

Algebraically, the set of zeros of an ideal corresponds to a set of maximal ideals in the polynomial ring, as our next proposition shows.

Proposition 2.6.11. *Let K be an algebraically closed field, let I be a proper ideal in $P = K[x_1, \ldots, x_n]$, and let Σ be the set of maximal ideals in P which contain I. Then the map*

$$\varphi : \mathcal{Z}(I) \longrightarrow \Sigma$$

defined by $\varphi(a_1, \ldots, a_n) = (x_1 - a_1, \ldots, x_n - a_n)$ is bijective.

Proof. For $p = (a_1, \ldots, a_n) \in K^n$, we denote by $\mathfrak{m}_p = (x_1 - a_1, \ldots, x_n - a_n)$ the corresponding maximal ideal in P. Then the map φ can be described by $\varphi(p) = \mathfrak{m}_p$. First we prove that φ is well-defined. For a point $p \in \mathcal{Z}(I)$, all polynomials in I vanish at p. Using Theorem 1.6.4, we get the representation $f = q_1(x_1 - a_1) + \cdots + q_n(x_n - a_n) + p$, and we see that those polynomials belong to $\mathfrak{m}_p$.

The map φ is clearly injective. Hence it suffices to show that it is surjective. We choose a maximal ideal $\mathfrak{m} \in \Sigma$. By Corollary 2.6.9, there exists a point $p = (a_1, \ldots, a_n) \in K^n$ such that $\mathfrak{m} = \mathfrak{m}_p$. By the definition of Σ, we have $\mathfrak{m}_p \supseteq I$. It follows that $p \in \mathcal{Z}(I)$, and the proof is complete.   □

Our next result is useful for comparing the set of zeros of I in L^n for different extension fields L of K. Remember that if $K \subseteq L$ is a field extension and I is an ideal of $P = K[x_1, \ldots, x_n]$, we use the notation $IL[x_1, \ldots x_n]$ to denote the ideal of $L[x_1, \ldots x_n]$ generated by the set I.

Proposition 2.6.12. *Let $K \subseteq L$ be a field extension and I an ideal of $K[x_1, \ldots, x_n]$. Then*

$$IL[x_1, \ldots, x_n] \cap K[x_1, \ldots, x_n] = I$$

In particular, we have $IL[x_1, \ldots, x_n] = L[x_1, \ldots, x_n]$ if and only if we have $I = K[x_1, \ldots, x_n]$.

Proof. Obviously we only need to prove that the left-hand side is contained in I. We choose a term ordering σ on $\mathbb{T}^n$ and let $G = \{g_1, \ldots, g_s\}$ be a σ-Gröbner basis of I. From Lemma 2.4.16 it follows that the set G is also a σ-Gröbner basis of the ideal $IL[x_1, \ldots, x_n]$. Now let f be a polynomial in $IL[x_1, \ldots, x_n] \cap K[x_1, \ldots, x_n]$. If we compute the normal form $\mathrm{NF}_\sigma(f)$ using the Division Algorithm 1.6.4, we only perform operations inside $K[x_1, \ldots, x_n]$, and therefore $f - \mathrm{NF}_\sigma(f)$ is in the ideal generated in $K[x_1, \ldots, x_n]$ by the set of polynomials $\{g_1, \ldots, g_s\}$, which is I. But $f \in IL[x_1, \ldots, x_n]$ implies $\mathrm{NF}_\sigma(f) = 0$, hence we have $f \in I$. $\square$

The questions which ideals have zeros and how one can check that are now answered by the following theorem and its corollary.

Theorem 2.6.13. (Weak Nullstellensatz)
Let K be a field, and let I be a proper ideal of $P = K[x_1, \ldots, x_n]$, i.e. let $I \subset P$. Then $\mathcal{Z}(I) \neq \emptyset$.

Proof. Let $\overline{K}$ be the algebraic closure of K, and let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$. Then $I\overline{P}$ is a proper ideal of $\overline{P}$ by Proposition 2.6.12. Since we know that $\overline{P}$ is Noetherian, the ideal $I\overline{P}$ is contained in a maximal ideal $\mathfrak{m}$ of $\overline{P}$ by Proposition 2.4.5.c. Now Corollary 2.6.9 says that there is a point $(a_1, \ldots, a_n) \in \overline{K}^n$ such that $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$. Hence $(a_1, \ldots, a_n)$ is a zero of $\mathfrak{m}$, and therefore also of $I \subseteq I\overline{P} \subseteq \mathfrak{m}$. $\square$

Of course, one cannot hope to get $\mathcal{Z}_K(I) \neq \emptyset$ if K is not algebraically closed, since for instance $\mathcal{Z}_{\mathbb{Q}}(x^2 + 1) = \emptyset$. Moreover, although the question of whether $\mathcal{Z}_L(I) = \emptyset$ or not does not depend on which algebraically closed field $L \supseteq K$ we choose, the set $\mathcal{Z}_L(I)$ itself clearly does. For instance, if $I = (y - x^2) \subseteq \mathbb{Q}[x, y]$, then $(\pi, \pi^2) \in \mathcal{Z}_{\mathbb{C}}(I)$, but $(\pi, \pi^2) \notin \mathcal{Z}_{\overline{\mathbb{Q}}}(I)$.

Corollary 2.6.14. *Let L be a field which contains the algebraic closure of K, and let I be an ideal of $K[x_1, \ldots, x_n]$. Then the following conditions are equivalent.*

a) $\mathcal{Z}_L(I) = \emptyset$
b) $1 \in I$

In particular, this result holds if K is the field of definition of I.

Proof. Clearly b) implies a). For the converse, we observe that $\mathcal{Z}_L(I) = \emptyset$ implies $\mathcal{Z}(I) = \emptyset$, and then $1 \in I$ by the Weak Nullstellensatz. $\square$

Recall that, for a ring R and an ideal I in R, the set $\{r \in R \mid r^i \in I$ for some $i \geq 0\}$ is again an ideal of R which is called the **radical** of I and denoted by $\sqrt{I}$. An ideal I such that $I = \sqrt{I}$ is called a **radical ideal**. Equivalently, an ideal I is a radical ideal in R if the residue class ring R/I has no non-zero nilpotent elements. Thus, for instance, prime ideals are radical ideals.

In the case of an ideal I of $K[x_1, \ldots, x_n]$, it is easy to see that I and $\sqrt{I}$ have the same set of zeros. Thus the operation of assigning the set of zeros to an ideal $I \subseteq K[x_1, \ldots, x_n]$ is not one-to-one. In order to study this operation more closely, let us define an operation going in the other direction.

Definition 2.6.15. Let $K \subseteq L$ be a field extension, and let $S \subseteq L^n$. Then the set of all polynomials $f \in K[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$ for all points $(a_1, \ldots, a_n) \in S$ forms an ideal of the polynomial ring $K[x_1, \ldots, x_n]$. This ideal is called the **vanishing ideal** of S in $K[x_1, \ldots, x_n]$ and denoted by $\mathcal{I}(S)$.

Using this notation, the strong version of Hilbert's Nullstellensatz says that the operation $\mathcal{I}(\ldots)$ is an inverse to $\mathcal{Z}(\ldots)$ if one considers only radical ideals in polynomial rings over algebraically closed fields.

Theorem 2.6.16. (Hilbert's Nullstellensatz)
Let K be an algebraically closed field, and let I be a proper ideal of $K[x_1, \ldots, x_n]$. Then

$$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$$

Proof. To show the inclusion $\mathcal{I}(\mathcal{Z}(I)) \supseteq \sqrt{I}$, suppose that a polynomial $f \in P = K[x_1, \ldots, x_n]$ satisfies $f^i \in I$ for some $i \geq 0$. Then we have $f^i(a_1, \ldots, a_n) = 0$ for every point $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$. Thus we also have $f(a_1, \ldots, a_n) = 0$ for every point $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$, i.e. $f \in \mathcal{I}(\mathcal{Z}(I))$.

To prove the other inclusion, we may assume that $\mathcal{I}(\mathcal{Z}(I)) \neq (0)$. We choose $f \in \mathcal{I}(\mathcal{Z}(I)) \setminus \{0\}$ and generators $\{g_1, \ldots, g_s\}$ of I. Let x_{n+1} be a new indeterminate, and consider the ideal $I' = IP[x_{n+1}] + (x_{n+1}f - 1)$ in the polynomial ring $P[x_{n+1}]$. For every point $(a_1, \ldots, a_{n+1}) \in \mathcal{Z}(I')$ we have $a_{n+1}f(a_1, \ldots, a_n) = 1$ and $g_i(a_1, \ldots, a_n) = 0$ for $i = 1, \ldots, s$. But then $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$ and $f(a_1, \ldots, a_n) \neq 0$ contradict the choice of f. Consequently, such a point does not exist, i.e. $\mathcal{Z}(I') = \emptyset$, and the Weak Nullstellensatz 2.6.13 yields $1 \in I'$.

Therefore there are $s + 1$ polynomials $h, h_1, \ldots, h_s \in P[x_{n+1}]$ such that $1 = \sum_{i=1}^{s} h_i \cdot g_i + h \cdot (x_{n+1}f - 1)$. In the field $K(x_1, \ldots, x_n, x_{n+1})$ we may substitute $\frac{1}{f}$ for x_{n+1}. We get the equality

$$1 = \sum_{i=1}^{s} h_i(x_1, \ldots, x_n, \tfrac{1}{f}) \cdot g_i$$

By clearing the denominators, we find $f^m = \sum_{i=1}^{s} \tilde{h}_i \cdot g_i$ for some $m \geq 0$ and suitable polynomials $\tilde{h}_1, \ldots, \tilde{h}_s \in P$, which means that $f \in \sqrt{I}$. $\square$

Our final result in this section provides a reformulation of Hilbert's Nullstellensatz which will prove useful in the final section of this book.

Corollary 2.6.17. *Let K be a field, let I be a proper ideal in the polynomial ring $P = K[x_1, \ldots, x_n]$, let $\overline{K}$ be the algebraic closure of K, let*

$\overline{P} = \overline{K}[x_1, \ldots, x_n]$, and let f be a polynomial in P. If f belongs to all maximal ideals containing $I\overline{P}$, then $f \in \sqrt{I}$.

Proof. First we observe that Proposition 2.6.11 implies $f \in \mathcal{I}(\mathcal{Z}(I\overline{P}))$. This ideal equals $\sqrt{I\overline{P}}$ by Hilbert's Nullstellensatz 2.6.16. Therefore there exists a number $i \in \mathbb{N}$ such that $f^i \in I\overline{P}$. The claim now follows from Proposition 2.6.12. $\qquad\square$

Exercise 1. Give a direct proof for the fact that condition b) of Theorem 2.6.6 implies condition a) of that theorem.

Exercise 2. Let K be a field and $f(x) \in K[x]$ an irreducible polynomial. Find a maximal ideal $\mathfrak{m}$ in $K[x, y]$ which contains the ideal $I = (f(x), f(y))$, and compute the intersection of $\mathfrak{m}$ with $K[x]$ and $K[y]$.

Exercise 3. (Structure of Maximal Ideals in $\mathbb{R}[x_1, \ldots, x_n]$)
Let $\mathfrak{m}$ be a maximal ideal in $\mathbb{R}[x_1, \ldots, x_n]$.
a) Let $n = 1$. Show that $\mathfrak{m}$ is either generated by a polynomial of type $x_1 - a$ with $a \in \mathbb{R}$, or a polynomial of type $x_1^2 + ax_1 + b$ with $a, b \in \mathbb{R}$ and $a^2 - 4b < 0$.
   Hint: Use the fact that if $a + ib$ is a complex zero of a polynomial in $\mathbb{R}[x]$, then also $a - ib$ is a zero, to characterize irreducible polynomials in $\mathbb{R}[x]$.
b) Let $n = 2$ and $f_1 = x_1^2 + a_1 x_1 + b_1$, $f_2 = x_2^2 + a_2 x_2 + b_2$ with $a_1, b_1, a_2, b_2 \in \mathbb{R}$ and $a_1^2 - 4b_1 < 0$, $a_2^2 - 4b_2 < 0$. Show that the ideal $I = (f_1, f_2)$ is not maximal in $\mathbb{R}[x_1, x_2]$.
   Hint: Use the fact that $\mathbb{R}[x_1, x_2]/(f_1)$ is isomorphic to $\mathbb{C}[x_2]$.
c) Let $n = 2$ and assume that $x_1^2 + a_1 x_1 + b_1 \in \mathfrak{m}$ with $a_1, b_1 \in \mathbb{R}$ and $a_1^2 - 4b_1 < 0$. Show that there exist $a_2, b_2 \in \mathbb{R}$ such that we have $\mathfrak{m} = (x_1^2 + a_1 x_1 + b_1, x_2 - a_2 x_1 - b_2)$.
d) In the general case prove the following fact: either there exist numbers $a_1, \ldots, a_n \in \mathbb{R}$ such that $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ or, up to a permutation of the indeterminates, there exist $a_1, b_1, a_2, b_2 \ldots, a_n, b_n \in \mathbb{R}$ such that $a_1^2 - 4b_1 < 0$ and $\mathfrak{m} = (x_1^2 + a_1 x_1 + b_1, x_2 - a_2 x_1 - b_2, \ldots, x_n - a_n x_1 - b_n)$.

Exercise 4. Let $f \in \mathbb{Q}[x, y]$ be a non-constant polynomial. Prove that $\mathcal{Z}_{\mathbb{Q}}(f) \subset \mathcal{Z}(f)$.

Exercise 5. Let $K \subseteq L$ be a field extension, let $P = K[x_1, \ldots, x_n]$, let $f, f_1, \ldots, f_s \in P$, and let $I = (f_1, \ldots, f_s)$.
a) Show that $\mathcal{Z}_L(f) = \mathcal{Z}_L((f))$.
b) Show that $\mathcal{Z}_L(I) = \cap_{i=1}^{s} \mathcal{Z}_L(f_i)$.
c) Show that $\mathcal{Z}_L(I) = \mathcal{Z}_L(\sqrt{I})$.

Exercise 6. Let $K \subseteq L$ be a field extension, let I be an ideal in $K[x_1, \ldots, x_n]$, and let S be a subset of L^n.
a) Show that $\mathcal{I}(\mathcal{Z}_L(I)) \supseteq I$.
b) Show that $\mathcal{Z}_L(\mathcal{I}(S)) \supseteq S$.

Exercise 7. Let R be a ring, and let I and J be ideals in R. Prove the following rules.

a) $\sqrt{\sqrt{I}} = \sqrt{I}$

b) $\sqrt{I \cap J} = \sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$

c) $\sqrt{I^i} = \sqrt{I}$ for all $i \geq 1$.

d) If I is an intersection of prime ideals, then $\sqrt{I} = I$.

e) $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$

Exercise 8. Let K be an algebraically closed field and I a proper ideal of $P = K[x_1, \dots, x_n]$. In this exercise we use the Zariski topology on K^n defined in Tutorial 27.

The ideal I is said to be **reducible** if it is the intersection of two strictly bigger ideals. A closed set of a topological space is said to be **reducible** if it is the union of two properly contained closed subsets.

a) Show that if $\mathcal{Z}(I)$ is reducible, then I is reducible.

b) Give an example which shows that the converse is not true.

c) Show that the converse of a) is true if I is a radical ideal.

d) Let I be a radical ideal. Prove that the following conditions are equivalent.

   1) There exist two ideals $I_1, I_2 \subset P$ such that $I = I_1 \cap I_2$ and $I_1 + I_2 = P$.
   2) $\mathcal{Z}(I)$ is disconnected, i.e. it is the union of two disjoint closed sets.

Exercise 9. Let K be an algebraically closed field, and let I be a proper radical ideal of $P = K[x_1, \dots, x_n]$.

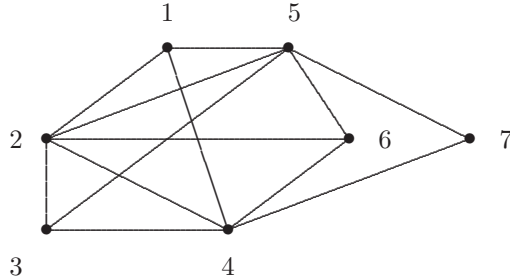a) Prove that $\mathcal{Z}(I)$ is finite if and only if I is of the form

$$I = \bigcap_{i=1}^{s} (x_1 - a_{i1}, \dots, x_n - a_{in})$$

   with pairwise different points $(a_{11}, \dots, a_{1n}), \dots, (a_{s1}, \dots, a_{sn}) \in K^n$.

b) Show that if a) holds, then $\mathcal{Z}_L(I) = \mathcal{Z}(I)$ for every extension field $L \supseteq K$.

Tutorial 26: Graph Colourings

Suppose we are given 3 different colours and a graph Γ having n nodes and at most one arch between any two nodes, e.g.

Our goal is to find out if the nodes can be coloured in such a way that no arch connects two nodes of the same colour. In order to use the theory of Gröbner bases to solve this problem, we introduce the following notation.

The colours will be called -1, 0, and 1. They will be identified with the elements of the field $\mathbb{F}_3 = \mathbb{Z}/(3)$. For $i = 1, \ldots, n$, we choose an indeterminate x_i and form the polynomial ring $P = \mathbb{F}_3[x_1, \ldots, x_n]$. We shall identify a colouring of the graph with a point of $\mathbb{F}_3^n$ such that the ith coordinate of the point corresponds to the colour of the ith node.

a) Show that the set of zeros of the ideal $(x_1^3 - x_1, \ldots, x_n^3 - x_n)$ is precisely the set of all colourings.

b) Prove that the ith and j^{th} node of the graph have different colours if and only if the colouring is a zero of the polynomial $x_i^2 + x_i x_j + x_j^2 - 1$.

c) In addition, we may assume that the first and second nodes are connected, that the first node has colour "0", and that the second node has colour "1". What polynomial equations does this imply for the colourings under consideration?

d) Write a CoCoA program $\texttt{Colouring}(\ldots)$ which takes a list of pairs from $\{1, \ldots, n\}^2$ representing the arches and computes an ideal $I \subseteq P$ whose zeros are precisely the colourings of the graph represented by those pairs which satisfy our additional conditions.

e) Apply your function $\texttt{Colouring}(\ldots)$ to the graph above. Then use CoCoA to compute the reduced **Lex**-Gröbner basis of this ideal. Does the graph have a colouring of the desired kind? If yes, how many different ones? (*Hint:* Use Hilbert's Nullstellensatz to interpret the answer of your calculation.)

f) Consider the graph formed by connecting the center of a regular 7-gon to its vertices. (It has 8 nodes and 14 arches.) Use CoCoA and the Weak Nullstellensatz to show that this graph cannot be coloured as required above.

Tutorial 27: Affine Varieties

Let $K \subseteq L$ be a field extension. For every ideal I in $K[x_1, \ldots, x_n]$ we consider the set $\mathcal{Z}_L(I) \subseteq L^n$ as given in Definition 2.6.10. For the moment, let us call a subset of L^n a **zero-set** if it is of the form $\mathcal{Z}_L(I) \subseteq L^n$ for some ideal $I \subseteq K[x_1, \ldots, x_n]$.

a) Prove the following claims.

1) $\emptyset$ is a zero-set.
2) L^n is a zero-set.
3) If $E_1, \ldots, E_s$ are zero-sets, then $\cup_{i=1}^s E_i$ is a zero-set.
4) If J is a set of indices and $\{E_j\}_{j \in J}$ a set of zero-sets indexed by J, then $\cap_{j \in J} E_j$ is a zero-set.

Deduce that the zero-sets of L^n can be taken as the closed sets of a topology, which we denote by $\mathrm{Top}_{K,L}$. If $K = L$, then $\mathrm{Top}_{K,K}$ is called the **Zariski topology** on K^n. Moreover, K^n with the Zariski topology is called the n**-dimensional affine space** over K and denoted by $\mathbb{A}_K^n$. Zero-sets in $\overline{K}^n$ are called **affine varieties** (or **affine sets**).

b) Let p_1 and p_2 be two distinct points in K^n. Then the set of points $\overline{p_1 p_2} = \{p_1 + \lambda(p_2 - p_1) \mid \lambda \in K\}$ is called the **line** passing through p_1 and p_2. Show that $\overline{p_1 p_2}$ is a closed set in the Zariski topology.

c) Let $K \subset K' \subseteq L$ be field extensions and $\mathrm{Top}_{K,L}$, $\mathrm{Top}_{K',L}$ the corresponding topologies on L^n. Show that $\mathrm{Top}_{K',L}$ is finer than $\mathrm{Top}_{K,L}$, i.e. that every closed set with respect to $\mathrm{Top}_{K,L}$ is also closed with respect to $\mathrm{Top}_{K',L}$.

d) Let K be algebraically closed and consider the Zariski topology on K^n. Show that there is a bijection between the set of radical ideals in $K[x_1, \ldots, x_n]$ and the closed sets in $\mathbb{A}_K^n$. Then show that the statement is false if K is not algebraically closed.

e) Let K be algebraically closed, let I be an ideal in $P = K[x_1, \ldots, x_n]$, and assume that the dimension of P/I as a vector space over K is finite. Then show that $\mathcal{Z}(I)$ is a finite set of points.
Hint: For $i = 1, \ldots, n$, show that $I \cap K[x_i] = (f_i) \neq (0)$ and conclude that $\mathcal{Z}(I) \subseteq \mathcal{Z}((f_1, \ldots, f_n))$.

f) Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, and let I be an ideal in P. Write two CoCoA programs which perform the following tasks.

1) Given I and a point $p \in \mathbb{Q}^n$, check if $p \in \mathcal{Z}_{\mathbb{Q}}(I)$ and return the corresponding Boolean value.
2) If $I \neq (0)$, find a point p which is not in $\mathcal{Z}_{\mathbb{Q}}(I)$ and return it.

g) Let S be a subset of $\mathbb{A}_K^n$. Show that the set of all Zariski-closed subsets of $\mathbb{A}_K^n$ containing S has a unique minimal element (with respect to inclusion). This zero-set is called the **Zariski closure** of S.

h) Let K be an algebraically closed field, and let $S \subseteq \mathbb{A}_K^n$. Prove that the Zariski closure of S is given by $\mathcal{Z}(\mathcal{I}(S))$.

3. First Applications

It has already been a long journey. From the snowy hills down to the valleys and up again, we have encountered many milestones and discovered impressive tools. Meanwhile time has passed, the colours of the landscape have changed, and now it is time to go back to the hills and do the harvesting.

Do you realize that you have accumulated the knowledge of many facts which you might be able to use now? Possibly you have already forgotten that you knew them. Let us remind you of the factoriality of polynomial rings over fields, and of the games played in Chapter 1 with terms and term orderings. Then, in Chapter 2, we planned a strategy, made our moves, and discovered Gröbner bases, Buchberger's Algorithm, Hilbert's Nullstellensatz, and numerous other devices. In particular, by now you should be able to see clearly how fundamental the notion of a syzygy is, for instance because it plays an essential role in the construction of Buchberger's Algorithm.

However, the importance of syzygies in Algebra goes far beyond what we have seen up to now. Therefore it is highly relevant to be able to compute them. In fact, our first achievement in this chapter is the solution of the problem of computing $\mathrm{Syz}_P(g_1, \ldots, g_s)$ for arbitrary vectors $g_1, \ldots, g_s \in P^r$, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over a field K (see Theorem 3.1.8). Exploiting this new ability, we will then discover ways to explicitly perform basic operations among ideals and modules such as intersections, colon ideals, and colon modules (see Section 3.2).

Next, we enjoy a trip into the realms of Computational Linear Algebra and Computational Homological Algebra. Using syzygy computations, we can find presentations for the kernel and the image of a linear map between finitely generated P-modules, and we can lift a linear map along another one. Even more challenging, but within our grasp, is the task of computing presentations of Hom-modules. Using the ingredients gathered earlier, we shall concoct an algorithm in Subsection 3.3.B.

Having safely put in store many fruits of syzygy calculations, we move to the next orchard. Elimination theory provides us with a particularly fertile soil for further applications. This is a fascinating subject whose roots lie in

classical geometry, where it is related to projections. From the point of view of Computational Commutative Algebra, we have to perform an important switch. From here on we are no longer allowed to use an arbitrary module term ordering. Instead, we have to limit ourselves to the more restrictive class of elimination orderings.

After we explain the main theorem for computing elimination modules in Section 3.4, many other ripening fruits will become ready for picking. Using the method of tag variables, we obtain new ways to perform the basic operations on modules. Then, in Section 3.5, we learn how to compute saturations and how to check radical membership.

Other important applications are collected in Section 3.6, where we discuss ring homomorphisms. Among other things, we show how to find presentations for the kernel and the image of a homomorphism of finitely generated algebras, how to solve the implicitization problem, how to compute minimal polynomials of elements in affine algebras, how to check membership in finitely generated subalgebras, and how to analyze surjective and bijective homomorphisms between polynomial rings.

The final Section 3.7 of this chapter, and hence of this volume, represents the ultimate act of harvesting. It is devoted to the problem of solving systems of polynomial equations effectively. At that stage of your reading, you will be challenged to recall almost all the knowledge that you gathered during the journey, to become aware of the skills and the tools which you have learned, and to use them to dig out the *roots* of systems of equations. Our last field of investigation also contains algorithms for checking whether the set of solutions of a system of equations is finite, for computing squarefree parts of polynomials, and for finding radicals of zero-dimensional ideals.

And what then? There are countless other applications of Gröbner bases, and new ones are discovered almost daily. But since we wanted to finish this book before the new millennium, we decided to stop here. Other applications and interesting topics will be contained in Volume 2. So, see you later!

Some Words About Notation

> *Such is the advantage of a well-constructed language*
> *that its simplified notation often becomes*
> *the source of profound theories.*
> (Pierre-Simon de Laplace)

Before moving into *medias res*, let us mention a problem which could come to haunt us, namely the choice of a convenient notation. As usual, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $r \geq 1$, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of vectors in P^r.

In this situation, the question arises how we should interpret $\mathcal{G}$. It is clear that tuples of vectors and matrices representing them are different objects. But to ease the notation and to keep the usage of symbols under control,

it would be convenient to *identify* them in a natural way. The key point is that when we look at $\mathcal{G} = (g_1, \ldots, g_s)$, we see that it is already written as a *row*. Thus we are naturally lead to think of the vectors $g_1, \ldots, g_s$ as *column vectors*, and to identify $\mathcal{G}$ with the matrix having those columns.

Indeed, from now on we shall make this identification. It allows us to interpret an expression $\sum_{i=1}^{s} f_i g_i$ as the result of a matrix multiplication in the following way.

$$\sum_{i=1}^{s} f_i g_i = (g_1, \ldots, g_s) \begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix}$$

Here the row $(g_1, \ldots, g_s)$ is written as a tuple, with the appropriate commas, and interpreted as a matrix. Now recall that a syzygy of $\mathcal{G}$ has been defined as a tuple of polynomials $(f_1, \ldots, f_s) \in P^s$ such that $\sum_{i=1}^{s} f_i g_i = 0$. So, given a tuple of syzygies $\mathcal{S}$ of $\mathcal{G}$, we can read the formula $\mathcal{G}\mathcal{S} = 0$ as the corresponding matrix expression.

On the other hand, given a matrix $\mathcal{M}$ of size $r \times t$, we can speak about the P-submodule of P^r generated by the t vectors represented by the columns of $\mathcal{M}$. Consequently, when we write $\mathrm{Syz}(\mathcal{M})$, we mean the module of syzygies of the vectors represented by the columns of $\mathcal{M}$. For a tuple of syzygies $\mathcal{S}$ of $\mathcal{M}$, the corresponding matrix expression is again $\mathcal{M}\mathcal{S} = 0$.

Finally, a map $\lambda : P^s \longrightarrow P^r$ defined by sending e_i to the vector g_i for $i = 1, \ldots, s$ can be represented by the s-tuple $\mathcal{G} = (g_1, \ldots, g_s)$ as well as by the matrix whose columns represent the vectors in $\mathcal{G}$. And now it should be clear that this matrix can safely be called $\mathcal{G}$ again.

The upshot of this discussion is that we represent a linear map between free modules by the matrix whose *columns* are the images of the canonical basis vectors, that the generators of the syzygy module of a tuple of vectors are the *columns* of the syzygy matrix, and that the syzygy matrix is on the *right-hand side* of the corresponding matrix product.

3.1 Computation of Syzygy Modules

> *The greatest of these [things common to all living beings]*
> *happen to be four pairs ($\sigma\upsilon\zeta\upsilon\gamma\acute{\iota}\alpha\iota$, syzygíai) in number:*
> *wakefulness and sleep, youth and old age,*
> *inhalation and exhalation, and life and death.*
> (Aristoteles)

Although not a matter of life and death, the computation of syzygies is one of the first and foremost applications of Buchberger's Algorithm. We have encountered them already twice: in Section 2.3 we saw that finding the Gröbner basis of a submodule of P^r is equivalent to being able to lift syzygies, and they played a central role in Buchberger's Algorithm in Section 2.5. Many of the applications discussed in the present chapter involve syzygy modules in one way or another. They will become the air that we breathe.

So, how do we compute syzygy modules? Given a tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of non-zero elements in P^r, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over a field, we know their definition in our sleep:

$$\mathrm{Syz}(\mathcal{G}) = \{(f_1, \ldots, f_s) \in P^s \mid f_1\, g_1 + \cdots + f_s\, g_s = 0\}$$

Moreover, we know that the syzygies of the leading terms of $\mathcal{G}$ can be lifted to syzygies of $\mathcal{G}$ if $\mathcal{G}$ is a Gröbner basis. How can one get a set of generators for the module $\mathrm{Syz}(\mathcal{G})$ from those liftings?

Our strategy for answering this question is to proceed as follows. Let $M = \langle g_1, \ldots, g_s \rangle$ be the submodule of P^r generated by $\mathcal{G}$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$. First we define a suitable module term ordering on the monomodule of terms $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s \rangle$ of P^s, namely the ordering τ *induced* by $(\sigma, \mathcal{G})$. Then we show that the fundamental syzygies σ_{ij} defined in Theorem 2.3.7 form a τ-Gröbner basis of the syzygy module of $(\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))$. Next we assume that $\mathcal{G}$ is a Gröbner basis of M with respect to σ and prove that the liftings s_{ij} of those elements constitute a τ-Gröbner basis of $\mathrm{Syz}(\mathcal{G})$.

The final step is to compute the syzygy module $\mathrm{Syz}(\mathcal{H})$ for any tuple $\mathcal{H} = (h_1, \ldots, h_t)$ of vectors which generate M. This goal is achieved in Theorem 3.1.8 by using a clever combination of the Division Algorithm 1.6.4 and the Extended Buchberger Algorithm 2.5.11. As a consequence, we see how to obtain all explicit representations of an element of a module as a combination of a given set of generators (see Corollary 3.1.9). And as a final byproduct we show how one can extract an irredundant system of generators of a module from a given one (see Corollary 3.1.12).

As in the previous chapter, we let K be a field, $P = K[x_1, \ldots, x_n]$ a polynomial ring, $M \subseteq P^r$ a non-zero P-submodule, and $\mathcal{G} = (g_1, \ldots, g_s)$ a tuple of non-zero vectors which generate M. Furthermore, we let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$, and we write $\mathrm{LM}_\sigma(g_i) = c_i\, t_i e_{\gamma_i}$ with $c_i \in K$, $t_i \in \mathbb{T}^n$, and $\gamma_i \in \{1, \ldots, r\}$ for $i = 1, \ldots, s$. If we denote the

canonical basis of the P-module P^s by $\{\varepsilon_1, \ldots, \varepsilon_s\}$, the s-tuple $\mathcal{G}$ corresponds to the surjective P-linear map $\lambda : P^s \longrightarrow M$ given by $\lambda(\varepsilon_i) = g_i$ for $i = 1, \ldots, s$. Recall that the syzygy module $\mathrm{Syz}(\mathcal{G})$ is nothing but the kernel of λ.

Our first goal is to introduce a certain module term ordering on the set of terms of P^s such that the map λ is somehow "compatible" with the module term orderings on P^s and P^r.

Definition 3.1.1. On $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s \rangle$, we define a complete relation τ in the following way. Let $t\varepsilon_i$ and $t'\varepsilon_j$ be two elements of $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s \rangle$, where $t, t' \in \mathbb{T}^n$ and $i, j \in \{1, \ldots, s\}$.

Then we let $t\varepsilon_i \geq_\tau t'\varepsilon_j$ if we have $\mathrm{LT}_\sigma(tg_i) >_\sigma \mathrm{LT}_\sigma(t'g_j)$, or if we have $\mathrm{LT}_\sigma(tg_i) = \mathrm{LT}_\sigma(t'g_j)$ and $i \leq j$. The relation τ is called the **ordering induced by** $(\sigma, \mathcal{G})$ **on** $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s \rangle$.

Using Definition 2.3.4 and Proposition 2.3.5, we can rephrase the definition of τ by saying that $t\varepsilon_i \geq_\tau t'\varepsilon_j$ if $\deg_{\sigma,\mathcal{G}}(t\varepsilon_i) >_\sigma \deg_{\sigma,\mathcal{G}}(t'\varepsilon_j)$, or if $\deg_{\sigma,\mathcal{G}}(t\varepsilon_i) = \deg_{\sigma,\mathcal{G}}(t'\varepsilon_j)$ and $i \leq j$. Now we check that this relation is indeed a module term ordering.

Lemma 3.1.2. *The relation τ defined above is a module term ordering on $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s \rangle$.*

Proof. According to Definition 1.4.15 we have to check that τ is reflexive, antisymmetric, transitive, compatible with the monomodule structure, and that it defines a term ordering. All the proofs are straightforward; here we prove the transitivity. Let $t, t', t'' \in \mathbb{T}^n$ and $i, j, k \in \{1, \ldots, s\}$ such that we have $t\varepsilon_i \geq_\tau t'\varepsilon_j \geq_\tau t''\varepsilon_k$. From the definition of τ we get $\mathrm{LT}_\sigma(tg_i) \geq_\sigma \mathrm{LT}_\sigma(t'g_j) \geq_\sigma \mathrm{LT}_\sigma(t''g_k)$. Furthermore, we either have $\mathrm{LT}_\sigma(tg_i) >_\sigma \mathrm{LT}_\sigma(t''g_k)$, or we have $\mathrm{LT}_\sigma(tg_i) = \mathrm{LT}_\sigma(t'g_j) = \mathrm{LT}_\sigma(t''g_k)$ and $i \leq j \leq k$. Both times we end up with $t\varepsilon_i \geq_\tau t''\varepsilon_k$. $\square$

What is τ good for? If the vectors in $\mathcal{G}$ form a σ-Gröbner basis of M, we can try to compute $\mathrm{Syz}(\mathcal{G})$ via the following steps: from Theorem 2.3.7 we know an explicit system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, by Condition D_1) those syzygies lift to syzygies of $\mathcal{G}$, and by Proposition 2.3.11 those liftings generate the desired syzygy module. So the main task is to make the process of lifting more explicit.

Let us recall some notation from Chapter 2. For $i, j \in \{1, \ldots, s\}$, we defined $t_{ij} = \frac{\mathrm{lcm}(t_i, t_j)}{t_i}$ and $\sigma_{ij} = \frac{1}{c_i} t_{ij}\varepsilon_i - \frac{1}{c_j} t_{ji}\varepsilon_j$. Furthermore, we define $\mathbb{B} = \{(i, j) \mid 1 \leq i < j \leq s, \gamma_i = \gamma_j\}$. Theorem 2.3.7 says that the set $\Sigma = \{\sigma_{ij} \mid (i, j) \in \mathbb{B}\}$ generates $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. The importance of τ derives from the remarkable property that Σ is actually a τ-Gröbner basis of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, as our next proposition shows.

Proposition 3.1.3. *Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero vectors which generates the P-module M. Then the set of fundamental syzygies $\Sigma = \{\sigma_{ij} \mid (i, j) \in \mathbb{B}\}$ is a τ-Gröbner basis of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.*

Proof. If $\text{Syz}(\text{LM}_\sigma(\mathcal{G})) = 0$, then $\Sigma = \emptyset$ is a σ-Gröbner basis of this module. Now let $z \in \text{Syz}(\text{LM}_\sigma(\mathcal{G})) \setminus \{0\}$, and let $z' = \text{LF}_{\sigma,\mathcal{G}}(z)$. We want to show that $\text{LT}_\tau(z) \in \langle \text{LT}_\tau(\sigma_{ij}) \mid (i,j) \in \mathbb{B} \rangle$. The definition of τ implies that $\text{LT}_\tau(z) = \text{LT}_\tau(z')$. Thus we may assume that z is homogeneous with respect to the $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$-grading on P^s defined in Proposition 2.3.3. This means that if we write $z = \sum_{i=1}^s c_i' t_i' \varepsilon_i$ with $c_i' \in K$ and $t_i' \in \mathbb{T}^n$, then we have $t_i' \text{LT}_\sigma(g_i) = t_j' \text{LT}_\sigma(g_j)$ for all $1 \le i < j \le s$ such that $c_i' c_j' \ne 0$.

Next, let $\mu = \min\{i \mid c_i' \ne 0\}$. Then z is in fact a syzygy in the module $\text{Syz}(\text{LM}_\sigma(g_\mu), \ldots, \text{LM}_\sigma(g_s))$, and the definition of τ implies $\text{LT}_\tau(z) = t_\mu' \varepsilon_\mu$. Using Theorem 2.3.7, we find that the set $\Sigma_\mu = \{\sigma_{ij} \in \Sigma \mid \mu \le i < j \le s\}$ is a system of generators of the syzygy module $\text{Syz}(\text{LM}_\sigma(g_\mu), \ldots, \text{LM}_\sigma(g_s))$. Therefore we have a representation $z = \sum_{\mu \le i < j \le s} a_{ij} \sigma_{ij}$, where $a_{ij} \in P$. By looking at the coefficient of ε_μ in this representation, we see that t_μ' is in the ideal generated by the set $\{t_{\mu j} \mid \mu < j \le s\}$. Thus t_μ' is a multiple of one of those terms, say of $t_{\mu k}$. Since $\text{LT}_\tau(\sigma_{\mu k}) = t_{\mu k} \varepsilon_\mu$, it follows that $\text{LT}_\tau(z) \in \langle \text{LT}_\tau(\sigma_{\mu j}) \mid \mu < j \le s \rangle$. $\qquad\square$

Based on this result, we can now make the process of lifting the syzygies σ_{ij} explicit and obtain at the same time that the set of liftings is in fact a τ-Gröbner basis of $\text{Syz}(\mathcal{G})$.

Proposition 3.1.4. *Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero vectors in P^r which form a σ-Gröbner basis of M.*

a) *For all $(i,j) \in \mathbb{B}$, we have either $\sigma_{ij} \in \text{Syz}(\mathcal{G})$, i.e. $\lambda(\sigma_{ij}) = 0$, or a representation $\lambda(\sigma_{ij}) = \sum_{k=1}^s f_{ijk} g_k$ with $f_{ijk} \in P$ and such that $\deg_{\sigma,\mathcal{G}}(\sigma_{ij}) >_\sigma \text{LT}_\sigma(\lambda(\sigma_{ij})) = \max_\sigma \{\text{LT}_\sigma(f_{ijk} g_k) \mid k \in \{1, \ldots, s\}\}$.*

Now we define $s_{ij} = \sigma_{ij}$ if $\lambda(\sigma_{ij}) = 0$ and $s_{ij} = \sigma_{ij} - \sum_{k=1}^s f_{ijk} \varepsilon_k$ otherwise.

b) *The set $\{s_{ij} \mid (i,j) \in \mathbb{B}\}$ is a τ-Gröbner basis of $\text{Syz}(\mathcal{G})$. In particular, it is a system of generators of $\text{Syz}(\mathcal{G})$.*

c) *Let $\mathbb{B}' \subseteq \mathbb{B}$ be such that $\{\sigma_{ij} \mid (i,j) \in \mathbb{B}'\}$ generates $\text{Syz}(\text{LM}_\sigma(\mathcal{G}))$. Then the set $\{s_{ij} \mid (i,j) \in \mathbb{B}'\}$ is a system of generators of $\text{Syz}(\mathcal{G})$.*

Proof. To prove a), we recall that σ_{ij} is a homogeneous element of P^s of σ-degree $\deg_{\sigma,\mathcal{G}}(\sigma_{ij}) = \text{lcm}(t_i, t_j) e_{\gamma_i}$ by Theorem 2.3.7.a. Therefore we get $\text{LF}(\sigma_{ij}) = \sigma_{ij} \in \text{Syz}(\text{LM}_\sigma(\mathcal{G}))$. Consequently, if $\lambda(\sigma_{ij}) \ne 0$, then $\text{LT}_\sigma(\lambda(\sigma_{ij})) <_\sigma \deg_{\sigma,\mathcal{G}}(\sigma_{ij})$ by Proposition 2.3.6.b, and the desired representation follows from Condition A_2) in Theorem 2.4.1.

Next we prove b). If $\text{Syz}(\mathcal{G}) = 0$, then also $\text{Syz}(\text{LM}_\sigma(\mathcal{G})) = 0$ by Condition D_1) of Theorem 2.4.1, and we have $\mathbb{B} = \emptyset$. Thus we can assume that $\text{Syz}(\mathcal{G}) \ne 0$. From a) and the definition of τ we deduce that $\text{LT}_\tau(s_{ij}) = t_{ij} \varepsilon_i$. Now we take any non-zero element z of $\text{Syz}(\mathcal{G})$. We have to show that $\text{LT}_\tau(z)$ is a multiple of one of the terms in $\{\text{LT}_\tau(s_{ij}) \mid (i,j) \in \mathbb{B}\}$. The definition of τ yields $\text{LT}_\tau(z) = \text{LT}_\tau(\text{LF}_{\sigma,\mathcal{G}}(z))$. By Proposition 2.3.6.d, we have $\text{LF}_{\sigma,\mathcal{G}}(z) \in \text{Syz}(\text{LM}_\sigma(\mathcal{G}))$. Hence Proposition 3.1.3 implies the claim.

The proof of c) follows from Proposition 2.3.11. $\qquad\square$

As a straightforward consequence of the preceding proposition, we have the following algorithm for computing syzygy modules of Gröbner bases.

Corollary 3.1.5. (Computing Syzygy Modules of Gröbner Bases)
Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero vectors in P^r which form a σ-Gröbner basis of M. Consider the following sequence of instructions.

1) *Create a matrix $\mathcal{M}$ over P with s rows and initially zero columns. Then compute the set $B = \{(i, j) \mid 1 \le i < j \le s, \gamma_i = \gamma_j\}$.*
2) *If $B = \emptyset$, return the matrix $\mathcal{M}$. Otherwise, choose a pair $(i, j) \in B$ and delete it from B.*
3) *Form the vectors $\sigma_{ij} = \frac{1}{c_i} t_{ij} \varepsilon_i - \frac{1}{c_j} t_{ji} \varepsilon_j$ and calculate $S_{ij} = \lambda(\sigma_{ij})$. If $S_{ij} \ne 0$, use the Division Algorithm 1.6.4 to compute a representation $S_{ij} = \sum_{k=1}^{s} f_{ijk} g_k$ such that $\mathrm{LT}_\sigma(f_{ijk} g_k) \le_\sigma \mathrm{LT}_\sigma(S_{ij})$ for $k = 1, \ldots, s$.*
4) *If $S_{ij} = 0$, append σ_{ij}, expanded into a column vector, to the matrix $\mathcal{M}$, and if $S_{ij} \ne 0$, append the column $s_{ij} = \sigma_{ij} - \sum_{k=1}^{s} f_{ijk} \varepsilon_k$ to the matrix $\mathcal{M}$. Then continue with step 2).*

This is an algorithm which returns a matrix $\mathcal{M}$ over P whose columns represent a τ-Gröbner basis of $\mathrm{Syz}(\mathcal{G})$, and in particular a system of generators of $\mathrm{Syz}(\mathcal{G})$.

Remark 3.1.6. Using Proposition 3.1.4.c, we can modify the above algorithm in the following way. Suppose that for some reason we know a subset $\mathbb{B}' \subset \mathbb{B}$ such that $\Sigma' = \{\sigma_{ij} \in \Sigma \mid (i, j) \in \mathbb{B}'\}$ is a set of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Then we may start with $B = \mathbb{B}'$ in step 1), and we still get a system of generators of $\mathrm{Syz}(\mathcal{G})$.

Let us illustrate the course of this algorithm with an example.

Example 3.1.7. In the ring $P = K[x_1, x_2, x_3, x_4]$, consider the polynomials $g_1 = x_1 x_4 - x_2 x_3$, $g_2 = x_1 x_3^2 - x_2^2 x_4$, $g_3 = x_1^2 x_3 - x_2^3$, and $g_4 = x_2 x_4^2 - x_3^3$. Let $\mathcal{G} = (g_1, g_2, g_3, g_4) \in P^4$, and let $I = (g_1, g_2, g_3, g_4) \subseteq P$. In order to compute the syzygy module of $\mathcal{G}$, we observe that $\{g_1, g_2, g_3, g_4\}$ is a Gröbner basis of I with respect to $\sigma = \mathtt{DegLex}$. According to the corollary, we calculate

$$S_{12} = x_3^2 g_1 - x_4 g_2 = x_2^2 x_4^2 - x_2 x_3^3 = x_2 g_4$$
$$S_{13} = x_1 x_3 g_1 - x_4 g_3 = -x_1 x_2 x_3^2 + x_2^3 x_4 = -x_2 g_2$$
$$S_{14} = x_2 x_4 g_1 - x_1 g_4 = x_1 x_3^3 - x_2^2 x_3 x_4 = x_3 g_2$$
$$S_{23} = x_1 g_2 - x_3 g_3 = -x_1 x_2^2 x_4 + x_2^3 x_3 = -x_2^2 g_1$$
$$S_{24} = x_2 x_4^2 g_2 - x_1 x_3^3 g_4 = x_1 x_3^5 - x_2^3 x_4^3 = x_3^3 g_2 - x_2^2 x_4 g_4$$
$$S_{34} = x_2 x_4^2 g_3 - x_1^2 x_3 g_4 = x_1^2 x_3^4 - x_2^4 x_4^2 = x_2^2 x_3^2 g_1 + x_1 x_3^2 g_2 - x_2^3 g_4$$

Therefore the P-module $\mathrm{Syz}(\mathcal{G})$ is generated by the columns of the matrix

$$\mathcal{M} = \begin{pmatrix} x_3^2 & x_1 x_3 & x_2 x_4 & x_2^2 & 0 & -x_2^2 x_3^2 \\ -x_4 & x_2 & -x_3 & x_1 & x_2 x_4^2 - x_3^3 & -x_1 x_3^2 \\ 0 & -x_4 & 0 & -x_3 & 0 & x_2 x_4^2 \\ -x_2 & 0 & -x_1 & 0 & -x_1 x_3^2 + x_2^2 x_4 & -x_1^2 x_3 + x_2^3 \end{pmatrix}$$

In fact, the columns of $\mathcal{M}$ are a Gröbner basis of $\text{Syz}(\mathcal{G})$ with respect to the ordering induced by $(\sigma, \mathcal{G})$.

At this point we know how to compute a system of generators of the syzygy module of a Gröbner basis. Now we become more ambitious and want to be able to calculate the syzygy module of an arbitrary system of generators $\{h_1, \ldots, h_t\}$ of M, where we even allow zero vectors.

The key ingredients will be the following. Using the Extended Buchberger Algorithm 2.5.11, we can calculate a Gröbner basis $\{g_1, \ldots, g_s\}$ of M together with representations $g_j = a_{1j}h_1 + \cdots + a_{tj}h_t$ for $j = 1, \ldots, s$. Furthermore, after we have calculated this Gröbner basis, we can use the Division Algorithm 1.6.4 to find representations $h_j = b_{1j}g_1 + \cdots + b_{sj}g_s$ for $j = 1, \ldots, t$. Thus we can explicitly calculate the matrices $\mathcal{A} = (a_{ij})$ and $\mathcal{B} = (b_{ij})$ required by the following theorem.

But before, we remind the reader that a tuple of vectors can also be viewed as a matrix, namely the matrix whose columns consist of the coordinates of the vectors.

Theorem 3.1.8. (Computation of Syzygy Modules)
Let $\{h_1, \ldots, h_t\}$ be a system of generators of a P-submodule M of P^r, let $\mathcal{H} = (h_1, \ldots, h_t)$, let $\{g_1, \ldots, g_s\}$ be a σ-Gröbner basis of M, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$. Furthermore, suppose we are given a $t \times s$-matrix $\mathcal{A} = (a_{ij})$ and an $s \times t$-matrix $\mathcal{B} = (b_{ij})$ over P such that $\mathcal{G} = \mathcal{H}\mathcal{A}$ and $\mathcal{H} = \mathcal{G}\mathcal{B}$. Finally, let $\mathcal{M}$ be a matrix whose columns generate $\text{Syz}(\mathcal{G})$, and let $\mathcal{I}_t$ be the $t \times t$ identity matrix. Then the columns of the matrix $\mathcal{N} = (\mathcal{A}\mathcal{M} \mid \mathcal{I}_t - \mathcal{A}\mathcal{B})$ generate the module $\text{Syz}(\mathcal{H})$.

Proof. From $\mathcal{G} = \mathcal{H}\mathcal{A}$ and $\mathcal{H} = \mathcal{G}\mathcal{B}$ we get

$$\mathcal{H}\mathcal{N} = (\mathcal{H}\mathcal{A}\mathcal{M} \mid \mathcal{H} - \mathcal{H}\mathcal{A}\mathcal{B}) = (\mathcal{G}\mathcal{M} \mid \mathcal{H} - \mathcal{G}\mathcal{B}) = (0 \mid \mathcal{H} - \mathcal{H}) = 0$$

Hence the columns of $\mathcal{N}$ are syzygies of $\mathcal{H}$. Conversely, if a column vector v is a syzygy of $\mathcal{H}$, we have $\mathcal{G}\mathcal{B} \cdot v = \mathcal{H} \cdot v = 0$. Hence we have $\mathcal{B} \cdot v \in \text{Syz}(\mathcal{G})$, and therefore this vector lies in the column space of $\mathcal{M}$. From the identity $v = \mathcal{A}(\mathcal{B} \cdot v) + (\mathcal{I}_t - \mathcal{A}\mathcal{B}) \cdot v$ we may then conclude that v lies in the column space of $\mathcal{N}$. $\square$

Corollary 3.1.9. (Explicit Membership)
With the same assumptions as in Theorem 3.1.8, let $m = \sum_{i=1}^{s} f_i g_i \in M$, where $f_i \in P$ for $i = 1, \ldots, s$, and let $\mathcal{F}$ be the matrix consisting of one column whose entries are $f_1, \ldots, f_s$.

a) *The equality $m = \mathcal{H}(\mathcal{A}\mathcal{F})$ provides an explicit expression of m as a combination of the given generators $h_1, \ldots, h_t$ of M.*

b) *Let $\mathcal{N} = (\mathcal{A}\mathcal{M} \mid \mathcal{I}_t - \mathcal{A}\mathcal{B})$. Then every explicit expression of m as a combination of the given generators $h_1, \ldots, h_t$ of M is of the form $m = \mathcal{H}(\mathcal{A}\mathcal{F} + \mathcal{N}\mathcal{P})$ for a suitable matrix $\mathcal{P}$ consisting of one column of polynomials.*

Proof. To prove a), it suffices to combine the two equalities $m = \mathcal{G}\,\mathcal{F}$ and $\mathcal{G} = \mathcal{H}\,\mathcal{A}$. Now we prove b). If $m = \mathcal{H}\,\mathcal{Q}$ with a $t \times 1$-matrix $\mathcal{Q}$ of polynomi-als, we deduce from a) that $\mathcal{H}\,\mathcal{Q} - \mathcal{H}\,(\mathcal{A}\,\mathcal{F}) = 0$. Hence $\mathcal{Q} - \mathcal{A}\,\mathcal{F}$ is a syzygy of $\mathcal{H}$. From Theorem 3.1.8 we deduce that $\mathcal{Q} - \mathcal{A}\,\mathcal{F} = \mathcal{N}\,\mathcal{P}$ for a suitable column matrix $\mathcal{P}$. Now we combine $m = \mathcal{H}\,\mathcal{Q}$ with $\mathcal{Q} = \mathcal{A}\,\mathcal{F} + \mathcal{N}\,\mathcal{P}$ and obtain the claim. $\qquad\square$

Our next example shows how one can apply the previous theorem in prac-tice. It also demonstrates that the system of generators of $\mathrm{Syz}(\mathcal{H})$ provided by the theorem is in general not minimal.

Example 3.1.10. In Example 2.5.7 we saw that $\{g_1, g_2, g_3\}$ with $g_1 = x^2$, $g_2 = xy + y^2$, and $g_3 = y^3$ is a Gröbner basis of the ideal $I = (g_1, g_2)$ in $P = K[x, y]$ with respect to $\sigma = \texttt{Lex}$. We let $\mathcal{G} = (g_1, g_2, g_3)$, $h_1 = g_1$, and $h_2 = g_2$, and we want to compute the syzygy module of $\mathcal{H} = (h_1, h_2)$.

Using the Extended Buchberger Algorithm 2.5.11, we calculate the ma-trix $\mathcal{A}$, and using the Division Algorithm 1.6.4, we calculate the matrix $\mathcal{B}$. We find

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & -x+y \end{pmatrix} \qquad \text{and} \qquad \mathcal{B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

An application of Corollary 3.1.5 now yields the system of generators $s_{12} = y\varepsilon_1 + (-x+y)\varepsilon_2 - \varepsilon_3$, $s_{13} = y^3\varepsilon_1 - x^2\varepsilon_3$, and $s_{23} = y^2\varepsilon_2 + (-x-y)\varepsilon_3$ of the P-module $\mathrm{Syz}(\mathcal{G})$. Therefore we get

$$\mathcal{M} = \begin{pmatrix} y & y^3 & 0 \\ -x+y & 0 & y^2 \\ -1 & -x^2 & -x-y \end{pmatrix}$$

and

$$\mathcal{N} = \begin{pmatrix} 0 & -y(x^2 - y^2) & -y(x+y) & 0 & 0 \\ 0 & x^2(x-y) & x^2 & 0 & 0 \end{pmatrix}$$

Even if we delete the zero columns in $\mathcal{N}$, we still have no minimal system of generators of $\mathrm{Syz}(\mathcal{H})$, since the second column is a multiple of the third. Altogether, we find

$$\mathrm{Syz}(\mathcal{H}) = \langle -y(x+y)\varepsilon_1 + x^2\varepsilon_2 \rangle \subseteq P^2$$

It is apparent that in the preceding example we actually could have done without using the Extended Buchberger Algorithm or the Division Algorithm, since the Gröbner basis $\{g_1, g_2, g_3\}$ contained the system of gen-erators $\{h_1, h_2\}$ whose syzygy module we wanted to compute. This happens quite often if we start with an arbitrary system of generators of M and determine a Gröbner basis from it by using Buchberger's Algorithm. So, let us study this case.

Corollary 3.1.11. *Suppose that, in the situation of Theorem 3.1.8, the matrix $\mathcal{A}$ is of the form $\mathcal{A} = (\mathcal{I}_t \mid \mathcal{C})$ with a $t \times (s-t)$-matrix $\mathcal{C}$ over P. Let $\mathcal{M}$ be a matrix whose columns generate $\mathrm{Syz}(\mathcal{G})$. If we decompose it in the form $\mathcal{M} = (\frac{\mathcal{M}'}{\mathcal{M}''})$ with a matrix $\mathcal{M}'$ having t rows and a matrix $\mathcal{M}''$ having $s-t$ rows, then the syzygy module $\mathrm{Syz}(\mathcal{H})$ is generated by the columns of the matrix $\mathcal{M}' + \mathcal{C} \cdot \mathcal{M}''$.*

Proof. By assumption, the matrix $\mathcal{B}$ is of the form $\mathcal{B} = (\frac{\mathcal{I}_t}{0})$. Therefore we obtain $\mathcal{I}_t - \mathcal{A}\mathcal{B} = \mathcal{I}_t - \mathcal{I}_t = 0$, and the right-hand part of the matrix $\mathcal{N}$ in the theorem contributes nothing to $\mathrm{Syz}(\mathcal{H})$. The left-hand part of $\mathcal{N}$ is given by $\mathcal{A}\mathcal{M} = (\mathcal{I}_t \mid \mathcal{C}) \cdot (\frac{\mathcal{M}'}{\mathcal{M}''}) = \mathcal{M}' + \mathcal{C} \cdot \mathcal{M}''$. □

As an application of Theorem 3.1.8, we have the following method to determine an irredundant system of generators of a P-submodule $M \subseteq P^r$, i.e. a system of generators such that no proper subset of it generates M. Notice that the second condition in the following corollary can be checked effectively using the Submodule Membership Test 2.4.10.a.

Corollary 3.1.12. *Let $\{h_1, \ldots, h_t\}$ be a system of generators of a P-submodule $M \subseteq P^r$, let $\mathcal{H} = (h_1, \ldots, h_t)$, and let $\mathcal{N}$ be a matrix over P whose columns generate the P-module $\mathrm{Syz}(\mathcal{H})$. For every $i \in \{1, \ldots, t\}$, the following conditions are equivalent.*

a) *We have $h_i \in \langle h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_t \rangle$.*
b) *The ideal generated by the ith row of $\mathcal{N}$ is the unit ideal of P.*

In particular, a repeated application of this equivalence allows us to find an irredundant system of generators of M which is contained in $\{h_1, \ldots, h_t\}$.

Proof. Both conditions are equivalent to the condition that there exists a column in the column space of $\mathcal{N}$ whose i^{th} entry is 1. □

Example 3.1.13. Let $h_1 = x^2 y^2 - 1$, $h_2 = x^4 y^4 - 2x^2 y^2 + xyz^2 - \frac{1}{2}z^4 + \frac{1}{2}$, $h_3 = xyz^2 - \frac{1}{2}z^4 - \frac{1}{2}$, and $h_4 = xy - z^2$ be polynomials in $\mathbb{Q}[x, y, z]$, and let I be the ideal generated by $\{h_1, h_2, h_3, h_4\}$. Using the method described in the corollary, we try to shorten this system of generators. Since $\mathrm{Syz}(h_1, h_2, h_3, h_4) = \langle (1, 0, -2, -xy + z^2), (0, 0, -2xy + 2z^2, 2xyz^2 - z^4 - 1), (x^2 y^2 - 1, -1, 1, 0) \rangle$, we can delete h_1 from the system of generators of I. Since $\mathrm{Syz}(h_2, h_3, h_4) = \langle (0, -2xy + 2z^2, 2xyz^2 - z^4 - 1), (1, -x^2 y^2 - \frac{1}{2}xyz^2 - \frac{1}{2}z^4 + 1, -x^3 y^3 + \frac{1}{4}z^6 + \frac{3}{2}xy - \frac{3}{4}z^2) \rangle$, we can then delete h_2. The remaining system of generators $\{h_3, h_4\}$ of I is irredundant, because we can check that $\mathrm{Syz}(h_3, h_4) = \langle (-2xy + 2z^2, 2xyz^2 - z^4 - 1) \rangle$.

This example also shows that we can shorten some systems of generators in different ways. For instance, we could have deleted h_2 and then h_3 in order to get the irredundant system of generators $\{h_1, h_4\}$ of I.

Exercise 1. Let $f_1, f_2 \in P$ be two non-zero polynomials. Show that the module $\text{Syz}(f_1, f_2) \subseteq P^2$ is generated by a single vector $(g_1, g_2) \in P^2$. Then show that f_2 is a multiple of g_1, and that $\gcd(f_1, f_2) = f_2/g_1$.

Exercise 2. Compute a set of generators of $\text{Syz}(\mathcal{H})$ in Example 3.1.10, using the method described in Corollary 3.1.11.

Exercise 3. Let $P = K[x, y, z]$, let σ be a term ordering on $\mathbb{T}^3$, let $g_1 = yz$, $g_2 = xz$, $g_3 = xy$, and let $\mathcal{G} = (g_1, g_2, g_3)$. Find a subset $\mathbb{B}' \subseteq \mathbb{B}$ such that the corresponding set $\Sigma' = \{\sigma_{ij} \in \Sigma \mid (i, j) \in \mathbb{B}'\}$ is a set of generators of $\text{Syz}(\text{LM}_\sigma(\mathcal{G}))$, but $\{s_{ij} \mid (i, j) \in \mathbb{B}'\}$ is not a τ-Gröbner basis of $\text{Syz}(\mathcal{G})$, where τ is the ordering induced by $(\sigma, \mathcal{G})$.

Exercise 4. Let $\mathcal{G} = (g_1, \ldots, g_s)$, where $g_i \in P$ for $i = 1, \ldots, s$. Prove that $\text{Syz}(\mathcal{G}) = (0)$ if and only if $s = 1$ and $g_1 \neq 0$.

Exercise 5. Let $\mathcal{G} = (g_1, \ldots, g_s)$, where $g_i \in P$ for $i = 1, \ldots, s$ and $g_1 = 1$. Describe an explicit set of generators of $\text{Syz}(\mathcal{G})$ consisting of $s - 1$ elements.

Exercise 6. Let I be an ideal in $P = K[x_1, \ldots, x_n]$.
  a) Assume that I is a principal ideal generated by a non-zero element f. Then show that every element of I has a unique representation as a multiple of f.
  b) Assume that $I = (f_1, \ldots, f_r)$, where $f_i \in P$ for $i = 1, \ldots, r$ and $r > 1$, and let $f \in I$. Then show that f can be represented in more than one way as a combination of $f_1, \ldots, f_r$.

Exercise 7. Let $\{h_1, \ldots, h_t\}$ be a set of vectors in P^r which generates a module $M \subseteq P^r$, let $m \in M$, and let σ be a term ordering of type `PosTo` on $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_{t+1} \rangle$. Explain how one can use the knowledge of a σ-Gröbner basis of the syzygy module $\text{Syz}(m, h_1, \ldots, h_t)$ to give an alternative method for computing explicit membership.

Tutorial 28: Splines

Suppose we have a closed interval $[a, b] \subseteq \mathbb{R}$, where $a, b \in \mathbb{R}$ and $a < b$. For $k \geq 1$, a tuple $\mathcal{C} = (c_0, \ldots, c_k) \in \mathbb{R}^{k+1}$ such that $a = c_0 < c_1 < \cdots < c_k = b$ defines a decomposition of the interval $[a, b]$ into subintervals. Furthermore, suppose that we are given numbers $d_0, \ldots d_k \in \mathbb{R}$. A tuple of polynomials $(s_1, \ldots, s_k) \in \mathbb{R}[x]^k$ is called a $\mathcal{C}$**-spline** with values $(d_0, \ldots, d_k)$ if we have $s_i(c_{i-1}) = d_{i-1}$ and $s_i(c_i) = d_i$ for $i = 1, \ldots, k$. The set of all $\mathcal{C}$-splines will be denoted by $\mathbb{S}(\mathcal{C})$. Notice that we did not fix the tuple $(d_0, \ldots, d_k)$ here, i.e. that $\mathbb{S}(\mathcal{C})$ contains the $\mathcal{C}$-splines for all tuples $(d_0, \ldots, d_k)$. Our goal in this tutorial is to study the set of $\mathcal{C}$-splines and to compute it effectively.

To each spline $(s_1, \ldots, s_k) \in \mathbb{S}(\mathcal{C})$ we can associate the **spline function** $s : [a, b] \longrightarrow \mathbb{R}$ given by $s(t) = s_i(t)$ for $t \in [c_{i-1}, c_i]$ and $i = 1, \ldots, k$. A natural situation in which spline functions are useful occurs when we have a

bounded function $f : [a, b] \longrightarrow \mathbb{R}$ (which may be very complicated) for which we know finitely many values $d_i = f(c_i)$ for $i = 0, \ldots, k$. In this case we are looking for a spline function $s : [a, b] \longrightarrow \mathbb{R}$ which approximates f well, i.e. for which the number $\| f - s \|_\infty = \sup_{t \in [a,b]} \{ |f(t) - s(t)| \}$ is small.

a) The simplest cases of splines are single polynomials passing through the points $(c_0, d_0), \ldots, (c_k, d_k)$. For $i = 0, \ldots, k$, we define $\ell_i = \prod_{j \neq i} \frac{x - c_j}{c_i - c_j}$.

   Show that the **Lagrange interpolation polynomial** $\ell = \sum_{i=0}^{k} d_i \ell_i$ has degree $\leq k$ and passes through the points $(c_0, d_0), \ldots, (c_k, d_k)$. Write a CoCoA function `Lagrange(...)` which takes the list of pairs (c_i, d_i) and computes the Lagrange interpolation polynomial.

b) Take the functions $f : [0, 2\pi] \longrightarrow \mathbb{R}$ given by $f(t) = \sin(t)$ and $g : [-2, 2] \longrightarrow \mathbb{R}$ given by $g(t) = \frac{1}{1 + 25t^2}$. In each case, divide the interval into $k = 4$ equal parts and compute the corresponding Lagrangean interpolation polynomial.

   Hint: First write a CoCoA function `Sin(...)` which uses the Taylor expansion to compute the value of $\sin(t)$ up to a certain number of decimal digits. Then write a CoCoA function `Values(...)` which takes the tuple $(c_0, \ldots, c_k)$ and the name of the function and computes the list of pairs $[(c_0, d_0), \ldots, (c_k, d_k)]$. Finally, this list can be used in `Lagrange(...)`.
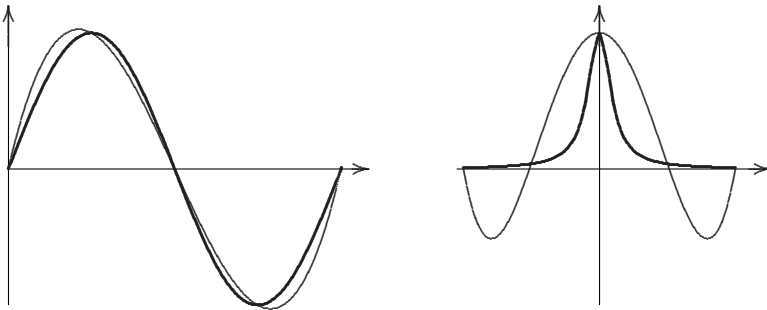
c) Repeat part b) with $k = 8$. Use CoCoA to compute approximations for $\| f - s \|_\infty$ and $\| g - s \|_\infty$ in all cases. Conclude that the approximation of f by its interpolation polynomial got better when we increased k, whereas the approximation of g got worse.

   Hint: Compute $|f(t) - s(t)|$ resp. $|g(t) - s(t)|$ for all t increasing in steps of 0.01 from a to b.
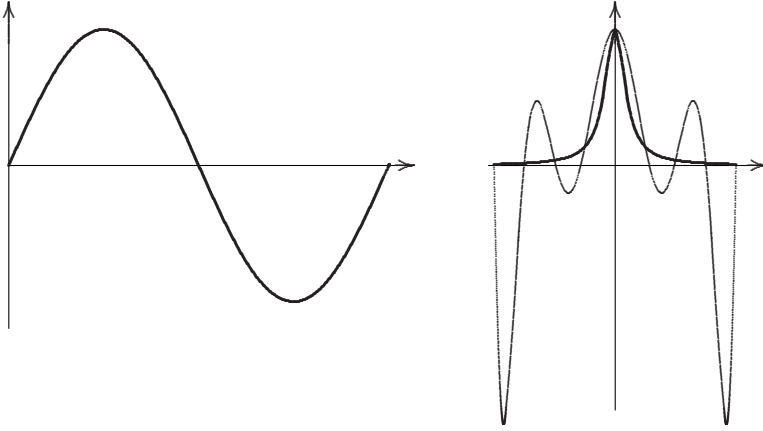
d) Let $r \geq 0$, and let $\mathcal{A}_r$ be the matrix

$$\begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & (x-c_1)^{r+1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & -1 & 0 & & \cdots & 0 & (x-c_{k-1})^{r+1} \end{pmatrix}$$

of size $(k-1) \times (2k-1)$. Prove that, for a spline $(s_1, \ldots, s_k) \in \mathbb{S}(\mathcal{C})$, the following conditions are equivalent.

1) The associated spline function $s : [a, b] \longrightarrow \mathbb{R}$ is r times differentiable and its rth derivative is continuous.
2) For $i = 1, \ldots, k-1$, the difference $s_i - s_{i+1}$ is divisible by $(x-c_i)^{r+1}$.
3) There are polynomials $s_{k+1}, \ldots, s_{2k-1} \in \mathbb{R}[x]$ such that the tuple $(s_1, \ldots, s_{2k-1})$ is contained in $\text{Syz}(\mathcal{A}_r)$.

The set of all $\mathcal{C}$-splines $(s_1, \ldots, s_k)$ satisfying these conditions will be denoted by $\mathbb{S}^r(\mathcal{C})$.

e) Using d), conclude that $\mathbb{S}^r(\mathcal{C})$ is an $\mathbb{R}[x]$-submodule of $\mathbb{R}[x]^k$. Write a CoCoA function `Splines(...)` which takes r and a tuple $\mathcal{C} \in \mathbb{Q}^{k+1}$ and computes a system of generators for the $\mathbb{R}[x]$-module $\mathbb{S}^r(\mathcal{C})$.
Hint: Use Lemma 2.4.16 to show that it suffices to compute a system of generators of the corresponding $\mathbb{Q}[x]$-module.

f) Let $d \geq 0$. We say that a $\mathcal{C}$-spline $(s_1, \ldots, s_k) \in \mathbb{S}^r(\mathcal{C})$ has **degree** $\leq d$ if $\deg(s_i) \leq d$ for $i = 1, \ldots, k$. Prove that the subset $\mathbb{S}^r_d(\mathcal{C}) \subseteq \mathbb{S}^r(\mathcal{C})$ of all $\mathcal{C}$-splines of degree $\leq d$ is an $\mathbb{R}$-vector subspace of $\mathbb{R}[x]^k$ of dimension

$$\dim_{\mathbb{R}}(\mathbb{S}^r_d(\mathcal{C})) = \begin{cases} d+1 & \text{if } d < r+1 \\ (k-1)(d-r)+d+1 & \text{if } d \geq r+1 \end{cases}$$

Hint: Consider the vectors $(x^i, \ldots, x^i)$, where $i = 0, \ldots, d$, and the vectors $(0, \ldots, 0, x^i(x-c_j)^{r+1}, \ldots, x^i(x-c_j)^{r+1})$, where $i = 0, \ldots, d-r-1$ and $j = 1, \ldots, k-1$. (There are j zeros.)

g) A $\mathcal{C}$-spline $(s_1, \ldots, s_k) \in \mathbb{S}_3^2(\mathcal{C})$ is called a **natural $\mathcal{C}$-spline** if it satisfies the additional conditions $s_1''(a) = 0$ and $s_k''(b) = 0$. Let $(s_1, \ldots, s_k)$ be a natural $\mathcal{C}$-spline with values $(d_0, \ldots, d_k)$.

   1) Prove that the tuple $(0, s_1''(c_1), \ldots, s_{k-1}''(c_{k-1}), 0)$ is the unique solution of the system of equations

$$(c_i - c_{i-1})x_{i-1} + 2\,(c_{i+1} - c_{i-1})x_i + (c_{i+1} - c_i)x_{i+1} = 6\left(\frac{d_{i+1} - d_i}{c_{i+1} - c_i} - \frac{d_i - d_{i-1}}{c_i - c_{i-1}}\right)$$

     where $i = 1, \ldots, k-1$ and $x_0 = x_k = 0$.

   2) Show that the spline $(s_1, \ldots, s_k)$ can be computed from this tuple via the formulas $s_i = \alpha_i(x - c_{i-1})^3 + \beta_i(x - c_{i-1})^2 + \gamma_i(x - c_{i-1}) + d_{i-1}$, where $\alpha_i = \frac{1}{6(c_i - c_{i-1})} \cdot (s_i''(c_i) - s_{i-1}''(c_{i-1}))$, where $\beta_i = \frac{1}{2}\, s_{i-1}''(c_{i-1})$, and where $\gamma_i = \frac{c_{i-1} - c_i}{6} \cdot (s_i''(c_i) + 2s_{i-1}''(c_{i-1})) + \frac{d_i - d_{i-1}}{c_i - c_{i-1}}$ for every $i \in \{1, \ldots, k\}$.

   3) Write a CoCoA function `NatSpline(...)` which takes the tuple of pairs $((c_0, d_0), \ldots, (c_k, d_k))$ and computes the corresponding natural $\mathcal{C}$-spline.

h) Apply your function `NatSpline(...)` to compute the natural $\mathcal{C}$-spline approximating the function $h : [0,3] \longrightarrow \mathbb{R}$ given by $h(t) = \sin(e^t)$, where $\mathcal{C}$ is the equidistant decomposition of $[0,3]$ into 12 parts.

i) Redo part h) using the decomposition $\mathcal{C}' = (0, 0.45, 1.15, 1.55, 1.85, 2.05, 2.25, 2.4, 2.55, 2.65, 2.75, 2.85, 3)$. Show that the corresponding spline function becomes a much better approximation of h.
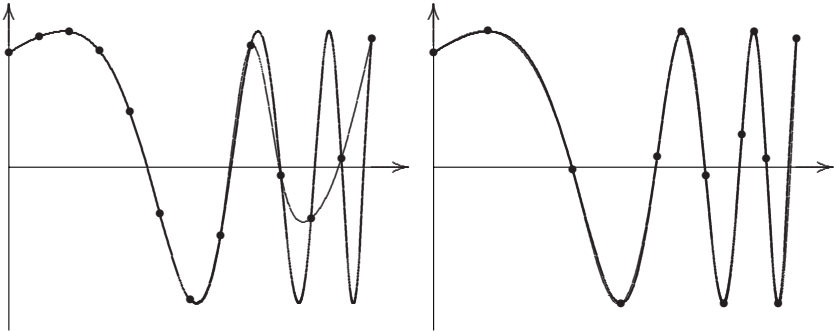
Tutorial 29: Hilbert's Syzygy Theorem

Let K be a field, let $P = K[x_1, \ldots, x_n]$, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$, let $M \subseteq P^r$ be a P-submodule, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero vectors which form a σ-Gröbner basis of M.

a) Suppose, in addition, that for every $i = 1, \ldots, s$ there exists an index $\gamma_i \in \{1, \ldots, r\}$ such that $\mathrm{LT}_\sigma(g_i) = e_{\gamma_i}$. Show that the P-modules M and P^r/M are free. (*Hint:* Reduce the proof to the case where $\gamma_i \neq \gamma_j$ for $i \neq j$. Then argue as in Exercise 7 of Section 2.3.)

Now assume instead that $\mathrm{LT}_\sigma(g_1) >_{\texttt{PosLex}} \cdots >_{\texttt{PosLex}} \mathrm{LT}_\sigma(g_s)$ and that there exists a number $m \in \{1, \ldots, n\}$ such that $\mathrm{LT}_\sigma(g_i) \in K[x_m, \ldots, x_n]^r$ for $i = 1, \ldots, s$.

b) Prove that $\mathrm{LT}_\tau(\sigma_{ij}) \in K[x_{m+1}, \ldots, x_n]^s$ for all syzygies σ_{ij} of $\mathcal{G}$ constructed in Corollary 3.1.5, where τ is the ordering induced by $(\sigma, \mathcal{G})$ on $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s \rangle$.

c) Conclude that, in the situation of b), there exists an exact sequence

$$0 \longrightarrow F_{n-m} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

with finitely generated free P-modules $F_0, \ldots, F_{n-m}$.

d) Let N be a non-zero, finitely generated P-module. Represent the module N as $N \cong P^r/M$ for a suitable $r \geq 1$ and a P-submodule M of P^r. Then use c) to show that there exists an exact sequence

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow N \longrightarrow 0$$

with finitely generated free P-modules $F_0, \ldots, F_n$, some of which may be zero. This is an effective proof of **Hilbert's Syzygy Theorem** due to F. Schreyer.

e) Let $n = 3$. Write a CoCoA program `HilbRes`$(\ldots)$ which takes a tuple of non-zero vectors $\mathcal{G}$ which form a Gröbner basis of a module M and computes a resolution of the residue class module P^r/M in the way described above. (Do not use the built-in CoCoA function `Res`$(\ldots)$.)

3.2 Elementary Operations on Modules

> *'And you do Addition?' the White Queen asked.*
> *'What's one and one and one and one and one*
> *and one and one and one and one and one?'*
> *'I don't know,' said Alice. 'I lost count.'*
> *'She can't do Addition,' the Red Queen interrupted.*
> *'Can you do Subtraction? Take nine from eight.'*
> *'Nine from eight I can't, you know,' Alice replied very readily: 'but – '*
> *'She can't do Subtraction,' said the White Queen. 'Can you do Division?*
> *Divide a loaf by a knife – what's the answer to that?'*
> *'I suppose –' Alice was beginning, but the Red Queen answered for her.*
> *'Bread-and-butter, of course'.*
> (Charles L. Dodgson)

This is rather a long section, much longer than the average. Even the quotation is longer than usual! Why? As the title suggests, we want to describe techniques for computing elementary operations on modules such as sums, products, intersections, colon ideals, annihilators, etc. The key ingredient will be the computation of syzygy modules explained in the previous section. Then, in later sections and in Volume 2, our elementary operations on modules will themselves become the key ingredients for a host of other applications of Computational Commutative Algebra.

It is a fact that there are many different ways to perform these operations, and our goal is to describe the most important ones in sufficient detail so that the propositions we present can be easily translated into algorithms. We are aware that the general appearance of the entire section is rather technical, with many matrices and indices floating around. However, if you are interested both in the theoretical background and in how to implement the operations described here, then we hope that you are ready to pay this price.

Now let us have a closer look at the contents of the current section. We decided to split it into three subsections which deal with intersections, colon ideals and annihilators, and colon modules, respectively.

Do we do Addition? Not really, because we consider it trivial. *Can we do Subtraction?* Nor that. We don't know what the difference of two ideals or modules could mean. The first non-obvious operation is the computation of the intersection of two ideals or submodules. First, consider the following simple case. For two non-zero principal ideals $I = (f)$ and $J = (g)$ in $P = K[x]$ we saw in Proposition 1.2.8.a that their intersection is $I \cap J = (\text{lcm}(f, g))$.

What happens if we consider ideals I and J in $P = K[x_1, \ldots, x_n]$? How can we compute a set of generators of $I \cap J$ from given sets of generators of I and J? There is no obvious answer, but in Section 3.1 we expended a lot of effort to compute syzygies, and now it is time to reap the rewards. With the tools developed there we will be able to solve the problem even in the more general case of modules (see Propositions 3.2.3 and 3.2.7).

A nice consequence is the possibility of presenting a module of the form $M/(M \cap N)$ via generators and relations (see Corollary 3.2.6). Another nice extra bonus is the discovery that syzygies provide a method for computing greatest common divisors and least common multiples of multivariate polynomials, without having to resort to factorizing algorithms (see Corollary 3.2.9).

Can we do Division? Suppose we are given two non-zero polynomials $g, h \in P$ such that $g = fh$ for some polynomial $f \in P$. This equation implies that f is a generator of the ideal $\{a \in P \mid a \cdot h \in (g)\}$. For two ideals $I, J \subseteq P$, a natural generalization is to consider the ideal $I :_P J = \{a \in P \mid a \cdot J \subseteq I\}$. We call it the *colon ideal* of I by J. This construction is particularly useful in the computation of the so-called primary decompositions (see Tutorial 43) and in algebraic geometry, where it is related to the process of removing irreducible components from an algebraic variety.

The definition of colon ideals can be extended in two ways into the realm of modules. One method describes an operation on two modules which produces an ideal, called the *colon ideal*. It can also be viewed as the *annihilator* of a certain quotient module (see Definition 3.2.10). The other method yields an operation on two modules and an ideal which produces a module called the *colon module* (see Definition 3.2.17).

In the subsection "Colon Ideals and Annihilators" we show two different approaches to the computation of colon ideals, one based on intersections and the other based on syzygies of a suitable matrix (see Proposition 3.2.15). And in the subsection "Colon Modules" we show two different approaches to the computation of colon modules. Again, one is based on intersections and the other on syzygies of a suitable matrix (see Proposition 3.2.22). A final application of the techniques developed above is a method for checking whether a given sequence of polynomials is a regular sequence, a property which we shall reexamine in Tutorial 33 and in Volume 2.

Let K be a field, $n \geq 1$, $P = K[x_1, \ldots, x_n]$ a polynomial ring, $r \geq 1$, σ a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, and $\mathcal{G} = (g_1, \ldots, g_s) \in (P^r)^s$ a tuple of vectors which generate a P-submodule M of P^r. Furthermore, we let $\mathcal{H} = (h_1, \ldots, h_t) \in (P^r)^t$ be a tuple of vectors which generate another P-submodule N of P^r.

For an $r' \times s'$ matrix $\mathcal{M}$ with entries in P, we let $\mathrm{Syz}(\mathcal{M})$ be the syzygy module of the tuple of the columns of $\mathcal{M}$, each viewed as a vector in $P^{r'}$, as already explained in the introduction of the chapter. The following remark collects some operations on modules which can be computed in a completely trivial way.

Remark 3.2.1. Let $M = \langle g_1, \ldots, g_s \rangle$ and $N = \langle h_1, \ldots, h_t \rangle$ be two P-submodules of P^r as above, and let $I \subseteq P$ be an ideal which is generated by a set of polynomials $\{f_1, \ldots, f_u\} \subseteq P$.

 a) The sum $M + N$ is the P-submodule of P^r generated by the set of vectors $\{g_1, \ldots, g_s, h_1, \ldots, h_t\} \subseteq P^r$.

b) The product $I \cdot M$ is the P-submodule of P^r generated by the set of vectors $\{f_i g_j \mid 1 \le i \le u, \, 1 \le j \le s\} \subseteq P^r$.

c) For every $d \ge 1$, the power I^d is the ideal of P generated by the set of polynomials $\{f_{j_1} \cdots f_{j_d} \mid j_1, \ldots, j_d \in \{1, \ldots, u\}\} \subseteq P$.

3.2.A   Intersections

The first non-trivial operation we consider is the computation of the intersection of two submodules of P^r. One method for performing this computation is based on the following result about the preimage of a submodule of P^r under a P-linear map $\lambda : P^s \longrightarrow P^r$. Recall that the canonical basis of P^s is denoted by $\{\varepsilon_1, \ldots, \varepsilon_s\}$.

Lemma 3.2.2. *Let $N = \langle h_1, \ldots, h_t \rangle$ be a P-submodule of P^r, and let the P-linear map $\lambda : P^s \longrightarrow P^r$ be given by $\lambda(\varepsilon_i) = g_i$ for $i = 1, \ldots, s$. We let $\{v_1, \ldots, v_u\} \subseteq P^{s+t}$ be a system of generators of $\mathrm{Syz}(g_1, \ldots, g_s, h_1, \ldots, h_t)$, and we write $v_j = (f_{1j}, \ldots, f_{s+t\, j})$ with $f_{1j}, \ldots, f_{s+t\, j} \in P$ for $j = 1, \ldots, u$. Then we have*

$$\lambda^{-1}(N) = \langle (f_{1j}, \ldots, f_{sj}) \mid 1 \le j \le u \rangle$$

Proof. Since we have $\lambda(f_{1j}, \ldots, f_{sj}) = \sum_{i=1}^{s} f_{ij} g_i = -\sum_{i=1}^{t} f_{s+i\, j} h_i \in N$ for $j = 1, \ldots, u$, it suffices to prove the reverse inclusion. Given a vector $v = (a_1, \ldots, a_s) \in \lambda^{-1}(N)$, we can find polynomials $a_{s+1}, \ldots, a_{s+t} \in P$ such that $\lambda(v) = \sum_{i=1}^{s} a_i g_i = -\sum_{i=1}^{t} a_{s+i} h_i$. Then $(a_1, \ldots, a_{s+t})$ is in $\mathrm{Syz}(g_1, \ldots, g_s, h_1, \ldots, h_t)$, and we can find polynomials $p_1, \ldots, p_u \in P$ such that $(a_1, \ldots, a_{s+t}) = \sum_{j=1}^{u} p_j v_j$. In particular, we get $v = (a_1, \ldots, a_s) = \sum_{j=1}^{u} p_j (f_{1j}, \ldots, f_{sj})$ which proves the claim. $\qquad\square$

Proposition 3.2.3. (Intersection of Two Submodules)
Let $M = \langle g_1, \ldots, g_s \rangle$ and $N = \langle h_1, \ldots, h_t \rangle$ be two P-submodules of P^r, and let $\lambda : P^s \longrightarrow P^r$ be the P-linear map given by $\lambda(\varepsilon_i) = g_i$ for $i = 1, \ldots, s$.

a) *Let $\{v_1, \ldots, v_u\} \subseteq P^{s+t}$ be a system of generators of the P-module $\mathrm{Syz}(g_1, \ldots, g_s, h_1, \ldots, h_t)$, and let $v_j = (f_{1j}, \ldots, f_{s+t\, j})$ with polynomials $f_{1j}, \ldots, f_{s+t\, j} \in P$ for $j = 1, \ldots, u$. Then we have*

$$M \cap N = \lambda(\lambda^{-1}(N)) = \langle \sum_{i=1}^{s} f_{ij} g_i \mid 1 \le j \le u \rangle$$

b) *Consider the following block matrix of size $2r \times (r + s + t)$*

$$\mathcal{M} = \begin{pmatrix} \mathcal{I}_r & \mathcal{G} & 0 \\ \mathcal{I}_r & 0 & \mathcal{H} \end{pmatrix}$$

where $\mathcal{I}_r$ is the $r \times r$ identity matrix. Let $\{v_1, \ldots, v_u\} \subseteq P^{r+s+t}$ be a system of generators of $\mathrm{Syz}(\mathcal{M})$, and let $v_j = (f_{1j}, \ldots, f_{r+s+t\, j})$ with $f_{1j}, \ldots, f_{r+s+t\, j} \in P$ for $j = 1, \ldots, u$. Then

$$M \cap N = \langle (f_{1j}, \ldots, f_{rj}) \mid 1 \le j \le u \rangle$$

Proof. Since claim a) follows immediately from the lemma, it suffices to show claim b). Let $w_1, \ldots, w_{r+s+t}$ be the column vectors of $\mathcal{M}$. If we look at the first and the last r components of $f_{1j}w_1 + \cdots + f_{r+s+t\,j}\,w_{r+s+t} = 0$, we obtain

$$\begin{pmatrix} f_{1j} \\ \vdots \\ f_{rj} \end{pmatrix} = -f_{r+1\,j}\,g_1 - \cdots - f_{r+s\,j}\,g_s = -f_{r+s+1\,j}\,h_1 - \cdots - f_{r+s+t\,j}\,h_t$$

for $j = 1, \ldots, u$, and therefore $(f_{1j}, \ldots, f_{rj}) \in M \cap N$. Conversely, if we start with an element $v \in M \cap N$, and if we write $v = (a_1, \ldots, a_r)$ with polynomials $a_1, \ldots, a_r \in P$, then there are polynomials $a_{r+1}, \ldots, a_{r+s+t} \in P$ such that

$$v = -a_{r+1}g_1 - \cdots - a_{r+s}g_s = -a_{r+s+1}h_1 - \cdots - a_{r+s+t}h_t$$

By combining those representations of v, we get the vector equation

$$a_1 w_1 + \cdots + a_{r+s+t}w_{r+s+t} = 0$$

Thus there are polynomials $p_1, \ldots, p_u \in P$ such that

$$(a_1, \ldots, a_{r+s+t}) = \sum_{j=1}^{u} p_j(f_{1j}, \ldots, f_{r+s+t\,j})$$

The first r components of this equality now prove the claim. □

Example 3.2.4. Let us compute the intersection of the ideals $I_1 = (x_1, x_2)$ and $I_2 = (x_1^2 - x_2^2,\ x_1 x_2 x_3,\ x_3^2 - x_1)$ in the ring $K[x_1, x_2, x_3]$ using the two methods provided by this proposition.

Following the first method, we compute generators of the syzygy module $\mathrm{Syz}(x_1, x_2, x_1^2 - x_2^2, x_1 x_2 x_3, x_3^2 - x_1)$ and get the set $\{v_1, v_2, v_3, v_4, v_5\}$, where $v_1 = (x_2, -x_1, 0, 0, 0)$, $v_2 = (x_1, -x_2, -1, 0, 0)$, $v_3 = (-x_2, x_3^2, 0, 0, -x_2)$, $v_4 = (x_3^2 - x_1, 0, 0, 0, -x_1)$, and $v_5 = (x_2 x_3, 0, 0, -1, 0)$. Therefore we conclude that $I_1 \cap I_2 = (x_1^2 - x_2^2,\ x_2 x_3^2 - x_1 x_2,\ x_1 x_3^2 - x_1^2,\ x_1 x_2 x_3)$.

Following the second method, we compute a system of generators of the syzygy module of the columns of

$$\mathcal{M} = \begin{pmatrix} 1 & x_1 & x_2 & 0 & 0 & 0 \\ 1 & 0 & 0 & x_1^2 - x_2^2 & x_1 x_2 x_3 & x_3^2 - x_1 \end{pmatrix}$$

The computation yields the set $\{\langle 0, x_2, -x_1, 0, 0, 0\rangle, \langle -x_1^2 + x_2^2, x_1, -x_2, 1, 0, 0\rangle,$ $\langle -x_2 x_3^2 + x_1 x_2, 0, x_3^2 - x_1, 0, 0, x_2\rangle, \langle -x_1 x_3^2 + x_2^2, x_3^2, -x_2, 1, 0, x_1\rangle, \langle -x_1 x_2 x_3,$ $0, x_1 x_3, 0, 1, 0\rangle\}$. We pick the first non-zero coordinates of these vectors and get $I_1 \cap I_2 = (-x_1^2 + x_2^2,\ -x_2 x_3^2 + x_1 x_2,\ -x_1 x_3^2 + x_2^2,\ -x_1 x_2 x_3)$, in agreement with the above result.

Next we use the preceding proposition to solve an important problem. Before, let us introduce a little bit of terminology.

Definition 3.2.5. Let R be a ring, and let $M = \langle m_1, \ldots, m_s \rangle$ be a finitely generated R-module. Suppose that the syzygy module $\mathrm{Syz}(m_1, \ldots, m_s)$ has a finite system of generators $\{v_1, \ldots, v_u\} \subseteq R^s$. Moreover, let $\{e_1, \ldots, e_s\}$ be the canonical basis of R^s and $\{\varepsilon_1, \ldots, \varepsilon_u\}$ the canonical basis of R^u.

   We define an R-linear map $\varphi : R^s \longrightarrow M$ by $\varphi(e_i) = m_i$ for $i = 1, \ldots, s$ and an R-linear map $\psi : R^u \longrightarrow R^s$ by $\psi(\varepsilon_j) = v_j$ for $j = 1, \ldots, u$. Then the sequence

$$R^u \xrightarrow{\ \psi\ } R^s \xrightarrow{\ \varphi\ } M \longrightarrow 0$$

is clearly exact. It is called a **presentation of M via generators and relations**, or simply a **presentation of M**. Equivalently, we shall also call the induced isomorphism $M \cong R^s/\langle v_1, \ldots, v_u \rangle$ a presentation of M. Here the residue classes of the canonical basis vectors of R^s correspond to the generators of M, and the vectors $v_1, \ldots, v_u$ generate the module of relations among those generators.

   Given two submodules M, N of P^r, it is natural to ask for a presentation of $M/(M \cap N)$ via generators and relations. More generally, we have the following result.

Corollary 3.2.6. *Given the situation of Proposition 3.2.3, we define vectors* $w_j = (f_{1j}, \ldots, f_{sj})$ *for* $j = 1, \ldots, u$*. The map* λ *induces a P-linear map* $\overline{\lambda} : P^s \longrightarrow M/(M \cap N)$*. Moreover, let* $\psi : P^u \longrightarrow P^s$ *be the P-linear map which sends* ε_j *to* w_j *for* $j = 1, \ldots, u$*. Then the sequence*

$$P^u \xrightarrow{\ \psi\ } P^s \xrightarrow{\ \overline{\lambda}\ } M/(M \cap N) \longrightarrow 0$$

is a presentation of $M/(M \cap N)$*. In other words, there is an isomorphism of P-modules* $M/(M \cap N) \cong P^s/\langle w_1, \ldots, w_u \rangle$*.*

Proof. Since the image of λ is M, it is clear that $\overline{\lambda}$ is surjective. The kernel of $\overline{\lambda}$ is $\lambda^{-1}(M \cap N) = \lambda^{-1}(N)$. By Lemma 3.2.2, this preimage equals $\langle w_1, \ldots, w_u \rangle = \mathrm{Im}(\psi)$. $\qquad\qquad\square$

   If we need to compute the intersection of a finite number of submodules $M_1, \ldots, M_\ell$ of P^r, we may either proceed recursively or try to intersect all submodules simultaneously.

Proposition 3.2.7. (Computation of Multiple Intersections)
Let $\ell \geq 2$*, and let* $M_1, \ldots, M_\ell \subseteq P^r$ *be P-submodules. For every index* $i \in \{1, \ldots, \ell\}$*, let* $\mathcal{M}_i$ *be a matrix whose column vectors generate* M_i*.*

   a) *We have* $M_1 \cap \cdots \cap M_\ell = (\cdots((M_1 \cap M_2) \cap M_3) \cap \cdots) \cap M_\ell$*. Therefore we can compute* $M_1 \cap \cdots \cap M_\ell$ *by iteratively applying Proposition 3.2.3.*
   b) *Consider the block matrix*

$$\mathcal{M} = \begin{pmatrix} \mathcal{I}_r & \mathcal{M}_1 & 0 & \cdots & 0 \\ \mathcal{I}_r & 0 & \mathcal{M}_2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \mathcal{I}_r & 0 & \cdots & 0 & \mathcal{M}_\ell \end{pmatrix}$$

Let $\{v_1, \ldots, v_u\}$ be a system of generators of the syzygy module $\mathrm{Syz}(\mathcal{M})$, and write $v_j = (f_{1j}, f_{2j}, \ldots)$ with $f_{1j}, f_{2j}, \ldots \in P$ for $j = 1, \ldots, u$. Then we have

$$M_1 \cap \cdots \cap M_\ell = \langle (f_{1j}, \ldots, f_{rj}) \mid 1 \le j \le u \rangle$$

Proof. The proof of the second method follows in the same way as the proof of Proposition 3.2.3.b.   □

Example 3.2.8. Let us compute the intersection of the three prime ideals $\mathfrak{p}_1 = (x, y)$, $\mathfrak{p}_2 = (x^2 - y^3, y^2 - z)$, and $\mathfrak{p}_3 = (x - y^3, y^2 - z)$ in $K[x, y, z]$ using the two methods explained in this proposition.

First, we compute $I = \mathfrak{p}_1 \cap \mathfrak{p}_2$ and get $I = (y^3 - yz, xy^2 - xz, x^2 - yz)$. Then we calculate $I \cap \mathfrak{p}_3$ and get $\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 = (y^3 - yz, xy^2 - xz, x^2 yz - y^2 z^2 - x^3 + xyz)$.

Following the second method, we compute a system of generators of the syzygy module of the columns of

$$\mathcal{M} = \begin{pmatrix} 1 & x & y & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & x^2 - y^3 & y^2 - z & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & x - y^3 & y^2 - z \end{pmatrix}$$

The computation yields a complicated set of generators, from which we extract the first coordinates and get $\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 = (-y^3 + yz, -xy^2 + xz, -x^2 yz + y^2 z^2 + x^3 - xyz, -x^2 y^2 + y^3 z + x^2 z - yz^2, -x^3 y + xy^2 z + x^2 z^2 - yz^3)$. An irredundant subset of generators is $\{-y^3 + yz, -xy^2 + xz, -x^2 yz + y^2 z^2 + x^3 - xyz\}$. Thus we see that we get the same ideal as above.

As an application of the preceding two propositions, we can show how to compute greatest common divisors and least common multiples of polynomials in n indeterminates. We point out that the following corollary provides an algorithm which works over any base field K over which we can compute Gröbner bases. In particular, it does not require factorization of multivariate polynomials.

As in Section 1.2, the expressions $\gcd(f_1, \ldots, f_m)$ resp. $\mathrm{lcm}(f_1, \ldots, f_m)$ shall represent any greatest common divisor resp. least common multiple of a set of polynomials $\{f_1, \ldots, f_m\} \subseteq P$.

Corollary 3.2.9. (Computation of gcd and lcm)
Let $m \ge 2$, let $f_1, \ldots, f_m \in P$, and let σ be a term ordering on $\mathbb{T}^n$.

a) The reduced σ-Gröbner basis of the intersection ideal $(f_1) \cap \cdots \cap (f_m)$ consists of precisely one element, namely the element $\mathrm{lcm}(f_1, \ldots, f_m)$. Thus least common multiples can be computed using Proposition 3.2.7.

b) *A greatest common divisor of two polynomials can be computed via a) and the formula* $\gcd(f_1, f_2) = f_1 f_2 / \operatorname{lcm}(f_1, f_2)$. *A greatest common divisor of more than two polynomials can be computed recursively using the formula* $\gcd(f_1, \ldots, f_m) = \gcd(\gcd(f_1, \ldots, f_{m-1}), f_m)$.

Proof. By Proposition 1.2.8.a, the ideal $I = (f_1) \cap \cdots \cap (f_m)$ is generated by the polynomial $f = \operatorname{lcm}(f_1, \ldots, f_m)$. Since I is a principal ideal, we have $\operatorname{LT}_\sigma(I) = (\operatorname{LT}_\sigma(f))$, and therefore the reduced σ-Gröbner basis of I consists of precisely one polynomial, namely f. This proves a), and b) is an immediate consequence of a) and Proposition 1.2.8.b. $\qquad\square$

3.2.B   Colon Ideals and Annihilators

Now we start to consider the problem of computing colon ideals and annihilators. They are defined as follows.

Definition 3.2.10. Let R be a ring, and let U be an R-module.

a) Given two R-submodules M and N of U, the set

$$N :_R M = \{r \in R \mid r \cdot M \subseteq N\}$$

   is an ideal of R. It is called the **colon ideal** (or the **ideal quotient** if $U = R$) of N by M.

b) Let M be an R-module. The set $\operatorname{Ann}_R(M) = \{r \in R \mid r \cdot M = 0\}$ is an ideal of R. It is called the **annihilator** of M.

Colon ideals and annihilators are essentially the same thing, as our next proposition shows.

Proposition 3.2.11. *Let R be a ring, let U be an R-module, and let M and N be two R-submodules of U. Then*

$$N :_R M = \operatorname{Ann}_R(M/(N \cap M))$$

Proof. The definition yields $\operatorname{Ann}_R(M/(N \cap M)) = \{r \in R \mid r \cdot M \subseteq N \cap M\}$. Since $r \cdot M$ is contained in M for every $r \in R$, we get $\operatorname{Ann}_R(M/(N \cap M)) = \{r \in R \mid r \cdot M \subseteq N\}$, and this proves the claim. $\qquad\square$

Our goal is to compute the above objects effectively when we deal with finitely generated modules over affine algebras. We just saw that computing colon ideals is the same thing as computing annihilators. The next remark says that for our purposes it suffices to compute annihilators of finitely generated P-modules, where $P = K[x_1, \ldots, x_n]$ is the polynomial ring over a field K as usual.

Remark 3.2.12. Let J be an ideal in P, let M be a finitely generated module over the affine K-algebra P/J, and let $\pi : P \longrightarrow P/J$ be the canonical homomorphism. We can view M as a finitely generated P-module via π, i.e. via $f \cdot m = \pi(f)m$ for $f \in P$ and $m \in M$.

Then the annihilator $\operatorname{Ann}_{P/J}(M)$ is the image of the ideal $\operatorname{Ann}_P(M)$ under π, because $\pi(f) \in \operatorname{Ann}_{P/J}(M)$ for some $f \in P$ means $\pi(f) \cdot M = f \cdot M = 0$, i.e. it means $f \in \operatorname{Ann}_P(M)$.

The following lemma solves our problem in the case of a cyclic module M.

Lemma 3.2.13. *Let $M = \langle g \rangle$ and $N = \langle h_1, \ldots, h_t \rangle$ be two P-submodules of P^r, where M is cyclic. Let $\{v_1, \ldots, v_u\} \subseteq P^{t+1}$ be a system of generators of $\operatorname{Syz}(g, h_1, \ldots, h_t)$. We write $v_j = (f_{1j}, \ldots, f_{t+1\,j})$ with $f_{1j}, \ldots, f_{t+1\,j} \in P$ for $j = 1, \ldots, u$. Then*

$$N :_P \langle g \rangle = \operatorname{Ann}_P(M/(N \cap M)) = (f_{11}, \ldots, f_{1u})$$

Proof. It suffices to apply Lemma 3.2.2 to the map $\lambda : P \longrightarrow P^r$ given by $1 \mapsto g$, because we have $N :_P \langle g \rangle = \lambda^{-1}(N)$. $\qquad\square$

Example 3.2.14. Consider the intersection $I = \mathfrak{p}_1 \cap \mathfrak{p}_2$ of the two prime ideals $\mathfrak{p}_1 = (y, z)$ and $\mathfrak{p}_2 = (x - y^2, y^3 - z)$ in the ring $P = K[x, y, z]$. Using Proposition 3.2.3, we find $I = (xy - z, y^3 - z)$. In fact, Corollary 3.1.12 allows us to check that $\{xy - z, y^3 - z\}$ is an irredundant system of generators of I.

Now we want to compute the colon ideal $I :_P (f)$, where f is the polynomial $f = x - y^2$. The lemma tell us that we have to calculate $\operatorname{Syz}(x - y^2, xy - z, y^3 - z)$. The result is the module generated by the two vectors $(-y, 1, 1)$ and $(z - xy, x - y^2, 0)$. Thus we obtain $I :_P (f) = (-y, z - xy) = (y, z) = \mathfrak{p}_1$.

The explanation of this result is simple, and we can prove it directly. For $g \in \mathfrak{p}_1$, we have $fg \in \mathfrak{p}_1$, and also $fg \in \mathfrak{p}_2$, since $f \in \mathfrak{p}_2$. Therefore we have $fg \in I$, and this means that $g \in I :_P (f)$. Conversely, let $fg \in I$. Then $fg \in \mathfrak{p}_1$ and $f \notin \mathfrak{p}_1$ implies $g \in \mathfrak{p}_1$, because $\mathfrak{p}_1$ is a prime ideal.

Proposition 3.2.15. (Computation of Colon Ideals)
Let $M = \langle g_1, \ldots, g_s \rangle$ and $N = \langle h_1, \ldots, h_t \rangle$ be two P-submodules of P^r, and let $\mathcal{H} = (h_1, \ldots, h_t)$.

a) *The colon ideal $N :_P M$ and the annihilator of $M/(N \cap M)$ can be computed using Lemma 3.2.13 and the formula*

$$N :_P M = \operatorname{Ann}_P(M/(N \cap M)) = \bigcap_{i=1}^{s} (N :_P \langle g_i \rangle)$$

b) *Consider the following block matrix of size $rs \times (st + 1)$*

$$\mathcal{M} = \begin{pmatrix} g_1 & \mathcal{H} & 0 & \cdots & 0 \\ g_2 & 0 & \mathcal{H} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ g_s & 0 & \cdots & 0 & \mathcal{H} \end{pmatrix}$$

Let $\{v_1, \ldots, v_u\} \subseteq P^{st+1}$ be a system of generators of the syzygy module $\mathrm{Syz}(\mathcal{M})$. *We write* $v_j = (f_{0j}, f_{1j}^{(1)}, \ldots f_{tj}^{(1)}, \ldots \ldots, f_{1j}^{(s)}, \ldots, f_{tj}^{(s)})$ *with* $f_{0j}, f_{1j}^{(1)}, \ldots, f_{tj}^{(s)} \in P$ *for* $j = 1, \ldots, u$. *Then we have*

$$N :_P M = \mathrm{Ann}_P(M/(N \cap M)) = (f_{01}, \ldots, f_{0u})$$

Proof. Part a) follows directly from the definitions. Therefore we prove claim b). Let $w_0, w_1^{(1)}, \ldots, w_t^{(1)}, \ldots \ldots, w_1^{(s)}, \ldots, w_t^{(s)} \in P^{rs}$ be the column vectors of $\mathcal{M}$. For $j = 1, \ldots, u$ we have $f_{0j}w_0 = -\sum_{k=1}^{s}(\sum_{i=1}^{t} f_{ij}^{(k)} w_i^{(k)})$. For a fixed $\ell \in \{1, \ldots, s\}$, we get $f_{0j}g_\ell = -\sum_{i=1}^{t} f_{ij}^{(\ell)} h_i$ for $j = 1, \ldots, u$. Since this holds for every ℓ between 1 and s, we get $f_{0j} \in N :_P M$ for $j = 1, \ldots, u$.

Conversely, let $a_0 \in N :_P M$ be given. Then there are polynomials $a_{11}, \ldots, a_{st} \in P$ such that $a_0 g_j = \sum_{i=1}^{t} a_{ij} h_i$ for $j = 1, \ldots, s$. By combining these equations into a vector equation, we get

$$a_0 w_0 - (a_{11}w_1^{(1)} + \cdots + a_{t1}w_t^{(1)} + \cdots\cdots + a_{1s}w_1^{(s)} + \cdots + a_{ts}w_t^{(s)}) = 0$$

Therefore there exist polynomials $p_1, \ldots, p_u \in P$ such that the column vector given by $(a_0, -a_{11}, \ldots, -a_{t1}, \ldots\ldots, -a_{1s}, \ldots, -a_{ts})^{\mathrm{tr}}$ is equal to $\sum_{j=1}^{u} p_j v_j$. By considering the first component of this equation, we get $a_0 = \sum_{j=1}^{u} p_j f_{0j}$, and this completes the proof. $\square$

Example 3.2.16. Let $I \subseteq \mathbb{Q}[x_1, x_2, x_3]$ be the ideal which is given by the intersection of the three prime ideals $\mathfrak{p}_1 = (x_1, x_2)$, $\mathfrak{p}_2 = (x_1^2 - x_2^3, x_2 - x_3)$, and $\mathfrak{p}_3 = (x_1 - x_2^2, x_1^2 - x_3)$, and let $J = (x_2 - x_3, x_1^2 - x_3)$.

If we want to compute $I :_P J$ using part a) of the proposition, we have to calculate $I_1 = I :_P (x_2 - x_3)$ via Lemma 3.2.13. The result is the ideal $I_1 = (x_2^2 - x_1, x_1^2 x_2 - x_2 x_3, x_1^3 - x_1 x_3)$. Similarly, we compute the ideal $I_2 = I :_P (x_1^2 - x_3) = (x_2^2 - x_2 x_3, x_1^2 - x_2 x_3, x_1 x_2 - x_1 x_3)$. Finally, we intersect I_1 and I_2 and get $I :_P J = I_1 \cap I_2 = I$.

Again the result can be explained in the following way. We can prove as in Example 3.2.14 that $I :_P (x_2 - x_3) = \mathfrak{p}_1 \cap \mathfrak{p}_3$, and that $I :_P (x_1^2 - x_3) = \mathfrak{p}_1 \cap \mathfrak{p}_2$. Now the conclusion follows from part a) of the proposition again.

3.2.C   Colon Modules

Given two ideals I and J in a ring R, we have seen how to compute the colon ideal $I :_R J$. The colon ideal of one R-module by another was a generalization of this colon ideal operation between ideals. But there is another way to generalize it from ideals to modules, namely the colon module operation.

Definition 3.2.17. Let R be a ring, let I be an ideal in R, let U be an R-module, and let M and N be two R-submodules of U. Then the set $N :_M I = \{m \in M \mid I \cdot m \subseteq N\}$ is an R-submodule of M (and of U). It is called the **colon module** of N by I in M.

The purpose of this subsection is to explain several methods for computing colon modules of finitely generated modules over affine K-algebras. We first reduce the problem to the case of submodules of a finitely generated free P-module, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring as above.

Proposition 3.2.18. *Let J be an ideal in P, let U be a finitely generated module over the K-algebra P/J, and let M and N be two P/J-submodules of U. Furthermore, let I be an ideal in P containing J. Our goal is to compute $N :_M (I/J)$.*
   Suppose we are given a presentation $U \cong P^r/V$ with a P-submodule V of P^r. We can write $M \cong M'/V$ and $N \cong N'/V$ with P-submodules M' and N' of P^r containing V. Then $N :_M (I/J)$ is the residue class module of $N' :_{M'} I$ in U.

Proof. The module $N :_M (I/J)$ is given by $\{\bar{v} \in M'/V \mid (I/J) \cdot \bar{v} \subseteq N'/V\}$. This set is $\{\bar{v} \in M'/V \mid I \cdot v \subseteq N' \text{ for every } v \in M' \text{ with residue class } \bar{v} \in U\}$. Therefore it is the image of $\{v \in M' \mid I \cdot v \subseteq N'\}$ in U. The last set is nothing but $N' :_{M'} I$ which proves the claim.   □

Example 3.2.19. Let R be the K-algebra with K-basis $\{1, \varepsilon\}$, where we have $\varepsilon^2 = 0$, let $N = \langle (1, \varepsilon) \rangle \subseteq R^2$, and let $\bar{I}$ be the ideal $\bar{I} = (\varepsilon)$ in R. Suppose we want to compute $N :_{R^2} \bar{I}$.
   To this end, we first write R in the form $R = P/(x^2)$ with $P = K[x]$. Here ε is the image of x in R, and $\bar{I}$ is the image of the ideal $I = (x)$. Then we notice that $R^2 = P^2/V$ for $V = \langle (x^2, 0), (0, x^2) \rangle$, and that $N = N'/V$ for $N' = \langle (1, x), (x^2, 0), (0, x^2) \rangle$. Thus the desired colon module is the image of $N' :_{P^2} I$ in R^2.

As a consequence of this proposition, we shall now restrict our attention to the case where M and N are P-submodules of P^r and I is an ideal in P. In a manner similar to the last subsection, we begin by explaining the computation of the colon module of a submodule by a principal ideal. We present two methods for doing this calculation, one based on a syzygy module computation, and one based on performing a certain intersection of two submodules.

Lemma 3.2.20. *Let* $M = \langle g_1, \ldots, g_s \rangle$ *and* $N = \langle h_1, \ldots, h_t \rangle$ *be two* P*-submodules of* P^r*, and let* $f \in P \setminus \{0\}$*. Furthermore, let* $\{v_1, \ldots, v_u\} \subseteq P^r$ *be a system of generators of the* P*-module* $fM \cap N$*. For* $i = 1, \ldots, u$*, we may write* $v_i = fw_i$ *for some* $w_i \in M$*. Then we have*

$$N :_M (f) = \langle w_1, \ldots, w_u \rangle$$

In particular, we compute $N :_M (f)$ *as follows. Let* $\{\tilde{v}_1, \ldots, \tilde{v}_\ell\} \subseteq P^{s+t}$ *be a system of generators of the module* $\mathrm{Syz}(fg_1, \ldots, fg_s, h_1, \ldots, h_t)$*. If we write* $\tilde{v}_j = (f_{1j}, \ldots, f_{s+tj})$ *with* $f_{1j}, \ldots, f_{s+tj} \in P$ *for* $j = 1, \ldots, \ell$*, then*

$$N :_M (f) = \langle \sum_{i=1}^{s} f_{ij} g_i \mid 1 \le j \le \ell \rangle$$

Proof. First we observe that $f \cdot w_i = v_i \in fM \cap N \subseteq N$ implies that $w_i \in N :_M (f)$ for $i = 1, \ldots, u$. Conversely, if we start with an element $m \in N :_M (f)$, we have $fm \in fM \cap N$. Thus we can represent fm in the form $fm = \sum_{i=1}^{u} a_i v_i = \sum_{i=1}^{u} a_i f w_i$ with $a_1, \ldots, a_u \in P$. We cancel f and obtain $m = \sum_{i=1}^{u} a_i w_i \in \langle w_1, \ldots, w_u \rangle$, as we wanted to show.

To prove the additional claim, it suffices to apply Proposition 3.2.3.a to compute the intersection $fM \cap N$. $\square$

Example 3.2.21. When we apply the first part of this lemma in the situation of the previous example, we see that we have to compute $xP^2 \cap N' = \langle (x, 0), (0, x) \rangle \cap \langle (1, x), (x^2, 0), (0, x^2) \rangle$. The result is $\langle (x, 0), (0, x^2) \rangle$. Therefore we have $N' :_{P^2} I = \langle (1, 0), (0, x) \rangle$, and the colon module $N :_{R^2} \bar{I}$ we were originally interested in equals $\langle (1, 0), (0, \varepsilon) \rangle$.

For the computation of colon modules in the general case, we have again the choice between reductions to the case of principal ideals and a direct method. As we saw before, it is enough to treat submodules of P^r.

Proposition 3.2.22. (Computation of Colon Modules)
Let $M = \langle g_1, \ldots, g_s \rangle$ *and* $N = \langle h_1, \ldots, h_t \rangle$ *be two* P*-submodules of* P^r*, let* $\mathcal{G} = (g_1, \ldots, g_s)$*, let* $\mathcal{H} = (h_1, \ldots, h_t)$*, and let* $I \subseteq P$ *be an ideal generated by a set of polynomials* $\{f_1, \ldots, f_\ell\}$*.*

a) We may compute $N :_M I$ *by using Lemma 3.2.20 and the formula*

$$N :_M I = \bigcap_{i=1}^{\ell} N :_M (f_i)$$

b) Consider the following block matrix of size $r\ell \times (s + \ell t)$

$$\mathcal{M} = \begin{pmatrix} f_1 \mathcal{G} & \mathcal{H} & 0 & \cdots & 0 \\ f_2 \mathcal{G} & 0 & \mathcal{H} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ f_\ell \mathcal{G} & 0 & \cdots & 0 & \mathcal{H} \end{pmatrix}$$

Let $\{v_1, \ldots, v_u\} \subseteq P^{s+\ell t}$ be a system of generators of the syzygy module $\mathrm{Syz}(\mathcal{M})$. We write $v_j = (f_{1j}, \ldots, f_{sj}, f_{1j}^{(1)}, \ldots f_{tj}^{(1)}, \ldots \ldots, f_{1j}^{(\ell)}, \ldots, f_{tj}^{(\ell)})$ with $f_{1j}, \ldots, f_{tj}^{(\ell)} \in P$ for $j = 1, \ldots, u$. Then we have

$$N :_M I = \langle \sum_{i=1}^{s} f_{ij} g_i \mid j = 1, \ldots, u \rangle$$

Proof. Part a) follows directly from the definitions. Therefore we prove claim b). Let $w_1, \ldots, w_s, w_1^{(1)}, \ldots, w_t^{(1)}, \ldots \ldots, w_1^{(\ell)}, \ldots, w_t^{(\ell)}$ be the column vectors of $\mathcal{M}$. We have $\sum_{i=1}^{s} f_{ij} w_i = -\sum_{m=1}^{\ell} (\sum_{i=1}^{t} f_{ij}^{(m)} w_i^{(m)})$ for every $j = 1, \ldots, u$. If we consider the kth batch of t components of this equation, we see that $f_k(\sum_{i=1}^{s} f_{ij} g_i) = \sum_{i=1}^{t} f_{ij}^{(k)} h_i$ for $j = 1, \ldots, u$ and $k = 1, \ldots, \ell$. Hence we get $\sum_{i=1}^{s} f_{ij} g_i \in N :_M I$ for $j = 1, \ldots, u$.

Conversely, let $v = \sum_{i=1}^{s} a_i g_i \in N :_M I$ with $a_1, \ldots, a_s \in P$. Then there exist polynomials $a_{11}, \ldots, a_{t\ell} \in P$ such that $f_k v = \sum_{i=1}^{t} a_{ik} h_i$ for $k = 1, \ldots, \ell$. By combining these equations into a vector equation, we get

$$a_1 w_1 + \cdots + a_s w_s - (a_{11} w_1^{(1)} + \cdots + a_{t1} w_t^{(1)} + \cdots \cdots + a_{1\ell} w_1^{(\ell)} + \cdots + a_{t\ell} w_t^{(\ell)}) = 0$$

Therefore there exist polynomials $p_1, \ldots, p_u \in P$ such that the column vector given by $(a_1, \ldots, a_s, -a_{11}, \ldots, -a_{t1}, \ldots \ldots, -a_{1\ell}, \ldots, -a_{t\ell})^{\mathrm{tr}}$ is equal to $\sum_{j=1}^{u} p_j v_j$. The first s components of this equality yield the claim. $\qquad\square$

The previous propositions provide us with a way to check whether a given sequence of polynomials is a regular sequence for a given finitely generated P-module. Regular sequences are defined as follows.

Definition 3.2.23. Let R be a ring and U an R-module.
a) An element $f \in R$ is called a **non-zerodivisor** for U if $f \cdot m = 0$ implies $m = 0$ for all $m \in U$.
b) A sequence of elements $f_1, \ldots, f_\ell \in R$ is called a **regular sequence** for U or an U**-regular sequence** if we have $(f_1, \ldots, f_\ell)U \neq U$ and if f_i is a non-zerodivisor for $U/(f_1, \ldots, f_{i-1})U$ for $i = 1, \ldots, \ell$.

The definition of a non-zerodivisor for U obviously generalizes the one given for $U = R$ in Section 1.1. If the ring R in this definition is our polynomial ring P, two polynomials $f, g \in P \setminus \{0\}$ form a P-regular sequence if and only if they are coprime. For three polynomials in P, the question whether they form a P-regular sequence may depend on their order (see Tutorial 33.b).

Now let U be a finitely generated P-module. In order to check whether a given sequence of polynomials is a regular sequence for U, we can choose a presentation $U \cong P^r/N$ and apply the following corollary.

Corollary 3.2.24. (Regular Sequence Test)
Let $M = \langle g_1, \ldots, g_s \rangle$ be a P-submodule of P^r, let N be a P-submodule of M, and let $f_1, \ldots, f_\ell \in P$. For $j = 0, \ldots, \ell$, we define $N_j = (f_1, \ldots, f_j)M + N$. Then the following conditions are equivalent.

a) *The sequence $f_1, \ldots, f_\ell$ is a regular sequence for M/N.*
b) *There exists an index $i \in \{1, \ldots, s\}$ such that $g_i \notin N_\ell$, and we have $N_{j-1} :_M (f_j) \subseteq N_{j-1}$ for $j = 1, \ldots, \ell$.*
c) *Let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. For $j = 1, \ldots, \ell$, we let $\{h_{j1}, \ldots, h_{ju_j}\}$ be a system of generators of $N_{j-1} :_M (f_j)$. Then there exists an index $i \in \{1, \ldots, s\}$ such that $\mathrm{NF}_{\sigma, N_\ell}(g_i) \neq 0$, and we have $\mathrm{NF}_{\sigma, N_{j-1}}(h_{j1}) = \cdots = \mathrm{NF}_{\sigma, N_{j-1}}(h_{ju_j}) = 0$ for $j = 1, \ldots, \ell$.*

Proof. The equivalence of a) and b) is an immediate consequence of the definition if we use $U = M/N$ and observe that $(f_1, \ldots, f_j)U = N_j/N$ and $U/(f_1, \ldots, f_j)U = M/N_j$. The equivalence of b) and c) follows from the Submodule Membership Test 2.4.10. $\qquad\square$

The following example gives a non-trivial case of three polynomials $f_1, f_2, f_3 \in P$ which do not form a regular sequence.

Example 3.2.25. In the ring $P = K[x_1, x_2, x_3, x_4]$, consider $f_1 = x_2 x_4 - x_3^2$, $f_2 = x_1 x_4 - x_2 x_3$, and $f_3 = x_1 x_3 - x_2^2$. We want to use the corollary to check whether f_1, f_2, f_3 is a regular sequence for P.

The ideal (f_1, f_2, f_3) is proper, so only the conditions on the colon ideals have to be checked. Clearly, any two of the three polynomials are coprime, and thus form a regular sequence. The computation of $(f_1, f_2) :_P (f_3)$ yields (x_3, x_4). Neither of the two elements x_3, x_4 is contained in (f_1, f_2). Therefore f_1, f_2, f_3 is not a regular sequence for P.

Exercise 1. In this exercise we anticipate a theme which will be discussed more thoroughly in Chapter IV. Let K be a field, let $P = K[x_1]$, and let $f, g \in P \setminus \{0\}$. In $\overline{P} = K[x_0, x_1]$, we consider the **homogenizations** $F = x_0^{\deg(f)} \cdot f(\frac{x_1}{x_0})$ and $G = x_0^{\deg(g)} \cdot g(\frac{x_1}{x_0})$. Show that

$$\gcd(f, g) = \gcd(F, G)|_{x_0 = 1}$$

Deduce an algorithm which finds $\gcd(f, g)$ by computing the elements of degree $\leq \deg(f) + \deg(g)$ of a Gröbner basis of the ideal (F, G).
Hint: First show that x_0 does not divide the homogenization of any polynomial and that the homogenization of a product is the product of the homogenizations.

Exercise 2. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let σ be a term ordering on $\mathbb{T}^n$, and let $f, g \in P$ be such that $\mathrm{LT}_\sigma(f)$ and $\mathrm{LT}_\sigma(g)$ are coprime. Show that f and g are coprime.

Exercise 3. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and let $r \geq 3$. Find r non-zero submodules $M_1, \ldots, M_r$ of P^r such that $M_i \cap M_j \neq 0$ for $1 \leq i < j \leq s$ and $\cap_{i=1}^r M_i = 0$.

Exercise 4. Let R be a ring, and let M, N, as well as U be three R-submodules of a given R-module. Assume that $M \supseteq N$ or $M \supseteq U$. Then prove the **modular law**

$$M \cap (N + U) = M \cap N + M \cap U$$

Exercise 5. Let R be a ring, let $\mathfrak{a}$, I, and J be ideals of R, and let S be the residue class ring $S = R/\mathfrak{a}$. Denote by $\bar{I}$ and $\bar{J}$ the ideals of S generated by the images of I and J, respectively. Prove that

$$\bar{I} \cap \bar{J} = ((I + \mathfrak{a}) \cap (J + \mathfrak{a}))/\mathfrak{a}$$

Exercise 6. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and let $M = \langle g_1, \ldots, g_s \rangle$ and $N = \langle h_1, \ldots, h_t \rangle$ be two P-submodules of P^r. Prove that the following conditions are equivalent.

a) $N \subseteq M$

b) There exists a matrix $\mathcal{A} = \binom{\mathcal{B}}{\mathcal{I}_t}$ over P, where $\mathcal{B}$ is of size $s \times t$ and $\mathcal{I}_t$ is the identity matrix of size $t \times t$, such that the columns of $\mathcal{A}$ are contained in the module $\mathrm{Syz}(g_1, \ldots, g_s, h_1, \ldots, h_t)$.

Exercise 7. Let R be a ring, and let $I, J, I_1, I_2, \ldots, I_n$ be ideals in R. Prove the following rules for colon ideals.

a) $(I :_R J) \cdot J \subseteq I$

b) $(I_1 :_R I_2) :_R I_3 = (I_1 :_R I_3) :_R I_2$

c) $(I_1 :_R I_2) :_R I_3 = I_1 :_R (I_2 I_3)$

d) $(I_1 \cap \cdots \cap I_n) :_R J = (I_1 :_R J) \cap \cdots \cap (I_n :_R J)$

e) $I :_R (I_1 + \cdots + I_n) = (I :_R I_1) \cap \cdots \cap (I :_R I_n)$

Exercise 8. Let $\mathfrak{p}$ and $\mathfrak{q}$ be prime ideals in a ring R such that $\mathfrak{q}$ is not contained in $\mathfrak{p}$. Show that $(\mathfrak{p} \cap \mathfrak{q}) :_R \mathfrak{q} = \mathfrak{p}$.

Exercise 9. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and let $a, b, c, d \in P \setminus \{0\}$. Prove that the following conditions are equivalent.

a) $\langle (a, b) \rangle :_P \langle (c, d) \rangle \neq 0$

b) $ad = bc$

Exercise 10. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $r \geq 1$, and let M be a P-submodule of P^r with a system of generators of the form $\{fg_1, \ldots, fg_s\}$, where $f \in P$ and $g_1, \ldots, g_s \in P^r \setminus \{0\}$.

a) Show that $M :_{P^r} (f) = \langle g_1, \ldots, g_s \rangle$.

b) Now let $r = 1$ and $g_i' = g_i/\gcd(g_1, \ldots, g_s)$ for $i = 1, \ldots, s$. Prove that $(g_1, \ldots, g_s) :_P (\gcd(g_1, \ldots, g_s)) = (g_1', \ldots, g_s')$.

Exercise 11. Triples of integers $(a, b, c) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ satisfying the equation $a^2 + b^2 = c^2$ are called **Pythagorean triples**. A Pythagorean triple (a, b, c) is called **fundamental** if $\gcd(a, b, c) = 1$. A Pythagorean triple (a, b, c) is called **positive** if $(a, b, c) \in \mathbb{N}^3 \setminus \{(0, 0, 0)\}$.

a) Prove that fundamental Pythagorean triples are in 1–1 correspondence with rational points on the circle $C = \mathcal{Z}(x^2 + y^2 - 1) \subseteq \overline{\mathbb{Q}}^2$, i.e. with points $(a, b) \in \mathbb{Q}^2$ such that $a^2 + b^2 - 1 = 0$.

b) Find a point on C which does not correspond to a Pythagorean triple.

Let $\ell \in \mathbb{Q}[x, y]$ be a linear polynomial defining a line $L = \mathcal{Z}(\ell) \subseteq \overline{\mathbb{Q}}^2$ through the point $P = (0, 1)$.

c) Prove that L intersects C in precisely one other point P', unless ℓ is a multiple of $y - 1$.

d) Show that P' is a rational point of C and that its vanishing ideal is the colon ideal $(x^2 + y^2 - 1, \ell) :_{\mathbb{Q}[x,y]} (x, y-1) = (x^2 + y^2 - 1, \ell) :_{\mathbb{Q}[x,y]} (y-1)$.

e) Write a CoCoA function `Pythagoras(...)` which computes a specified number of fundamental positive Pythagorean triples in the following way.

1) Choose random numbers $a, b \in \mathbb{Q} \setminus \{0\}$ and let $\ell = ax + b(y - 1)$.
2) Compute the vanishing ideal $\mathcal{I}(P')$.
3) Determine the monic generators $x - p$ and $y - q$ of $\mathcal{I}(P')$.
4) Find the corresponding fundamental positive Pythagorean triple.

Tutorial 30: Computation of Intersections

The purpose of this tutorial is to implement and study the algorithms for computing intersections of submodules of P^r introduced in the first subsection. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $r \geq 1$, let $\ell \geq 2$, and let $M_1, \ldots, M_\ell \subseteq P^r$ be P-submodules given by sets of vectors which generate them.

a) Write CoCoA functions `Intersect1(...)` and `Intersect2(...)` which compute the intersection module $M_1 \cap M_2$ using the methods of Proposition 3.2.3.a and 3.2.3.b, respectively.

b) Apply your functions `Intersect1(...)` and `Intersect2(...)` to compute the intersections of the following ideals and modules.

1) $M_1 = (x^2 y^2 - x^2)$ and $M_2 = (x^2 y + xy^2)$ in $\mathbb{Q}[x, y]$
2) $M_1 = (x^3 + y^2 - 1, xy - x + 3)$ and $M_2 = (xy^2 - 1)$ in $\mathbb{Q}[x, y]$
3) $M_1 = \langle (x, y - z), (z, y) \rangle$ and $M_2 = \langle (z, y+1), (x, y-1) \rangle$ in $\mathbb{Q}[x, y, z]^2$
4) $M_1 = \langle (xy, y, x), (y^2, y, x), (x, -y, -y) \rangle$ and $M_2 = \langle (0, x - y, x - y), (x, x, x), (0, 0, x^2 + x + y^2 - y - 2xy), (0, x^2 + x, x^2 + x) \rangle$ in $\mathbb{Q}[x, y]^3$

c) Write CoCoA functions `MultiIntersect1(...)` and `MultiIntersect2(...)` which compute the intersection module $M_1 \cap \cdots \cap M_\ell$ using the methods of Proposition 3.2.7.a and 3.2.7.b, respectively.

d) Apply your functions `MultiIntersect1(...)` and `MultiIntersect2(...)` to compute the intersections of the ideals and modules given in b) and the following additional ideals and modules.

1) $M_3 = (x^2 y - xy^2)$
2) $M_3 = (x, y)$ and $M_4 = (x - y^2 + 2)$

3) $M_3 = \langle(x,y),(0,y^2-1)\rangle$ and $M_4 = \langle(xyz,0)\rangle$
4) $M_3 = \langle(xy,0,0),(x^2,0,0),(y^2,0,0)\rangle$

e) Let $r = 1$. Prove that if we compute a Gröbner basis of $\mathrm{Syz}(\mathcal{M})$ with respect to a module term ordering of type `PosTo` in Proposition 3.2.3.b, then the resulting system of generators $\{f_{11},\ldots,f_{1u}\}$ of the intersection ideal $M_1 \cap M_2$ is a Gröbner basis with respect to the term ordering `To`.

f) Find an example which shows that the claim of e) is not true if we use a module term ordering of type `ToPos`.

g) Let $R = P/I$ be an affine K-algebra, where I is an ideal in P, and let $N_1,\ldots,N_\ell$ be R-submodules of R^r/U, where U is an R-submodule of R^r. Suppose we are given lists of vectors in P^r representing systems of generators of $N_1,\ldots,N_\ell$. Explain how one can compute a list of vectors in P^r whose residue classes generate $N_1 \cap \cdots \cap N_\ell$.

Tutorial 31: Computation of Colon Ideals and Colon Modules

In the second and third subsection we saw a number of different ways to compute colon ideals and colon modules. In this tutorial we want to implement those methods and compare their efficiency. We shall also see some useful properties of colon ideals and study the associated primes of a module.

Let K be a field, let $P = K[x_1,\ldots,x_n]$, let $f \in P$, let $r \geq 1$, and let $M = \langle g_1,\ldots,g_s\rangle$ and $N = \langle h_1,\ldots,h_t\rangle$ be two P-submodules of P^r.

a) Show that $N :_P M = P$ if and only if $M \subseteq N$.

b) For $r = 1$, show that $N :_P M \supseteq N$. Find ideals $N \subset M \subset P$ such that $N :_P M = N$.

c) Using the two methods of Proposition 3.2.15, write two CoCoA functions `ColonI1(...)` and `ColonI2(...)` which take the tuples $\mathcal{G} = (g_1,\ldots,g_s)$ and $\mathcal{H} = (h_1,\ldots,h_t)$ and compute the colon ideal $N :_P M$.

d) Apply your functions `ColonI1(...)` and `ColonI2(...)` in the following cases.

1) $M = (x^4, x^3z, x^2z^2, xz^3, z^4)$ and $N = (x^4z^4, x^3yz^3, x^2y^2z^2, xy^3z, y^4)$ in $P = \mathbb{Q}[x,y,z]$
2) $M = (x-1, y-1, z-1)^5$ and $N = (x+y+z-3)^3$ in $P = \mathbb{Q}[x,y,z]$
3) $M = (x-1, y-1, z-1)^2 \cap (x,y,z)$ and $N = (x,y,z)$ in $P = \mathbb{Q}[x,y,z]$
4) $M = \langle(x,y),(y,x)\rangle$ and $N = \langle(x^2,y^2)\rangle$ in $P^2 = \mathbb{Q}[x,y]^2$

Which function tends to be faster?

In what follows, we let R be a Noetherian ring and U a non-zero finitely generated R-module. A prime ideal of R is called an **associated prime** of U if it is the annihilator of a cyclic R-submodule of U.

e) Show that there always exists an associated prime of U.
   Hint: Prove that the set of ideals $\{\mathrm{Ann}_R(u) \mid u \in U\setminus\{0\}\}$ has a maximal element with respect to inclusion and that this maximal element is a prime ideal.

f) Prove that the union of the associated primes of U is precisely the set of zerodivisors for this module.

g) Prove that there are only finitely many associated primes of U.
   Hint: First show that there exists a chain of R-submodules $0 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_\ell = U$ such that $U_i/U_{i-1} \cong R/\mathfrak{p}_i$ with a prime ideal $\mathfrak{p}_i \subseteq R$ for $i = 1, \ldots, \ell$. Then prove that the associated primes of U are contained in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell\}$.

h) In the following cases, try to use your function $\mathtt{ColonI1}(\ldots)$ to find an associated prime $\mathfrak{p}$ of the P-module P^r/M and an element $v \in P^r/M$ such that $\mathfrak{p} = \mathrm{Ann}_P(v)$. Can you find all associated primes in each case?

   1) $M = (x^3 + 3x^2y + y^2 + y, y^2 + 2x + y)$ in $P = \mathbb{Q}[x, y]$
   2) $M = \langle(y^2 - 2y + 1, z^2), (xz, yz - z)\rangle$ in $P^2 = \mathbb{Q}[x, y, z]^2$

i) Implement the different methods for computing $N :_M (I)$, where I is an ideal in P, which derive from Proposition 3.2.22 and Proposition 3.2.7.a in three CoCoA functions $\mathtt{ColonM1}(\ldots)$ and $\mathtt{ColonM2}(\ldots)$ and $\mathtt{ColonM3}(\ldots)$. Apply your functions in the following cases. Which function tends to be faster?

   1) $P = \mathbb{Q}[x, y, z]$, $N = \langle(x, y), (y, xy)\rangle$, $M = \langle(xy, yz)\rangle$, $I = (x^2, y^2)$.
      Hint: The result is $\langle(x^3y - xy^3, x^2yz - y^3z)\rangle$.
   2) $P = \mathbb{Q}[x, y, z]$, $N = \langle(x^2, xy, y^2), (y^2, yz, z^2)\rangle$, $M = \langle(x, 0, 0), (y, 0, 0)\rangle$, $I = (x, y, z)$.
   3) $P = \mathbb{Q}[x, y, z]$, $N = \langle(x^2, xy, y^2), (y^2, yz, z^2), (x^2, xz, z^2)\rangle$, $M = \langle(x, 0, 0), (0, y, 0), (0, 0, z)\rangle$, $I = (x, y, z)$.

3.3 Homomorphisms of Modules

> *The four seasons are salt, pepper, mustard, and vinegar.*
> (from "Kids Say the Darndest Things")

In this section we dish up two courses: our first subsection gives a brief outline of *computational linear algebra*, and the second makes an initial step into the realm of *computational homological algebra*. As in the previous section, our recipe will be to reduce all computational tasks to calculations of syzygy modules.

For starters, we treat the standard fare of linear algebra. We consider the problem of computing presentations for the kernels and images of linear maps between modules (see Proposition 3.3.1). Then we add a little spice by discussing liftings along linear maps (see Proposition 3.3.6). This topic gives us a foretaste of more advanced applications such as pullbacks (see also Tutorial 32), inductive and projective limits, and maps between complexes.

In the second part of this section we try to cook up a recipe for calculating Hom-modules. More precisely, we observe that the set of homomorphisms between two finitely generated modules carries a natural module structure itself, and we aim to find a presentation of this module. We need a number of refined ingredients, each of which merits careful sampling: flattening isomorphisms (see Proposition 3.3.9), explicit descriptions of the functoriality of the covariant and the contravariant Hom-functors (see Proposition 3.3.13), and some exactness properties of those Hom-functors (see Proposition 3.3.14).

Finally, we can serve up the resulting algorithm for computing a presentation of a Hom-module (see Theorem 3.3.15) which reduces this task to the calculation of the kernel of a linear map. This second part of the section is more difficult to digest, not so much because the matter is deeper, but rather because the complexity of the objects makes the reading more challenging. Although it is peppered by healthy tidbits of knowledge for your further mathematical life, there is no great harm in skipping it at first reading, since in the rest of this volume we do not make further use of it.

As usual, in order to perform effective computations we have to assume certain finiteness conditions. As in preceding sections, it turns out that the appropriate generality we can deal with is the theory of finitely generated modules over affine K-algebras over a field K. However, we still have a choice as to how to represent such modules. We could consider only submodules of finitely generated free modules over a polynomial ring $P = K[x_1, \ldots, x_n]$. Or we could consider modules given by subquotients, i.e. by residue class modules of submodules of finitely generated free modules over P, and so on.

The best choice, in our opinion, is to present the theory for quotients of finitely generated free modules over P, i.e. for modules of the form P^r/M, where M is a P-submodule of P^r. The reason goes back to Corollary 3.2.6 where we saw how to find such a presentation for an arbitrary subquotient. In Remark 3.3.3 we give hints on how to deal with some other situations.

For the remainder of this section, we let K be a field, $P = K[x_1, \ldots, x_n]$ a polynomial ring over K, and $R = P/I$ an affine K-algebra. Given two finitely generated R-modules, we write them as P^r/M and P^s/N, where $r, s > 0$ and $M \subseteq P^r$ as well as $N \subseteq P^s$ are P-submodules. In this section, to avoid overburdening the notation, we denote the canonical basis of P^a by $\{e_1, \ldots, e_a\}$.

3.3.A   Kernels, Images, and Liftings of Linear Maps

Our first goal is to show how one can compute presentations of the kernel and the image of a P-linear map $\varphi : P^r/M \longrightarrow P^s/N$. To this end, we write

$$\varphi(e_j + M) = w_j + N$$

where $w_j = (f_{1j}, \ldots, f_{sj})$ and $f_{ij} \in P$ for $i = 1, \ldots, s$ and $j = 1, \ldots, r$. Furthermore, let $\{g_1, \ldots, g_\alpha\}$ be a system of generators of M, and let $\{h_1, \ldots, h_\beta\}$ be a system of generators of N.

Proposition 3.3.1. (Kernels and Images of Linear Maps)
Let $\varphi : P^r/M \longrightarrow P^s/N$ be a P-linear map as above, and let $\{v_1, \ldots, v_u\}$ be a system of generators of the syzygy module $\mathrm{Syz}(w_1, \ldots, w_r, h_1, \ldots, h_\beta)$. For $j = 1, \ldots, u$, we write those syzygies as $v_j = (k_{1j}, \ldots, k_{r+\beta\, j})$ with $k_{1j}, \ldots, k_{r+\beta\, j} \in P$.

a) The kernel of φ is given by $\mathrm{Ker}(\varphi) = \langle (k_{1j}, \ldots, k_{rj}) + M \mid j = 1, \ldots, u \rangle$.

b) A presentation of the image of φ is given by the exact sequence

$$P^u \xrightarrow{\ \psi\ } P^r \xrightarrow{\ \varphi \circ \pi\ } \mathrm{Im}(\varphi) \longrightarrow 0$$

  where ψ is defined by $\psi(e_j) = (k_{1j}, \ldots, k_{rj})$ for $j = 1, \ldots, u$, and where $\pi : P^r \longrightarrow P^r/M$ is the canonical homomorphism.

c) Let $\{(\ell_{1j}, \ldots, \ell_{u+\alpha\, j}) \mid j = 1, \ldots, u'\}$ be a system of generators of the module $\mathrm{Syz}(\psi(e_1), \ldots, \psi(e_u), g_1, \ldots, g_\alpha)$, where $\ell_{1j}, \ldots, \ell_{u+\alpha\, j} \in P$ for $j = 1, \ldots, u'$. Then a presentation of the kernel of φ is given by the exact sequence

$$P^{u'} \xrightarrow{\ \psi'\ } P^u \xrightarrow{\ \pi \circ \psi\ } \mathrm{Ker}(\varphi) \longrightarrow 0$$

  where ψ' is defined by $\psi'(e_j) = (\ell_{1j}, \ldots, \ell_{uj})$ for $j = 1, \ldots, u'$.

Proof. To prove a), we note that φ is induced by the map $\lambda : P^r \longrightarrow P^s$ which is given by $\lambda(e_j) = w_j$ for $j = 1, \ldots, r$. Thus $\mathrm{Ker}(\varphi)$ is the image of $\lambda^{-1}(N)$ in P^r/M, and the claim follows from Lemma 3.2.2.

The same result yields claim b), because $\mathrm{Ker}(\varphi \circ \pi) = \lambda^{-1}(N)$, as we can see from the commutative diagram

$$
\begin{array}{ccc}
P^r & \xrightarrow{\ \lambda\ } & P^s \\
\downarrow{\scriptstyle \pi} & & \downarrow \\
P^r/M & \xrightarrow{\ \varphi\ } & P^s/N
\end{array}
$$

Finally, we note that claim a) says that $\mathrm{Ker}(\varphi)$ is the image of the map $\pi \circ \psi : P^u \longrightarrow P^r/M$. Then claim c) follows by applying b) to this map. $\square$

Let us illustrate the results of this proposition with a concrete example.

Example 3.3.2. Consider the ring $P = \mathbb{Q}[x, y]$ and the two P-submodules $M = \langle (x, -y-1, 0) \rangle$ of P^3 and $N = \langle (x^2, 0), (0, x^3), (y, 0), (0, y) \rangle$ of P^2. The P-linear map $\varphi' : P^3 \longrightarrow P^2/N$ defined by $\varphi'(e_1) = (xy, y+1) + N$, $\varphi'(e_2) = (x^2, x) + N$, and $\varphi'(e_3) = (y, 1) + N$ vanishes on M, because $\varphi'(x, -y-1, 0) = x(xy, y+1) - (y+1)(x^2, x) + N = (-x^2, 0) + N = 0 + N$. Hence φ' induces a P-linear map $\varphi : P^3/M \longrightarrow P^2/N$.

In order to find the kernel of φ, we have to compute the syzygy module $\mathrm{Syz}((xy, y+1),\ (x^2, x),\ (y, 1),\ (x^2, 0),\ (0, x^3),\ (y, 0),\ (0, y))$. We get the system of generators $\{(0, 0, -y, 0, 0, y, 1),\ (1, 0, -1, 0, 0, -x+1, -1),$ $(0, 1, -x, -1, 0, x, 0),\ (x, -y, -x, 0, 0, x, 0),\ (0, 0, -x^3, 0, 1, x^3, 0)\}$. Therefore $\mathrm{Ker}(\varphi)$ is generated by $\{(0, 0, -y) + M,\ (1, 0, -1) + M,\ (0, 1, -x) + M,$ $(x, -y, -x) + M,\ (0, 0, -x^3) + M\}$, and $\mathrm{Im}(\varphi)$ has a presentation of the form $P^5 \longrightarrow P^3 \longrightarrow \mathrm{Im}(\varphi) \longrightarrow 0$.

To get a presentation of $\mathrm{Ker}(\varphi)$, we have to compute the syzygy module $\mathrm{Syz}((0, 0, -y),\ (1, 0, -1),\ (0, 1, -x), (x, -y, -x),\ (0, 0, -x^3),\ (x, -y-1, 0))$. We get the system of generators $\{(0, 0, -1, 1, 0, -1),\ (-x, -x, y, 1, 0, 0),$ $(0, x^3, -x^2 y, -x^2, y, 0)\}$. Notice that the second generator means that our system of generators of $\mathrm{Ker}(\varphi)$ can be shortened. By part c) of the proposition, $\mathrm{Ker}(\varphi)$ has a presentation of the form $P^3 \xrightarrow{\psi'} P^5 \longrightarrow \mathrm{Ker}(\varphi) \longrightarrow 0$, where $\psi'(e_1) = (0, 0, -1, 1, 0)$, $\psi'(e_2) = (-x, -x, y, 1, 0)$, and $\psi'(e_3) = (0, x^3, -x^2 y, -x^2, y)$.

The proposition above is often applied in slightly modified ways to compute various operations involving homomorphisms of modules. Here we mention just two of them and leave it to the imagination of the reader to find more.

Remark 3.3.3. Let $\varphi : P^r/M \longrightarrow P^s/N$ be a P-linear map as above, and let $U \subseteq P^s$ be a further P-submodule which contains N and is generated by vectors $\{u_1, \ldots, u_\gamma\} \subseteq P^s$.

a) A presentation of the preimage $\varphi^{-1}(U/N)$ of U/N under the homomorphism φ can be computed by applying Proposition 3.3.1.c to find a presentation of the kernel of the composite map $P^r/M \xrightarrow{\varphi} P^s/N \twoheadrightarrow P^s/U$, where the second homomorphism is the canonical homomorphism.

b) Suppose we want to find the kernel of a P-linear map $\varphi : U \longrightarrow P^s/N$, where $U = \langle u_1, \ldots, u_r \rangle$ is an explicitly given P-submodule of a finitely generated free P-module. We can compute the kernel of the P-linear map $\psi : P^r \longrightarrow P^s/N$ defined by $\psi(e_i) = \varphi(u_i)$ for $i = 1, \ldots, r$. Then $\mathrm{Ker}(\varphi)$ is the image of $\mathrm{Ker}(\psi)$ under the canonical map $P^r \twoheadrightarrow U$.

Besides being able to compute presentations of the kernel and the image of a linear map, we need one more ingredient which enables us to treat most linear algebra questions about finitely generated modules: we need to be able to lift a map from a free P-module to an arbitrary finitely generated module along a homomorphism to that module. More generally, liftings along linear maps are defined as follows.

Definition 3.3.4. Let R be a ring, let U, V, and W be R-modules, let $\mu : V \longrightarrow W$ be an R-linear map, and let $\psi : U \longrightarrow W$ be another R-linear map which satisfies $\mathrm{Im}(\psi) \subseteq \mathrm{Im}(\mu)$. Then a **lifting of ψ along μ** is an R-linear map $\lambda : U \longrightarrow V$ such that $\psi = \mu \circ \lambda$.

In other words, the map λ is a lifting of ψ along μ if it makes the following diagram commutative.

$$
\begin{array}{ccc}
 & & U \\
 & {}^{\lambda}\swarrow & \downarrow{\scriptstyle\psi} \\
V & \xrightarrow{\ \mu\ } & W
\end{array}
$$

Proposition 3.3.5. (Existence of a Lifting Along a Linear Map)
Let R be a ring, let $t \geq 1$, let V and W be R-modules, let $\mu : V \longrightarrow W$ be an R-linear map, and let $\psi : R^t \longrightarrow W$ be another R-linear map which satisfies $\mathrm{Im}(\psi) \subseteq \mathrm{Im}(\mu)$. Then there exists a lifting of ψ along μ.

Proof. Let $\{e_1, \ldots, e_t\}$ be the canonical basis of R^t, and let $w_i = \psi(e_i)$ for $i = 1, \ldots, t$. The assumption that $\mathrm{Im}(\psi) \subseteq \mathrm{Im}(\mu)$ implies that there exist $v_1, \ldots, v_t \in V$ such that $\mu(v_i) = w_i$ for $i = 1, \ldots, t$. Then it suffices to define the R-linear map $\lambda : R^t \longrightarrow V$ by $\lambda(e_i) = v_i$ for $i = 1, \ldots, t$. $\qquad\square$

In the case of a linear map $\varphi : P^r/M \longrightarrow P^s/N$ as above, we can compute a lifting along φ explicitly. The main ingredient to solve this task is our method to deal with explicit membership, as explained in Corollary 3.1.9.a.

Proposition 3.3.6. (Computation of a Lifting Along a Linear Map)
Let $\varphi : P^r/M \longrightarrow P^s/N$ be a P-linear map as above and $\psi : P^t \longrightarrow P^s/N$ another P-linear map which satisfies $\mathrm{Im}(\psi) \subseteq \mathrm{Im}(\varphi)$. Let ψ be given by $\psi(e_i) = p_i + N$ for $i = 1, \ldots, t$, where $p_1, \ldots, p_t \in P^s$.

Using Explicit Membership 3.1.9.a, we can compute a matrix $\mathcal{B} = (b_{ij})$ of polynomials such that $(p_1, \ldots, p_t) = (w_1, \ldots, w_r, h_1, \ldots, h_\beta) \cdot \mathcal{B}$. Then the P-linear map $\lambda : P^t \longrightarrow P^r/M$ defined by $e_j \longmapsto b_{1j} e_1 + \cdots + b_{rj} e_r + M$ for $j = 1, \ldots, t$ is a lifting of ψ along φ.

Proof. First of all, the assumption $\mathrm{Im}(\psi) \subseteq \mathrm{Im}(\varphi)$ implies $p_i \in \langle w_1, \ldots, w_r, h_1, \ldots, h_\beta \rangle$. Therefore we can use Corollary 3.1.9.a and get a matrix $\mathcal{B}$ with

the required property. Since we know that $\psi(e_j) = p_j + N$ for $j = 1, \ldots, t$, we can check that

$$(\varphi \circ \lambda)(e_j) = \varphi(b_{1j}e_1 + \cdots + b_{rj}e_r + M) = b_{1j}w_1 + \cdots + b_{rj}w_r + N = p_j + N$$

for $j = 1, \ldots, t$. Thus we see that $\psi = \varphi \circ \lambda$, as was claimed.   □

Let us do an explicit computation of a lifting using the map introduced in Example 3.3.2.

Example 3.3.7. Consider the map $\varphi : P^3/M \longrightarrow P^2/N$ defined in Example 3.3.2, and let $\psi : P \longrightarrow P^2/N$ be the P-linear map defined by $\psi(1) = (x^3 + y^2, 2x^2) + N$. This map satisfies $\operatorname{Im}(\psi) \subseteq \operatorname{Im}(\varphi)$, because we can use Explicit Membership 3.1.9.a to find a representation $(x^3 + y^2, 2x^2) = x(x^2, x) + (x^2 + y)(y, 1) - x^2(y, 0) - (0, y)$.

In particular, we see that $\psi(1) + N = x\varphi(e_2) + (x^2 + y)\varphi(e_3) + N$. Hence the map $\lambda : P \longrightarrow P^3/M$ defined by $\lambda(1) = (0, x, x^2 + y) + M$ is a lifting of ψ along φ.

3.3.B   Hom-Modules

<div align="right">

Pesto a-a zeneise.
(Genueser Delikatesse)

</div>

After having computed the most important objects associated to one module homomorphism, we now want to describe $\operatorname{Hom}_P(P^r/M, P^s/N)$, the module of *all* P-linear maps $\varphi : P^r/M \longrightarrow P^s/N$. Recall that for two such homomorphisms φ and ψ, and for $f \in P$, the module structure of $\operatorname{Hom}_P(P^r/M, P^s/N)$ is given by

$$(\varphi + \psi)(v + M) = \varphi(v + M) + \psi(v + M) \quad \text{and} \quad (f \cdot \varphi)(v + M) = f \cdot \varphi(v + M)$$

for all $v \in P^r$. Our goal is to describe $\operatorname{Hom}_P(P^r/M, P^s/N)$ by generators and relations, i.e. to compute an explicit presentation.

As a first step, we treat the easiest case $M = \langle 0 \rangle$ and $N = \langle 0 \rangle$. In this situation, there is clearly an isomorphism $\operatorname{Hom}_P(P^r, P^s) \longrightarrow P^{rs}$, and our only task is to make it explicit. Given $r, s > 0$, we denote by $\operatorname{Mat}_{s,r}(P)$ the set of matrices with s rows, r columns, and entries in P. Using componentwise sum and multiplication by a polynomial, $\operatorname{Mat}_{s,r}(P)$ has a natural P-module structure. The next definition recalls the well-known way to associate a matrix to a linear map and provides the other ingredient for solving the first step.

Definition 3.3.8. Let r and s be positive integers.

a) Given a P-module homomorphism $\varphi \in \mathrm{Hom}_P(P^r, P^s)$, let $\varphi(e_j) = (a_{1j}, \ldots, a_{sj})$ for $j = 1, \ldots, r$, and let $\mathcal{A}_\varphi = (a_{ij}) \in \mathrm{Mat}_{s,r}(P)$. This construction yields a map

$$\Lambda_{r,s} : \mathrm{Hom}_P(P^r, P^s) \longrightarrow \mathrm{Mat}_{s,r}(P)$$

We say that $\mathcal{A}_\varphi = \Lambda_{r,s}(\varphi) = (\varphi(e_1), \ldots, \varphi(e_r))$ is the **matrix associated** to φ.

b) The map $\mathrm{Fl}_{s,r} : \mathrm{Mat}_{s,r}(P) \longrightarrow P^{rs}$ which sends a matrix $\mathcal{A} = (a_{ij})$ to the vector $(a_{11}, a_{21}, \ldots, a_{s1}, a_{12}, a_{22}, \ldots, a_{s2}, \ldots \ldots, a_{1r}, a_{2r}, \ldots, a_{sr})$ is clearly an isomorphism of P-modules. It is called a **flattening isomorphism**.

Recall that, given two P-linear maps $\varphi : P^r \longrightarrow P^s$ and $\psi : P^s \longrightarrow P^t$, the matrix associated to their composition is the product of their associated matrices, i.e. we have $\Lambda_{r,t}(\psi \circ \varphi) = \Lambda_{s,t}(\psi) \cdot \Lambda_{r,s}(\varphi)$. By combining the two maps $\Lambda_{r,s}$ and $\mathrm{Fl}_{s,r}$, we obtain the desired explicit representation of the Hom-module $\mathrm{Hom}_P(P^r, P^s)$.

Proposition 3.3.9. *Let r and s be positive integers.*

a) *The P-linear map $\Lambda_{r,s} : \mathrm{Hom}_P(P^r, P^s) \longrightarrow \mathrm{Mat}_{s,r}(P)$ is an isomorphism.*

b) *The P-linear map $\Phi_{r,s} = \mathrm{Fl}_{s,r} \circ \Lambda_{r,s} : \mathrm{Hom}_P(P^r, P^s) \longrightarrow P^{rs}$ is an isomorphism.*

Proof. Since we have already noticed that $\mathrm{Fl}_{s,r}$ is an isomorphism, it suffices to prove a). The fact that the map $\Lambda_{r,s}$ is a P-module homomorphism comes from the very definitions. If $\Lambda_{r,s}(\varphi)$ is the zero matrix, then $\varphi(e_j) = 0$ for $j = 1, \ldots, r$, and thus φ is the zero map. Given a matrix $\mathcal{A} \in \mathrm{Mat}_{s,r}(P)$, we define a map $\varphi \in \mathrm{Hom}_P(P^r, P^s)$ by $\varphi(e_j) = (a_{1j}, \ldots, a_{sj})$ for $j = 1, \ldots, r$. Clearly, we have $\mathcal{A} = \Lambda_{r,s}(\varphi)$ which concludes the proof. $\square$

Our next goal is to understand better how the isomorphisms $\Phi_{r,s}$ behave when we compose them with maps which are defined using the *functoriality* of the Hom-module. The Hom-module is functorial in its two arguments in the following sense.

Definition 3.3.10. Let R be a ring, and let U, V, and W be R-modules.

a) For every R-linear map $\varphi : U \longrightarrow V$, we introduce a corresponding R-linear map $\varphi^* : \mathrm{Hom}_R(V, W) \longrightarrow \mathrm{Hom}_R(U, W)$ by $\varphi^*(\lambda) = \lambda \circ \varphi$ for all $\lambda \in \mathrm{Hom}_R(V, W)$. We denote it by $\varphi^* = \mathrm{Hom}_R(\varphi, W)$ and say that $\mathrm{Hom}_R(-, W)$ is the **contravariant Hom-functor**.

b) For every R-linear map $\psi : V \longrightarrow W$, we introduce a corresponding R-linear map $\psi_* : \mathrm{Hom}_R(U, V) \longrightarrow \mathrm{Hom}_R(U, W)$ by $\psi_*(\lambda) = \psi \circ \lambda$ for all $\lambda \in \mathrm{Hom}_R(U, V)$. We denote it by $\psi_* = \mathrm{Hom}_R(U, \psi)$ and say that $\mathrm{Hom}_R(U, -)$ is the **covariant Hom-functor**.

Given P-linear maps $\varphi : P^r \longrightarrow P^{r'}$ and $\psi : P^s \longrightarrow P^{s'}$, we can apply the above isomorphisms $\Phi_{i,j}$ to both ends of the homomorphisms $\varphi^* = \mathrm{Hom}_P(\varphi, P^s)$ and $\psi_* = \mathrm{Hom}_P(P^r, \psi)$. Then there are P-linear maps $\widetilde{\varphi}$ and $\widetilde{\psi}$ such that the diagrams

$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^{r'}, P^s) & \xrightarrow{\ \varphi^*\ } & \mathrm{Hom}_P(P^r, P^s) \\
\downarrow{\scriptstyle \Phi_{r',s}} & & \downarrow{\scriptstyle \Phi_{r,s}} \\
P^{r's} & \xrightarrow{\ \widetilde{\varphi}\ } & P^{rs}
\end{array}
$$

and

$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^s) & \xrightarrow{\ \psi_*\ } & \mathrm{Hom}_P(P^r, P^{s'}) \\
\downarrow{\scriptstyle \Phi_{r,s}} & & \downarrow{\scriptstyle \Phi_{r,s'}} \\
P^{rs} & \xrightarrow{\ \widetilde{\psi}\ } & P^{rs'}
\end{array}
$$

are commutative. In other words, we let $\widetilde{\varphi} = \Phi_{r,s} \circ \varphi^* \circ (\Phi_{r',s})^{-1}$ and $\widetilde{\psi} = \Phi_{r,s'} \circ \psi_* \circ (\Phi_{r,s})^{-1}$. In order to find the matrices associated to $\widetilde{\varphi}$ and $\widetilde{\psi}$, we proceed in two steps.

Remark 3.3.11. Given P-linear maps $\varphi : P^r \longrightarrow P^{r'}$ and $\psi : P^s \longrightarrow P^{s'}$, let $\varphi^* = \mathrm{Hom}_P(\varphi, P^s)$ and $\psi_* = \mathrm{Hom}_P(P^r, \psi)$. In this situation, we define a P-linear map $\overline{\varphi} : \mathrm{Mat}_{s,r'}(P) \longrightarrow \mathrm{Mat}_{s,r}(P)$ by **right multiplication** by $\mathcal{A}_\varphi$, i.e. by $\overline{\varphi}(\mathcal{B}) = \mathcal{B} \cdot \mathcal{A}_\varphi$ for every $\mathcal{B} \in \mathrm{Mat}_{s,r'}(P)$.

Furthermore, we define a P-linear map $\overline{\psi} : \mathrm{Mat}_{s,r}(P) \longrightarrow \mathrm{Mat}_{s',r}(P)$ by **left multiplication** by $\mathcal{A}_\psi$, i.e. by $\overline{\psi}(\mathcal{B}) = \mathcal{A}_\psi \cdot \mathcal{B}$ for every $\mathcal{B} \in \mathrm{Mat}_{s,r}(P)$. Then we have two diagrams

$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^{r'}, P^s) & \xrightarrow{\ \varphi^*\ } & \mathrm{Hom}_P(P^r, P^s) \\
\downarrow{\scriptstyle \Lambda_{r',s}} & & \downarrow{\scriptstyle \Lambda_{r,s}} \\
\mathrm{Mat}_{s,r'}(P) & \xrightarrow{\ \overline{\varphi}\ } & \mathrm{Mat}_{s,r}(P)
\end{array}
$$

and

$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^s) & \xrightarrow{\ \psi_*\ } & \mathrm{Hom}_P(P^r, P^{s'}) \\
\downarrow{\scriptstyle \Lambda_{r,s}} & & \downarrow{\scriptstyle \Lambda_{r,s'}} \\
\mathrm{Mat}_{s,r}(P) & \xrightarrow{\ \overline{\psi}\ } & \mathrm{Mat}_{s',r}(P)
\end{array}
$$

Both of these diagrams are commutative, because the matrix associated to a composition of two linear maps is the product of the two matrices associated to the individual maps.

Now we are going to make the second step, namely the explicit construction of the commutative diagrams involving $\overline{\varphi}$ and $\widetilde{\varphi}$ resp. $\overline{\psi}$ and $\widetilde{\psi}$. The necessary matrices are defined as follows.

Definition 3.3.12. Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{r,r'}(P)$ and $\mathcal{B} = (b_{ij}) \in \mathrm{Mat}_{s,s'}(P)$ be two matrices over P. Then the block matrix

$$\begin{pmatrix} a_{11}\mathcal{B} & \cdots & a_{1r'}\mathcal{B} \\ \vdots & & \vdots \\ a_{r1}\mathcal{B} & \cdots & a_{rr'}\mathcal{B} \end{pmatrix}$$

of size $rs \times r's'$ is called the **tensor product** or the **outer product** or the **Kronecker product** of $\mathcal{A}$ and $\mathcal{B}$, and is denoted by $\mathcal{A} \otimes \mathcal{B}$.

In linear algebra, there is the notion of the tensor product of linear maps between vector spaces. The preceding definition is related to that notion, but it would lead us too far away to discuss this connection. If the matrix $\mathcal{A}$ is the identity matrix of size $r \times r$, the tensor product $\mathcal{A} \otimes \mathcal{B}$ is simply the block matrix

$$\begin{pmatrix} \mathcal{B} & 0 & \cdots & 0 \\ 0 & \mathcal{B} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \mathcal{B} \end{pmatrix}$$

Proposition 3.3.13. Let $\varphi : P^r \longrightarrow P^{r'}$ and $\psi : P^s \longrightarrow P^{s'}$ be P-linear maps, let $\varphi^* = \mathrm{Hom}_P(\varphi, P^s)$, and let $\psi_* = \mathrm{Hom}_P(P^r, \psi)$.

a) Let $\overline{\varphi}$ be the map defined by right multiplication by $\mathcal{A}_\varphi$, and let $\widetilde{\varphi}$ be the map whose associated matrix is $\mathcal{A}_\varphi^{\mathrm{tr}} \otimes \mathcal{I}_s$. Then we have a commutative diagram of P-linear maps

$$\begin{array}{ccc} \mathrm{Mat}_{s,r'}(P) & \xrightarrow{\overline{\varphi}} & \mathrm{Mat}_{s,r}(P) \\ \downarrow{\scriptstyle \mathrm{Fl}_{s,r'}} & & \downarrow{\scriptstyle \mathrm{Fl}_{s,r}} \\ P^{r's} & \xrightarrow{\widetilde{\varphi}} & P^{rs} \end{array}$$

b) Let $\overline{\psi}$ be the map defined by left multiplication by $\mathcal{A}_\psi$, and let $\widetilde{\psi}$ be the map whose associated matrix is $\mathcal{I}_r \otimes \mathcal{A}_\psi$. Then we have a commutative diagram of P-linear maps

$$\begin{array}{ccc} \mathrm{Mat}_{s,r}(P) & \xrightarrow{\overline{\psi}} & \mathrm{Mat}_{s',r}(P) \\ \downarrow{\scriptstyle \mathrm{Fl}_{s,r}} & & \downarrow{\scriptstyle \mathrm{Fl}_{s',r}} \\ P^{rs} & \xrightarrow{\widetilde{\psi}} & P^{rs'} \end{array}$$

Proof. First we show claim a). Let $\mathcal{A}_\varphi = (a_{ij}) \in \mathrm{Mat}_{r',r}(P)$ be the matrix associated to φ. We start with a tuple $(f_{11}, f_{21}, \ldots, f_{s1}, \ldots, f_{1r'}, f_{2r'} \ldots, f_{sr'})$ in $P^{r's}$. This tuple is the image of the matrix $\mathcal{F} = (f_{ij})$ under the map $\mathrm{Fl}_{s,r'}$. By Remark 3.3.11, we have $\overline{\varphi}(\mathcal{F}) = \mathcal{F} \cdot \mathcal{A}_\varphi$, and for $i = 1, \ldots, s$ and

$j = 1, \ldots, r$, the (i, j)-entry of this matrix is $\sum_{k=1}^{r'} f_{ik} a_{kj}$. By applying the isomorphism $\mathrm{Fl}_{s,r}$, we see that the image of our original tuple $(f_{11}, f_{21}, \ldots, f_{sr'})$ under the map $\widetilde{\varphi}$ is

$$\left(\sum_{k=1}^{r'} f_{1k} a_{k1}, \sum_{k=1}^{r'} f_{2k} a_{k1}, \ldots, \sum_{k=1}^{r'} f_{sk} a_{k1}, \ldots, \sum_{k=1}^{r'} f_{1k} a_{kr}, \sum_{k=1}^{r'} f_{2k} a_{kr}, \ldots, \sum_{k=1}^{r'} f_{sk} a_{kr} \right)$$

Using this description of $\widetilde{\varphi}$, it is easy to check that its associated matrix is indeed $\mathcal{A}_{\varphi}^{\mathrm{tr}} \otimes \mathcal{I}_s$.

Now we prove claim b) in a similar fashion. Let $\mathcal{A}_{\psi} = (a_{ij}) \in \mathrm{Mat}_{s',s}(P)$ be the matrix associated to ψ. Starting again with a tuple $(f_{11}, f_{21}, \ldots, f_{s1}, \ldots, f_{1r}, f_{2r}, \ldots, f_{sr})$ in P^{rs} whose preimage under $\mathrm{Fl}_{s,r}$ is $\mathcal{F} = (f_{ij})$, we see that the (i, j)-entry of $\overline{\psi}(\mathcal{F}) = \mathcal{A}_{\psi} \cdot \mathcal{F}$ is given by $\sum_{k=1}^{s} a_{ik} f_{kj}$ for $i = 1, \ldots, s'$ and $j = 1, \ldots, r$. Thus the image under $\widetilde{\psi}$ of the original tuple is given by

$$\left(\sum_{k=1}^{s} a_{1k} f_{k1}, \sum_{k=1}^{s} a_{2k} f_{k1}, \ldots, \sum_{k=1}^{s} a_{s'k} f_{k1}, \ldots, \sum_{k=1}^{s} a_{1k} f_{kr}, \sum_{k=1}^{s} a_{2k} f_{kr}, \ldots, \sum_{k=1}^{s} a_{s'k} f_{kr} \right)$$

Again it is easy to use this description to check that $\mathcal{I}_r \otimes \mathcal{A}_{\psi}$ is the associated matrix of $\widetilde{\psi}$. $\qquad\square$

To perform our computation of Hom-modules in the general case, i.e. when M and N are not necessarily zero, we still need one more ingredient, namely the following exactness properties of the covariant and the contravariant Hom-functors.

Proposition 3.3.14. *Let R be a ring, let $U_1 \xrightarrow{\varphi} U_2 \xrightarrow{\psi} U_3 \longrightarrow 0$ be an exact sequence of R-modules, let $t \geq 1$, and let V be a further R-module.*

a) If we let $\varphi_* = \mathrm{Hom}_R(R^t, \varphi)$ and $\psi_* = \mathrm{Hom}_R(R^t, \psi)$, then

$$\mathrm{Hom}_R(R^t, U_1) \xrightarrow{\varphi_*} \mathrm{Hom}_R(R^t, U_2) \xrightarrow{\psi_*} \mathrm{Hom}_R(R^t, U_3) \longrightarrow 0$$

is an exact sequence of R-modules.

b) If we let $\varphi^* = \mathrm{Hom}_R(\varphi, V)$ and $\psi^* = \mathrm{Hom}_R(\psi, V)$, then

$$0 \longrightarrow \mathrm{Hom}_R(U_3, V) \xrightarrow{\psi^*} \mathrm{Hom}_R(U_2, V) \xrightarrow{\varphi^*} \mathrm{Hom}_R(U_1, V)$$

is an exact sequence of R-modules.

Proof. To prove a), we first show $\mathrm{Im}(\varphi_*) = \mathrm{Ker}(\psi_*)$. For every map $\lambda \in \mathrm{Hom}_R(R^r, U_1)$, we have $\mathrm{Im}(\varphi \circ \lambda) \subseteq \mathrm{Im}(\varphi) = \mathrm{Ker}(\psi)$, and therefore $\psi_*(\varphi_*(\lambda)) = \psi \circ \varphi \circ \lambda = 0$. Conversely, if we are given an element $\lambda \in \mathrm{Ker}(\psi_*)$, then $\psi \circ \lambda = 0$ implies $\mathrm{Im}(\lambda) \subseteq \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$. By Proposition 3.3.5, it follows that there exists a map $\lambda' \in \mathrm{Hom}_R(R^t, U_1)$ such that $\lambda = \varphi \circ \lambda' = \varphi_*(\lambda')$. Thus we get $\lambda \in \mathrm{Im}(\varphi_*)$, as we wanted to show.

Next we prove the surjectivity of the map ψ_*. Let $\{\varepsilon_1, \ldots, \varepsilon_t\}$ denote the canonical basis of R^t. Given a map $\lambda \in \mathrm{Hom}_R(R^t, U_3)$, we have $\lambda(\varepsilon_i) \in U_3 = \mathrm{Im}(\psi)$ for $i = 1, \ldots, t$. Therefore we can choose elements $u_1, \ldots, u_t \in U_2$ such that $\lambda(\varepsilon_i) = \psi(u_i)$ for $i = 1, \ldots, t$. Then we define an R-linear map $\lambda' : R^t \longrightarrow U_2$ by $\lambda'(\varepsilon_i) = u_i$ for $i = 1, \ldots, t$. Clearly, this map λ' satisfies $\psi_*(\lambda') = \psi \circ \lambda' = \lambda$, and we get $\lambda \in \mathrm{Im}(\psi_*)$, as desired.

To prove claim b), we start again by showing $\mathrm{Im}(\psi^*) = \mathrm{Ker}(\varphi^*)$. For a map $\lambda \in \mathrm{Hom}_R(U_3, V)$, we have $\varphi^*(\psi^*(\lambda)) = \lambda \circ \psi \circ \varphi = 0$, because $\psi \circ \varphi = 0$. This shows $\mathrm{Im}(\psi^*) \subseteq \mathrm{Ker}(\varphi^*)$. Conversely, let $\lambda \in \mathrm{Ker}(\varphi^*)$ be given, i.e. let $\lambda : U_2 \longrightarrow V$ be an R-linear map such that $\lambda \circ \varphi = 0$. Then $\mathrm{Ker}(\psi) = \mathrm{Im}(\varphi) \subseteq \mathrm{Ker}(\lambda)$ shows that λ induces $\overline{\lambda} : U_2/\mathrm{Ker}(\psi) \longrightarrow V$. Similarly, the surjection ψ induces an isomorphism $\overline{\psi} : U_2/\mathrm{Ker}(\psi) \longrightarrow U_3$. Thus we obtain a map $\lambda' = \overline{\lambda} \circ (\overline{\psi})^{-1} : U_3 \longrightarrow V$. Now we denote the canonical homomorphism $U_2 \longrightarrow U_2/\mathrm{Ker}(\psi)$ by ε and get from $\overline{\lambda} = \lambda' \circ \overline{\psi}$ the desired conclusion $\lambda = \overline{\lambda} \circ \varepsilon = \lambda' \circ \overline{\psi} \circ \varepsilon = \lambda' \circ \psi = \psi^*(\lambda') \in \mathrm{Im}(\psi^*)$.

Finally, we show that the map ψ^* is injective. Suppose that we have $\psi^*(\lambda) = \lambda \circ \psi = 0$ for some map $\lambda \in \mathrm{Hom}_R(U_3, V)$. Then we obtain the relations $U_3 = \mathrm{Im}(\psi) \subseteq \mathrm{Ker}(\lambda) \subseteq U_3$ which imply $\mathrm{Ker}(\lambda) = U_3$, i.e. $\lambda = 0$, and we are done. $\square$

At this point we have all the necessary ingredients for cooking up our algorithm. After all the trouble we had to go through in this subsection in order to arrive here, the following theorem yields an algorithm for computing Hom-modules which is of surprising simplicity. The final meal does not always show the efforts which went into preparing it!

Theorem 3.3.15. (Computation of Hom-Modules)
Let $M = \langle g_1, \ldots, g_\alpha \rangle \subseteq P^r$ and $N = \langle h_1, \ldots, h_\beta \rangle \subseteq P^s$ be two P-submodules. Let $\mathcal{G}$ be the matrix of size $r \times \alpha$ whose columns are $g_1, \ldots, g_\alpha$, let $\mathcal{H}$ be the matrix of size $s \times \beta$ whose columns are $h_1, \ldots, h_\beta$, let U be the P-submodule of P^{rs} which is generated by the column vectors of the matrix $\mathcal{I}_r \otimes \mathcal{H}$ of size $rs \times r\beta$, and let V be the P-submodule of $P^{\alpha s}$ which is generated by the column vectors of the matrix $\mathcal{I}_\alpha \otimes \mathcal{H}$ of size $\alpha s \times \alpha \beta$. Finally, let $\lambda : P^{rs} \longrightarrow P^{\alpha s}$ be the P-linear map whose associated matrix is $\mathcal{G}^{\mathrm{tr}} \otimes \mathcal{I}_s$.

a) *The map λ satisfies the inclusion $\lambda(U) \subseteq V$ and induces a P-linear map $\overline{\lambda} : P^{rs}/U \longrightarrow P^{\alpha s}/V$.*

b) *The P-module $\mathrm{Hom}_P(P^r/M, P^s/N)$ is isomorphic to $\mathrm{Ker}(\overline{\lambda})$. In particular, a presentation of $\mathrm{Hom}_P(P^r/M, P^s/N)$ can be computed by using Proposition 3.3.1.c to find a presentation of the kernel of $\overline{\lambda}$.*

c) *Let $\vartheta \in \mathrm{Hom}_P(P^r/M, P^s/N)$ be represented, as an element of $\mathrm{Ker}(\overline{\lambda})$, by the residue class $(a_{11}, a_{21}, \ldots, a_{s1}, \ldots\ldots, a_{1r}, a_{2r}, \ldots, a_{sr}) + U$. Then the map ϑ is induced by the P-linear map $\Theta : P^r \longrightarrow P^s$ whose associated matrix is $\mathcal{A}_\Theta = (a_{ij})$.*

Proof. First we apply Proposition 3.3.14 to the presentations

$$P^\alpha \xrightarrow{\varphi} P^r \longrightarrow P^r/M \longrightarrow 0 \qquad \text{and} \qquad P^\beta \xrightarrow{\psi} P^s \longrightarrow P^s/N \longrightarrow 0$$

where $\varphi(e_i) = g_i$ for $i = 1, \dots, \alpha$ and $\psi(e_j) = h_j$ for $j = 1, \dots, \beta$. We get the following fundamental diagram (1). Its maps are defined by applying the covariant and contravariant Hom-functors to the various maps in the two presentations. It is easy to check that this diagram is in fact commutative.

(1)
$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^\beta) & \longrightarrow & \mathrm{Hom}_P(P^\alpha, P^\beta) \\
\downarrow & & \downarrow \\
\mathrm{Hom}_P(P^r, P^s) & \longrightarrow & \mathrm{Hom}_P(P^\alpha, P^s) \\
\downarrow & & \downarrow \\
0 \longrightarrow \mathrm{Hom}_P(P^r/M, P^s/N) \longrightarrow \mathrm{Hom}_P(P^r, P^s/N) & \longrightarrow & \mathrm{Hom}_P(P^\alpha, P^s/N) \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}
$$

In order to prove a), we need to construct four further commutative diagrams. By the definition of the P-linear map $\varphi_s^* = \mathrm{Hom}_P(\varphi, P^s)$, we have a commutative diagram

(2)
$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^s) & \xrightarrow{\varphi_s^*} & \mathrm{Hom}_P(P^\alpha, P^s) \\
\downarrow{\scriptstyle \Phi_{r,s}} & & \downarrow{\scriptstyle \Phi_{\alpha,s}} \\
P^{rs} & \xrightarrow{\widetilde{\varphi}_s} & P^{\alpha s}
\end{array}
$$

By Proposition 3.3.13.a, the map λ is precisely $\widetilde{\varphi}_s$.

Similarly, by the definition of the P-linear maps $(\psi_\alpha)_* = \mathrm{Hom}_P(P^\alpha, \psi)$ and $(\psi_r)_* = \mathrm{Hom}_P(P^r, \psi)$, we have two commutative diagrams

(3)
$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^\alpha, P^\beta) & \xrightarrow{(\psi_\alpha)_*} & \mathrm{Hom}_P(P^\alpha, P^s) \\
\downarrow{\scriptstyle \Phi_{\alpha,\beta}} & & \downarrow{\scriptstyle \Phi_{\alpha,s}} \\
P^{\alpha\beta} & \xrightarrow{\widetilde{\psi}_\alpha} & P^{\alpha s}
\end{array}
$$

and (4)
$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^\beta) & \xrightarrow{(\psi_r)_*} & \mathrm{Hom}_P(P^r, P^s) \\
\downarrow{\scriptstyle \Phi_{r,\beta}} & & \downarrow{\scriptstyle \Phi_{r,s}} \\
P^{r\beta} & \xrightarrow{\widetilde{\psi}_r} & P^{rs}
\end{array}
$$

Using Remark 3.3.11 and Proposition 3.3.13.b, we see that the matrices associated to the maps $\widetilde{\psi}_\alpha$ and $\widetilde{\psi}_r$ are $\mathcal{I}_\alpha \otimes \mathcal{H}$ and $\mathcal{I}_r \otimes \mathcal{H}$, and their images are V and U, respectively.

Finally, we let $\varphi_\beta^* = \mathrm{Hom}_P(\varphi, P^\beta)$ and observe that the diagram

(5)
$$
\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^\beta) & \xrightarrow{(\psi_r)_*} & \mathrm{Hom}_P(P^r, P^s) \\
\downarrow{\scriptstyle \varphi_\beta^*} & & \downarrow{\scriptstyle \varphi_s^*} \\
\mathrm{Hom}_P(P^\alpha, P^\beta) & \xrightarrow{(\psi_\alpha)_*} & \mathrm{Hom}_P(P^\alpha, P^s)
\end{array}
$$

is commutative, because $\varphi_s^*((\psi_r)_*(\gamma)) = \psi \circ \gamma \circ \varphi = (\psi_\alpha)_*(\varphi_\beta^*(\gamma))$ for all $\gamma \in \mathrm{Hom}_P(P^r, P^\beta)$.

Now we are ready to prove claim a). Using the above diagrams, we calculate

$$\lambda(U) \underset{}{=} \mathrm{Im}(\lambda \circ \widetilde{\psi}_r) = \mathrm{Im}(\widetilde{\varphi}_s \circ \widetilde{\psi}_r \circ \Phi_{r,\beta}) \underset{(4)}{=} \mathrm{Im}(\widetilde{\varphi}_s \circ \Phi_{r,s} \circ (\psi_r)_*)$$

$$\underset{(2)}{=} \mathrm{Im}(\Phi_{\alpha,s} \circ \varphi_s^* \circ (\psi_r)_*) \underset{(5)}{=} \mathrm{Im}(\Phi_{\alpha,s} \circ (\psi_\alpha)_* \circ \varphi_\beta^*)$$

$$\underset{(3)}{=} \mathrm{Im}(\widetilde{\psi}_\alpha \circ \Phi_{\alpha,\beta} \circ \varphi_\beta^*) \subseteq \mathrm{Im}(\widetilde{\psi}_\alpha) = V$$

To prove b), we note that in diagram (4) both $\Phi_{r,\beta}$ and $\Phi_{r,s}$ are isomorphisms. Therefore also the induced map $\overline{\Phi}_{r,s}$ between the cokernels of $(\psi_r)_*$ and $\widetilde{\psi}_r$ is an isomorphism. Similarly, we can use diagram (3) and get an induced isomorphism $\overline{\Phi}_{\alpha,s}$ between the cokernels of $(\psi_\alpha)_*$ and $\widetilde{\psi}_\alpha$. Thus we have two more commutative diagrams

(6)
$$\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^s) & \longrightarrow\!\!\!\!\rightarrow & \mathrm{Hom}_P(P^r, P^s/N) \\
\downarrow{\scriptstyle \Phi_{r,s}} & & \downarrow{\scriptstyle \overline{\Phi}_{r,s}} \\
P^{rs} & \longrightarrow & P^{rs}/U
\end{array}$$

and (7)
$$\begin{array}{ccc}
\mathrm{Hom}_P(P^\alpha, P^s) & \longrightarrow & \mathrm{Hom}_P(P^\alpha, P^s/N) \\
\downarrow{\scriptstyle \Phi_{\alpha,s}} & & \downarrow{\scriptstyle \overline{\Phi}_{\alpha,s}} \\
P^{\alpha s} & \longrightarrow\!\!\!\!\rightarrow & P^{\alpha s}/V
\end{array}$$

By combining diagrams (2), (6), (7), and the lower right part of the fundamental diagram (1), we find that also the diagram

$$\begin{array}{ccc}
\mathrm{Hom}_P(P^r, P^s/N) & \overset{\Lambda}{\longrightarrow} & \mathrm{Hom}_P(P^\alpha, P^s/N) \\
\downarrow{\scriptstyle \overline{\Phi}_{r,s}} & & \downarrow{\scriptstyle \overline{\Phi}_{\alpha,s}} \\
P^{rs}/U & \overset{\overline{\lambda}}{\longrightarrow} & P^{\alpha s}/V
\end{array}$$

is commutative, where $\Lambda = \mathrm{Hom}_P(\varphi, P^s/N)$. Since $\mathrm{Hom}_P(P^r/M, P^s/N)$ is isomorphic to the kernel of Λ by the fundamental diagram (1), and since the two vertical maps are isomorphisms, the claim $\mathrm{Hom}_P(P^r/M, P^s/N) \cong \mathrm{Ker}(\overline{\lambda})$ follows.

To prove c), we let $\Theta : P^r \longrightarrow P^s$ be the P-linear map whose associated matrix is $\mathcal{A}_\Theta = (a_{ij})$. Using Definition 3.3.8.b, we see that the image of Θ in P^{rs} is the tuple $(a_{11}, \ldots, a_{rs})$. In view of diagrams (2) and (7), this implies that the map $\vartheta : P^r/M \longrightarrow P^s/N$ induced by Θ corresponds to the residue class $(a_{11}, \ldots, a_{rs}) + U \in P^{rs}/U$. $\qquad \square$

To conclude this section, we compute an explicit example.

Example 3.3.16. Once more we let $P = \mathbb{Q}[x,y]$, and we use the P-submodules $M = \langle(x, -y-1, 0)\rangle$ of P^3 and $N = \langle(x^2, 0), (0, x^3), (y, 0),$ $(0, y)\rangle$ of P^2 introduced in Example 3.3.2. Our goal is to compute a presentation of $\operatorname{Hom}_P(P^3/M, P^2/N)$ using Theorem 3.3.15. In our case $\alpha = 1$, $r = 3$, $\beta = 4$, $s = 2$, $\mathcal{G} = \begin{pmatrix} x \\ -y-1 \\ 0 \end{pmatrix}$, $\mathcal{H} = \begin{pmatrix} x^2 & 0 & y & 0 \\ 0 & x^3 & 0 & y \end{pmatrix}$, U is the P-submodule of P^6 generated by the columns of the matrix $\mathcal{I}_3 \otimes \mathcal{H}$, and V is the submodule of P^2 generated by the columns of the matrix $\mathcal{I}_1 \otimes \mathcal{H} = \mathcal{H}$. Moreover, the matrix $\mathcal{G}^{\mathrm{tr}} \otimes \mathcal{I}_2 = \begin{pmatrix} x & 0 & -y-1 & 0 & 0 & 0 \\ 0 & x & 0 & -y-1 & 0 & 0 \end{pmatrix}$ defines a P-linear map $\lambda : P^6 \longrightarrow P^2$, and it is easy to check that $\lambda(U) \subseteq V$. Thus we obtain a P-linear map $\overline{\lambda} : P^6/U \longrightarrow P^2/V$.

Our goal is to find a presentation of the P-module $\operatorname{Hom}_P(P^3/M, P^2/N)$. In view of the theorem, we can apply Proposition 3.3.1.a to compute a system of generators of $\operatorname{Ker}(\overline{\lambda})$. We get $\operatorname{Hom}_P(P^3/M, P^2/N) = \langle \varphi_1, \varphi_2, \ldots, \varphi_8 \rangle$, where φ_1 corresponds to $(x, 0, 0, 0, 0, 0) + U$, φ_2 to $(0, x^2, 0, 0, 0, 0) + U$, φ_3 to $(0, 0, 0, 0, 1, 0) + U$, φ_4 to $(0, 0, 0, 0, 0, 1) + U$, φ_5 to $(0, 0, y, 0, 0, 0) + U$, φ_6 to $(0, 0, 0, y, 0, 0) + U$, φ_7 to $(1, 0, x, 0, 0, 0) + U$, and φ_8 to $(0, 1, 0, x, 0, 0) + U$.

Next we use Proposition 3.3.1.c and compute the presentation

$$P^{12} \xrightarrow{\mu} P^8 \xrightarrow{\nu} \operatorname{Hom}_P(P^3/M, P^2/N) \longrightarrow 0$$

where ν is given by $\nu(e_i) = \varphi_i$ for $i = 1, \ldots, 8$ and μ is associated to

$$\mathcal{A}_\mu = \begin{pmatrix} 0 & 0 & 0 & 0 & y & x & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y & x & -1 & 0 \\ y & 0 & 0 & 0 & 0 & 0 & 0 & x^2 & 0 & 0 & 0 & 0 \\ 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^3 \\ 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -y & 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -y & 0 & 0 & 0 & 0 & 0 & 0 & x^2 & 0 \end{pmatrix}$$

Finally, let us consider the P-linear map $\varphi : P^3/M \longrightarrow P^2/N$ defined in Example 3.3.2. It is induced by the P-linear map $\Phi : P^3 \longrightarrow P^2$ whose associated matrix is $\mathcal{A}_\Phi = \begin{pmatrix} xy & x^2 & y \\ y+1 & x & 1 \end{pmatrix}$. By part c) of the theorem, the map φ is represented by $(xy, y+1, x^2, x, y, 1) + U$ as an element of $\operatorname{Ker}(\overline{\lambda})$. Using Explicit Membership 3.1.9.a, we can find the representation $\varphi = (y-1)\varphi_1 + y\varphi_3 + \varphi_4 - x\varphi_6 + x\varphi_7 + (y+1)\varphi_8$ of φ in terms of the generators of $\operatorname{Hom}_P(P^3/M, P^2/N)$.

Exercise 1. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and let $\varphi : P^r/M \longrightarrow P^s/N$ be a P-linear map as in Subsection 3.3.A. Explain how one can compute a presentation of $\mathrm{Coker}(\varphi) = (P^s/N)/\mathrm{Im}(\varphi)$.

Exercise 2. Let K be a field, let $P = K[x, y]$, let $f = x + y - 1$, and let $I = (y(y-1), f) \subseteq P$. Compute the kernel of the multiplication map $\mu_f : P/I^2 \longrightarrow P/I^2$ defined by $g + I^2 \mapsto fg + I^2$.

Exercise 3. Let $P = K[x, y, z]$ be a polynomial ring over a field K, and let $a, b \in \mathbb{N}$ such that $b \geq a$. Prove that multiplication by $x^{b-a}y^{b-a}z^{b-a}$ yields a well-defined P-linear map $\varphi : P/(x^a, y^a, z^a) \longrightarrow P/(x^b, y^b, z^b)$ and that φ is injective.

Exercise 4. Let $P = K[x, y]$ be a polynomial ring in two indeterminates over a field K, let $\mathcal{G} = (x, y)$, and let I be the ideal generated by $\{x, y\}$.
  a) Show that there is no P-linear map $\varphi : I \longrightarrow P$ such that we have $\varphi(fx + gy) = f$ for all $f, g \in P$.
  b) Use a presentation of I to prove that $\mathrm{Hom}_P(I, P) \cong \langle (x, y) \rangle \subseteq P^2$.
  c) Find a non-trivial P-linear map $\varphi : I \longrightarrow P$.

Exercise 5. Let R be a ring, let I be an ideal in R, and let M be an R-module. Prove that $\mathrm{Hom}_R(R/I, M) \cong 0 :_M I$.

Exercise 6. Let R be a ring, let M and N be R-modules, and let $\varphi : M \longrightarrow N$ be an R-linear map. The map

$$\tilde{\varphi} = \mathrm{Hom}_R(\varphi, R) : \ \mathrm{Hom}_R(N, R) \ \longrightarrow \ \mathrm{Hom}_R(M, R)$$

is called the **dual map** of φ.

  a) Given an exact sequence $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ of R-modules, show that the **dual sequence**

$$0 \ \longrightarrow \ \mathrm{Hom}_R(M'', R) \xrightarrow{\tilde{\psi}} \mathrm{Hom}_R(M, R) \xrightarrow{\tilde{\varphi}} \mathrm{Hom}_R(M', R)$$

  is exact. Give an example in which the map $\tilde{\varphi}$ is not surjective.
  b) Prove that the map $\tilde{\varphi}$ in a) is surjective if there exists an R-linear map $\varrho : M'' \longrightarrow M$ such that $\psi \circ \varrho = \mathrm{id}_{M''}$.
  c) Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $\varphi : P^r \longrightarrow P^s$. What is the matrix associated to the composition of P-linear maps

$$P^s \xrightarrow{\Phi_{s,1}^{-1}} \mathrm{Hom}_P(P^s, P) \xrightarrow{\tilde{\varphi}} \mathrm{Hom}_P(P^r, P) \xrightarrow{\Phi_{r,1}} P^r?$$

Exercise 7. Let R be a ring, and let M be an R-module. Show that the following conditions are equivalent.
  a) Given R-modules U and V and R-linear maps $\varphi : U \longrightarrow V$ and $\psi : M \longrightarrow V$ such that $\mathrm{Im}(\psi) \subseteq \mathrm{Im}(\varphi)$, there always exists a lifting of ψ along φ.
  b) Given R-modules U and V and an R-linear map $\varphi : U \longrightarrow V$ which is surjective, the map $\mathrm{Hom}_R(M, \varphi) : \mathrm{Hom}_R(M, U) \longrightarrow \mathrm{Hom}_R(M, V)$ is also surjective.
  c) For every surjective R-linear map $\pi : V \longrightarrow M$, there is an R-linear map $\psi : M \longrightarrow V$ such that $\pi \circ \psi = \mathrm{id}_M$.
  d) There exists a free R-module U and an R-submodule $V \subseteq U$ such that $U \cong V \oplus M$.

A module M satisfying these conditions is called a **projective module**. Clearly, free R-modules are projective modules. (*Hint:* To prove that c) implies d), use the surjective map $\oplus_{m \in M} R \cdot e_m \longrightarrow M$ given by $e_m \mapsto m$ for all $m \in M$.)

Exercise 8. Let R be a ring, let $0 \longrightarrow U_1 \overset{\varphi}{\longrightarrow} U_2 \overset{\psi}{\longrightarrow} U_3$ be an exact sequence of R-modules, and let V be a further R-module. For the maps $\varphi_* = \operatorname{Hom}_R(V, \varphi)$ and $\psi_* = \operatorname{Hom}_R(V, \psi)$, show that

$$0 \longrightarrow \operatorname{Hom}_R(V, U_1) \overset{\varphi_*}{\longrightarrow} \operatorname{Hom}_R(V, U_2) \overset{\psi_*}{\longrightarrow} \operatorname{Hom}_R(V, U_3)$$

is an exact sequence of R-modules.

Tutorial 32: Computing Kernels and Pullbacks

Most of the computations presented in the previous sections can be considered as special cases of computations of kernels of certain module homomorphisms. The purpose of this tutorial is to study some concrete instances of this general phenomenon.

We start with the situation introduced at the beginning of this section. In particular, we let $M = \langle g_1, \ldots, g_\alpha \rangle \subseteq P^r$ and $N = \langle h_1, \ldots, h_\beta \rangle \subseteq P^s$ be two P-submodules and $\varphi : P^r/M \longrightarrow P^s/N$ a P-module homomorphism.

a) Implement the algorithms of Proposition 3.3.1 for the computation of generators of $\operatorname{Ker}(\varphi)$ and presentations of $\operatorname{Im}(\varphi)$ and $\operatorname{Ker}(\varphi)$ in CoCoA functions `KernelGens(...)`, `ImagePres(...)`, and `KernelPres(...)`, respectively.

b) Apply your functions from a) to compute the kernels and images of the following homomorphisms $\varphi : P^r/M \longrightarrow P^s/N$, where $P = \mathbb{Q}[x, y, z]$, $r = 3$, $M = \langle (-x, -y, 1) \rangle$, $s = 2$, and $N = \langle (x, y), (y, z), (z, x) \rangle$. (Notice that $\varphi(e_3 + M)$ is determined uniquely by $\varphi(e_1 + M)$ and $\varphi(e_2 + M)$.)

   1) $\varphi(e_1 + M) = (1, x^2 + xy + y^2) + N$, $\varphi(e_2 + M) = (xyz - 1, 0) + N$
   2) $\varphi(e_1 + M) = (x^3 - z - 1, y^3 - z - 1) + N$, $\varphi(e_2 + M) = (1, 1) + N$
   3) $\varphi(e_1 + M) = (x - 1, y - 1) + N$, $\varphi(e_2 + M) = (y - 1, z - 1) + N$

c) Let R be a ring, let M_1, M_2, and M_3 be three R-modules, and let $\varphi_1 : M_1 \longrightarrow M_3$ and $\varphi_2 : M_2 \longrightarrow M_3$ be two R-linear maps. Show that there exists an R-module N with the following properties.

   1) There are R-linear maps $\psi_1 : N \longrightarrow M_1$ and $\psi_2 : N \longrightarrow M_2$ such that $\varphi_1 \circ \psi_1 = \varphi_2 \circ \psi_2$.
   2) If N' is a further R-module such that there are two R-linear maps $\psi_1' : N' \longrightarrow M_1$ and $\psi_2' : N' \longrightarrow M_2$ satisfying $\varphi_1 \circ \psi_1' = \varphi_2 \circ \psi_2'$, then there exists an R-linear map $\lambda : N' \longrightarrow N$ such that $\psi_1' = \psi_1 \circ \lambda$ and $\psi_2' = \psi_2 \circ \lambda$.

Furthermore, this module N is unique up to a unique isomorphism of R-modules. Together with the two maps ψ_1 and ψ_2, the module N is called the **pullback** of φ_1 and φ_2. Property 2) is called the **universal property** of the pullback.

Hint: Look at d) to get a clue how to construct the pullback.
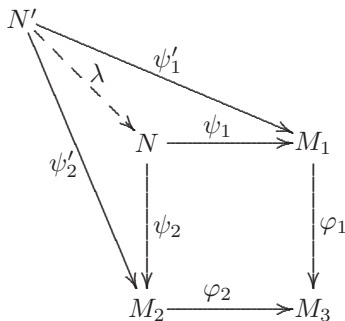
d) Prove that, given two P-linear maps $\varphi_1 : P^k \longrightarrow P^r$ and $\varphi_2 : P^l \longrightarrow P^r$ between finitely generated free P-modules, the pullback of φ_1 and φ_2 can be computed as the kernel of the P-linear map $\psi : P^{k+l} \longrightarrow P^r$ defined by $\psi((f_1, \ldots, f_{k+l})) = \varphi_1((f_1, \ldots, f_k)) - \varphi_2((f_{k+1}, \ldots, f_{k+l}))$.

e) Write a CoCoA function `Pullback(...)` which takes two matrices over P having the same number of rows and computes the pullback of the two P-linear maps defined by those matrices.

f) Show that the intersection $M \cap N$ can be computed using the pullback of the maps $\lambda : P^\alpha \longrightarrow P^r$ given by $\lambda(e_i) = g_i$ for $i = 1, \ldots, \alpha$ and $\mu : P^\beta \longrightarrow P^r$ given by $\mu(e_i) = h_i$ for $i = 1, \ldots, \beta$. Use your function `Pullback(...)` to compute the intersections of the submodules defined in Tutorial 30.b and compare your results with those of that tutorial.

g) Show that the annihilator of an element $m + M$ of P^r/M can be computed using the pullback of the map λ and the map $\nu : P \longrightarrow P^r$ given by $1 \mapsto m$.
Can you find the annihilator $\operatorname{Ann}_P(P^r/M)$ using a single pullback computation? (*Hint:* Look at Proposition 3.2.15.b.)

h) Show that, for a polynomial $f \in P$, the colon module $M :_{P^r} (f)$ can be computed using the pullback of the map λ and the map $\delta : P^r \longrightarrow P^r$ given by $e_i \mapsto f e_i$ for $i = 1, \ldots, r$.
Can you find the colon module $M :_{P^r} I$ for an ideal $I \subseteq P$ using a single pullback computation? (*Hint:* Look at Proposition 3.2.22.b.)

Tutorial 33: The Depth of a Module

Let R be a Noetherian ring, let M be a finitely generated R-module, and let I be an ideal in R such that $IM \neq M$. Generalizing Definition 3.2.23 slightly, we shall say that a tuple of elements $(f_1, \ldots, f_\ell) \in R^\ell$ is called an M-**regular sequence in** I if $f_1, \ldots, f_\ell$ is a regular sequence for M and if $f_i \in I$ for $i = 1, \ldots, \ell$.

An M-regular sequence $(f_1, \ldots, f_\ell)$ in I is called **maximal** if there is no M-regular sequence in I of the form $(f_1, \ldots, f_\ell, f_{\ell+1})$. It can be shown that all maximal M-regular sequences in I have the same length (cf. [Ku80], VI.3.1). This length is called the I-**depth** of M and is denoted by $\mathrm{depth}_I(M)$. In this tutorial we want to study some properties of the I-depth of a module and find a way to compute it.

a) Let $f, g \in R$ such that (f, g) is an M-regular sequence in I, and assume that g is a non-zerodivisor for M. Then show that also (g, f) is an M-regular sequence in I.

b) Let $R = K[x, y, z]$ be the polynomial ring in three indeterminates over a field K. Prove that the tuple $(x^2 - x, xy - 1, xz)$ is an R-regular sequence in the ideal it generates, but $(x^2 - x, xz, xy - 1)$ is not an R-regular sequence in that ideal.

c) Prove that if the ideal I is contained in the union of finitely many prime ideals of R, it is already contained in one of them.

d) Show that the following conditions are equivalent.

   1) $\mathrm{depth}_I(M) = 0$
   2) $\langle 0 \rangle :_M I \neq \langle 0 \rangle$
   3) $\mathrm{Hom}_R(R/I, M) \neq 0$

   Hint: Use Tutorial 31 and part c).

e) Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K and let M be a finitely generated R-module given by an explicit presentation $M = R^r/\langle g_1, \ldots, g_s \rangle$, where $g_1, \ldots, g_s \in R^r$. Write a CoCoA program `IsDepth0(...)` which takes a tuple of vectors $(g_1, \ldots, g_s)$ and a tuple of polynomials $(f_1, \ldots, f_t)$, checks whether the R-module M has I-depth zero with respect to $I = (f_1, \ldots, f_t)$, and returns the corresponding Boolean value.

   Hint: Use part d) and Theorem 3.3.15.

f) Let $r \geq 1$, and let $0 \longrightarrow N \longrightarrow R^r \longrightarrow M \longrightarrow 0$ be an exact sequence of R-modules. Prove that

   1) $\mathrm{depth}_I(N) = \mathrm{depth}_I(M)$ if $\mathrm{depth}_I(R) = \mathrm{depth}_I(M)$, and
   2) $\mathrm{depth}_I(N) = \mathrm{depth}_I(M) + 1$ if $\mathrm{depth}_I(R) > \mathrm{depth}_I(M)$.

   Hint: If $\mathrm{depth}_I(M) > 0$, then choose $x \in I$ which is a non-zerodivisor for both R and M. Construct the commutative diagram

$$0 \longrightarrow N \longrightarrow R^r \longrightarrow M \longrightarrow 0$$

$$\downarrow \mu_x \qquad \downarrow \mu_x \qquad \downarrow \mu_x$$

$$0 \longrightarrow N \longrightarrow R^r \longrightarrow M \longrightarrow 0$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$N/xN \qquad R^r/xR^r \qquad M/xM$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$0 \qquad\qquad 0 \qquad\qquad 0$$

notice that $\operatorname{depth}_I(M/xM) = \operatorname{depth}_I(M) - 1$, and continue.

g) Let $\cdots F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} R/I \longrightarrow 0$ be a finite free resolution of R/I, i.e. an exact sequence of R-modules such that $F_0, F_1, F_2, \ldots$ are finitely generated free R-modules, and let $\varphi_i^* = \operatorname{Hom}_R(\varphi_i, M)$ for $i \geq 0$. Show that the sequence

$$0 \longrightarrow \operatorname{Hom}_R(R/I, M) \xrightarrow{\varphi_0^*} \operatorname{Hom}_R(F_0, M) \xrightarrow{\varphi_1^*} \operatorname{Hom}_R(F_1, M) \xrightarrow{\varphi_2^*} \cdots$$

is a **complex**, i.e. that $\operatorname{Im}(\varphi_i^*) \subseteq \operatorname{Ker}(\varphi_{i+1}^*)$ for $i \geq 0$.

h) In the situation of g), let $N_i = \operatorname{Ker}(\varphi_i)$ for $i \geq 0$. For $i \geq 0$, the cokernel of the map $\operatorname{Hom}_R(F_i, M) \longrightarrow \operatorname{Hom}_R(N_i, M)$ is called the $(i+1)^{\mathrm{st}}$ **Ext-module** of R/I with values in M, and is denoted by $\operatorname{Ext}_R^{i+1}(R/I, M)$. Prove that $\operatorname{Ext}_R^{i+1}(R/I, M) \neq 0$ if and only if we have $\operatorname{Im}(\varphi_i^*) \neq \operatorname{Ker}(\varphi_{i+1}^*)$ in g).

i) *(This part requires some knowledge of homological algebra.)* For $d \geq 1$, prove that $\operatorname{depth}_I(M) = d$ if and only if $\operatorname{Ext}_R^i(R/I, M) = 0$ for $0 \leq i < d$ and $\operatorname{Ext}_R^d(R/I, M) \neq 0$. (Here we let $\operatorname{Ext}_R^0(R/I, M) = \operatorname{Hom}_R(R/I, M)$.) *Hint:* Use induction on d. Choose a non-zerodivisor x for M and apply $\operatorname{Hom}_R(R/I, -)$ to the exact sequence $0 \longrightarrow M \xrightarrow{\mu_x} M \longrightarrow M/xM \longrightarrow 0$.

j) Now let $R = K[x_1, \ldots, x_n]$ and $M = R^r/\langle g_1, \ldots, g_s \rangle$ again. Using i), develop an algorithm for the computation of $\operatorname{depth}_I(M)$. Implement your algorithm in a CoCoA function `Depth(...)`.
Hint: Using Proposition 3.3.13.a, show that the map φ_i^* is induced by the map whose associated matrix is $\mathcal{A}_{\varphi_i} \otimes \mathcal{I}_r$ under the representation of $\operatorname{Hom}_R(F_i, M)$ given by Theorem 3.3.15.b. Then show how one can find a presentation of $\operatorname{Ker}(\varphi_{i+1}^*)/\operatorname{Im}(\varphi_i^*)$ with the aid of Corollary 3.2.6.

k) Apply your CoCoA function `Depth(...)` in the following cases.

1) $I = (x, y, z)$ and $M = (xy - z, yz - x, xz - y)$ in $\mathbb{Q}[x, y, z]$
2) $I = (x_1, x_2, x_3, x_4)$ and $M = (x_2 x_3 - x_1 x_4,\ x_2^3 - x_1^2 x_3,\ x_1 x_3^2 - x_2^2 x_4,\ x_3^3 - x_2 x_4^2)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$
3) $I = (x, 5y - 3, 5z - 4)$ and $M = \langle (x, y, z) \rangle$ in $\mathbb{Q}[x, y, z]^3$

3.4 Elimination

Eliminate, eliminate, eliminate.
Eliminate the eliminators of elimination theory.
(Shreeram S. Abhyankar)

So far in this chapter we have solved all problems by computing syzygies. Another common feature of our approach has been that it didn't matter which module term ordering we chose to compute the Gröbner bases we needed. Starting from now, we have to eliminate this freedom in order to gather the additional power we need for tackling other kinds of applications of Computational Commutative Algebra.

For instance, given an ideal I in a polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K and a number $j \in \{1, \ldots, n-1\}$, we can consider the set of all polynomials in I which involve only the indeterminates $x_1, \ldots, x_j$. This set $I \cap K[x_1, \ldots, x_j]$ is clearly an ideal in $K[x_1, \ldots, x_j]$. It is called the *elimination ideal* of I with respect to the indeterminates $\{x_{j+1}, \ldots, x_n\}$, because passing from I to this ideal means eliminating all polynomials in which one of these latter indeterminates occurs. Now the key observation is that, for solving the problem of computing elimination ideals, we need to compute the Gröbner basis of I with respect to special term orderings called *elimination orderings*.

But why couldn't we eliminate the elimination problem instead? Let us show you a couple of examples where elimination appears naturally. Suppose we have a hunch that there could exist a formula which expresses the area s of a triangle in terms of the three side lengths a, b, and c. We choose a system of coordinates in the plane such that the situation looks as follows.
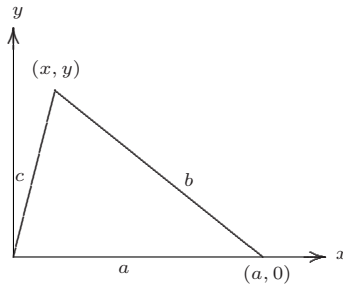
By Pythagoras's Theorem, we have $b^2 = (a-x)^2 + y^2$ and $c^2 = x^2 + y^2$. Furthermore, we observe that $2s = ay$. Then we construct the polynomial ideal $I = (b^2 - (a-x)^2 - y^2, \ c^2 - x^2 - y^2, \ 2s - ay)$ in the ring $K[x, y, a, b, c, s]$. The desired formula should be a polynomial relation among the indeterminates a, b, c, s. It should arise as a consequence of the algebraic relations coded in the ideal I. Thus it should be contained in $I \cap K[a, b, c, s]$. Indeed, when we compute the elimination ideal $I \cap K[a, b, c, s]$, we find just one generator which corresponds to *Heron's Formula*

$$s^2 = \tfrac{1}{16}(a+b+c)(a+b-c)(a-b+c)(-a+b+c)$$

In the second example we consider the set of all points $(x, y, z) \in \mathbb{A}_{\mathbb{Q}}^3$ such that
$$x = t^3, \ y = t^4, \ z = t^5 \qquad\qquad \text{for some } t \in \mathbb{Q}$$
This set of points is an affine variety. In the language of algebraic geometry, it is called a *parametrically defined space curve*. If we want an ideal I in $\mathbb{Q}[x, y, z]$ such that this space curve equals $\mathcal{Z}_{\mathbb{Q}}(I)$, we have to form the larger ideal $J = (x - t^3, y - t^4, z - t^5)$ in $\mathbb{Q}[x, y, z, t]$ and to eliminate t. The resulting ideal $I = J \cap \mathbb{Q}[x, y, z] = (x^3 - yz, y^2 - xz, x^2 y - z^2)$ has the space curve as its zero set.

The remainder of this chapter will consist almost entirely of applications of elimination. This goes a long way to show how important it is. The current section provides the basis for those applications. Namely, we show how to compute generators of an *elimination module* of a P-submodule $M \subseteq P^r$, i.e. of a P-module of the form $M \cap K[x_i \mid x_i \notin L]^r$, where L is a subset of the set of indeterminates $\{x_1, \ldots, x_n\}$ (see Theorem 3.4.5).

Then we provide the reader with an additional technique for effectively performing the elementary operations on ideals and modules discussed earlier (see Proposition 3.4.6 and Proposition 3.4.9). This technique, sometimes also known as the *method of tag variables*, will later help us solve a variety of other problems. The geometric interpretation of elimination is that we want to *project* objects which are in big spaces into smaller spaces. A discussion of this geometric point of view will be suggested in Tutorial 39.

In the following we let K be a field, $P = K[x_1, \ldots, x_n]$ a polynomial ring , $r \geq 1$, and $M \subseteq P^r$ a P-submodule. Moreover, let $L \subseteq \{x_1, \ldots, x_n\}$ be a subset of the set of indeterminates, and let $\widehat{P} = K[x_i \mid x_i \notin L]$ be the polynomial ring in the remaining indeterminates.

Definition 3.4.1. Let $L \subseteq \{x_1, \ldots, x_n\}$ be a subset of the set of indeterminates as above.

a) A module term ordering σ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ is called an **elimination ordering** for L if every element $m \in P^r \setminus \{0\}$ such that $\mathrm{LT}_\sigma(m) \in \widehat{P}^r$ is contained in $\widehat{P}^r$.

b) Given a P-submodule M of P^r, the $\widehat{P}$-submodule $M \cap \widehat{P}^r$ of $\widehat{P}^r$ is called the **elimination module** of M with respect to L.

In other words, an elimination ordering for L has the property that if the indeterminates in L do not occur in the leading term of an element, they do not occur in the element at all. In Section 1.4, we have already defined some kind of elimination orderings. In fact, they are a special case of elimination orderings in the sense of the above definition.

Example 3.4.2. Let $r = 1$ and $L = \{x_1, \ldots, x_j\}$ for $j \in \{1, \ldots, n - 1\}$. Then the elimination ordering $\mathtt{Elim(L)}$ defined in Example 1.4.10 is an elimination ordering for L in the sense of Definition 3.4.1.a. Namely, let $f \in P \setminus \{0\}$

be a polynomial whose leading term satisfies $\mathrm{LT}_{\mathtt{Elim(L)}}(f) \in K[x_{j+1}, \ldots, x_n]$. If we write $\mathrm{LT}_{\mathtt{Elim(L)}}(f) = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, and if $t = x_1^{\beta_1} \cdots x_n^{\beta_n}$ is any term in $\mathrm{Supp}(f)$, then the definition of $\mathtt{Elim(L)}$ implies $0 = \alpha_1 + \cdots + \alpha_j \geq \beta_1 + \cdots + \beta_j$. Thus we obtain $\beta_1 = \cdots = \beta_j = 0$, i.e. $t \in K[x_{j+1}, \ldots, x_n]$. Since $t \in \mathrm{Supp}(f)$ was arbitrary, we find $f \in K[x_{j+1}, \ldots, x_n]$ as desired.

For module term orderings on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ with $r \geq 2$, examples of elimination orderings can be obtained as follows.

Example 3.4.3. Let $1 \leq j \leq n - 1$, and let $L = \{x_1, \ldots, x_j\}$. Then the module term ordering $\mathtt{LexPos}$ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ is an elimination ordering for L. To check this, we suppose a vector $m \in P^r \setminus \{0\}$ has a leading term such that $\mathrm{LT}_{\mathtt{LexPos}}(m) \in K[x_{j+1}, \ldots, x_n]^r$. We write $\mathrm{LT}_{\mathtt{LexPos}}(m) = t e_\gamma$, where $t \in \mathbb{T}^n$ and $1 \leq \gamma \leq r$. Let $t' e_{\gamma'}$ be an element of $\mathrm{Supp}(m)$, where $t' \in \mathbb{T}^n$ and $1 \leq \gamma' \leq r$. By definition of $\mathtt{LexPos}$, we have $t \geq_{\mathtt{Lex}} t'$. Since the term t does not involve $x_1, \ldots, x_j$, we get $t' \in K[x_{j+1}, \ldots, x_n]$. Thus we have $m \in K[x_{j+1}, \ldots, x_n]^r$, as we needed to show.

In particular, given $j \in \{1, \ldots, n - 1\}$, this example shows that the lexicographic term ordering on $\mathbb{T}^n$ is an elimination ordering for the first j indeterminates (see also Proposition 1.5.10). Other kinds of elimination orderings on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ will be studied in Tutorial 34.

Our first goal in this section is to learn how to compute elimination modules. The following preparatory result generalizes Proposition 1.4.13.

Proposition 3.4.4. Let σ be a module ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. Moreover, we let $\widehat{\mathbb{T}} \langle e_1, \ldots, e_r \rangle$ be the set of terms involving only the indeterminates $\{x_i \mid x_i \notin L\}$.

a) The restriction $\hat{\sigma}$ of σ to $\widehat{\mathbb{T}} \langle e_1, ..., e_r \rangle$ is a module ordering.

b) If σ is a module term ordering, then also $\hat{\sigma}$ is a module term ordering.

Proof. The case $L = \{x_i\}$ is a straightforward generalization of Proposition 1.4.13 to $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$. The general case follows by repeated application of this result. $\square$

After we have computed the Gröbner basis of M with respect to an elimination ordering σ on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, it is easy to read off a system of generators for the corresponding elimination module. This is the essence of the following theorem which is the main result of the current section and lies at the heart of many applications of Computational Commutative Algebra.

Theorem 3.4.5. (Computation of Elimination Modules)
Let M be a P-submodule of P^r, let $L \subseteq \{x_1, \ldots, x_n\}$ be a subset of the set of indeterminates, and let σ be an elimination ordering for L. Furthermore, consider the polynomial subring $\widehat{P} = K[x_i \mid x_i \notin L]$ of P as well as the restriction $\hat{\sigma}$ of σ to the set of terms $\widehat{\mathbb{T}} \langle e_1, \ldots, e_r \rangle$ in $\widehat{P}^r$.

a) *We have* $\mathrm{LT}_{\hat{\sigma}}(M \cap \widehat{P}^r) = \mathrm{LT}_\sigma(M) \cap \widehat{P}^r$.

b) *Let G be a σ-Gröbner basis of M, and let $\widehat{G}$ be the set of all elements of G which are contained in $\widehat{P}^r$. Then the set $\widehat{G}$ is a $\hat{\sigma}$-Gröbner basis of $M \cap \widehat{P}^r$.*

c) *Let G be the reduced σ-Gröbner basis of M. Then $\widehat{G} = G \cap \widehat{P}^r$ is the reduced $\hat{\sigma}$-Gröbner basis of $M \cap \widehat{P}^r$.*

Proof. In a), only the inclusion "$\supseteq$" needs to be shown. Let $G = \{g_1, \ldots, g_s\}$ be a σ-Gröbner basis of M. If we have $t e_i \in \mathrm{LT}_\sigma(M)$ for some term $t \in \widehat{P}$ and some $i \in \{1, \ldots, r\}$, then there exists a term $t' \in \mathbb{T}^n$ and a number $j \in \{1, \ldots, s\}$ such that $t e_i = t' \mathrm{LT}_\sigma(g_j)$. Since $t \in \widehat{P}$, we also have $t' \in \widehat{P}$ and $\mathrm{LT}_\sigma(g_j) \in \widehat{P}^r$. From the fact that σ is an elimination ordering for L, we can then conclude $g_j \in \widehat{P}^r$, and hence $t' g_j \in \widehat{P}^r$. Thus the claim follows from $t e_i = t' \mathrm{LT}_{\hat{\sigma}}(g_j) = \mathrm{LT}_{\hat{\sigma}}(t' g_j) \in \mathrm{LT}_{\hat{\sigma}}(M \cap \widehat{P}^r)$. Claim b) is an immediate consequence of a), and c) follows from b). $\qquad\square$

Notice that we allow $M = \langle 0 \rangle$ in this theorem. In this case we have $\mathrm{LT}_\sigma(M) = \langle 0 \rangle$ by definition, $G = \emptyset$ is a σ-Gröbner basis of M, and $\widehat{G} = \emptyset$ is a σ-Gröbner basis of $M \cap \widehat{P}^r = \langle 0 \rangle$.

As we indicated above, the preceding theorem has a number of important applications which will be explored in the remainder of this chapter. We begin by describing alternative ways to perform the elementary operations on modules discussed in the previous sections. The next proposition shows how one can compute the intersection of two submodules of P^r using elimination.

Proposition 3.4.6. *Let M and N be two submodules of P^r, let $\{g_1, \ldots, g_s\}$ be a system of generators of M, and let $\{h_1, \ldots, h_t\}$ be a system of generators of N. We choose a new indeterminate y and consider the $P[y]$-submodule*

$$U = \langle y g_1, \ldots, y g_s, (1-y) h_1, \ldots, (1-y) h_t \rangle$$

of $P[y]^r$. Then we have $M \cap N = U \cap P^r$.

Proof. For $v \in M \cap N$, there are polynomials $p_1, \ldots, p_s, q_1, \ldots, q_t \in P$ such that we have $v = \sum_{i=1}^s p_i g_i = \sum_{j=1}^t q_j h_j$. From this we get

$$v = yv + (1-y)v = p_1 y g_1 + \cdots + p_s y g_s + q_1(1-y)h_1 + \cdots + q_t(1-y)h_t \in U \cap P^r$$

Conversely, suppose we are given a vector $v \in U \cap P^r$. By definition of U, there exist polynomials $p_1, \ldots, p_s, q_1, \ldots, q_t \in P[y]$ such that we have $v = \sum_{i=1}^s p_i y g_i + \sum_{j=1}^t q_j(1-y)h_j$. Since $v \in P^r$, the element v is invariant under the substitution $y \mapsto 0$, i.e. we have $v = \sum_{i=1}^t q(x_1, \ldots, x_n, 0)h_i \in N$. Similarly, the element v is invariant under the substitution $y \mapsto 1$, i.e. we have $v = \sum_{i=1}^s p_i(x_1, \ldots, x_n, 1)g_i \in M$. Altogether, we get $v \in M \cap N$. $\quad\square$

Example 3.4.7. Let us redo the computation of the intersection of (x_1, x_2) and $(x_1^2 - x_2^2, x_1 x_2 x_3, x_3^2 - x_1)$ in $P = K[x_1, x_2, x_3]$ mentioned in Example 3.2.4. In the polynomial ring $P[y] = K[x_1, x_2, x_3, y]$, we consider the ideal $U = ((1-y)x_1, (1-y)x_2, y(x_1^2 - x_2^2), y(x_1 x_2 x_3), y(x_3^2 - x_1))$. The reduced Gröbner basis of this ideal with respect to $\mathtt{Elim(y)}$ is given by $\{x_1^2 - x_2^2, x_2 x_3^2 - x_1 x_2, x_1 x_3^2 - x_2^2, x_1 x_2 x_3, x_2^3, x_2 y - x_2, x_1 y - x_1, x_3^3 y - x_1\}$.

Since $x_2^3 = x_3(x_1 x_2 x_3) - x_2(x_1 x_3^2 - x_2^2)$, we can disregard the generator x_2^3, and the ideal $U \cap P$ equals $(x_1^2 - x_2^2, x_2 x_3^2 - x_1 x_2, x_1 x_3^2 - x_2^2, x_1 x_2 x_3)$, in agreement with the result obtained in Example 3.2.4.

A similar method can be used to compute the intersection of ℓ submodules $M_1, \dots, M_\ell$ of P^r simultaneously. In the case $\ell = 2$, it yields an alternative to the method explained in Proposition 3.4.6.

Proposition 3.4.8. *Let $\ell \geq 2$, and for every $i \in \{1, \dots, \ell\}$ let M_i be a P-submodule of P^r which is generated by a set of vectors $\{g_{i1}, \dots, g_{is_i}\}$. We choose new indeterminates $y_1, \dots, y_\ell$ and consider the $P[y_1, \dots, y_\ell]$-submodule U of $P[y_1, \dots, y_\ell]^r$ generated by*

$$\{y_i g_{ij} \mid 1 \leq i \leq \ell,\ 1 \leq j \leq s_i\} \cup \{(1 - y_1 - \dots - y_\ell)e_i \mid 1 \leq i \leq r\}$$

Then we have $M_1 \cap \dots \cap M_\ell = U \cap P^r$.

Proof. Let $v \in M_1 \cap \dots \cap M_\ell$. For $i = 1, \dots, \ell$, we choose $f_{i1}, \dots, f_{is_i} \in P$ such that $v = f_{i1}g_{i1} + \dots + f_{is_i}g_{is_i}$. Then we have

$$v = y_1 v + \dots + y_\ell v + (1 - y_1 - \dots - y_\ell)v$$

$$= \sum_{i=1}^{\ell} \sum_{j=1}^{s_i} f_{ij} y_i g_{ij} + (1 - y_1 - \dots - y_\ell)v \quad \in U \cap P^r$$

Conversely, given a vector $v \in U \cap P^r$, we can write it in the form $v = \sum_{i=1}^{\ell} \sum_{j=1}^{s_i} f_{ij} y_i g_{ij} + \sum_{k=1}^{r} h_k(1 - y_1 - \dots - y_\ell)e_k$ with polynomials $f_{ij}, h_k \in P[y_1, \dots, y_\ell]$. Let $i \in \{1, \dots, \ell\}$. Since $v \in P^r$, this vector is invariant under the substitution $y_j \mapsto \delta_{ij}$ for $j = 1, \dots, \ell$, where $\delta_{ij} = 0$ for $j \neq i$ and $\delta_{ii} = 1$. Therefore we get $v = \sum_{j=1}^{s_i} f_{ij}(x_1, \dots, x_n, \delta_{i1}, \dots, \delta_{i\ell})g_{ij} \in M_i$ for $i = 1, \dots, \ell$. $\square$

Finally, we indicate how one can use elimination to compute colon modules. A similar method can be used to find the annihilator of a module (see Exercise 11). Given a P-submodule $M \subseteq P^r$ and a new indeterminate y, we denote the $P[y]$-submodule of $P[y]^r$ generated by the elements of M by $MP[y]$.

Proposition 3.4.9. *Let M and N be submodules of P^r, let $\{g_1, \dots, g_s\}$ be a system of generators of M, and let $\{h_1, \dots, h_t\}$ be a system of generators of N.*

a) *Given a polynomial $f \in P$, we choose a new indeterminate y and let U be the $P[y]$-submodule of $P[y]^r$ generated by the set of polynomials $\{fyg_1, \ldots, fyg_s, (1-y)h_1, \ldots, (1-y)h_t\}$. Furthermore, we let $\{v_1, \ldots, v_u\}$ be a system of generators of the elimination module $U \cap P^r$. For $i = 1, \ldots, u$, we may write $v_i = fw_i$ for some $w_i \in M$. Then we have*

$$N :_M (f) = \langle w_1, \ldots, w_u \rangle$$

b) *Given an ideal $I = (f_1, \ldots, f_\ell)$ in P, we choose a new indeterminate y and consider the polynomial $f(y) = f_1 + f_2 y + \cdots + f_\ell y^{\ell-1}$ in $P[y]$. Then we have*

$$N :_M I = (NP[y] :_{MP[y]} (f(y))) \cap P^r$$

Proof. The first claim follows by combining Lemma 3.2.20 and Proposition 3.4.6. Now we prove claim b). For a vector $v \in M$ satisfying $f_i v \in N$ for $i = 1, \ldots, \ell$, we obviously have $f(y) v = (f_1 + \cdots + f_\ell y^{\ell-1}) v \in NP[y]$.

Conversely, let $v \in MP[y] \cap P^r$ be such that $f(y) v \in NP[y]$. Since, clearly, $MP[y] \cap P^r = M$, we actually have $v \in M$. We consider $P[y]$ as a polynomial ring in one indeterminate y over the ring P and equip it with the standard grading $\deg(y) = 1$. Then $NP[y]$ is a graded submodule of $P[y]^r$, because it is generated by homogeneous elements of degree zero (see Proposition 1.7.10). Thus $(f_1 + \cdots + f_\ell y^{\ell-1}) v \in NP[y]$ implies $f_i y^{i-1} v \in NP[y]$ for $i = 1, \ldots, \ell$. Next we write $f_i y^{i-1} v$ as an explicit $P[y]$-linear combination of the generators $\{h_1, \ldots, h_t\}$ of $NP[y]$ and perform the substitution $y \mapsto 1$. We obtain $f_i v \in N$ for $i = 1, \ldots, \ell$. Therefore we have $v \in N :_M I$. $\square$

Example 3.4.10. In Example 3.2.16 we computed the colon ideal $I :_P J$ in the ring $\mathbb{Q}[x_1, x_2, x_3]$, where $I = (x_2^3 - x_2^2 x_3 - x_1 x_2 + x_1 x_3,\ x_1 x_2^2 x_3 + x_2^2 x_3^2 - x_1^3 + x_1 x_2^2 - x_1^2 x_3 + x_2^2 x_3 - x_1 x_3^2 - x_1^2,\ x_2^2 x_3^3 - x_1^2 x_2 x_3 - x_1 x_3^3 + x_1^3 - x_1^2 x_3 + x_2 x_3^2)$ and $J = (x_2 - x_3,\ x_1^2 - x_3)$. Let us redo this computation with our new technique. We consider the ring $P[y] = K[x_1, x_2, x_3, y]$ and form the ideal $IP[y]$ and the polynomial $f(y) = (x_2 - x_3) + (x_1^2 - x_3)y$. Then we compute $IP[y] :_{P[y]} (f(y))$ using CoCoA and get a number of polynomials which are already contained in P and generate I.

In the following example we show a subtle feature of Proposition 3.4.9.b. Namely, we show that the inclusion $(N :_M I)P[y] \subseteq NP[y] :_{MP[y]} (f(y))$ can be strict even in the case where $M = P^r$. This contradicts a claim in [Ei95], Exercise 15.41.b.

Example 3.4.11. Over the polynomial ring $P = \mathbb{Z}/(101)[x_1, x_2, x_3, x_4]$, we consider the ideals $J = (x_1 x_3,\ x_2 x_4,\ x_1 x_4 + x_2 x_3)$ and $I = (x_3, x_4)$. We claim that $(J :_P I)P[y] \subset JP[y] :_{P[y]} (x_3 + x_4 y)$. If we compute $J :_P I$ with one of the above methods, we get $J :_P I = (x_1 x_2,\ x_1^2,\ x_1 x_3, x_1 x_4,\ x_2^2,\ x_2 x_3, x_2 x_4)$. On the other hand, $JP[y] :_{P[y]} (x_3 + x_4 y) = (x_1 x_2,\ x_1^2,\ x_1 x_3, x_1 x_4,\ x_2^2,\ x_2 x_3,\ x_2 x_4,\ x_2 y + x_1)$. Clearly, the polynomial $x_2 y + x_1$ is not contained in the ideal $(J :_P I)P[y]$.

Exercise 1. Consider the polynomial ring $P = K[x, y]$ over a field K. Prove that the only elimination ordering for $L = \{x\}$ is Lex.

Exercise 2. Consider the polynomial ring $P = K[x, y, z]$ over a field K. Describe at least two different elimination orderings for $L = \{z\}$.

Exercise 3. Let $\{x_1, \ldots, x_n\}$ be a set of indeterminates, and let $L \subseteq \{x_1, \ldots, x_n\}$. Find a matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$ such that $\mathrm{Ord}(V)$ is an elimination ordering for L on $\mathbb{T}^n$.

Exercise 4. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K and $I = (f)$ a principal ideal in P generated by a polynomial $f \in P \setminus \{0\}$. Moreover, let $L \subseteq \{x_1, \ldots, x_n\}$, and let $\widehat{P} = K[x_i \mid x_i \notin L]$. Show that we have $I \cap \widehat{P} = (0)$ if and only if $f \notin \widehat{P}$.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $t_1, \ldots, t_s \in \mathbb{T}^n$ be terms such that $t_1 >_{\text{Lex}} t_2 >_{\text{Lex}} \cdots >_{\text{Lex}} t_s$, and let I be the ideal in P generated by $\{t_1, \ldots, t_s\}$. Prove that we have $I \cap K[x_n] = (0)$ if and only if $t_s \notin K[x_n]$.

Exercise 6. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and let M be the P-submodule of P^n generated by $\{g_1, \ldots, g_n\}$, where $g_1 = (x_1, x_2, \ldots, x_n)$, where $g_2 = (x_n, x_1, \ldots, x_{n-1}), \ldots$, and where $g_n = (x_2, x_3, \ldots, x_n, x_1)$. Show that $M \cap K[x_2, \ldots, x_n]^n = (0)$.

Exercise 7. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $L \subseteq \{x_1, \ldots, x_n\}$, and let $\widehat{P} = K[x_i \mid x_i \notin L]$. Furthermore, let $I = (f_1, \ldots, f_r)$ be an ideal in P, and let A be the affine K-algebra P/I. Finally, let B be a residue class ring of $\widehat{P}$ such that the inclusion $\widehat{P} \subseteq P$ induces an injective K-algebra homomorphism $\varphi : B \longrightarrow A$.

$$
\begin{array}{ccc}
\widehat{P} & \longrightarrow & P \\
\downarrow & & \downarrow \\
B & \longrightarrow & A = P/I
\end{array}
$$

Explain how one can compute a set of generators of an ideal J in $\widehat{P}$ such that B is isomorphic to $\widehat{P}/J$.

Exercise 8. Let I be an ideal in a polynomial ring $P = K[x, y_1, \ldots, y_n]$ over a field K, and assume that $I \cap K[x] \neq (0)$. Let σ be an elimination ordering for $\{y_1, \ldots, y_n\}$, and let G be the reduced σ-Gröbner basis of I.
  a) Show that $G \cap K[x]$ consists of a single polynomial, say f.
  b) Prove that if I is a prime ideal, then f is irreducible.

Exercise 9. Use CoCoA to prove Heron's Formula.

Exercise 10. Use CoCoA to find the equations vanishing at the following parametrically defined curves.
  a) $\{(t^3, t^4, t^5) \mid t \in \mathbb{Q}\}$
  b) $\{(t, t^2, t^3) \mid t \in \mathbb{Q}\}$ (This is called the **twisted cubic curve**.)
  c) $\{(\frac{3t}{t^3+1}, \frac{3t^2}{t^3+1}) \mid t \in \mathbb{Q}\}$ (This is called the **folium of Descartes**.)

Exercise 11. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $r \geq 1$, let M be a P-submodule of P^r, let $\{g_1, \ldots, g_s\} \subseteq P^r$ be a system of generators of M, and let $v \in P^r$. We choose a new indeterminate y and consider the $P[y]$-submodule $U = \langle yg_1, \ldots, yg_s, (1-y)v \rangle$ of $P[y]^r$. Show that every element of a system of generators $\{h_1, \ldots, h_t\}$ of the elimination module $U \cap P^r$ is of the form $h_i = f_i v$ with $f_i \in P$ for $i = 1, \ldots, t$, and that the annihilator of the cyclic submodule $\langle v + M \rangle$ of P^r/M is the ideal $(f_1, \ldots, f_t)$.

Tutorial 34: Elimination of Module Components

In this section we studied module term orderings which had the property that if the leading term of an element did not involve certain indeterminates, then the whole element did not contain those indeterminates. Suppose we could consider also the canonical basis vectors $e_1, \ldots, e_r$ as "indeterminates". Then we could define a different kind of elimination ordering, namely one having the property that if the leading term of an element does not involve certain e_i, then the whole element does not contain a multiple of one of those e_i in its support.

More precisely, we introduce the following notion. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $r \geq 1$, and let $M \subseteq P^r$ be a P-submodule which is generated by a tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of vectors in P^r. Moreover, let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$, and let $L \subseteq \{1, \ldots, r\}$. The module term ordering σ is called a **component elimination ordering** for L if every element $m \in P^r \setminus \{0\}$ such that $\mathrm{LT}_\sigma(m) \in \bigoplus_{i \in \{1, \ldots, r\} \setminus L} Pe_i$ is contained in $\bigoplus_{i \in \{1, \ldots, r\} \setminus L} Pe_i$. The module $M \cap \bigoplus_{i \in \{1, \ldots, r\} \setminus L} Pe_i$ is called the **component elimination module** of M with respect to L.

In this tutorial we want to study component elimination orderings and show some of their applications. In particular, we shall see that they allow us to compute various operations in yet another way. For practical purposes, the methods explained here tend to be among the most efficient ones.

a) Let `To` be a term ordering on $\mathbb{T}^n$, let $i \in \{1, \ldots, r\}$, and let L be the set $\{1, \ldots, i\}$. Show that the module term ordering `PosTo` on $\mathbb{T}^n \langle e_1, \ldots, e_r \rangle$ (see Example 1.4.16.b) is a component elimination ordering for L.

b) State and prove a result for the restriction of σ to $\mathbb{T}^n \langle e_i \mid i \notin L \rangle$ which is analogous to Proposition 3.4.4.

c) Prove the following version of Theorem 3.4.5 for component elimination orderings.

Let $\widehat{P^r} = \bigoplus_{i \in \{1, \ldots, r\} \setminus L} Pe_i$, and let $\hat{\sigma}$ be the restriction of σ to the monomodule of terms in $\widehat{P^r}$.

a) We have $\mathrm{LT}_{\hat{\sigma}}(M \cap \widehat{P^r}) = \mathrm{LT}_\sigma(M) \cap \widehat{P^r}$.

b) For a σ-Gröbner basis G of M, the set $\widehat{G} = G \cap \widehat{P^r}$ is a $\hat{\sigma}$-Gröbner basis of the component elimination module $M \cap \widehat{P^r}$.

Hint: Use the canonical basis vectors $e_1, \ldots, e_r$ as indeterminates (see Exercise 10 in Section 1.4).

c) Consider the following block matrix of size $(r+s) \times s$.

$$\mathcal{U} = \begin{pmatrix} \mathcal{G} \\ \mathcal{I}_s \end{pmatrix}$$

Let U be the P-submodule of P^{r+s} generated by the columns of $\mathcal{U}$, let $L = \{1, \ldots, r\}$, and let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r, e_{r+1}, \ldots, e_{r+s} \rangle$ which is a component elimination ordering for L. Show that

$$U \cap \left(\bigoplus_{i=r+1}^{r+s} P e_i \right) \cong \mathrm{Syz}_P(\mathcal{G})$$

Hint: Consider a σ-Gröbner basis of U. Show that one can read off a σ-Gröbner basis of M and a σ-Gröbner basis of $\mathrm{Syz}_P(\mathcal{G})$.

d) Write a CoCoA function `CompElimSyz(...)` which takes the tuple $\mathcal{G}$ and uses the preceding method to compute a system of generators of the module $\mathrm{Syz}_P(\mathcal{G})$. Apply your function to compute Gröbner bases of the syzygy modules of the following tuples with respect to `PosDegRevLex` and `PosLex`.

1) $\mathcal{G} = (x^2, xy + y^2)$ in $\mathbb{Q}[x, y]^2$
2) $\mathcal{G} = ((x^2, x-y), (0, y), (xy, z))$ in $(\mathbb{Q}[x, y, z]^2)^3$
3) $\mathcal{G} = ((xy + y, x), (x - y, y), (x, x + y), (-x, y))$ in $(\mathbb{Q}[x, y]^2)^4$

e) Let N be another P-submodule of P^r, and let $\mathcal{H} = (h_1, \ldots, h_t)$ be a tuple of vectors which generate N. Consider the following block matrix of size $2r \times (s+t)$.

$$\mathcal{V} = \begin{pmatrix} \mathcal{G} & \mathcal{H} \\ 0 & \mathcal{H} \end{pmatrix}$$

Let V be the P-submodule of P^{2r} generated by the columns of $\mathcal{V}$, let $L = \{1, \ldots, r\}$, and let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_{2r} \rangle$ which is a component elimination ordering for L. Show that

$$V \cap \left(\bigoplus_{i=r+1}^{2r} P e_i \right) \cong M \cap N$$

Hint: Consider a σ-Gröbner basis of V. Show that one can read off a σ-Gröbner basis of $M + N$ and a σ-Gröbner basis of $M \cap N$.

f) Implement a CoCoA function `CompElimIntersection(...)` which takes tuples $\mathcal{G}$ and $\mathcal{H}$ generating P-submodules M and N of P^r and uses the preceding method to compute a system of generators of the intersection module $M \cap N$. Apply your function to compute the Gröbner bases of the intersection modules asked for in Tutorial 30.b with respect to `PosDegRevLex` and `PosLex`.

g) Given a vector $v \in P^r$, consider the following block matrix $\mathcal{W}$ of size $(r+1) \times (s+1)$.

$$\mathcal{W} = \begin{pmatrix} \mathcal{G} & v \\ 0 & 1 \end{pmatrix}$$

Let W be the P-submodule of P^{r+1} generated by the columns of $\mathcal{W}$, let L be the set $\{1, \ldots, r\}$, and let σ be a module term ordering on $\mathbb{T}^n \langle e_1, \ldots, e_r, e_{r+1} \rangle$ which is a component elimination ordering for L. Show that

$$W \cap Pe_{r+1} \cong M :_P \langle v \rangle$$

Hint: Consider a σ-Gröbner basis of W. Show that one can read off a σ-Gröbner basis of $M + \langle v \rangle$ and a σ-Gröbner basis of $M :_P \langle v \rangle$.

h) Write a CoCoA function `CompElimColon`(...) which takes the tuple $\mathcal{G}$ and a vector $v \in P^r$ and uses the preceding method to compute a system of generators of the colon ideal $M :_P \langle v \rangle$. Apply your function to compute Gröbner bases with respect to `PosDegRevLex` and `PosLex` of the colon ideals corresponding to the following cases (see Tutorial 31.d).

  1) $\mathcal{G}$ is a system of generators of the ideal $(x-1, y-1, z-1)^5$ and $v = (x+y+z-3)^3$ in $\mathbb{Q}[x,y,z]$
  2) $\mathcal{G}$ is a system of generators of the ideal $(x-1, y-1, z-1)^2 \cap (x,y,z)$ and $v = x$ in $\mathbb{Q}[x,y,z]$
  3) $\mathcal{G} = ((x,y),(y,x))$ and $v = (x^2, y^2)$ in $\mathbb{Q}[x,y]^2$

Tutorial 35: Projective Spaces and Graßmannians

In algebraic geometry, frequently a certain set of objects corresponds one-to-one to the set of points of another object. Some of the most important examples for this phenomenon will be introduced in this tutorial.

Let K be a field and V be a non-zero finite-dimensional K-vector space. For $v, v' \in V \setminus \{0\}$, we let $v \sim v'$ if and only if there exists an element $\lambda \in K \setminus \{0\}$ such that $v = \lambda v'$. It is easy to check that the relation $\sim$ is an equivalence relation. The set $(V \setminus \{0\})/\sim$ of its equivalence classes will be called the **projective space** associated to V and will be denoted by $\mathbb{P}(V)$.

In the special case $V = K^{n+1}$, we shall also say that $\mathbb{P}(V)$ is called the **n-dimensional projective space** over K, and we shall denote it by $\mathbb{P}^n_K$. The equivalence class of an element in V is called a **point** in $\mathbb{P}(V)$. If $(p_0, \ldots, p_n) \in K^{n+1} \setminus \{0\}$, then the point of $\mathbb{P}^n_K$ defined by its equivalence class will be denoted by $(p_0 : \ldots : p_n)$.

The set of equivalence classes of the non-zero elements of a 2-dimensional vector subspace of V will be called a **line** in $\mathbb{P}(V)$, and the set of equivalence classes of non-zero elements of an $(\dim(V)-1)$-dimensional vector subspace of V will be called a **hyperplane** in $\mathbb{P}(V)$.

a) Show that there is a bijection between $\mathbb{P}(V)$ and the set of 1-dimensional K-vector subspaces of V.

b) For every hyperplane $H \subseteq \mathbb{P}_K^n$, find a tuple $(a_0, \ldots, a_n) \in K^{n+1} \setminus \{0\}$ such that H is the set of all points $(p_0 : \ldots : p_n) \in \mathbb{P}_K^n$ which satisfy $a_0 p_0 + \cdots + a_n p_n = 0$. (First note that this condition is well-defined.) Moreover, prove that two tuples $(a_0, \ldots, a_n)$ and $(b_0, \ldots, b_n)$ give rise to the same hyperplane $H \subseteq \mathbb{P}_K^n$ in this way if and only if there exists an element $\lambda \in K \setminus \{0\}$ such that $(a_0, \ldots, a_n) = \lambda \cdot (b_0, \ldots, b_n)$.

c) Prove that any two distinct lines in $\mathbb{P}_K^2$ meet at a unique point.

d) Let $\mathrm{Hyp}(\mathbb{P}_K^n)$ be the set of all hyperplanes of $\mathbb{P}_K^n$. Show that one can define a map $\eta : \mathrm{Hyp}(\mathbb{P}_K^n) \longrightarrow \mathbb{P}_K^n$ by using b) to map H to the point $(a_0 : \ldots : a_n)$. Prove that the map η is bijective. Thus we can view the set $\mathrm{Hyp}(\mathbb{P}_K^n)$ as an n-dimensional projective space over K. It is called the **dual projective space** and sometimes denoted by $(\mathbb{P}_K^n)^{\check{}}$.

e) Show that the set of all elements of $(\mathbb{P}_K^n)^{\check{}}$ which correspond to hyperplanes passing through the point $(0 : \ldots : 0 : 1)$ is a hyperplane in $(\mathbb{P}_K^n)^{\check{}}$.

f) Let p be a prime number and $K = \mathbb{F}_p$. Write a CoCoA function `Hyperplanes(...)` which takes a point $(p_0 : \ldots : p_n) \in \mathbb{P}_K^n$ and computes the list of all tuples $(a_0, \ldots, a_n) \in K^{n+1}$ which correspond to the hyperplanes passing through the point.

g) Use your CoCoA function `Hyperplanes(...)` to compute the lines passing through each of the following points $\mathcal{P} \in \mathbb{P}_K^2$, where $K = \mathbb{F}_3$.

    1) $\mathcal{P} = (0 : 0 : 1)$
    2) $\mathcal{P} = (0 : 1 : 1)$
    3) $\mathcal{P} = (1 : 1 : 1)$

After having seen that the set of 1-dimensional K-vector subspaces of K^{n+1} can be identified with the set of points of the n-dimensional projective space over K, we now turn our attention to the set of $(m+1)$-dimensional K-vector subspaces of K^{n+1}, where $1 \le m < n$. We start with the first nontrivial case $m = 1$ and $n = 3$.

h) Explain how one can identify the set of all 2-dimensional K-vector subspaces of K^4 with the set $\mathrm{Lin}(\mathbb{P}_K^3)$ of lines in $\mathbb{P}_K^3$.

i) Now we define a map

$$\varphi : \ \mathrm{Lin}(\mathbb{P}_K^3) \ \longrightarrow \ \mathbb{P}_K^5$$

as follows. Every line $L \in \mathrm{Lin}(\mathbb{P}_K^3)$ corresponds to a 2-dimensional vector subspace V of K^4. We choose a K-basis of V and represent it as a 4×2-matrix

$$\mathcal{V} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \\ a_{41} & a_{42} \end{pmatrix}$$

with entries in K. Then we form the 6-tuple $(d_{12}, d_{13}, d_{14}, d_{23}, d_{24}, d_{34})$ of the 2×2-minors of $\mathcal{V}$. Each minor is specified by choosing two rows, i.e. by a pair of indices (i, j) such that $1 \le i < j \le 4$. We order the minors by ordering the pairs of indices decreasingly with respect to the lexicographic ordering on $\mathbb{N}^2$. Finally, we let $\varphi(L) = (d_{12} : d_{13} : d_{14} : d_{23} : d_{24} : d_{34})$. Prove that the map φ is well-defined and injective. The image of the map φ is called the **Graßmannian** of lines in $\mathbb{P}_K^3$ and is denoted by $\mathrm{Grass}_1(\mathbb{P}_K^3)$.

Hint: Show that we can assume $d_{12} \ne 0$ without loss of generality. Then prove that there exists a basis of V such that the corresponding matrix has the shape

$$\mathcal{V}' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a_{31} & a_{32} \\ a_{41} & a_{42} \end{pmatrix}$$

j) Show how one can extend the preceding results in order to define the **Graßmannian** $\mathrm{Grass}_m(\mathbb{P}_K^n)$ of m-dimensional subspaces of $\mathbb{P}_K^n$ for every $m \in \{1, \ldots, n-1\}$.

Hint: For every $(m+1)$-dimensional K-vector subspace of K^{n+1}, there exists a basis such that its associated matrix has the shape

$$\mathcal{V} = \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & & \cdots & 0 & 1 \\ a_{m+2\,1} & a_{m+2\,2} & \cdots & & a_{m+2\,m+1} \\ \vdots & \vdots & & & \vdots \\ a_{n+1\,1} & a_{n+1\,2} & \cdots & & a_{n+1\,m+1} \end{pmatrix}$$

The $(m+1) \times (m+1)$-minors of such a matrix are specified by the tuples $(i_1, \ldots, i_{m+1})$ of indices of chosen rows, where we assume that these indices are ordered by $1 \le i_1 < \cdots < i_{m+1} \le n+1$. Again we order those tuples decreasingly with respect to `Lex` and get an injective map of the set of $(m+1)$-dimensional K-vector subspaces of K^{n+1} to $\mathbb{P}_K^N$, where $N = \binom{n+1}{m+1} - 1$.

The final part of this tutorial is devoted to describing the Graßmannian $\mathrm{Grass}_m(\mathbb{P}_K^n)$ in more detail. In Volume 2 we shall introduce the notion of a projective variety as the set of zeros of a homogeneous ideal. In fact, Graßmannians are projective varieties. For the time being, we shall be content with finding some equations which vanish on the points of $\mathrm{Grass}_m(\mathbb{P}_K^n)$. This amounts to finding algebraic relations among the $(m+1) \times (m+1)$-minors of an $(n+1) \times (m+1)$-matrix.

k) Let us consider again the case $m = 1$ and $n = 3$. Show that the minors of size 2×2 of the matrix $\mathcal{V}'$ above are algebraically related by the

polynomial equation

$$d_{12}d_{34} - d_{13}d_{24} + d_{14}d_{23} = 0$$

l) Still in the case $m = 1$ and $n = 3$, consider the 2×2-minors $d_{12}, \ldots, d_{34}$ of the original matrix $\mathcal{V}$. In order to find the algebraic relations among these minors, we form the polynomial ring

$$P = K[d_{12}, d_{13}, d_{14}, d_{23}, d_{24}, d_{34}, a_{11}, a_{21}, a_{31}, a_{41}, a_{12}, a_{22}, a_{32}, a_{42}]$$

in 14 indeterminates over K. Define a suitable ideal $I \subseteq P$ such that the elimination ideal $I \cap K[d_{12}, d_{13}, d_{14}, d_{23}, d_{24}, d_{34}]$ is the desired ideal of algebraic relations. Write a CoCoA function which computes this elimination ideal, and show that it is principal.

m) More generally, for any $m \in \{1, \ldots, n\}$, the ideal of algebraic relations among the minors of size $(m+1) \times (m+1)$ of a matrix $\mathcal{V} = (a_{ij})$ of size $(n+1) \times (m+1)$ is called the ideal of **Plücker relations**. Implement a CoCoA function `Pluecker(...)` which takes m and n as input and computes a set of generators for the ideal of Plücker relations.

   Hint: Assume that the base ring has $\binom{n+1}{m+1}$ indeterminates. Then form a larger polynomial ring having $\binom{n+1}{m+1} + (m+1)(n+1)$ indeterminates, apply the CoCoA command `Minors(...)` appropriately, and transport the result of your computation back to the original ring using a suitable ring map.

Tutorial 36: Diophantine Systems and Integer Programming

Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a matrix having m rows, n columns, and integer entries. Furthermore, let $(b_1, \ldots, b_m) \in \mathbb{Z}^m$ be a vector having m integer entries, and let $z_1, \ldots, z_n$ be indeterminates. Our first goal in this tutorial is to study the set of non-negative integer solutions of the following **system of Diophantine inequalities**.

$$\begin{cases} a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n & \leq & b_1 \\ a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n & \leq & b_2 \\ \quad\vdots & \vdots & \vdots \\ a_{m1}z_1 + a_{m2}z_2 + \cdots + a_{mn}z_n & \leq & b_m \end{cases}$$

a) As a first step, we convert the above system of inequalities into a system of equations in the following way. We introduce new indeterminates $z_{n+1}, \ldots, z_{n+m}$ and consider the associated **system of Diophantine equations**

$$\begin{cases} a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n + z_{n+1} & = & b_1 \\ a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n + z_{n+2} & = & b_2 \\ \quad\vdots & \vdots & \vdots \\ a_{m1}z_1 + a_{m2}z_2 + \cdots + a_{mn}z_n + z_{n+m} & = & b_m \end{cases}$$

Prove that there is a one-to-one correspondence between the set of all solutions $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ of the above system of Diophantine inequalities and the set of non-negative integer solutions $(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_{n+m})$ in $\mathbb{N}^{n+m}$ of the associated system of Diophantine equations.

In view of this result, we shall from now on assume that our original system is in fact a system of Diophantine equations, i.e. that we want to find the non-negative integer solutions $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ of the system

$$\begin{cases} a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n &=& b_1 \\ a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n &=& b_2 \\ & \vdots & \vdots \;\; \vdots \\ a_{m1}z_1 + a_{m2}z_2 + \cdots + a_{mn}z_n &=& b_m \end{cases}$$

which we shall denote by $\mathcal{S}$.

For our next step in the solution process, we need some additional definitions. Let $y_1, \ldots, y_m$ be further indeterminates. A product of the form $y_1^{i_1} \cdots y_m^{i_m}$, where we have $(i_1, \ldots, i_m) \in \mathbb{Z}^m$, is called an **extended term** in the indeterminates $y_1, \ldots, y_m$. The set of all extended terms will be denoted by $\mathbb{E}^m$. It is clearly a monoid with respect to multiplication.

Now let K be a field. An expression of the form

$$f = \sum_{(i_1, \ldots, i_m) \in \mathbb{Z}^m} c_{(i_1, \ldots, i_m)}\, y_1^{i_1} \cdots y_m^{i_m}$$

where only finitely many elements $c_{(i_1, \ldots, i_m)} \in K$ are different from zero, is called a **Laurent polynomial** in the indeterminates $y_1, \ldots, y_m$. The set of all Laurent polynomials is clearly a K-algebra and will be denoted by $L = K[y_1, \ldots, y_m, y_1^{-1}, \ldots, y_m^{-1}]$.

b) Prove that the map $\log : \mathbb{E}^m \longrightarrow \mathbb{Z}^m$ defined by $y_1^{i_1} \cdots y_m^{i_m} \mapsto (i_1, \ldots, i_m)$ is an isomorphism of groups.

c) Prove that a tuple $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is a solution of $\mathcal{S}$ if and only if the following equations hold in L.

$$\begin{cases} y_1^{a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n} &=& y_1^{b_1} \\ y_2^{a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n} &=& y_2^{b_2} \\ & \vdots & \vdots \;\; \vdots \\ y_m^{a_{m1}\alpha_1 + a_{m2}\alpha_2 + \cdots + a_{mn}\alpha_n} &=& y_m^{b_m} \end{cases}$$

d) Prove that a tuple $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is a solution of $\mathcal{S}$ if and only if the following equation holds in L.

$$y_1^{a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n} \cdots y_m^{a_{m1}\alpha_1 + a_{m2}\alpha_2 + \cdots + a_{mn}\alpha_n} = y_1^{b_1} \cdots y_m^{b_m}$$

e) For $i = 1, \ldots, n$, we define the extended term $t_i = y_1^{a_{1i}} y_2^{a_{2i}} \cdots y_m^{a_{mi}}$. (Notice that its exponents correspond to the ith column of the matrix $\mathcal{A}$.)

Prove that a tuple $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is a solution of $\mathcal{S}$ if and only if the following equation holds in L.

$$t_1^{\alpha_1} \cdots t_n^{\alpha_n} = y_1^{b_1} \cdots y_m^{b_m}$$

Conclude that there exists a solution of $\mathcal{S}$ in $\mathbb{N}^n$ if and only if the extended term $y_1^{b_1} \cdots y_m^{b_m}$ is an element of the K-subalgebra $K[t_1, \ldots, t_n]$ of L.

In the second part of this tutorial, we try to apply the knowledge acquired above for solving the **integer programming problem** in a special case. For this, we shall from now on assume that the entries of the matrix $\mathcal{A}$ and the vector $b = (b_1, \ldots, b_m)$ are non-negative integers. Moreover, we suppose that we are given a non-zero tuple $(c_1, \ldots, c_n) \in \mathbb{N}^n$ of natural numbers.

The map $C : \mathbb{N}^n \longrightarrow \mathbb{N}$ defined by $(\alpha_1, \ldots, \alpha_n) \mapsto c_1\alpha_1 + \cdots + c_n\alpha_n$ is called the **linear cost function** associated to $(c_1, \ldots, c_n)$. The integer programming problem $\mathrm{IP}(\mathcal{A}, b, C)$ asks for those solutions of the system $\mathcal{S}$ for which the cost function C is minimal.

In the sequel, let $\{x_1, \ldots, x_n\}$ be new indeterminates, let Q be the ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, let $J = (x_1 - t_1, \ldots, x_n - t_n) \subseteq Q$, and let σ be an elimination ordering for $\{y_1, \ldots, y_m\}$ on $\mathbb{T}(x_1, \ldots, x_n, y_1, \ldots, y_m)$.

f) Show that $\mathrm{NF}_{\sigma, J}(y_1^{b_1} \cdots y_m^{b_m})$ is a term (see Exercise 5 of Section 2.5).
g) Prove that $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is a solution of $\mathcal{S}$ if and only if the polynomial $y_1^{b_1} \cdots y_m^{b_m} - x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is contained in J.
   Hint: Show that $t_1^{\alpha_1} \cdots t_n^{\alpha_n} \equiv x_1^{\alpha_1} t_2^{\alpha_2} \cdots t_n^{\alpha_n} \equiv \cdots \equiv x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ modulo J.
h) Prove that the system $\mathcal{S}$ has solutions if and only if $\mathrm{NF}_{\sigma, J}(y_1^{b_1} \cdots y_m^{b_m})$ is contained in the subring $K[x_1, \ldots, x_n]$ of Q.
i) Write a CoCoA function `IsSolvable`(...) which takes $\mathcal{A}$ and $(b_1, \ldots, b_m)$ and decides whether the corresponding system $\mathcal{S}$ is solvable.
j) Use your function `IsSolvable`(...) to check whether the following systems of Diophantine equations are solvable.

1)
$$\begin{pmatrix} 3 & 1 & 11 & 2 & 3 \\ 4 & 5 & 0 & 1 & 7 \\ 5 & 6 & 1 & 9 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} = \begin{pmatrix} 20 \\ 17 \\ 23 \end{pmatrix}$$

2)
$$\begin{pmatrix} 3 & 1 & 11 & 2 & 3 \\ 4 & 5 & 0 & 1 & 7 \\ 5 & 6 & 1 & 9 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} = \begin{pmatrix} 20 \\ 17 \\ 21 \end{pmatrix}$$

3)
$$\begin{pmatrix} 3 & 1 & 11 & 2 & 3 & 5 & 3 \\ 4 & 5 & 0 & 1 & 7 & 4 & 6 \\ 5 & 6 & 1 & 9 & 2 & 3 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_7 \end{pmatrix} = \begin{pmatrix} 31 \\ 27 \\ 38 \end{pmatrix}$$

k) Implement a CoCoA function `DioSysSolve`(...) which takes a matrix $\mathcal{A}$ and a tuple $(b_1, \ldots, b_m)$ such that the corresponding system $\mathcal{S}$ is solvable and uses the above results to find a solution of $\mathcal{S}$.

l) Use your function `DioSysSolve`(...) to find explicit solutions for those systems of Diophantine equations above which are solvable.

m) Find an elimination ordering σ for the set of indeterminates $\{y_1, \ldots, y_m\}$ on $\mathbb{T}(x_1, \ldots, x_n, y_1, \ldots, y_m)$ such that the restriction $\hat{\sigma}$ of σ to the monoid of terms $\mathbb{T}(x_1, \ldots, x_n)$ is **cost compatible**. By this we mean that $\hat{\sigma}$ has the property that whenever $C(\alpha_1, \ldots, \alpha_n) > C(\beta_1, \ldots, \beta_n)$ for two tuples $(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, then we have the inequality $x_1^{\alpha_1} \cdots x_n^{\alpha_n} >_{\hat{\sigma}} x_1^{\beta_1} \cdots x_n^{\beta_n}$.

n) Write a CoCoA function `CcOrd`(...) which takes $(c_1, \ldots, c_n) \in \mathbb{N}^n \setminus \{0\}$ and computes a matrix $V \in \mathrm{Mat}_{m+n}(\mathbb{Z})$ such that the associated term ordering $\mathrm{Ord}(V)$ is an elimination ordering for $\{y_1, \ldots, y_m\}$ whose restriction to $\mathbb{T}(x_1, \ldots, x_n)$ is cost-compatible.

o) Let σ be an elimination ordering for $\{y_1, \ldots, y_m\}$ whose restriction to $\mathbb{T}(x_1, \ldots, x_n)$ is cost-compatible. Assume that the system $\mathcal{S}$ has solutions, i.e. that there exist numbers $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ such that we have $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = \mathrm{NF}_{\sigma, J}(y_1^{b_1} \cdots y_m^{b_m})$. Then show that

$$C(\alpha_1, \ldots, \alpha_n) = \min\{C(\beta_1, \ldots, \beta_n) \,|\, (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n \text{ is a solution of } \mathcal{S}\}$$

In other words, the tuple $(\alpha_1, \ldots, \alpha_n)$ is a solution of the integer programming problem $\mathrm{IP}(\mathcal{A}, b, C)$.

p) Write a CoCoA function `IPSolve`(...) which takes $\mathcal{A}$, $(b_1, \ldots, b_m)$, and $(c_1, \ldots, c_n)$, checks whether the corresponding system $\mathcal{S}$ is solvable, and computes a solution of the integer programming problem $\mathrm{IP}(\mathcal{A}, b, C)$ in that case.

q) Use your function `IPSolve`(...) to solve the following integer programming problems.

   1) $\mathcal{A}$ and b as in j1), $(c_1, \ldots, c_5) = (23, 15, 6, 7, 1)$
   2) $\mathcal{A}$ and b as in j3), $(c_1, \ldots, c_7) = (23, 15, 67, 1, 53, 4, 22)$

3.5 Localization and Saturation

> *All generalizations are dangerous,*
> *even this one.*
> (Alexandre Dumas jr.)

In the previous sections, we saw several ways to compute colon ideals and colon modules. Let us apply our knowledge in an easy case. Suppose we are given the ideal $I = (x^2,\ xy^2,\ y^3z^4)$ in the polynomial ring $P = K[x, y, z]$ over a field K. When we compute the colon ideal $I : (y)$, we get $(x^2,\ xy,\ y^2z^4)$. When we compute $I : (y^2)$ instead, we get $I : (y^2) = (x,\ yz^4)$. Continuing this way, we find $I : (y^3) = (x,\ z^4)$, and it is easy to see that $I : (y^d) = (x,\ z^4)$ for every $d \geq 3$.

What conclusions can we draw from this example? First of all, we observe the phenomenon that the process of forming $I : (y^d)$ for $d = 1, 2, 3, \ldots$ stabilizes after a while. This leads to a new ideal which is called the *saturation* of I with respect to (y) and is denoted by $I : (y)^\infty$. In the case we just looked at, the ideal $I : (y)^\infty$ is generated by $\{x, z^4\}$.

But there is more to see. Suppose we could consider y as an invertible element. Then, clearly, the ideal I would be equal to the ideal generated by $\{x, z^4\}$. Two completely different approaches lead to the same result. A chain of colon ideals stabilizes exactly at the ideal which could be obtained by considering one element as invertible. Although it may appear to be dangerous to draw such general conclusions from such an easy example, this is not a coincidence. Rather, it is a special case of an algebraic process which we study in the first part of this section.

To do that, we need to make a brief detour in order to introduce *localization*. Localization allows us to consider some elements of a ring as invertible. Everybody is familiar with the operation of inverting all non-zero integers in order to get the field of rational numbers. Localization is a far-reaching generalization of this process to arbitrary rings, to arbitrary multiplicatively closed sets of elements which are to be inverted, and to arbitrary modules over those rings. We can even divide by zero! (If this looks like localization could turn into a nightmare, take solace in the fact that localizing in zero makes a module vanish.)

Since you know our style by now, it is clear that we are not going to treat the subject of localization in the style of *Bourbaki*. Instead, we content ourselves with pointing out one aspect which is relevant from the computational point of view. The localization of a ring R at one element can be represented as a residue class ring of $R[y]$ (see Proposition 3.5.6).

In the second subsection, we generalize the above example and define the saturation of a module N by an ideal I in another module M. As for colon modules, we immediately reduce the computation of saturations to the case of submodules of P^r, where P is a polynomial ring over a field. Generalizing the above example again, it turns out that the saturation of a module is the

limit of a suitable family of colon modules (see Proposition 3.5.9). This gives us a first naïve method for computing saturations.

More sophisticated methods can be derived from the link between saturations and localizations provided by Proposition 3.5.11. It says that the saturation with respect to a principal ideal can also be obtained by extending the module to the localization at the generating element and then contracting it back. Our main Theorem 3.5.13 offers several approaches to the computation of saturations based on this idea.

The most important uses of saturation calculations are for more advanced tasks such as computing primary decompositions (see Tutorial 43), local cohomology modules, and the defining ideals of projective algebraic varieties or schemes. At the end of the current section, we solve a more modest problem and show how to solve the *radical membership* problem (see Corollary 3.5.15).

After saturating you with promises, let us get going and do some real mathematics!

3.5.A   Localization

In this subsection we let R be a commutative ring and M an R-module.

Definition 3.5.1. A subset $S \subseteq R$ is called **multiplicatively closed** if $1_R \in S$ and the product of any two elements of S is again contained in S.

For instance, a multiplicatively closed set is obtained by taking an element $f \in R$ and considering the set of its powers $S = \{f^i \mid i \in \mathbb{N}\}$. Another common example occurs when R is an integral domain. Then $S = R \setminus \{0\}$ is a multiplicatively closed subset of R. In this case, we have already made use of the field of fractions of R, i.e. the field consisting of the fractions $\frac{r}{s}$, where $r \in R$ and $s \in S$.

Given a multiplicatively closed subset S of an arbitrary commutative ring R, the process of forming the field of fractions of a domain can be generalized as follows.

Proposition 3.5.2. *Let R be a commutative ring, let M be an R-module, and let S be a multiplicatively closed subset of R. We consider the set of pairs $\{(m, s) \mid m \in M, \ s \in S\}$. For two such pairs $(m, s), (m', s')$, we let $(m, s) \sim (m', s')$ if and only if there exists an element $s'' \in S$ such that $s''(sm' - s'm) = 0$.*

a) *The relation $\sim$ is an equivalence relation.*

b) *Let us denote the set of all equivalence classes by M_S and the equivalence class of a pair (m, s) by $\frac{m}{s}$. Then the rules*

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \qquad and \qquad r \cdot \frac{m}{s} = \frac{rm}{s}$$

for all $r \in R$, for all $m, m' \in M$, and for all $s, s' \in S$ make M_S into an R-module.

c) *The map $M \longrightarrow M_S$ defined by $m \longmapsto \frac{m}{1}$ is R-linear.*

d) *For $r, r' \in R$, for $m \in M$, and for $s, s' \in S$, the rules*

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'} \qquad \text{and} \qquad \frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'}$$

make R_S into a ring and M_S into an R_S-module.

Proof. Since the relation $\sim$ is clearly reflexive and symmetric, it suffices to show that it is transitive. Suppose that $(m, s) \sim (m', s') \sim (m'', s'')$, i.e. that there exist elements $t, u \in S$ such that we have $t(sm' - s'm) = 0$ and $u(s'm'' - s''m') = 0$. Then $tuss''m' = tus's''m$ and $tuss''m' = tuss'm''$. This implies $tus'(sm'' - s''m) = 0$, and therefore $(m, s) \sim (m'', s'')$. Thus claim a) is proved. The remaining claims follow from the observation that the stated rules and maps are independent of the choice of representatives of the involved equivalence classes. □

In particular, part c) of this proposition says that the map $R \longrightarrow R_S$ defined by $r \mapsto \frac{r}{1}$ is an R-algebra homomorphism. Clearly, the R_S-module M_S is generated by the elements in the image of the canonical map $M \longrightarrow M_S$.

Definition 3.5.3. In the situation of the proposition, the R_S-module M_S is called the **localization** of M at S or the **module of fractions** of M with respect to S.

Some authors use the notation $S^{-1}M$ or $M[S^{-1}]$ for the module of fractions M_S. If the multiplicatively closed set S is of the form $S = \{f^i \mid i \in \mathbb{N}\}$ with an element $f \in R$, we shall write M_f instead of M_S and speak of the localization of M at the element f.

Using the definition of $\sim$, it follows immediately that an element $m \in M$ maps to $\frac{m}{1} = 0$ in M_S if and only if $sm = 0$ for some $s \in S$. For a finitely generated R-module M, we can then see that $M_S = 0$ is equivalent to $\text{Ann}_R(M) \cap S \neq \emptyset$. In particular, we have $M_S = 0$ if $0 \in S$.

Example 3.5.4. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and let S be the set of polynomials with non-zero constant term. Then S is a multiplicatively closed subset of P, and the ring P_S consists of those rational functions which are defined at the point $(0, \ldots, 0)$.

More generally, let $\mathfrak{p}$ be a prime ideal in R. Then the set $S = R \setminus \mathfrak{p}$ is a multiplicatively closed subset of R, and we can form the ring R_S. In commutative algebra, this ring is usually denoted by $R_{\mathfrak{p}}$. In algebraic geometry, it is related to the ring of germs of functions at a point of a certain topological space. This is the reason why it is called the localization of R at $\mathfrak{p}$.

Our next objective is to understand the concept of localization at an element in a different way. The following auxiliary result will prove useful for this purpose. For a more general version, look at Exercise 5.

Proposition 3.5.5. (Extended Division)
Let R be a ring, let $f \in R$, let y be a new indeterminate, and let $g(y)$ be a non-zero polynomial in $R[y]$. Then there exist a polynomial $q(y) \in R[y]$ and an element $r \in R$ such that

$$f^{\deg(g)} g(y) = q(y) \cdot (fy - 1) + r$$

Proof. Writing $g(y) = \sum_{i=0}^{\gamma} c_i y^i$ with $\gamma = \deg(g) \in \mathbb{N}$ and $c_0, \dots, c_\gamma \in R$, we see that the polynomial $f^\gamma g(y) = \sum_{i=0}^{\gamma} f^{\gamma-i} c_i (fy)^i \in R[y]$ is of the form $\tilde{g}(fy)$ with a polynomial $\tilde{g}(y) \in R[y]$. Next, we substitute $y + 1$ for y and decompose $\tilde{g}(y+1)$ in the form $\tilde{g}(y+1) = \tilde{q}(y) \cdot y + r$, where $\tilde{q}(y) \in R[y]$ and $r \in R$. After we perform the substitution $y \mapsto fy - 1$, this equation becomes

$$f^\gamma g(y) = \tilde{g}(fy) = \tilde{q}(fy - 1) \cdot (fy - 1) + r = q(y) \cdot (fy - 1) + r$$

with $q(y) = \tilde{q}(fy - 1) \in R[y]$, as desired. $\square$

Proposition 3.5.6. *Let R be a ring, let $f \in R \setminus \{0\}$, and let y be a new indeterminate. Then there exists an isomorphism of R-algebras*

$$R_f \cong R[y]/(fy - 1)$$

Proof. The R-algebra homomorphism $\varphi : R[y] \longrightarrow R_f$ defined by $y \mapsto \frac{1}{f}$ is clearly surjective and satisfies $fy - 1 \in \mathrm{Ker}(\varphi)$. Suppose $g(y) \in \mathrm{Ker}(\varphi) \setminus \{0\}$. Using Extended Division 3.5.5, we find a representation $f^\gamma g(y) = q(y) \cdot (fy - 1) + r$, where $\gamma = \deg(g)$, where $q(y) \in R[y]$, and where $r \in R$. By applying the map φ, we get the equation $r = f^\gamma g(\frac{1}{f}) = 0$ in R_f, because we started with $g(y) \in \mathrm{Ker}(\varphi)$. Thus there exists an $i > 0$ such that $f^i r = 0$. Consequently, $f^{\gamma+i} g(y) = f^i q(y)(fy - 1)$ implies

$$\begin{aligned}
g(y) &= f^{\gamma+i} y^{\gamma+i} g(y) - (f^{\gamma+i} y^{\gamma+i} - 1) g(y) \\
&= f^i y^{\gamma+i} q(y) \cdot (fy - 1) - (f^{\gamma+i-1} y^{\gamma+i-1} + f^{\gamma+i-2} y^{\gamma+i-2} + \dots + 1) \\
&\quad \cdot (fy - 1) \cdot g(y) \\
&\in (fy - 1)
\end{aligned}$$

and therefore $\mathrm{Ker}(\varphi) = (fy - 1)$. $\square$

Of course this is only a very small portion of what can be said about the concept of localization. But for the time being, it is enough for us to understand the connection to saturation which follows now.

3.5.B   Saturation

The following definition of the saturation of a module by an ideal resembles the definition of the colon module. But there is one important difference: for each element $m \in M$, we may have to choose a different exponent i such that $I^i m \subseteq N$, and there is no a priori bound on those exponents.

Definition 3.5.7. Let R be a commutative ring, let I be an ideal in R, let U be an R-module, and let M and N be two R-submodules of U. Then the set

$$N :_M I^\infty = \bigcup_{i \in \mathbb{N}} N :_M I^i = \{m \in M \mid I^i \cdot m \subseteq N \text{ for some } i \in \mathbb{N}\}$$

is an R-submodule of M. It is called the **saturation** of N by I in M.

In this subsection we want to provide the reader with some explicit methods for computing saturations of finitely generated modules over affine algebras. As usual, we let K be a field and $P = K[x_1, \ldots, x_n]$ a polynomial ring over K. With the following result we reduce the general problem of computing saturations to the case of submodules of a finitely generated free P-module. The procedure is completely analogous to the one we followed in Proposition 3.2.18, and the proof is also the same.

Proposition 3.5.8. *Let J be an ideal in P, let U be a finitely generated module over the affine K-algebra P/J, and let M and N be P/J-submodules of U. Furthermore, let I be an ideal in P containing J. Our goal is to compute $N :_M (I/J)^\infty$.*

Suppose we are given a presentation $U \cong P^r/V$ with a P-submodule V of P^r. We can write $M = M'/V$ and $N = N'/V$ with P-submodules M' and N' of P^r containing V. Then $N :_M (I/J)^\infty$ is the residue class module of $N' :_{M'} I^\infty$ in U.

Again, as a consequence of this proposition, we shall from now on consider only the case of submodules M and N of P^r for some $r \geq 0$, and of an ideal $I \subseteq P$. The following naïve method for computing $N :_M I^\infty$ frequently works well in practice, although it requires the computation of an a priori unknown number of Gröbner bases.

Proposition 3.5.9. *For some number $i \in \mathbb{N}$ we have $N :_M I^i = N :_M I^{i+1}$. If we let $\mu = \min\{i \in \mathbb{N} \mid N :_M I^i = N :_M I^{i+1}\}$, then*

$$N :_M I^\infty = N :_M I^\mu = N :_M I^{\mu+1} = \cdots$$

Proof. For $m \in M$ such that $I^i m \subseteq N$ for some $i \geq 0$, we obviously have $I^{i+1}m \subseteq N$. Thus there is a chain $N :_M I \subseteq N :_M I^2 \subseteq \cdots \subseteq M$ which becomes stationary after a while, because M is a Noetherian P-module by Hilbert's Basis Theorem 2.4.6. This prove the first claim.

Now we assume that $N :_M I^i = N :_M I^{i+1}$ for some $i \geq 0$, and we let $m \in N :_M I^{i+2}$. Since $I^{i+2}m \subseteq N$, we get $I^{i+1}fm \subseteq N$ for all $f \in I$, and therefore $I^i fm \subseteq N$. Thus we have shown $N :_M I^{i+2} \subseteq N :_M I^{i+1}$, and since the other inclusion holds trivially, we find $N :_M I^{i+2} = N :_M I^{i+1}$. Inductively, we obtain $N :_M I^i = N :_M I^j$ for all $j \geq i$. In view of the above chain of submodules, this finishes the argument. $\square$

Notice that we have $N :_M I^{i+1} = (N :_M I^i) :_M I$, so that we can compute the colon modules required by this proposition also by repeatedly taking the colon module by I.

Example 3.5.10. Let I be the ideal $(x_1^2 x_2 - 2x_1 x_2^2 + x_2^3, x_1^3 - 3x_1 x_2^2 + 2x_2^3, x_1 x_2^2 x_3 - x_2^3 x_3^2 - x_1 x_3^2 + x_2^4, x_2^3 x_3^4 - 2x_2^4 x_3^2 + x_2^5)$ in the polynomial ring $P = \mathbb{Q}[x_1, x_2, x_3]$. Suppose we want to determine $I :_P (x_2)^\infty$.

When we compute $I_1 = I :_P (x_2)$, we get $I_1 = (x_1^2 - 2x_1 x_2 + x_2^2, x_1 x_2 x_3^2 - x_2^2 x_3^2 - x_1 x_3^2 + x_2^3, x_2^2 x_3^4 - 2x_2^3 x_3^2 + x_2^4)$. Then we can check that $I \subset I_1$. Thus we have to compute $I_2 = I_1 :_P (x_2)$ next. We get $I_2 = (x_1^2 - 2x_1 x_2 + x_2^2, x_1 x_3^2 - x_2 x_3^2 - x_1 x_2 + x_2^2, x_2 x_3^4 - 2x_2^2 x_3^2 + x_2^3)$. Again we can check that $I_1 \subset I_2$. Continuing this way, we calculate $I_3 = I_2 :_P (x_2) = (x_1^2 - 2x_1 x_2 + x_2^2, x_1 x_3^2 - x_2 x_3^2 - x_1 x_2 + x_2^2, x_3^4 - 2x_2 x_3^2 + x_2^2)$ and check that $I_2 \subset I_3$. Finally, the ideal $I_4 = I_3 :_P (x_2) = (x_1^2 - 2x_1 x_2 + x_2^2, x_1 x_3^2 - x_2 x_3^2 - x_1 x_2 + x_2^2, x_3^4 - 2x_2 x_3^2 + x_2^2)$ satisfies $I_3 = I_4$.

Using the proposition, we conclude that $I :_P (x_2)^\infty = I_3 = (x_1^2 - 2x_1 x_2 + x_2^2, x_1 x_3^2 - x_2 x_3^2 - x_1 x_2 + x_2^2, x_3^4 - 2x_2 x_3^2 + x_2^2)$.

Of course, it would be nice if we could predict the number μ in the proposition beforehand. Some attempts in this direction are contained in Tutorial 37.

The reason for the importance of localizations with respect to the problem of computing saturations is that the saturation of a submodule of P^r with respect to a principal ideal can be viewed as the combination of extending the submodule to the localization and contracting it back. In the next proposition, the module P^r will be considered as a subset of $(P^r)_f$ via the canonical map.

Proposition 3.5.11. (Saturation and Localization)
Let M and N be two P-submodules of P^r, and let $I = (f)$ be a principal ideal in P generated by a non-zero polynomial $f \in P$.

a) *The P_f-module N_f can be identified with the P_f-submodule of $(P^r)_f$ generated by the images of the elements of N under the canonical map $P^r \longrightarrow (P^r)_f$.*

b) *We have $N :_M I^\infty = N_f \cap M$.*

Proof. To prove a), we denote the canonical map $N \longrightarrow P^r$ by ι, and we let φ be the map $\varphi : N_f \longrightarrow (P^r)_f$ given by $\varphi(\frac{v}{f^i}) = \frac{\iota(v)}{f^i}$. It is easy to check that φ is well-defined and injective, and this implies the claim.

Now we show claim b). To prove "$\subseteq$", let $v \in M$ and $i \in \mathbb{N}$ such that $I^i \cdot v \subseteq N$. By a), the fact that $f^i v \in N$ implies $\frac{v}{1} = \frac{1}{f^i} \cdot f^i v \in N_f$. Next we show "$\supseteq$". Given a vector $v \in M$ such that $\frac{v}{1} = \frac{w}{f^i}$ for some $w \in N$ and some $i \in \mathbb{N}$, we have $f^{i+j} v = f^j w$ in P^r for some $j \in \mathbb{N}$, and thus $f^i v = w \in N$. Hence we get $v \in N :_M I^i \subseteq N :_M I^\infty$. $\square$

How can we use this connection between localizations and saturations? The key for turning it into an algorithm is the presentation we found in Proposition 3.5.6 for the localization at an element. Using this presentation, we can explicitly perform the process of extending the submodule and contracting it back. Thus we arrive at several new methods for computing saturations.

Lemma 3.5.12. *Let M and N be two P submodules of P^r, and let I and J be two ideals in P. Then we have*

$$(N :_M I^\infty) \cap (N :_M J^\infty) = N :_M (I + J)^\infty$$

Proof. Only the inclusion "$\subseteq$" needs to be shown. Let $v \in M$ such that $I^i v \subseteq N$ and $J^j v \subseteq N$ for some $i, j \in \mathbb{N}$. Then we have $(f + g)^{i+j} v \in N$ for all $f \in I$ and all $g \in J$, because in the expansion of $(f + g)^{i+j}$ every summand is divisible by f^i or g^j. Thus the claim is proved. $\square$

Theorem 3.5.13. (Computation of Saturations)
Let M and N be two non-zero P-submodules of P^r, let I be a non-zero ideal in P, and let y be a new indeterminate. In the following, we identify P^r with its image in $P[y]^r$.

a) *Suppose that $I = (f)$ is a principal ideal generated by a non-zero polynomial $f \in P$. Then we have*

$$N :_M (f)^\infty = \left(NP[y] + (fy - 1) \cdot P[y]^r \right) \cap M$$

b) *Let $\{f_1, \ldots, f_s\}$ be a system of generators of I. Then we have*

$$N :_M I^\infty = \bigcap_{i=1}^s N :_M (f_i)^\infty$$

c) *Let $\{f_1, \ldots, f_s\}$ be a system of generators of I. In $P[y]$, we form the polynomial $f(y) = f_1 + f_2 y + \cdots + f_s y^{s-1}$. Then we have*

$$N :_M I^\infty = \left(NP[y] :_{P[y]^r} (f(y))^\infty \right) \cap M$$

Proof. To prove the first claim, we take an element $v \in M$ which satisfies $I^i \cdot v \subseteq N$ for some $i \geq 1$. Then $v = f^i y^i v - (1 + fy + \cdots + f^{i-1} y^{i-1})(fy - 1)v$ is contained in the right-hand side. Conversely, let v be an element of $(NP[y] + (fy - 1)P[y]^r) \cap M$, and let $\{w_1, \ldots, w_u\} \subseteq N \setminus \{0\}$ be a system of generators of N. Then there are polynomials $g_1, \ldots, g_u, h_1, \ldots, h_r \in P[y]$ such that $v = g_1 w_1 + \cdots + g_u w_u + h_1(fy - 1)e_1 + \cdots + h_r(fy - 1)e_r$, where

$\{e_1, \ldots, e_r\}$ denotes the canonical basis of $P[y]^r$. After considering this as an equation in $(P_f[y])^r$, we perform the substitution $y \mapsto \frac{1}{f}$. Since $v \in P^r$ is invariant under this substitution, we obtain

$$v = g_1(x_1, \ldots, x_n, \tfrac{1}{f}) w_1 + \cdots + g_u(x_1, \ldots, x_n, \tfrac{1}{f}) w_u$$

Let f^j be a common denominator of $g_1(x_1, \ldots, x_n, \frac{1}{f}), \ldots, g_u(x_1, \ldots, x_n, \frac{1}{f})$. Now it suffices to multiply everything with f^j in order to see that $f^j v \in N$. Thus we have $v \in N :_M I^\infty$.

Claim b) follows by induction from the lemma. Finally, to prove c), we note that $I^i \cdot v \subseteq N$ for some vector $v \in M$ and some $i \in \mathbb{N}$ implies $f_{\alpha_1} \cdots f_{\alpha_i} v \in N$ for all $\alpha_1, \ldots, \alpha_i \in \{1, \ldots, s\}$. On the other hand, we have

$$f(y)^i v = \sum_{\alpha_1, \ldots, \alpha_i = 1}^{s} c_{(\alpha_1, \ldots, \alpha_i)} f_{\alpha_1} \cdots f_{\alpha_i} y^{\alpha_1 + \cdots + \alpha_i - i} v$$

for suitable coefficients $c_{(\alpha_1, \ldots, \alpha_i)} \in \mathbb{N}$. Hence we obtain $f(y)^i v \in NP[y]$.

To show the other inclusion, we proceed by induction on s and note that the case $s = 1$ is trivially true. For $s > 1$, we start with an element $v \in M$ satisfying $f(y)^i v \in NP[y]$ for some $i \in \mathbb{N}$ and expand $f(y)^i v$ as above. We consider $P[y]$ as a polynomial ring in one indeterminate y over the ring P and equip it with the standard grading $\deg(y) = 1$. Then the $P[y]$-submodule $NP[y]$ of $P[y]^r$ is a graded submodule, of $P[y]^r$, since it is generated by homogeneous elements of degree zero (see Proposition 1.7.10). Therefore we have $\sum_{\alpha_1 + \cdots + \alpha_i - i = j} c_{(\alpha_1, \ldots, \alpha_i)} f_{\alpha_1} \cdots f_{\alpha_i} v \in N$ for all $j \in \mathbb{N}$. In particular, the case $j = i(s-1)$ implies $f_s^i v \in N$.

Since we know $v \in NP[y] :_{P[y]^r} (f(y))^\infty$ and $v \in NP[y] :_{P[y]^r} (f_s y^{s-1})^\infty$, we can use the lemma to get $v \in NP[y] :_{P[y]^r} (f_1 + f_2 y + \cdots + f_{s-1} y^{s-2})^\infty$. Now we apply the induction hypothesis and obtain $v \in N :_M (f_1, \ldots, f_{s-1})^\infty$. Together with $v \in N :_M (f_s)^\infty$ and the lemma, this implies the claim. $\square$

Example 3.5.14. Consider again the ideal $I \subseteq P = \mathbb{Q}[x_1, x_2, x_3]$ given in Example 3.5.10. If we want to compute $I :_P (x_2)^\infty$ using the method suggested by part a) of the theorem, we have to form the polynomial ideal $J = I + (1 - x_1 y)$ in $P[y]$. Then we eliminate y and get again the correct answer $J \cap P = (x_1^2 - 2x_1 x_2 + x_2^2, x_1 x_3^2 - x_2 x_3^2 - x_1 x_2 + x_2^2, x_3^4 - 2x_2 x_3^2 + x_2^2) = I :_P (x_2)^\infty$.

As an application of the previous theorem, we find an effective criterion for checking whether a given polynomial is in the radical of some ideal. Notice that this problem is much easier than the problem of actually computing the radical of an ideal which will be studied in Section 3.7.

Corollary 3.5.15. (Radical Membership Test)
Let I be an ideal in P, let $f \in P \setminus \{0\}$, and let y be a new indeterminate. Then the following conditions are equivalent.

a) *We have $f \in \sqrt{I}$.*
b) *We have $IP_f = P_f$.*
c) *We have $1 \in I :_P (f)^\infty$.*
d) *In the ring $P[y]$ we have $1 \in IP[y] + (fy - 1)$.*
e) *Every Gröbner basis of the ideal $IP[y] + (fy - 1)$ in $P[y]$ contains an element of $K \setminus \{0\}$.*
f) *The reduced Gröbner basis of the ideal $IP[y] + (fy - 1)$ in $P[y]$ with respect to every term ordering is $\{1\}$.*

Proof. First we show the equivalence of a) and b). Let $f^i \in I$ for some $i \in \mathbb{N}$. Then $1 = f^i \cdot \frac{1}{f^i} \in IP_f$. Conversely, if $1 \in IP_f$, then there exist a polynomial $g \in I$ and a number $i \in \mathbb{N}$ such that $1 = \frac{g}{f^i}$. Using the definition of P_f, we get $f^i = g \in I$. The equivalence of b) and c) follows from Proposition 3.5.11.b, and the equivalence of c) and d) from Theorem 3.5.13.a. Finally, it is clear that the last two conditions are nothing but reformulations of d). $\qquad\square$

Example 3.5.16. Once again, let I be the ideal of $P = \mathbb{Q}[x_1, x_2, x_3]$ given in Example 3.5.10. Suppose we want to check whether $f = x_1 x_2 - x_1 x_3^2$ is contained in $\sqrt{I}$. In the ring $P[y]$, we compute a reduced Gröbner basis of the ideal $IP[y] + (fy - 1)$ and get $\{1\}$. Hence we conclude that $f \in \sqrt{I}$.

Exercise 1. Let R be a ring, let M be a finitely generated R-module, and let $S \subseteq R$ be a multiplicatively closed subset. Prove that the following conditions are equivalent.

a) $M_S = 0$
b) $\operatorname{Ann}_R(M) \cap S \neq 0$

Exercise 2. Let R be a ring and $\mathfrak{p}$ a prime ideal in R.

a) Show that $S = R \setminus \mathfrak{p}$ is a multiplicative set.
b) Prove that the ring R_S has a unique maximal ideal. Describe the elements of that ideal.

Exercise 3. Let R be a ring, let M be an R-module, and let $S \subseteq R$ be a multiplicatively closed set. Prove that the localization M_S has the following **universal property**.
If N is any R-module such that the multiplication map $\mu_s : N \longrightarrow N$ is bijective for every element $s \in S$, and if $\varphi : M \longrightarrow N$ is an R-linear map, then there exists precisely one R-linear map $\psi : M_S \longrightarrow N$ such that $\varphi = \psi \circ \iota$, where $\iota : M \longrightarrow M_S$ is the canonical map.

Exercise 4. Let P be a polynomial ring over a field K, let $f_1, \ldots, f_s \in P$ be non-zero polynomials, and let S be the multiplicative monoid generated by $\{f_1, \ldots, f_s\}$. Show that there is an isomorphism $P_S \cong P[y]/(fy - 1)$, where $f = \prod_{i=1}^s f_i$.

Exercise 5. Let R be a ring, let y be an indeterminate, and let $g(y), h(y) \in R[y] \setminus \{0\}$. Moreover, we let $\gamma = \max\{\deg(g) - \deg(h) + 1, 0\}$, and we let $a \in R$ be the leading coefficient of $h(y)$.

a) Prove that there exist polynomials $q(y), r(y) \in R[y]$ such that we have $r(y) = 0$ or $\deg(r) < \deg(h)$, and such that

$$a^\gamma g(y) = q(y)h(y) + r(y)$$

Hint: Proceed by induction on $\deg(g)$. If $\deg(g) \geq \deg(h)$, consider the polynomial $a\, g(y) - b\, y^{\deg(g) - \deg(h)} h(y)$, where b is the leading coefficient of $g(y)$.

b) In the situation of a), show that $q(y)$ and $r(y)$ are uniquely determined if a is a non-zerodivisor of R.

Exercise 6. Let R be a ring, let I be an ideal in R, and let $\mathfrak{p}$ be a prime ideal in R. Prove that if $r \in (R \setminus \mathfrak{p}) \cap \sqrt{I}$, then $(\mathfrak{p} \cap I) : r^\infty = \mathfrak{p}$.

Exercise 7. Let R be a ring, let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of R-modules, and let I be an ideal in R. Prove that there is an induced exact sequence of R-modules

$$0 \longrightarrow 0 :_{M'} I^\infty \longrightarrow 0 :_M I^\infty \longrightarrow 0 :_{M''} I^\infty$$

and give an example in which the induced map $0 :_M I^\infty \longrightarrow 0 :_{M''} I^\infty$ is not surjective.

Exercise 8. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $I = (f_1, \ldots, f_s)$ be an ideal in P, and let $g \in P \setminus \{0\}$. Write a CoCoA function which implements the algorithm for checking whether $g \in \sqrt{I}$ holds provided by Corollary 3.5.15.

Exercise 9. Let K be a field and $P = K[x_1, \ldots, x_5]$. Consider the two matrices

$$\mathcal{A} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_4 & x_5 \end{pmatrix} \qquad \text{and} \qquad \mathcal{B} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_4 & x_5 \\ x_3 & x_5 & 0 \end{pmatrix}$$

Let $d_1 = x_2 x_5 - x_3 x_4$, $d_2 = x_2 x_3 - x_1 x_5$, and $d_3 = x_1 x_4 - x_2^2$ be the 2×2-minors of $\mathcal{A}$, and let d be the determinant of $\mathcal{B}$. For $I = (d_1, d_2, d_3)$ and $J = (d_3, d)$, show that $\sqrt{I} = \sqrt{J}$.

Tutorial 37: Computation of Saturations

In this tutorial we ask you to implement the algorithms for computing saturations which we explained above. Furthermore, we want to study possible improvements of these algorithms.

Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $I \subseteq P$ be an ideal which is generated by a set of polynomials $\{f_1, \ldots, f_s\}$, and let M and N be two P-submodules of P^r.

a) Write a CoCoA function `Sat1(...)` which implements the method of Proposition 3.5.9 for computing $N :_M I^\infty$. In order to find the colon modules $N :_M I^i$, implement the method of Proposition 3.4.9.b in a CoCoA function `ElimColon(...)`.

b) Apply your function `Sat1(...)` to compute the saturation $N :_M I^\infty$ in the following cases.

1) $I = (x, y, z)$, $N = (x + y - 3z, y^2 - 3yz + 2z^2) \cap (x, y, z)^4$, $M = (1)$ in $\mathbb{Q}[x, y, z]$
2) $I = (x - y)$, $N = \langle xye_1, x^2e_1, y^2e_2 \rangle$, $M = \langle xye_1, xye_2 \rangle$ in $\mathbb{Q}[x, y]^2$
3) $I = (x, y + z)$, $N = \langle (yz - 2z^2)e_1, (y^2 - 4z^2)e_2, (xz - z^2)e_2, (x^2 - z^2)e_3 \rangle$, $M = \langle xe_1, ye_2, ze_3 \rangle$ in $\mathbb{Q}[x, y, z]^3$

c) Implement the method of Theorem 3.5.13.a,b for computing $N :_M I^\infty$ in a CoCoA function `Sat2(...)` and apply it to the cases given in b).

d) Implement the method of Theorem 3.5.13.c for computing $N :_M I^\infty$ in a CoCoA function `Sat3(...)` and apply it to the cases given in b).

e) Let $I = (f)$ be a non-zero principal ideal, and let $v \in N :_M I^\infty$. Describe two different ways how one can find an integer $i \geq 0$ such that $f^i v \in N$. *Hint:* One method uses Proposition 3.5.9, and the other one follows from the proof of Theorem 3.5.13.a.

f) Let I be again an arbitrary ideal in P. Use your answers of e) to write two CoCoA functions `RadPower1(...)` and `RadPower2(...)` which find for every polynomial $f \in \sqrt{I}$ an integer $i \geq 0$ such that $f^i \in I$. Apply your functions in the following cases.

1) $I = (x^3, y^3, z^3)$, $f = x + y + z$ in $\mathbb{Q}[x, y, z]$
2) $I = (x_1x_4 - x_2^2, x_2x_5 - x_3x_4, x_1x_5 - x_2x_3)$, $f = x_1x_5^2 - 2x_2x_3x_5 + x_3^2x_4$ in $\mathbb{Q}[x_1, \ldots, x_5]$

g) Prove the formula

$$N :_M (f_1 \cdots f_s)^\infty = (\cdots((N :_M (f_1)^\infty) :_M (f_2)^\infty) \cdots) :_M (f_s)^\infty$$

h) Use g) to write a CoCoA function `SatIndets(...)` which takes an ideal I in P and computes $I :_P (x_1 \cdots x_n)^\infty$. Apply this function in the following cases.

1) $I = (x_1^7 - x_2^2x_3, x_1^4x_4 - x_2^3)$ in $\mathbb{Q}[x_1, \ldots, x_4]$
2) $I = (x_1x_2x_3 - x_4x_5x_6, x_5x_7 - x_1x_2x_6)$ in $\mathbb{Q}[x_1, \ldots, x_7]$
3) $I = (x_2x_4 - x_6x_8, x_2x_8^2 - x_4^3, x_1x_3 - x_5x_7, x_1^2x_7 - x_3^2x_5)$ in $\mathbb{Q}[x_1, \ldots, x_8]$

i) Let $g_1, \ldots, g_t$ be further polynomials in P. Suppose that J is an ideal in P which contains the polynomial $f_1 \cdots f_s - g_1 \cdots g_t$. Then prove the formula

$$J :_P (f_1 \cdots f_s \cdot g_1 \cdots g_t)^\infty = J :_P (f_1 \cdots f_s)^\infty$$

Tutorial 38: Toric Ideals

In Tutorial 36, we found a solution of the integer programming problem $\mathrm{IP}(\mathcal{A}, b, C)$, where $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{N})$, $b = (b_1, \ldots, b_m) \in \mathbb{N}^m$, and $C : \mathbb{N}^n \longrightarrow \mathbb{N}$ is a non-zero linear function. Since the integer programming problem has many practical applications, it is important to solve it as efficiently as possible. Let us discuss our earlier solution in this respect.

The main step was to consider the terms $t_i = y_1^{a_{1i}} \cdots y_m^{a_{mi}}$ for all $i = 1, \ldots, n$, and to form the binomial ideal $J = (x_1 - t_1, \ldots, x_n - t_n)$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, where K is a field. Then we had to compute the Gröbner basis of the ideal J with respect to an elimination ordering for $\{y_1, \ldots, y_m\}$. Unfortunately, this computation is, in general, rather inefficient.

Let $P = K[x_1, \ldots, x_n]$. The ideal $I = J \cap P$ is called the **toric ideal** associated to the matrix $\mathcal{A}$. In this tutorial, we want to search for another way to compute I and to study possibilities for applying this method to optimize the solution of the integer programming problem. By $\mathcal{S}$, we denote again the system of Diophantine equations

$$\begin{cases} a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n &= b_1 \\ a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n &= b_2 \\ \qquad\qquad \vdots & \vdots \ \ \vdots \\ a_{m1}z_1 + a_{m2}z_2 + \cdots + a_{mn}z_n &= b_m \end{cases}$$

a) Let $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ be a solution of $\mathcal{S}$, let σ be a cost-compatible term ordering on $\mathbb{T}(x_1, \ldots, x_n)$, and let $(\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ be such that $x_1^{\beta_1} \cdots x_n^{\beta_n} = \mathrm{NF}_{\sigma,I}(x_1^{\alpha_1} \cdots x_n^{\alpha_n})$. Prove that $(\beta_1, \ldots, \beta_n)$ is a solution of the integer programming problem $\mathrm{IP}(\mathcal{A}, b, C)$.

Thus we can try to solve $\mathrm{IP}(\mathcal{A}, b, C)$ as follows. First we find a solution $(\alpha_1, \ldots, \alpha_n)$ of the system $\mathcal{S}$, for instance by an exhaustive search or as in Tutorial 36.k. Then we find a system of generators of I. Next, we choose a cost-compatible term ordering σ on $\mathbb{T}(x_1, \ldots, x_n)$. Finally, we calculate a σ-Gröbner basis of I and $\mathrm{NF}_{\sigma,I}(x_1^{\alpha_1} \cdots x_n^{\alpha_n})$.

Computationally, the most expensive step in this procedure is the second one, i.e. the determination of a system of generators of I. Let us implement a reference function against which we can judge possible optimizations.

b) Write a CoCoA function `Toric1(...)` which takes the matrix $\mathcal{A}$ and computes the toric ideal $I = J \cap P$ associated to $\mathcal{A}$ via the built-in command `Elim(...)`.

c) Apply your function `Toric1(...)` in the following cases. Each time, measure the execution time using `Time`.

$$1) \ \mathcal{A}_1 = \begin{pmatrix} 3 & 1 & 11 & 2 & 3 & 5 & 3 & 5 \\ 4 & 5 & 0 & 1 & 7 & 4 & 6 & 2 \\ 5 & 6 & 1 & 9 & 2 & 3 & 3 & 1 \end{pmatrix}$$

$$2) \; \mathcal{A}_2 = \begin{pmatrix} 1 & 4 & 9 & 5 & 8 & 7 & 3 & 3 & 6 & 7 \\ 1 & 6 & 2 & 4 & 4 & 1 & 2 & 4 & 0 & 4 \\ 4 & 3 & 4 & 4 & 3 & 6 & 6 & 5 & 2 & 9 \\ 3 & 1 & 9 & 6 & 9 & 7 & 1 & 9 & 2 & 9 \\ 9 & 7 & 0 & 6 & 3 & 9 & 2 & 0 & 8 & 4 \end{pmatrix}$$

$$3) \; \mathcal{A}_3 = \begin{pmatrix} 4 & 3 & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 1 & 1 & 0 & 0 & 0 & 3 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 4 & 3 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 2 & 1 & 0 & 3 & 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 3 & 0 & 0 \end{pmatrix}$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 3 & 2 & 1 & 0 & 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 4 \end{matrix}\Bigg)$$

Now we consider the homogeneous system of Diophantine equations associated to $\mathcal{S}$ and denote it by $\mathcal{S}_0$.

$$\begin{cases} a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n & = & 0 \\ a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}z_1 + a_{m2}z_2 + \cdots + a_{mn}z_n & = & 0 \end{cases}$$

Let $\mathcal{L} \subseteq \mathbb{Z}^n$ be the set of integer solutions of $\mathcal{S}_0$. A subset of $\mathbb{Z}^n$ is called a **lattice** in $\mathbb{Z}^n$ if it is a free $\mathbb{Z}$-submodule.

d) Show that $\mathcal{L}$ is a lattice of rank $n - \mathrm{rk}(\mathcal{A})$ in $\mathbb{Z}^n$.

e) Prove that the following construction yields a map $\varphi : \mathcal{L} \longrightarrow I$ which is well-defined. A tuple $(\alpha_1, \ldots, \alpha_n) \in \mathcal{L}$ can be uniquely written as $(\max(\alpha_1, 0), \ldots, \max(\alpha_n, 0)) - (\max(-\alpha_1, 0), \ldots, \max(-\alpha_n, 0))$. Then we define

$$\varphi(\alpha_1, \ldots, \alpha_n) = x_1^{\max(\alpha_1, 0)} \cdots x_n^{\max(\alpha_n, 0)} - x_1^{\max(-\alpha_1, 0)} \cdots x_n^{\max(-\alpha_n, 0)}$$

Hint: Use $I = J \cap P$ and a technique similar to Tutorial 36.g.

f) Conversely, let $x_1^{\alpha_1} \cdots x_n^{\alpha_n} - x_1^{\beta_1} \cdots x_n^{\beta_n} \in I$ for some tuples $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Prove that $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) \in \mathcal{L}$.

g) Let $L = K[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ be the ring of Laurent polynomials introduced in Tutorial 36. Describe an explicit isomorphism of K-algebras $P_{x_1 \cdots x_n} \cong L$.

h) Let $r = \mathrm{rk}(\mathcal{L}) = n - \mathrm{rk}(\mathcal{A}) > 0$, and let $\{v_1, \ldots, v_r\} \subseteq \mathcal{L}$ be a $\mathbb{Z}$-basis of $\mathcal{L}$. The ideal $I_{\mathcal{L}} = (\varphi(v_1), \ldots, \varphi(v_r))$ is called the **lattice ideal** associated to $\mathcal{L}$. Show that $I_{\mathcal{L}} \cdot P_{x_1 \cdots x_n} = I \cdot P_{x_1 \cdots x_n}$ and conclude that

$$I = I_{\mathcal{L}} :_P (x_1 \cdots x_n)^\infty$$

i) Use h) to write a CoCoA function `Toric2(...)` which takes the matrix $\mathcal{A}$ and computes its associated toric ideal I. For the computation of the saturation, apply the function `SatIndets(...)` of Tutorial 37.h.

Hint: Use the CoCoA function LinKer(...) at least eight times to get different $\mathbb{Z}$-bases of $\mathcal{L}$. (The function LinKer(...) is not deterministic.) In this way, produce many generators of $I_{\mathcal{L}}$.

 j) Calculate the toric ideals associated to the matrices in part c) using Toric2(...) and Time how long it takes.

 k) Explain how one can use Tutorial 37.i to avoid some saturations with respect to certain indeterminates in the function Toric2(...). Write a CoCoA function Toric3(...) which implements this optimization.

 l) Apply your function Toric3(...) in the cases of c), measure its execution times again, and compare the result with your previous timings.

3.6 Homomorphisms of Algebras

He who asks questions
cannot avoid the answers.
(Cameroon Proverb)

In Subsection 3.3.A we examined homomorphisms between finitely generated modules over an affine algebra P/I, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over a field K and $I \subseteq P$ is an ideal. We answered the question of how to compute presentations for the kernel and the image of such a homomorphism. Now we ask the same questions for K-algebra homomorphisms.

So, let $P' = K[y_1, \ldots, y_m]$ be another polynomial ring, and let $I' \subseteq P'$ be an ideal. How can we compute the kernel of a K-algebra homomorphism $\varphi : P/I \longrightarrow P'/I'$? Our earlier results are not applicable, because P'/I' is in general *not* a finitely generated P/I-module. Therefore we need a different approach. Fortunately, the elimination techniques introduced in Section 3.4 come to our rescue. We embed both P and P' into the larger polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and form $J = I'Q + (x_1 - f_1, \ldots, x_n - f_n)$, where $f_i \in P'$ are chosen such that $f_i + I' = \varphi(x_i + I)$ for $i = 1, \ldots, n$. Then $\mathrm{Ker}(\varphi)$ is simply the residue class ideal of the elimination ideal $J \cap P$.

A number of other questions can be reformulated as questions about the kernels of suitable K-algebra homomorphisms. For example, we can solve the *implicitization problem* which asks for the ideal of algebraic relations among a given set of polynomials.

Another application is the possibility to perform the following task. Let us consider the affine $\mathbb{Q}$-algebra $\mathbb{Q}[x, y]/(x^2 + 2xy + y^2 + 1)$, and let us denote by $\overline{x}$ and $\overline{y}$ the residue classes of x and y. Clearly, the element $\overline{x} + \overline{y}$ satisfies an algebraic equation, namely $(\overline{x} + \overline{y})^2 + 1 = 0$. Such an element is called *algebraic* over $\mathbb{Q}$. On the other hand, the element $\overline{x}$ does not satisfy an algebraic equation. It is called *transcendental* over $\mathbb{Q}$. Given an affine K-algebra and an element in it, it is possible to decide whether the element is transcendental or algebraic, and in the latter case to find its minimal polynomial over K (see Corollary 3.6.4).

Then we turn our attention to the study of the image of a K-algebra homomorphism $\varphi : P/I \longrightarrow P'/I'$. Proposition 3.6.6 allows us to check whether or not a given element of P'/I' is contained in the image of φ. In the first case, we show how one can represent it explicitly using the generators of $\mathrm{Im}(\varphi)$. The set $\mathrm{Im}(\varphi)$ is an affine K-algebra itself and will be presented using generators and relations. Another beautiful application of our elimination techniques is the possibility to decide whether φ is surjective just by looking at the shape of a particular Gröbner basis.

In the last part, this result is extended and sharpened for homomorphisms $\varphi : P \longrightarrow P'$ of polynomial rings over K. Once more the full power of reduced Gröbner bases shows up. In particular, we explain how the shape of a suitable reduced Gröbner basis allows us to compute an explicit right

inverse homomorphism if φ is surjective (see Proposition 3.6.9). Finally, we get a very explicit characterization of K-algebra automorphisms of P (see Proposition 3.6.12).

Several times in this section an interesting phenomenon occurs. We start with a fairly simple, innocent looking example and ask a straightforward question: what happens if we apply the theoretical results in this concrete case? Sometimes the answer can be much more complicated than we would ever have imagined. And we would not be surprised if, when you try your own examples using CoCoA, the answer fills screen after screen. Such is life!

In Section 1.1 we introduced evaluation homomorphisms on polynomial rings. Evaluation homomorphisms of the type $\psi : R[x_1, \ldots, x_n] \longrightarrow R$ were also called substitution homomorphisms. Since we want to study algebra homomorphisms in this section, the following facts about substitution homomorphisms will come in handy.

Proposition 3.6.1. *Let R be a ring, let $R[x_1, \ldots, x_n]$ be a polynomial ring over R, let $f_1, \ldots, f_n \in R$, and let $\psi : R[x_1, \ldots, x_n] \longrightarrow R$ be the substitution homomorphism defined by $\psi(x_i) = f_i$ for $i = 1, \ldots, n$.*

a) *The kernel of ψ is the ideal $(x_1 - f_1, \ldots, x_n - f_n)$ in $R[x_1, \ldots, x_n]$.*

b) *For every $g \in R[x_1, \ldots, x_n]$, there exist $h_1, \ldots, h_n \in R[x_1, \ldots, x_n]$ such that*

$$g = \sum_{i=1}^{n} h_i \, (x_i - f_i) + g(f_1, \ldots, f_n)$$

Proof. Obviously, claim b) implies a). Given $g \in R[x_1, \ldots, x_n]$, we apply the R-algebra homomorphism $\vartheta : R[x_1, \ldots, x_n] \longrightarrow R[x_1, \ldots, x_n]$ defined by $\vartheta(x_i) = x_i + f_i$ for $i = 1, \ldots, n$. Then we write $\vartheta(g)$ in the form

$$\vartheta(g) = g(x_1 + f_1, \ldots, x_n + f_n) = \sum_{i=1}^{n} \widetilde{h}_i \, x_i + r$$

where $\widetilde{h}_1, \ldots, \widetilde{h}_n \in R[x_1, \ldots, x_n]$ and $r \in R$. By applying the substitution homomorphism $x_i \mapsto 0$ for $i = 1, \ldots, n$ to both sides of this equation, we see that $r = g(f_1, \ldots, f_n)$.

Clearly, the R-algebra homomorphism $\vartheta' : R[x_1, \ldots, x_n] \longrightarrow R[x_1, \ldots, x_n]$ defined by $\vartheta'(x_i) = x_i - f_i$ for $i = 1, \ldots, n$ is inverse to ϑ. When we apply it to the above equation, we get $g = \vartheta'(\vartheta(g)) = \sum_{i=1}^{n} \vartheta'(\widetilde{h}_i)(x_i - f_i) + g(f_1, \ldots, f_n)$. By setting $h_i = \vartheta'(\widetilde{h}_i)$ for $i = 1, \ldots, n$, we obtain the desired result. $\qquad\square$

For the remainder of this section, we let K be a field, and we suppose that $P = K[x_1, \ldots, x_n]$ and $P' = K[y_1, \ldots, y_m]$ are two polynomial rings containing proper ideals $I \subset P$ and $I' \subset P'$. Then a K-algebra homomorphism

$$\varphi : P/I \longrightarrow P'/I'$$

is determined by polynomials $f_1, \ldots, f_n \in P'$ such that $\varphi(x_i + I) = f_i + I'$ for $i = 1, \ldots, n$. We can view P'/I' as a P/I-algebra via φ by letting $(f + I) \cdot (g + I') = \varphi(f + I) \cdot (g + I')$ for $f \in P$ and $g \in P'$. But as one can easily see, the P/I-module P'/I' is in general not finitely generated, so that the previous results on modules cannot be used for computing presentations of the P-modules $\mathrm{Ker}(\varphi)$ and $\mathrm{Im}(\varphi)$. Instead, we are now going to provide other effective methods for this purpose.

Proposition 3.6.2. (Kernels of K-Algebra Homomorphisms)
Let $\varphi : P/I \longrightarrow P'/I'$ be a K-algebra homomorphism which is given by $\varphi(x_i + I) = f_i + I'$ for $i = 1, \ldots, n$. We form the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and the ideal $J = I'Q + (x_1 - f_1, \ldots, x_n - f_n)$. Then $\mathrm{Ker}(\varphi)$ is the image of the ideal $J \cap P$ in P/I.

Proof. Let $g \in P$ be a polynomial such that $g + I \in \mathrm{Ker}(\varphi)$. Then the equality $\varphi(g+I) = g(f_1, \ldots, f_n)+I' = 0$ implies $g(f_1, \ldots, f_n) \in I'$. If we consider $h = g - g(f_1, \ldots, f_n) \in Q$ as a polynomial with coefficients in P' and indeterminates $x_1, \ldots, x_n$, we have $h(f_1, \ldots, f_n) = 0$. Therefore Proposition 3.6.1.a implies that h is in the ideal generated by $\{x_1 - f_1, \ldots, x_n - f_n\}$ in Q. In particular, we get $g = g(f_1, \ldots, f_n) + h \in J \cap P$.

Conversely, let $g \in J \cap P$, and let $\{h_1, \ldots, h_s\} \subseteq P'$ be a system of generators of I'. Since we have $g \in J$, we can represent g in the form $g = \sum_{i=1}^{s} g_i h_i + \sum_{j=1}^{n} k_j(x_j - f_j)$ with polynomials $g_i, k_j \in Q$. Now we substitute $x_i \longmapsto f_i$ for $i = 1, \ldots, n$ in this representation, and we get $g(f_1, \ldots, f_n) = \sum_{i=1}^{s} g_i(f_1, \ldots, f_n, y_1, \ldots, y_m)h_i \in I'$. Therefore we obtain $\varphi(g + I) = g(f_1, \ldots, f_n) + I' = 0$, as claimed. $\qquad\square$

In the introduction of the previous section we mentioned the **implicitization problem**. Given polynomials $f_1, \ldots, f_n \in P'$, it asks how one can find the ideal of algebraic relations among them. This problem can be solved by applying the preceding proposition in the case $I = (0)$ and $I' = (0)$.

Corollary 3.6.3. (Implicitization)
Given polynomials $f_1, \ldots, f_n \in P'$, we define a K-algebra homomorphism $\varphi : P \longrightarrow P'$ by $\varphi(x_i) = f_i$ for $i = 1, \ldots, n$. In $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, we consider the ideal $J = (x_1 - f_1, \ldots, x_n - f_n)$. Then the ideal of algebraic relations among $f_1, \ldots, f_n$ is given by

$$\mathrm{Ker}(\varphi) = J \cap P$$

Another application of the previous proposition is the possibility to check whether an element of an affine K-algebra is algebraic or transcendental over K, and to compute its minimal polynomial in the first case.

Corollary 3.6.4. (Minimal Polynomials)
Let I be an ideal in P, let R be the affine K-algebra $R = P/I$, and let $\overline{f} \in R \setminus \{0\}$ be the residue class of a polynomial $f \in P$. We consider a new

indeterminate y and form the ideal $J = I \cdot P[y] + (y - f)$ in the polynomial ring $P[y]$.

a) The element $\overline{f} \in R$ is transcendental over K if and only if we have $J \cap K[y] = (0)$.

b) If the element $\overline{f} \in R$ is algebraic over K, then any generating polynomial of the elimination ideal $J \cap K[y]$ is a minimal polynomial of $\overline{f}$ over K.

Proof. Both claims follow from the proposition. We observe that $\overline{f}$ is transcendental over K if and only if the kernel of the K-algebra homomorphism $K[y] \longrightarrow R$ defined by $y \mapsto \overline{f}$ is trivial. If this kernel is non-trivial, the minimal polynomial of $\overline{f}$ over K generates it.   □

Example 3.6.5. Consider the affine $\mathbb{Q}$-algebra $R = \mathbb{Q}[x]/(x^7 - x - 1)$. The polynomial $x^7 - x - 1$ is irreducible over $\mathbb{Q}$. Therefore R is a field. The residue class of the polynomial $f = x^6 - 9x^5 + x + 11$ in R has the minimal polynomial

$$y^7 - 83\,y^6 + 2999\,y^5 - 61029\,y^4 + 726440\,y^3 - 4538196\,y^2 - 9285526\,y + 22670839$$

over $\mathbb{Q}$. To check this, we have to form the ideal $J = (x^7 - x - 1, y - f)$ in $\mathbb{Q}[x, y]$ and to compute $J \cap \mathbb{Q}[y]$. In spite of the apparent simplicity of the question, the answer shows that you should not try to calculate this by hand. Of course, CoCoA does it in a split-second!

Next we want to study the image of $\varphi : P/I \longrightarrow P'/I'$. Clearly, $\mathrm{Im}(\varphi)$ is the K-subalgebra of P'/I' generated by $f_1 + I', \ldots, f_n + I'$. In particular, it is an affine K-algebra. (In Example 2.6.4 we saw that, in general, subalgebras of affine K-algebras need not be affine algebras.) Moreover, we recall from above that P'/I' is, in general, not a finitely generated module over its subalgebra $\mathrm{Im}(\varphi)$.

This leads us to a number of questions. How can we decide effectively whether a given residue class of P'/I' lies in $\mathrm{Im}(\varphi)$? And if it does, how can we represent it using the generators of that K-algebra? How can we check whether φ is surjective? How can we find an explicit presentation of $\mathrm{Im}(\varphi)$ as a K-algebra? These questions are answered by the following proposition.

Proposition 3.6.6. (Images of K-Algebra Homomorphisms)
Let $\varphi : P/I \longrightarrow P'/I'$ be a K-algebra homomorphism which is given by $\varphi(x_i + I) = f_i + I'$ for $i = 1, \ldots, n$. We form the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and the ideal $J = I'Q + (x_1 - f_1, \ldots, x_n - f_n)$, and we let σ be an elimination ordering for $\{y_1, \ldots, y_m\}$. Furthermore, we let $G = \{g_1, \ldots, g_s\}$ be the reduced σ-Gröbner basis of J, and we assume that $G \cap P = \{g_1, \ldots, g_t\}$ for some $t \leq s$.

a) For a polynomial $g \in P'$, we have $g + I' \in \mathrm{Im}(\varphi)$ if and only if we have $\mathrm{NF}_{\sigma, J}(g) \in P$. (For the computation of this normal form, we view g as an element of Q.)

b) *If a polynomial $g \in P'$ satisfies $h = \mathrm{NF}_{\sigma,J}(g) \in P$, then the equation $g + I' = h(f_1, \ldots, f_n) + I'$ provides an explicit representation of its residue class as an element of $\mathrm{Im}(\varphi)$.*

c) *The affine K-algebra $\mathrm{Im}(\varphi)$ has the presentation*

$$\mathrm{Im}(\varphi) \cong K[x_1, \ldots, x_n]/(g_1, \ldots, g_t)$$

d) *The K-algebra homomorphism $\varphi : P/I \longrightarrow P'/I'$ is surjective if and only if G contains elements of the form $y_i - h_i$, where $h_i \in P$ for $i = 1, \ldots, m$.*

Proof. By applying the Division Algorithm 1.6.4 and Corollary 2.4.9.a, we obtain a representation

$$g = q_1 g_1 + \cdots + q_s g_s + \mathrm{NF}_{\sigma,J}(g)$$

with $q_1, \ldots, q_s \in Q$. If we have $\mathrm{NF}_{\sigma,J}(g) \in P$ here, we substitute $x_i \mapsto f_i$ for $i = 1, \ldots, n$. Since $g_1, \ldots, g_s$ are contained in J, they yield elements of I' under this substitution. Hence we get $g - (\mathrm{NF}_{\sigma,J}(g))(f_1, \ldots, f_n) \in I'$. This proves b) and the implication "$\Leftarrow$" of a).

Now we assume that $g \in P'$ satisfies $g + I' \in \mathrm{Im}(\varphi)$. We want to show $\mathrm{NF}_{\sigma,J}(g) \in P$. By assumption, there exists a polynomial $h \in P$ such that we have $g + I' = \varphi(h + I) = h(f_1, \ldots, f_n) + I'$. Since $g - h(f_1, \ldots, f_n) \in I'Q \subseteq J$ and $h - h(f_1, \ldots, f_n) \in (x_1 - f_1, \ldots, x_n - f_n) \subseteq J$ by Proposition 3.6.1.b, the polynomials g, h, and $h(f_1, \ldots, f_n)$ have the same normal form by Proposition 2.4.10.a. Using the fact that σ is an elimination ordering for $\{y_1, \ldots, y_m\}$, we see that $h \in P$ implies $\mathrm{NF}_{\sigma,J}(g) = \mathrm{NF}_{\sigma,J}(h(f_1, \ldots, f_n)) = \mathrm{NF}_{\sigma,J}(h) \in P$. Thus also the implication "$\Rightarrow$" of a) holds.

Next we prove c). By Theorem 3.4.5, the ideal $(g_1, \ldots, g_t)$ is precisely the elimination ideal $J \cap P$, which in turn maps to $\mathrm{Ker}(\varphi)$ in P/I by Proposition 3.6.2. Thus we have $\mathrm{Im}(\varphi) \cong (P/I)/\mathrm{Ker}(\varphi) \cong P/(J \cap P) = P/(g_1, \ldots, g_t)$.

Finally, we prove d). Suppose that φ is surjective. Let $i \in \{1, \ldots, m\}$. As $y_i + I' \in \mathrm{Im}(\varphi)$, part a) yields $h_i = \mathrm{NF}_{\sigma,J}(y_i) \in P$. Thus we have $y_i - h_i = y_i - \mathrm{NF}_{\sigma,J}(y_i) \in J$. Since $\mathrm{LM}_\sigma(y_i - h_i) = y_i$, the polynomial $y_i - h_i$ is monic. Moreover, $Q/J \cong P'/I'$ shows that J is a proper ideal of Q. Thus y_i is a minimal generator of $\mathrm{LT}_\sigma(J)$. The reduced σ-Gröbner basis of J has to contain an element of the form $y_i - k_i$, where $k_i \in P$. Since both h_i and k_i are irreducible and $(y_i - h_i) - (y_i - k_i) = k_i - h_i$, it follows that $h_i = k_i$, i.e. that the polynomial $y_i - h_i$ is contained in the reduced σ-Gröbner basis of J.

Conversely, let G be the reduced σ-Gröbner basis of J. If $y_i - h_i \in G$ for some $i \in \{1, \ldots, m\}$, then we have $h_i = \mathrm{NF}_{\sigma,J}(y_i)$, and therefore a) shows $y_i + I' \in \mathrm{Im}(\varphi)$. $\square$

In Tutorial 41.c you can see a discussion of the generalization of part c) of this proposition to the case of subalgebras generated by rational functions.

As in Corollary 3.6.3, we now restrict our attention to the case $I = I' = 0$, i.e. the case of homomorphisms of polynomial rings over K. In this case, parts a) and b) of the proposition specialize to the following result.

Corollary 3.6.7. (Subalgebra Membership Test)
Let $f_1, \ldots, f_n \in P'$, let $S = K[f_1, \ldots, f_n]$ be the K-subalgebra of P' generated by $\{f_1, \ldots, f_n\}$, let $J = (x_1 - f_1, \ldots, x_n - f_n) \subseteq K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, and let σ be an elimination ordering for $\{y_1, \ldots, y_m\}$.

    Then a polynomial $g \in P'$ is contained in the subalgebra S if and only if $\mathrm{NF}_{\sigma,J}(g) \in P$. In this case, if we let $h = \mathrm{NF}_{\sigma,J}(g)$, then $g = h(f_1, \ldots, f_n)$ is an explicit representation of g as an element of S.

    As an application of this corollary, we can compute the representation of a symmetric polynomial in terms of elementary symmetric polynomials discussed in Tutorial 12 in a different way.

Example 3.6.8. In Tutorial 12 we proved that the elementary symmetric polynomials $s_1, \ldots, s_n$ generate the K-subalgebra of all symmetric polynomials in $P' = K[y_1, \ldots, y_n]$. We define a K-algebra homomorphism $\varphi : K[x_1, \ldots, x_n] \longrightarrow P'$ by mapping x_i to s_i for $i = 1, \ldots, n$. Then we form the ideal $J = (x_1 - s_1, \ldots, x_n - s_n)$ in the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_n]$. By the corollary, we can compute the representation of a symmetric polynomial $f \in P'$ in terms of the elementary symmetric polynomials by calculating the normal form $\mathrm{NF}_{\sigma,J}(f)$ and substituting $x_i \mapsto s_i$ for $i = 1, \ldots, n$.

    For surjective homomorphisms $\varphi : P \longrightarrow P'$, we can strengthen Proposition 3.6.6.d as follows.

Proposition 3.6.9. (Surjective K-Algebra Homomorphisms Between Polynomial Rings)
  Let $\varphi : P \longrightarrow P'$ be a surjective K-algebra homomorphism which is given by $\varphi(x_i) = f_i$ for $i = 1, \ldots, n$. In the ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, we consider the ideal $J = (x_1 - f_1, \ldots, x_n - f_n)$. Let σ be an elimination ordering for $\{y_1, \ldots, y_m\}$.

a) There exist polynomials $h_1, \ldots, h_m, g_1, \ldots, g_s \in P$ such that the reduced σ-Gröbner basis of J is $\{y_1 - h_1, \ldots, y_m - h_m, g_1, \ldots, g_s\}$.

b) The set $\{g_1, \ldots, g_s\}$ is the reduced Gröbner basis of $\mathrm{Ker}(\varphi)$ with respect to the term ordering obtained by restricting σ to $\mathbb{T}(x_1, \ldots, x_n)$.

c) The homomorphism $\psi : P' \to P$ defined by $\psi(y_i) = h_i$ for $i = 1, \ldots, m$ is a right inverse of φ, i.e. we have $\varphi \circ \psi = \mathrm{id}_{P'}$.

Proof. First we prove a). Since φ is surjective, Proposition 3.6.6.d shows that the reduced σ-Gröbner basis G of J contains elements of the form $y_i - h_i$, where $h_i \in P$ for $i = 1, \ldots, m$. Let g be another element in G. Since the Gröbner basis is reduced, the term $\mathrm{LT}_\sigma(g)$ is not divisible by any

indeterminate in $\{y_1, \ldots, y_m\}$. Therefore we have $\mathrm{LT}_\sigma(g) \in P$. We know that σ is an elimination ordering for $\{y_1, \ldots, y_m\}$. Hence $\mathrm{LT}_\sigma(g) \in P$ implies $g \in P$, and a) is proved.

Claim b) follows from Proposition 3.6.2 and Theorem 3.4.5.c. To prove c), it suffices to show that $y_i = h_i(f_1, \ldots, f_n)$ for $i = 1, \ldots, m$. Let $u_i = y_i - h_i$ for $i = 1, \ldots, m$. Consider u_i as a polynomial in $P'[x_1, \ldots, x_n]$. Since we have $u_i \in J = (x_1 - f_1, \ldots, x_n - f_n)$, it is clear that $u_i(f_1, \ldots, f_n) = 0$. This means $y_i - h_i(f_1, \ldots, f_n) = 0$ for $i = 1, \ldots, m$, as we wanted to show. $\square$

The following example shows how one can apply this proposition in practice.

Example 3.6.10. Using the rings $P = \mathbb{Q}[x_1, x_2, x_3]$ and $P' = \mathbb{Q}[y_1, y_2]$, we let $\varphi : P \to P'$ be the $\mathbb{Q}$-algebra homomorphism which is defined by $\varphi(x_1) = \frac{1}{5}y_1 + y_2^4$, $\varphi(x_2) = 2y_1^2 + y_2$, and $\varphi(x_3) = \frac{1}{3}y_2$. We compute the reduced Gröbner basis of the ideal $J = (x_1 - \frac{1}{5}y_1 - y_2^4, x_2 - 2y_1^2 - y_2, x_3 - \frac{1}{3}y_2)$ with respect to an elimination ordering for $\{y_1, y_2\}$. Using CoCoA, we get $\{y_1 - 5x_1 + 405x_3^4, y_2 - 3x_3, x_3^8 - \frac{2}{81}x_1x_3^4 + \frac{1}{6561}x_1^2 - \frac{1}{328050}x_2 + \frac{1}{109350}x_3\}$.

Thus Proposition 3.6.6.d shows that φ is surjective, Proposition 3.6.9.b shows $\mathrm{Ker}(\varphi) = (x_3^8 - \frac{2}{81}x_1x_3^4 + \frac{1}{6561}x_1^2 - \frac{1}{328050}x_2 + \frac{1}{109350}x_3)$, and Proposition 3.6.9.c shows that a right inverse of φ is given by the $\mathbb{Q}$-algebra homomorphism $\psi : P' \to P$ defined by $\psi(y_1) = -405x_3^4 + 5x_1$ and $\psi(y_2) = 3x_3$.

Our last topic in this section is the computational treatment and characterization of bijective K-algebra homomorphisms. In Volume 2, we shall see that a surjective K-algebra homomorphism $\varphi : P \longrightarrow P'$ can only exist if $n \geq m$. If φ is bijective, then it is easy to check that also the inverse map $\varphi^{-1} : P' \longrightarrow P$ is a K-algebra homomorphism. Thus, if φ is bijective, we must have $n = m$. Hence the map φ is a **K-algebra automorphism** of P in this case, i.e. a K-algebra homomorphism $\varphi : P \longrightarrow P$ such that there exists a K-algebra homomorphism $\psi : P \longrightarrow P$ which satisfies $\psi \circ \varphi = \mathrm{id}_P$ and $\varphi \circ \psi = \mathrm{id}_P$.

The following lemma shows that surjective K-algebra homomorphisms $\varphi : P \longrightarrow P$ are already K-algebra automorphisms.

Lemma 3.6.11. *Let R be a Noetherian ring, and let $\varphi : R \longrightarrow R$ be a ring homomorphism. Then the following conditions are equivalent.*

a) *The map φ is surjective.*
b) *The map φ is bijective.*

Proof. It suffices to show "a)$\Rightarrow$b)". For every $i \geq 1$, we obviously have $\mathrm{Ker}(\varphi^i) \subseteq \mathrm{Ker}(\varphi^{i+1})$. Since R is a Noetherian ring, there exists a number $j \in \mathbb{N}$ such that $\mathrm{Ker}(\varphi^i) = \mathrm{Ker}(\varphi^j)$ for all $i \geq j$. Now let $r \in \mathrm{Ker}(\varphi)$. The surjectivity of φ implies the surjectivity of φ^j. Hence there exists an element $r' \in R$ such that $r = \varphi^j(r')$. Then $0 = \varphi(r) = \varphi^{j+1}(r')$ implies $r' \in \mathrm{Ker}(\varphi^{j+1}) = \mathrm{Ker}(\varphi^j)$, and therefore $r = \varphi^j(r') = 0$. Consequently, the map φ is injective. $\square$

By combining the preceding results, we can characterize K-algebra auto-morphisms of P as follows.

Proposition 3.6.12. (Automomorphisms of Polynomial Rings)
Let $P = K[x_1, \ldots, x_n]$, and let $\varphi : P \longrightarrow P$ be a K-algebra homo-morphism given by $\varphi(x_i) = f_i$ for $i = 1, \ldots, n$. Furthermore, let $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_n]$, let $J = (x_1 - f_1(y_1, \ldots, y_n), \ldots, x_n - f_n(y_1, \ldots, y_n))$, and let σ be an elimination ordering for $\{y_1, \ldots, y_n\}$. Then the following conditions are equivalent.

a) The map φ is a K-algebra automorphism of P.
b) The homomorphism φ is surjective.
c) There exist polynomials $h_1, \ldots, h_n \in P$ such that the reduced σ-Gröbner basis of J is $\{y_1 - h_1, \ldots, y_n - h_n\}$.

If these conditions hold, the K-algebra homomorphism $\psi : P \to P$ defined by $\psi(x_i) = h_i$ for $i = 1, \ldots, n$ is the inverse of φ, i.e. we have $\psi = \varphi^{-1}$.

Proof. The equivalence of a) and b) is a special case of Lemma 3.6.11. By Proposition 3.6.9, condition a) implies c). Given c), we can apply Proposition 3.6.6.d to conclude that φ is surjective. By Lemma 3.6.11, it is then an isomorphism of K-algebras. Since Proposition 3.6.9.c shows that ψ is a right inverse of φ, it is the inverse of φ. $\qquad\square$

Once again, we can take a concrete K-algebra automorphism of P and ask for a computation of its inverse. But even if we start with a fairly simple map, the size and the intricacy of the answer may surprise us.

Example 3.6.13. Using the polynomial ring $P = \mathbb{Q}[x_1, x_2, x_3]$, let us con-sider the two $\mathbb{Q}$-algebra homomorphisms

$$
\begin{array}{ccc}
\psi_1 : & P & \longrightarrow & P \\
& x_1 & \longmapsto & x_1 \\
& x_2 & \longmapsto & x_2 + x_1^2 \\
& x_3 & \longmapsto & x_3 + x_1 x_2
\end{array}
\qquad \text{and} \qquad
\begin{array}{ccc}
\psi_2 : & P & \longrightarrow & P \\
& x_1 & \longmapsto & x_1 + x_2 x_3 \\
& x_2 & \longmapsto & x_2 - x_3 + x_3^2 \\
& x_3 & \longmapsto & x_3
\end{array}
$$

It is easy to apply the preceding proposition in order to see that those two maps are $\mathbb{Q}$-algebra automorphisms of P. Thus also $\varphi = \psi_2 \circ \psi_1$ is a $\mathbb{Q}$-algebra automorphism of P. Let $f_i = \varphi(x_i)$ for $i = 1, 2, 3$, i.e. let $f_1 = x_1 + x_2 x_3$, let $f_2 = x_2 - x_3 + x_1^2 + x_3^2 + 2x_1 x_2 x_3 + x_2^2 x_3^2$, and let $f_3 = x_3 + x_1 x_2 - x_1 x_3 + x_1 x_3^2 + x_2^2 x_3 - x_2 x_3^2 + x_2 x_3^3$. It follows that x_1, x_2, and x_3 can be expressed as polynomials in f_1, f_2, and f_3 by the method explained at the end of the last proposition. In the case at hand, the results are the impressive expressions

$$
\begin{aligned}
x_1 \;=\; & f_1^9 - 3f_1^7 f_2 + 3f_1^5 f_2^2 + 3f_1^6 f_3 - f_1^6 - f_1^3 f_2^3 - 6f_1^4 f_2 f_3 + f_1^5 + 2f_1^4 f_2 \\
& + 3f_1^2 f_2^2 f_3 + 3f_1^3 f_3^2 - 2f_1^3 f_2 - f_1^2 f_2^2 - 2f_1^3 f_3 - 3f_1 f_2 f_3^2 + f_1 f_2^3 \\
& + 2f_1 f_2 f_3 + f_3^3 - f_2 f_3 - f_2^2 + f_1 \\
x_2 \;=\; & -f_1^6 + 2f_1^4 f_2 - f_1^2 f_2^2 - 2f_1^3 f_3 + f_1^3 + 2f_1 f_2 f_3 - f_1^2 - f_1 f_2 - f_3^2 \\
& + f_2 + f_3 \\
x_3 \;=\; & f_1^3 - f_1 f_2 + f_3
\end{aligned}
$$

Exercise 1. Find a K-algebra homomorphism $\varphi : P/I \longrightarrow P'/I'$ such that P'/I' is not a finitely generated P/I-module via φ.

Exercise 2. Solve the implicitization problems for the following tuples of polynomials.
a) $(t^3, t^4 - t, t^5 + t - 1) \in \mathbb{Q}[t]^3$
b) $(t^{31} + t^6 + t, t^8, t^{10}) \in \mathbb{Q}[t]^3$
c) $(\frac{1}{2} t^3, t^4 - \frac{1}{3} s, t^5 + t - s^2) \in \mathbb{Q}[s, t]^3$
d) $(s + t, s(s + 2t), s^2(s + 3t)) \in \mathbb{Q}[s, t]^3$ (The set of zeros of the solution is called the **tangent surface to the twisted cubic**.)
e) $(s^3 - 3st^2 - 3s, t^3 - 3s^2t - 3t, 3s^2 - 3t^2) \in \mathbb{Q}[s, t]^3$ (The set of zeros of the solution is called the **Enneper surface**.)

Exercise 3. Let P/I be an affine K-algebra such that $\dim_K(P/I)$ is finite. Prove that every element in P/I is algebraic over K.

Exercise 4. Given polynomials $f_1, \ldots, f_s \in P = K[x_1, \ldots, x_n]$ and an ideal $I \subseteq P$, how can one decide effectively whether the residue classes $f_1 + I, \ldots, f_s + I$ of $f_1, \ldots, f_s$ in the affine K-algebra $R = P/I$ are algebraically independent over K?

Exercise 5. Let $P = K[x, y]$ be a polynomial ring over a field K, and let I be a non-zero principal ideal in P. Prove that at least one element of the set $\{x + I, y + I\} \subseteq P/I$ is transcendental over K.

Exercise 6. Implement the method of Example 3.6.8 to compute the representation of a symmetric polynomial in terms of the elementary symmetric polynomials by writing a CoCoA function `ReprSym2(...)`.
Hint: Use the Gröbner basis of $J = (x_1 - s_1, \ldots, x_n - s_n)$ provided by Tutorial 23.d.

Exercise 7. Let $\varphi : K[x] \to K[y]$ be a K-algebra homomorphism, and let $f = \varphi(x)$.
a) Prove that φ is injective if and only if $f \notin K$.
b) Prove that φ is surjective if and only if $\deg(f) = 1$.

Exercise 8. Let $\varphi : R \to S$ be a ring homomorphism.
a) Prove that φ is a ring isomorphism (i.e. that there exists a ring homomorphism $\psi : S \longrightarrow R$ such that $\psi \circ \varphi = \mathrm{id}_R$ and $\varphi \circ \psi = \mathrm{id}_S$) if and only if φ is bijective.
b) Give an example of an injective ring homomorphism $\varphi : R \longrightarrow S$ such that there is no ring homomorphism $\psi : S \longrightarrow R$ which satisfies $\psi \circ \varphi = \mathrm{id}_R$.
c) Give an example of a surjective ring homomorphism $\varphi : R \longrightarrow S$ such that there exists no ring homomorphism $\psi : S \longrightarrow R$ satisfying $\varphi \circ \psi = \mathrm{id}_S$.

Exercise 9. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and let $\varphi : P \longrightarrow P$ be a K-algebra homomorphism. Prove that if φ is a K-algebra automorphism of P and $\varphi(x_i) = f_i$ for $i = 1, \ldots, n$, then the **Jacobian determinant** $\det(\frac{\partial f_i}{\partial x_j})$ is an element of $K \setminus \{0\}$.
The question whether over fields K of characteristic zero the converse of this statement holds is the famous (and as yet unsolved) **Jacobian Conjecture**.

Exercise 10. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $R = K[f_1, \ldots, f_m] \subseteq P$ be a finitely generated subalgebra with $f_1, \ldots, f_m \in P$, and let $I \subseteq P$ be an ideal.

a) Show that we can get a presentation of the affine K-algebra $R/(I \cap R)$ as follows. Let $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, and let J be the ideal $J = IQ + (y_1 - f_1, \ldots, y_m - f_m)$ in Q. Then there is an isomorphism of K-algebras

$$R/(I \cap R) \cong K[y_1, \ldots, y_m]/(J \cap K[y_1, \ldots, y_m])$$

b) How can one compute a system of generators of the ideal $I \cap R$ in R? Write a CoCoA function which computes this system of generators.

c) Generalize parts a) and b) to P-submodules of P^r for some $r \geq 1$ and their intersection with R^r.

Tutorial 39: Projections

In Section 3.4, we promised to provide you with a geometric interpretation of elimination. This interpretation is based on projections. It is the topic of the present tutorial. Since we shall need to use the language of algebraic geometry, we assume that you have read Section 2.6 and Tutorial 27.

Let K be a field. The affine space $\mathbb{A}_K^n$ was defined as the set K^n together with the Zariski topology. As usual in mathematics, we do not only consider objects, but we also introduce the appropriate kind of maps between them. A **polynomial map** (or a **morphism of affine spaces**) is defined as a map $\psi : \mathbb{A}_K^m \to \mathbb{A}_K^n$ for which there exist polynomials $f_1, \ldots, f_n \in K[y_1, \ldots, y_m]$ such that $\psi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$ for all points $(a_1, \ldots, a_m) \in \mathbb{A}_K^m$.

In the first part of this tutorial, we examine some general properties of polynomial maps. In particular, we want to study their fibers and images. Let $P = K[x_1, \ldots, x_n]$ and $P' = K[y_1, \ldots, y_m]$ be two polynomial rings over K, let $f_1, \ldots, f_n \in P'$, let $\varphi : P \longrightarrow P'$ be the K-algebra homomorphism defined by $\varphi(x_i) = f_i$ for $i = 1, \ldots, n$, and let $\psi : \mathbb{A}_K^m \longrightarrow \mathbb{A}_K^n$ be the polynomial map satisfying $\psi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$ for all $(a_1, \ldots, a_m) \in \mathbb{A}_K^m$.

a) Let I be an ideal in P, and let $V = \mathcal{Z}(I)$ be the zero-set in $\mathbb{A}_K^n$ defined by I. Show that $\psi^{-1}(V)$ is the zero-set in $\mathbb{A}_K^m$ defined by the ideal $J = (\varphi(f) \mid f \in I) \subseteq P'$.

b) Let $\mathcal{P} = (a_1, \ldots, a_n) \in \mathbb{A}_K^n$. Use a) to describe the **fiber** $\psi^{-1}(\mathcal{P})$ of the polynomial map ψ over the point $\mathcal{P}$. Write a CoCoA program `Fiber(...)` which computes the ideal defining this fiber.

c) Let $g \in P$ be an element of the vanishing ideal of $\mathrm{Im}(\psi)$. Show that the polynomial $g(f_1, \ldots, f_n) \in P'$ vanishes on all points of $\mathbb{A}_K^m$. Recall that we proved in Tutorial 16.c that this implies $g(f_1, \ldots, f_n) = 0$ if K is infinite.

d) Let p be a prime number, let $q = p^e$ for some $e > 0$, and let K be the finite field $K = \mathbb{F}_q$ (see Tutorial 3). Prove that the ideal of all polynomials $h \in P'$ with the property that $h(a_1, \ldots, a_m) = 0$ for all $(a_1, \ldots, a_m) \in \mathbb{A}_K^m$ is generated by $\{y_1^q - y_1, \ldots, y_m^q - y_m\}$.
Hint: It suffices to show that $h = 0$ if $\deg_{y_i}(h) < q$ for $i = 1, \ldots, m$. Consider $h(a_1, \ldots, a_{m-1}, y_m)$ and argue by induction on m.

To avoid the problems encountered in d), we assume from now on that K is an infinite field. Then we know that $g(f_1, \ldots, f_n) = 0$ for all $g \in \mathcal{I}(\mathrm{Im}(\psi))$. We introduce the same notation as in the section and let Q be the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, and J the ideal $J = (x_1 - f_1, \ldots, x_n - f_n)$ in Q.

e) Prove that J is a prime ideal in Q, and conclude that $I = J \cap P$ is a prime ideal in P.

f) Show that the elimination ideal $I = J \cap P$ agrees with the vanishing ideal of $\mathrm{Im}(\psi)$.
Hint: Apply Proposition 3.6.1.b.

g) Write a CoCoA function `Image(...)` which takes the tuple $(f_1, \ldots, f_n)$ and computes the vanishing ideal of the image of the associated polynomial map ψ. Apply your function `Image(...)` and calculate the vanishing ideals of the images of the following maps.

1) $\psi : \mathbb{A}_\mathbb{Q}^2 \longrightarrow \mathbb{A}_\mathbb{Q}^3$ defined by $(a_1, a_2) \mapsto (a_1 a_2, a_1 a_2^2, a_2^3)$
2) $\psi : \mathbb{A}_\mathbb{Q}^2 \longrightarrow \mathbb{A}_\mathbb{Q}^3$ defined by $(a_1, a_2) \mapsto (a_1, a_1 a_2, a_2^2)$
   (The image of this map is called **Whitney's umbrella**.)
3) $\psi : \mathbb{A}_\mathbb{Q}^2 \longrightarrow \mathbb{A}_\mathbb{Q}^5$ defined by $(a_1, a_2) \mapsto (a_1, a_2, a_1^2, a_1 a_2, a_2^2)$
   (The image of this map is called the **Veronese surface** in $\mathbb{A}_\mathbb{Q}^5$.)

h) Let $I = J \cap P$. Prove that $\mathcal{Z}(I)$ is the Zariski closure of $\mathrm{Im}(\psi)$.
Hint: Tutorial 27.h implies this claim if K is algebraically closed. In the general case, embed K in its algebraic closure and argue that any zero-set in $\mathbb{A}_K^n$ containing $\mathrm{Im}(\psi)$ has to contain $\mathcal{Z}(I)$.

i) Show that $\mathrm{Im}(\psi) \subset \mathcal{Z}(I)$ in the first example of part g) above. Moreover, prove that the same thing happens even if replace the field $\mathbb{Q}$ by $\mathbb{C}$.
Hint: Consider the line $\mathcal{Z}(x_2, x_3)$.

The last part of this tutorial is devoted to explaining its title. Given positive integers $m \geq n$ and n distinct numbers $i_1, \ldots, i_n \in \{1, \ldots, m\}$, the map $\pi_{i_1, \ldots, i_n} : \mathbb{A}_K^m \longrightarrow \mathbb{A}_K^n$ defined by $(a_1, \ldots, a_m) \mapsto (a_{i_1}, \ldots, a_{i_n})$ is called the **projection** of $\mathbb{A}_K^m$ onto its components $(i_1, \ldots, i_n)$. It is clearly a polynomial map. Using projections, we can give the following geometric interpretation of the ideal J and its elimination ideal $I = J \cap P$.

j) The set of all points $(a_1, \ldots, a_m, b_1, \ldots, b_n) \in \mathbb{A}_K^{m+n}$ such that we have $b_i = f_i(a_1, \ldots, a_m)$ for $i = 1, \ldots, n$ is called the **graph** of the map ψ. Let us denote it by G. Prove that $G = \mathcal{Z}(J)$ and $J = \mathcal{I}(G)$.

k) Prove that the two projections $\pi^{(1)} = \pi_{1,\ldots,m} : \mathbb{A}_K^{m+n} \longrightarrow \mathbb{A}_K^m$ and $\pi^{(2)} = \pi_{m+1,\ldots,m+n} : \mathbb{A}_K^{m+n} \longrightarrow \mathbb{A}_K^n$ induce surjections $\pi_G^{(1)} : G \longrightarrow \mathbb{A}_K^m$ and $\pi_G^{(2)} : G \longrightarrow \mathcal{Z}(I)$, and that we have a commutative diagram

$$
\begin{array}{ccc}
 & G & \\
\pi_G^{(1)} \swarrow & & \searrow \pi_G^{(2)} \\
\mathbb{A}_K^m \xrightarrow{\quad \psi \quad} & & \mathcal{Z}(I) \subseteq \mathbb{A}_K^n
\end{array}
$$

Thus the formation of the elimination ideal $I = J \cap P$ is the exact algebraic analogue of the formation of the projection $\pi_G^{(2)} : G \longrightarrow \mathcal{Z}(I)$.

Tutorial 40: Gröbner Bases and Invariant Theory

In Tutorial 12 and Example 3.6.8 we saw that the K-subalgebra of all symmetric polynomials in the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K is generated by the elementary symmetric polynomials, and we saw how one can represent an arbitrary symmetric polynomial as a polynomial expression in those elementary symmetric polynomials. In this tutorial we want to generalize these results to K-subalgebras of P consisting of polynomials which are invariant under the action of a finite matrix group.

Let $\mathrm{GL}_n(K) \subseteq \mathrm{Mat}_n(K)$ be the group of all invertible $n \times n$-matrices over K. It is called the **general linear group** over K and operates on the polynomial ring P by

$$
\begin{array}{ccc}
\mathrm{GL}_n(K) \times P & \longrightarrow & P \\
(\mathcal{A}, f) & \longmapsto & f(\mathcal{A} \cdot \boldsymbol{x})
\end{array}
$$

where we use $\boldsymbol{x}$ to denote the column vector $\boldsymbol{x} = (x_1, \ldots, x_n)^{\mathrm{tr}}$, and where we let $\mathcal{A} \cdot \boldsymbol{x} = (a_{11}x_1 + \cdots + a_{1n}x_n, \ldots, a_{n1}x_1 + \cdots + a_{nn}x_n)$ for $\mathcal{A} = (a_{ij})$. In the sequel, we let $G \subseteq \mathrm{GL}_n(K)$ be a finite subgroup. We shall say that G is a **finite matrix group**.

a) Write a CoCoA function `IsGroup(...)` which takes a list of matrices in $\mathrm{Mat}_n(K)$ and checks whether they form a finite matrix group. Apply your function to verify that the following sets of matrices do indeed form finite matrix groups.

1) $C_2 = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix} \right) \right\}$ (**cyclic group** of order 2)

2) $C_3 = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix} \right), \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix} \right) \right\}$ (**cyclic group** of order 3)

3) $C_4 = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right) \right\}$ (**cyclic group** of order 4)

4) $V_4 = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right), \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix} \right) \right\}$ (**Klein four group**)

5) $C_6 = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\}$ **(cyclic group** of order 6)

6) $S_3 = \left\{ \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right), \right.$
$\left. \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right) \right\}$ **(permutation group** on three elements)

7) $D_4 = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \right.$
$\left. \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \right\}$ **(dihedral group** of order 8)

8) $R_8 = \left\{ \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \right.$
$\left. \left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right) \right\}$ **(reflection group** of the coordinate planes)

9) $A_4 = \left\{ \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right), \right.$
$\left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right), $
$\left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{smallmatrix}\right) \right\}$ **(alternating group** on four elements)

10) $W_{24} = \left\{ \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right), \right.$
$\left(\begin{smallmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right), $
$\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{smallmatrix}\right), $
$\left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{smallmatrix}\right), $
$\left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right) \right\}$
(rotation group of the cube)

b) A polynomial $f \in P$ is said to be **invariant** under G if it satisfies $f(\mathcal{A} \cdot \boldsymbol{x}) = f(x_1, \ldots, x_n)$ for all matrices $\mathcal{A} \in G$. Write a CoCoA function `IsInvariant(...)` which takes a list of matrices representing a finite matrix group and a polynomial $f \in P$, checks whether f is invariant under this group, and returns the corresponding Boolean value. Apply your function in the following cases.

1) $G = C_2$, $f = x^2 - xy + y^2$
2) $G = C_4$, $f = x^3y + 2x^2y^2 - xy^3$
3) $G = W_{24}$, $f = (x^2 - y^2)(x^2 - z^2)(y^2 - z^2)$
4) $G = W_{24}$, $f = xyz(x^2 - y^2)(x^2 - z^2)(y^2 - z^2)$

c) Show that the set of all polynomials in P which are invariant under G is a graded K-subalgebra of P. We denote this subalgebra by P^G and

call it the **ring of invariants** of G. (Here we equip P with the standard grading.)

Recall that not every K-subalgebra of P is finitely generated (see Example 2.6.4). Our next goal is to show that P^G is a finitely generated subalgebra if $\mathrm{char}(K) = 0$. Thus we assume from here on that K is a field of characteristic zero. The map $\varrho_G : P \longrightarrow P$ defined by $\varrho_G(f) = \frac{1}{\#G} \sum_{\mathcal{A} \in G} f(\mathcal{A} \cdot \boldsymbol{x})$ is called the **Reynolds operator** of G.

d) Show that $\varrho_G : P \longrightarrow P$ is a homogeneous K-linear map which has the following properties.

  1) For all $f \in P^G$ and $g \in P$, we have $\varrho_G(fg) = f \varrho_G(g)$.
  2) We have $\mathrm{Im}(\varrho_G) = P^G$ and $\varrho_G \circ \varrho_G = \varrho_G$.

e) Write a CoCoA function `Reynolds(...)` which takes a list of matrices representing the elements of G and a polynomial f and computes $\varrho_G(f)$. Apply this function in the following cases.

  1) $G = V_4$, $f = x + y$
  2) $G = D_4$, $f = x^3 - xy + y^3$
  3) $G = A_4$, $f = x_1 - x_2 + x_3 - x_4$

f) Prove that there are finitely many homogeneous polynomials $f_1, \ldots, f_s$ in P such that $P^G = K[f_1, \ldots, f_s]$.

  Hint: Let I be the ideal in P which is generated by all homogeneous polynomials $f \in P^G$ such that $\deg(f) > 0$, and let $\{f_1, \ldots, f_s\}$ be a homogeneous system of generators of I. Assume that $K[f_1, \ldots, f_s] \subset P^G$ and choose a homogeneous polynomial $g \in P^G \setminus K[f_1, \ldots, f_s]$ of minimal degree. Then use Corollary 1.7.11 to write $g = \sum_{i=1}^{s} h_i f_i$ with homogeneous polynomials $h_1, \ldots, h_s \in P$ of positive degree. Now apply ϱ_G and use d).

Unfortunately, the proof of f) does not tell us how we can find finitely many homogeneous polynomials $f_1, \ldots, f_s \in P$ such that $P^G = K[f_1, \ldots, f_s]$. Below we formulate an algorithm which does this job, although it is rather inefficient. If you are adventurous, you can try to reconstruct Emmy Noether's proof for the correctness of this algorithm later in part j). A more powerful computational approach to the problem of finding the ring of invariants is based on *Molien's Theorem* and will be discussed in Volume 2.

g) Consider the following sequence of instructions.

  1) Let $L = \emptyset$. Choose a degree-compatible term ordering σ on $\mathbb{T}^n$ and compute the tuple $(t_1, \ldots, t_N)$ of all terms of degree $\leq \#G$ in P, ordered increasingly with respect to σ. (Here N is the number of such terms.)
  2) For $i = 1, \ldots, N$, compute $\varrho_G(t_i)$. Use the Subalgebra Membership Test 3.6.7 to check whether $\varrho_G(t_i) \in K[f \mid f \in L]$. If this is not the case, append $\varrho_G(t_i)$ to the set L.
  3) Return L.

Later we shall prove that this is an algorithm which returns a set L of homogeneous polynomials such that $P^G = K[f \mid f \in L]$. Implement this algorithm in a CoCoA function `Invariants(...)` whose input is a list of matrices representing the elements of G.

h) Apply your function `Invariants(...)` to compute the ring of invariants for as many of the groups listed in part a) as possible. How far can you get? Can you think of possible optimizations of your function?

i) After you have found a system of algebra generators for P^G, you can use Corollary 3.6.7 to represent any invariant polynomial as a polynomial expression in those algebra generators. Write a CoCoA function `ReprInvariants(...)` which performs this task and apply it in the following cases.

1) $G = C_2$, $f = x^{10} + 2x^9 y + 3x^8 y^2 + \cdots + 11 y^{10}$
2) $G = C_4$, $f = 3x^6 y^2 - 2x^5 y^3 + 6x^4 y^4 + 2x^3 y^5 + 3x^2 y^6$
3) $G = C_6$, $f = x^4 y^2 - 2x^3 y^3 + x^2 y^4$

j) *(This part is a more challenging project.)* Prove the correctness of the algorithm in g) using the following steps.

1) For $d \geq 0$, let $p_d = x_1^d + \cdots + x_n^d$. Using induction on n, prove **Newton's identities**

$$p_d - s_1 p_{d-1} + \cdots + (-1)^{d-1} s_{d-1} p_1 + (-1)^d d s_d = 0$$

where $s_1, \ldots, s_n$ are the elementary symmetric polynomials, and where $s_i = 0$ for $i > n$ (see Tutorial 12.c).

2) Using induction on $d \geq 0$, prove that s_d is a polynomial in $p_1, \ldots, p_n$. Conclude that every symmetric polynomial is a polynomial in $p_1, \ldots, p_n$. (You need to use $\mathrm{char}(K) = 0$ here.)

3) Show that it suffices to prove $\varrho_G(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) \in K[f \mid f \in L]$ for all tuples $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ in order to show the correctness of the algorithm.

4) Let $d \geq 1$ and $\gamma = \#G$. Introduce new indeterminates $y_1, \ldots, y_n$. For every matrix $\mathcal{A} \in G$, we let $a_1, \ldots, a_n$ be the rows of $\mathcal{A}$ and $q_{\mathcal{A}}$ the polynomial $q_{\mathcal{A}} = (a_1 \cdot \boldsymbol{x}) y_1 + \cdots + (a_n \cdot \boldsymbol{x}) y_n$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$. Prove the formula

$$\sum_{\mathcal{A} \in G} (q_{\mathcal{A}})^d = \gamma \cdot \sum_{\alpha_1 + \cdots + \alpha_n = d} \frac{d!}{\alpha_1! \cdots \alpha_n!} \varrho_G(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) y_1^{\alpha_1} \cdots y_n^{\alpha_n}$$

Hint: Substitute $(a_i \cdot \boldsymbol{x}) y_i$ in the expansion of $(x_1 + \cdots + x_n)^d$ and sum over all $\mathcal{A} \in G$.

5) Using step 2), write $\sum_{\mathcal{A} \in G} (q_{\mathcal{A}})^d$ as a polynomial in the expressions

$$\sum_{\mathcal{A} \in G} (q_{\mathcal{A}}), \ldots, \sum_{\mathcal{A} \in G} (q_{\mathcal{A}})^\gamma.$$

6) Then substitute the formulas of step 4) in this polynomial and compare the coefficients of $y_1^{\alpha_1} \cdots y_n^{\alpha_n}$ for all $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

Tutorial 41: Subalgebras of Function Fields

The purpose of this tutorial is to study finitely generated subalgebras of algebraic function fields. More precisely, we let R be an integral domain and $Q(R)$ its field of fractions.

a) Show that $Q(R)$ is a finitely generated R-algebra if and only if it is generated by a single element.

b) Given $a_1, \ldots, a_r, b_1, \ldots, b_r \in R$ and a polynomial $f \in R[y_1, \ldots, y_r]$, prove that there exist $i_1, \ldots, i_r > 0$ such that

$$b_1^{i_1} \cdots b_r^{i_r} f = g(a_1, \ldots, a_r) + h$$

where $g \in R[y_1, \ldots, y_r]$ and $h \in (b_1 y_1 - a_1, \ldots, b_r y_r - a_r) \subseteq R[y_1, \ldots, y_r]$.

c) Let $a_1, \ldots, a_r \in R$ and $b_1, \ldots, b_r \in R \setminus \{0\}$. Show that the finitely generated R-subalgebra $R[\frac{a_1}{b_1}, \ldots, \frac{a_r}{b_r}]$ of $Q(R)$ has a presentation

$$R[\tfrac{a_1}{b_1}, \ldots, \tfrac{a_r}{b_r}] \cong R[y_1, \ldots, y_r]/I \cap R[y_1, \ldots, y_r]$$

where $y_1, \ldots, y_r, z_1, \ldots, z_r$ are independent indeterminates over R and where I is the ideal $I = (b_1 y_1 - a_1, \ldots, b_r y_r - a_r, b_1 z_1 - 1, \ldots, b_r z_r - 1)$ in the ring $R[y_1, \ldots, y_r, z_1, \ldots, z_r]$. (*Hint:* Define an R-algebra homomorphism $\varphi : R[y_1, \ldots, y_r] \longrightarrow R[\frac{a_1}{b_1}, \ldots, \frac{a_r}{b_r}]$ by $y_i \longmapsto \frac{a_i}{b_i}$ for $i = 1, \ldots, r$ and show that its kernel is $I \cap R[y_1, \ldots, y_r]$.)

d) Now let K be a field and $R = K[x_1, \ldots, x_n]/\mathfrak{p}$ an affine K-algebra, where $\mathfrak{p} \subseteq K[x_1, \ldots, x_n]$ is a prime ideal. Prove that for polynomials $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ and $g_1, \ldots, g_r \in K[x_1, \ldots, x_n] \setminus \{0\}$ we have a presentation

$$R[\tfrac{f_1}{g_1}, \ldots, \tfrac{f_r}{g_r}] \cong K[x_1, \ldots, x_n, y_1, \ldots, y_r]/(I + \bar{\mathfrak{p}}) \cap K[x_1, \ldots, x_n, y_1, \ldots, y_r]$$

where I is defined in an analogous way as above and $\bar{\mathfrak{p}}$ is the extension ideal of $\mathfrak{p}$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_r, z_1, \ldots, z_r]$.

e) Write a CoCoA function `FFSubAlg(...)` which finds a presentation of $R[\frac{f_1}{g_1}, \ldots, \frac{f_r}{g_r}]$ for $R = K[x_1, \ldots, x_n]/J$ from the lists $[f_1, \ldots, f_r]$ and $[g_1, \ldots, g_r]$, and from a system of generators of J.

f) Apply the function `FFSubAlg(...)` to compute a presentation of $R[\frac{\bar{x}_2}{\bar{x}_1}]$ for $R = \mathbb{Q}[x_1, x_2, x_3, x_4]/(x_1 x_3 - x_2 x_4)$. Show also that $R[y_1]/(x_1 y_1 - x_2)$ is not an integral domain.

g) Prove $R[\frac{a}{b}] \cong R[y]/(by - a)$ if R is a factorial domain and $a, b \in R \setminus \{0\}$ are coprime. Note that $R[\frac{1}{b}] \cong R[y]/(by - 1)$ is true without the assumption that R is a factorial domain (see Proposition 3.5.6).

3.7 Systems of Polynomial Equations

<div align="right">

ella va amica da cima a valle
[from hilltop to valley lightly she drifts]
(Lorenzo Robbiano, palindromic verse.
It is painted on a sundial in Castelletto d'Orba)

</div>

This is the last section, but in some sense it could also be considered as a chapter by itself, or perhaps as the starting point of Volume 2, or as a motivation for the subjects dealt with in this book. We are not trying to suggest a palindromic reading of the topics treated so far. Rather, we would like to convince you that the ideas developed here should not be considered as steps of a linear evolution with a clear direction.

Mathematics moves as other human activities do. Sometimes it seems to climb up a steep mountain, sometimes it slowly drifts down into fertile valleys. What is the ultimate goal? It could be the solution of a famous problem, the development of a new theory, a better understanding of an old theory, or the pursuit of concrete applications in the *real* world. Mathematicians go back and forth between those goals, following old paths or creating new ones.

During this perennial wandering, almost certainly they are going to encounter systems of polynomial equations. They appear in many mathematical models of physical systems, in the study of algebraic structures, and in the algebraic description of geometric objects. We should keep in mind that the main goal is to *solve* them. Thus they lie at the heart of Computational Commutative Algebra.

Our choice, to devote this final section to systems of polynomial equations, was made because we wanted to show how many of the computational skills acquired so far have to be used in order to get a better grip on the problem. No more wandering about. Digging the ground and finding the *roots* is the main task now. Let us have a closer look at the difficulties which lie ahead.

Given polynomials $f_1, \ldots, f_s$ in the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K, we can study the following system of polynomial equations:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \quad \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

Three fundamental questions suggest themselves.

<div align="center">

1. What does it mean to solve this system of equations?

</div>

If the polynomials $f_1, \ldots, f_s$ have degrees ≤ 1, the answer is a well-known result in Linear Algebra: there are finitely many vectors in K^n such that their linear combinations are precisely the set of solutions of the system of equations. As soon as one of the polynomials $f_1, \ldots, f_s$ has degree ≥ 2, the situation becomes much more complicated.

It turns out that it is more promising to look for the set of solutions of the above system of equations in $\overline{K}^n$, where $\overline{K}$ is the algebraic closure of K. Thus, to solve the above system of equations means to determine the set of zeros of the ideal $I = (f_1, \ldots, f_s)$ in the sense of Section 2.6.

2. How can we describe this set of solutions?

For a single solution $(a_1, \ldots, a_n) \in \overline{K}^n$, we can try to determine the minimal polynomials of $a_1, \ldots, a_n$ over K. This specifies those algebraic numbers up to conjugates. And if $K = \mathbb{Q}$, we could then use methods of numerical analysis to single out the precise solution from that set of conjugates by finding a sufficiently good approximation in $\mathbb{Q}[i]$. Already if K is a finite field, those methods do not apply.

Thus, in most cases, we shall have to content ourselves with solving the system of equations in a symbolic way. This leaves us with the following problem. Suppose that a solution $(a_1, \ldots, a_n) \in \overline{K}^n$ is described by the minimal polynomials of $a_1, \ldots, a_n$ over K.

3. How many and which tuples of conjugates form the set of solutions?

Towards the end of this section we shall give what we view as a good answer to this question. We shall show how to compute a single polynomial in one indeterminate such that if you assign symbols to its roots, then you can write down the exact solutions of the system as polynomial expressions in those symbols.

To organize the material, we decided to split this section into three subsections. They deal with a bound for the number of solutions, radicals of zero-dimensional ideals, and with solving systems effectively. Let us look at their contents one-by-one.

First, it is important to be able to recognize which systems have only a finite number of solutions. This is achieved by the Finiteness Criterion 3.7.1. If the set of solutions is infinite, we cannot list them anyway, so let us assume it is finite. Then we shall provide estimates for the number of solutions. It turns out that $\dim_K(P/I)$ provides such a bound (see Proposition 3.7.5). However this bound is not sharp (see Example 3.7.6), because it is unable to distinguish between *simple* and *multiple* roots.

In the second subsection we turn our attention to radical ideals. Starting from this point we shall assume that either $\mathrm{char}(K) = 0$ or K is a perfect field of characteristic $\mathrm{char}(K) = p > 0$ which has effective p^{th} roots (see Definition 3.7.10). In order to find an algorithm which computes the radical of the given ideal $I = (f_1, \ldots, f_s)$, we first have to explain how one can compute the squarefree part of a polynomial in $K[x]$ (see Proposition 3.7.12). Then we prove Seidenberg's Lemma 3.7.15 which provides a criterion for a zero-dimensional ideal I to be radical and permits us to develop an algorithm which computes the radical of I (see Corollary 3.7.16). If the ideal is radical, we finally get the optimal bound for the number of solutions (see Theorem 3.7.19).

After all this preparatory work, we are ready to handle the problem of solving systems effectively in the third subsection. Given a zero-dimensional radical ideal, we show how to change coordinates in order to put the zeros in normal x_n-position (see Proposition 3.7.22), i.e. to transform the given system into a new one which is better suited for revealing its solutions. Then the Shape Lemma 3.7.25 says that, after we compute the reduced Lex-Gröbner basis of the resulting ideal, we can write down the solution set of the system in a very explicit way. The last step is made in Corollary 3.7.26 where we present an algorithm which combines all the pieces of information acquired before and computes the solutions in a suitable format.

A final remark is necessary here. We do not claim that the algorithms contained in this section are particularly efficient. They are mainly intended to show that an algorithmic solution of the problem is possible, and to indicate the twists and turns one encounters when the computation has to be carried out in a symbolic environment.

In the sequel, let K be a field, let $P = K[x_1, \ldots, x_n]$, let $f_1, \ldots, f_s \in P$, and let $I = (f_1, \ldots, f_s)$. Moreover, let $\overline{K}$ be the algebraic closure of K, and let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$. By $\mathcal{S}$ we shall denote the system of polynomial equations

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \quad\vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

3.7.A A Bound for the Number of Solutions

Given a system of polynomial equations $\mathcal{S}$ as above, there can be finitely or infinitely many solutions $(a_1, \ldots, a_n) \in \overline{K}^n$. Our first proposition provides an algorithmic criterion for finiteness, since Buchberger's Algorithm allows us to check condition e) effectively.

Proposition 3.7.1. (Finiteness Criterion)
Let σ be a term ordering on $\mathbb{T}^n$. The following conditions are equivalent.

a) *The system of equations $\mathcal{S}$ has only finitely many solutions.*
b) *The ideal $I\overline{P}$ is contained in only finitely maximal ideals of $\overline{P}$.* nontrivi
c) *For $i = 1, \ldots, n$, we have $I \cap K[x_i] \neq (0)$.* I contains a univariate polynomial in X_i
d) *The K-vector space $K[x_1, \ldots, x_n]/I$ is finite-dimensional.*
e) *The set $\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\}$ is finite.*
f) *For every $i \in \{1, \ldots, n\}$, there exists a number $\alpha_i \geq 0$ such that we have $x_i^{\alpha_i} \in \mathrm{LT}_\sigma(I)$.*

Proof. First we show a) $\Rightarrow$ b). By Corollary 2.6.9, every maximal ideal $\mathfrak{m}$ of $\overline{P}$ is of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ with $a_1, \ldots, a_n \in \overline{K}$. If $\mathfrak{m}$ contains $I\overline{P}$, then the polynomials $f_1, \ldots, f_s$ lie in the kernel of the substitution homomorphism $\varphi : \overline{P} \longrightarrow \overline{K}$ which is defined by $x_i \mapsto a_i$ for

$i = 1, \ldots, n$. Therefore $(a_1, \ldots, a_n)$ is a solution of $\mathcal{S}$. Since there are only finitely many such solutions, there can be only finitely many maximal ideals $\mathfrak{m}$ containing $I\overline{P}$.

Now we prove $b) \Rightarrow f)$. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ be the maximal ideals of $\overline{P}$ containing $I\overline{P}$. By Corollary 2.6.9, there are tuples $(a_{i1}, \ldots, a_{in})$ such that $\mathfrak{m}_i = (x_1 - a_{i1}, \ldots, x_n - a_{in})$ for $i = 1, \ldots, t$. For $j = 1, \ldots, n$, we form the polynomials $g_j = \prod_{i=1}^{t}(x_j - a_{ij}) \in \overline{K}[x_j]$. From what we have shown in the proof of $a) \Rightarrow b)$ it follows that g_j vanishes on every solution of $\mathcal{S}$. Thus Hilbert's Nullstellensatz 2.6.16 yields a number $\alpha_j \geq 0$ such that $g_j^{\alpha_j} \in I\overline{P}$. Hence we have $x_j^{t\alpha_j} \in \mathrm{LT}_\sigma(I\overline{P})$. Now Lemma 2.4.16 shows $x_j^{t\alpha_j} \in \mathrm{LT}_\sigma(I)$.

The implication $f) \Rightarrow e)$ is clear, because every term of a sufficiently high degree is divisible by one of the terms $x_1^{t\alpha_1}, \ldots, x_n^{t\alpha_n}$, and $e) \Rightarrow d)$ is a consequence of Macaulay's Basis Theorem 1.5.7. Thus we prove $d) \Rightarrow c)$ next. Since P/I is a finite-dimensional K-vector space, the residue classes $1 + I, x_i + I, x_i^2 + I, \ldots$ are K-linearly dependent. Hence there are non-zero polynomials $g_i \in I \cap K[x_i]$ for every $i \in \{1, \ldots, n\}$. Finally, given non-zero polynomials $g_i \in I \cap K[x_i]$ for $i = 1, \ldots, n$, the i-th coordinate of any solution of $\mathcal{S}$ is a zero of g_i. Therefore there are at most $\deg(g_1) \cdots \deg(g_n)$ such solutions, proving $c) \Rightarrow a)$. $\qquad\square$

The proof of the preceding proposition yields an easy bound for the number of solutions of $\mathcal{S}$ if this number is finite. We saw that, for $i = 1, \ldots, n$, the elimination ideal $I \cap K[x_i]$ is non-zero, and therefore generated by a non-zero polynomial $g_i \in K[x_i]$. Then the number of solutions of $\mathcal{S}$ was shown to be at most $\deg(g_1) \cdots \deg(g_n)$. In fact, a much sharper bound is available. Before we proceed to derive it, let us introduce the following terminology.

Definition 3.7.2. An ideal $I = (f_1, \ldots, f_s)$ in $P = K[x_1, \ldots, x_n]$ is called **zero-dimensional** if it satisfies the equivalent conditions of the Finiteness Criterion 3.7.1.

Corollary 3.7.3. *With the same assumptions and notation as in the Finiteness Criterion 3.7.1, let I and J be ideals in P.*

a) If I is maximal, then I is zero-dimensional. ← amongst all proper ideals

b) If I is zero-dimensional and $I \subseteq J$, then J is zero-dimensional.

c) If I is zero-dimensional, then $I\overline{P}$ is also zero-dimensional and

$$\dim_K(P/I) = \dim_{\overline{K}}(\overline{P}/I\overline{P})$$

Proof. First we observe that a) is a consequence of Theorem 2.6.6.b and the Finiteness Criterion 3.7.1.d. The proof of b) follows from the fact that $\dim_K(P/J) \leq \dim_K(P/I)$. Since $K \subseteq \overline{K}$, a combination of Lemma 2.4.16.a and Macaulay's Basis Theorem 1.5.7 yields $\dim_K(P/I) = \dim_{\overline{K}}(\overline{P}/I\overline{P})$. This proves both claims of c). $\qquad\square$

Since we are interested in describing the solutions of the system of poly-
nomial equations $\mathcal{S}$ explicitly, we shall assume from now on that there are
only finitely many such solutions, i.e. that the ideal $I = (f_1, \ldots, f_s)$ is zero-
dimensional. To prove the desired bound for the number of solutions of $\mathcal{S}$
we need one more ingredient, namely a ring-theoretic version of the Chinese
Remainder Theorem.

Lemma 3.7.4. (Chinese Remainder Theorem)
Let R be a ring, and let $I_1, \ldots, I_t$ be ideals in R.

a) *The canonical R-linear map $\varphi : R/(I_1 \cap \cdots \cap I_t) \longrightarrow \prod_{i=1}^{t} R/I_i$ is
injective.*

b) *If the ideals $I_1, \ldots, I_t$ are pairwise **comaximal**, i.e. if $I_i + I_j = R$ for
$i \neq j$, then the map φ is an isomorphism of R-modules.*

Proof. Since the map φ is clearly injective, it suffices to show claim b). Fix
a number $i \in \{1, \ldots, t\}$, and let $J_i = \cap_{j \neq i} I_j$. Since I_i and I_j are comaximal
for all $j \neq i$, we find $a_j \in I_i$ and $b_j \in I_j$ such that $a_j + b_j = 1$. Then
$1 = \prod_{j \neq i}(a_j + b_j) \in I_i + \prod_{j \neq i} I_j \subseteq I_i + J_i$ shows that the ideals I_i and J_i are
comaximal. Thus there are elements $p_i \in I_i$ and $q_i \in J_i$ such that $p_i + q_i = 1$.
Now it is easy to check that an element $(r_1 + I_1, \ldots, r_t + I_t)$ of $\prod_{i=1}^{t} R/I_i$ is
the image of the residue class of $q_1 r_1 + \cdots + q_t r_t = (1 - p_1)r_1 + \ldots + (1 - p_t)r_t$
under φ. $\qquad\square$

Proposition 3.7.5. (Bound for the Number of Solutions)
*Let $f_1, \ldots, f_s \in P$ be polynomials which generate a zero-dimensional ideal
$I = (f_1, \ldots, f_s)$. Then the system of equations*

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$$

has at most $\dim_K(P/I)$ solutions in $\overline{K}^n$.

Proof. Let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$. By Proposition 2.6.11, the solutions of
$\mathcal{S}$ correspond one-to-one to the maximal ideals in $\overline{P}$ containing $I\overline{P}$. Let
$\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ be those maximal ideals. From $I\overline{P} \subseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$ we get
$\dim_{\overline{K}}(\overline{P}/I\overline{P}) \geq \dim_{\overline{K}}(\overline{P}/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t))$. Now the Chinese Remainder The-
orem yields $\overline{P}/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t) \cong \prod_{i=1}^{t} \overline{P}/\mathfrak{m}_i$, and Corollary 2.6.9 shows
$\overline{P}/\mathfrak{m}_i \cong \overline{K}$ for $i = 1, \ldots, t$. Finally, using Corollary 3.7.3.c, we obtain
$\dim_{\overline{K}}(\overline{P}/I\overline{P}) = \dim_K(P/I)$. Altogether, we get

$$t = \dim_{\overline{K}}\left(\prod_{i=1}^{t} \overline{P}/\mathfrak{m}_i \right) = \dim_{\overline{K}}(\overline{P}/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t))$$
$$\leq \dim_{\overline{K}}(\overline{P}/I\overline{P}) = \dim_K(P/I)$$

which is the desired inequality. $\qquad\square$

Of course, knowing that there are only finitely many solutions and having a bound for their number is only a small step towards actually solving a system of polynomial equations. Let us try to study solutions $(a_1, \ldots, a_n) \in \overline{K}^n$ of $\mathcal{S}$ more closely. Starting from a zero-dimensional ideal $I = (f_1, \ldots, f_s)$ in P, we may compute a generator $g_i \in K[x_i]$ of the elimination ideal $I \cap K[x_i]$ for every $i \in \{1, \ldots, n\}$. Then every coordinate a_i of a solution $(a_1, \ldots, a_n)$ of $\mathcal{S}$ is a zero of g_i.

Suppose we are able to factor polynomials in $K[x_i]$ effectively (see for instance Tutorial 6). The irreducible factors of g_i are precisely the minimal polynomials over K of the ith coordinates of the solutions of $\mathcal{S}$. In simple cases, this easy observation may suffice to solve the system of equations completely, as the following example shows.

Example 3.7.6. Let us consider the three polynomials $f_1 = x^2 + y + z - 1$, $f_2 = x + y^2 + z - 1$, and $f_3 = x + y + z^2 - 1$ in $P = \mathbb{Q}[x, y, z]$. They define a system of polynomial equations $f_1 = f_2 = f_3 = 0$ and generate an ideal $I = (f_1, f_2, f_3)$ in P. We observe that $\{f_1, f_2, f_3\}$ is a `DegRevLex`-Gröbner Basis of I and deduce that $\text{LT}_{\text{DegRevlex}}(I) = (x^2, y^2, z^2)$, so that $\dim_{\mathbb{Q}}(P/I) = 8$. Therefore 8 is an upper bound for the number of solutions of $\mathcal{S}$.

How sharp is this bound? When we compute generators g_i of the elimination ideals $I \cap \mathbb{Q}[x_i]$ for $i = 1, 2, 3$ and factor them, we get

$$
\begin{aligned}
g_1 &= x^6 - 4x^4 + 4x^3 - x^2 = x^2(x-1)^2(x+1+\sqrt{2})(x+1-\sqrt{2}) \\
g_2 &= y^6 - 4y^4 + 4y^3 - y^2 = y^2(y-1)^2(y+1+\sqrt{2})(y+1-\sqrt{2}) \\
g_3 &= z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z+1+\sqrt{2})(z+1-\sqrt{2})
\end{aligned}
$$

Each of those polynomials has four different zeros. By substituting them into the original system of equations, we see that of the 64 possible combinations only the five tuples $\{(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}),$ $(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})\}$ are actual solutions.

In this example, we see other phenomena emerging. For instance, it is clear that the last step of the procedure applied in this example breaks down if the zeros of the polynomials $g_1, \ldots, g_n$ cannot be represented by radicals. Another important fact is that, while the bound given by Proposition 3.7.5 is 8, the actual number of solutions is 5.

Let us try to explain this phenomenon. If a polynomial f vanishes at the set of solutions of $\mathcal{S}$, then also sqfree(f) vanishes at that set. Consequently, the system $\mathcal{S}$ has the same set of solutions as the system $\mathcal{S}'$, where $\mathcal{S}'$ is obtained from $\mathcal{S}$ by adding the squarefree parts of some polynomials in $\mathcal{S}$. Looking at the example above, we can now understand why the upper bound given by Proposition 3.7.5 is not sharp. In the next subsection, we investigate this aspect of the theory more closely.

3.7.B   Radicals of Zero-Dimensional Ideals

In the last example we encountered a case in which the system $\mathcal{S}$ had *multiple* solutions. What does this mean exactly? Arguing as above, we note that the system of equations defined by $I = (f_1, \ldots, f_s)$ has the same solutions as the system of equations defined by a set of generators of its radical

$$\sqrt{I} = \{ f \in P \mid f^i \in I \text{ for some } i \geq 0 \}$$

So, the next goal is to reduce the solution of systems of polynomial equations to the case where the polynomials generate a radical ideal. To this end, we need to introduce the notion of a perfect field.

Definition 3.7.7. A field K is called a **perfect field** if either its characteristic is 0 or its characteristic is $p > 0$ and we have $K = K^p$, i.e. every element in K has a pth-root in K.

   Let us immediately point out that, for a perfect field K of characteristic $p > 0$, the pth root of an element $a \in K$ is uniquely determined, because if $b, c \in K$ satisfy $b^p = c^p = a$, then $b^p - c^p = (b - c)^p = 0$ implies $b = c$.
   For instance, given a prime number $p \in \mathbb{N}$, the field $K = \mathbb{F}_p$ is perfect, since every element is its own p^{th} root. More generally, if $K = \mathbb{F}_q$ is any finite field, where $q = p^e$ and $e > 0$, then the map $x \mapsto x^{p^{e-1}}$ provides p^{th} roots, because we have $(x^{p^{e-1}})^p = x^q = x$ for all $x \in K$. At this point we know that fields of characteristic 0 and finite fields are perfect. Are there non-perfect fields? The answer is yes, as the following example shows.

Example 3.7.8. Let $p \in \mathbb{N}$ be a prime number, let $K = \mathbb{F}_p$, let x be an indeterminate, and let $L = K(x)$ be the field of fractions of $K[x]$. Then, using the factoriality of $K[x]$, we can easily see that x has no p^{th} root in L. Therefore the field L is not perfect.

   Is there an effective method for computing the radical of a zero-dimensional ideal? The radical of a zero-dimensional ideal $I = (f)$ in $K[x]$ is easy to describe. It is the principal ideal generated by $\text{sqfree}(f)$. Thus we shall first show how one can compute the squarefree part of a univariate polynomial. The algorithm is based on the following collection of useful facts about $\text{sqfree}(f)$.

Proposition 3.7.9. *Let K be a field and $f \in K[x]$ a non-constant polynomial.*

a) *If $\gcd(f, f') = 1$, then f is squarefree.*
b) *Assume that one of the following conditions holds.*
   1) *We have $\text{char}(K) = 0$.*
   2) *We have $\text{char}(K) = p > 0$ and $f = c f_1^{\alpha_1} \cdots f_t^{\alpha_t}$, where $c \in K \setminus \{0\}$, where $\alpha_1, \ldots, \alpha_t > 0$ satisfy $p \nmid \alpha_i$ for $i = 1, \ldots, t$, and where $f_1, \ldots, f_t$ are pairwise distinct irreducible monic polynomials.*

Then the squarefree part of f is given by $\mathrm{sqfree}(f) = f/\gcd(f, f')$.

c) Let K be a perfect field of characteristic $p > 0$. Then we have $f' = 0$ if and only if f is of the form $f = g^p$ for some polynomial $g \in K[x]$.

d) Let K be a perfect field. Then the converse of a) holds, i.e. if f is square-free, then we have $\gcd(f, f') = 1$.

Proof. First we prove a). Suppose that f is not squarefree. Then we can write f in the form $f = f_1^2 f_2$ with polynomials $f_1, f_2 \in K[x]$ such that f_1 is not constant. We compute the derivative of f and get $f' = 2f_1 f_1' f_2 + f_1^2 f_2'$. Thus we have $f_1 \mid \gcd(f, f')$, a contradiction.

In order to see that claim b) holds, we write down a factorization $f = c f_1^{\alpha_1} \cdots f_t^{\alpha_t}$ as in 2). Then we note that $\gcd(f, f') = f_1^{\alpha_1 - 1} \cdots f_t^{\alpha_t - 1}$ in both cases. Thus we get $f/\gcd(f, f') = c f_1 \cdots f_t = \mathrm{sqfree}(f)$.

To prove c), we observe that if $f = g^p$, then $f' = p g' g^{p-1} = 0$. Conversely, suppose that $f' = 0$. We write $f = \sum_{i \geq 0} a_i x^i$ with $a_i \in K$, and we see that $f' = \sum_{i \geq 1} i a_i x^{i-1} = 0$ implies $a_i = 0$ for all $i \geq 0$ such that $p \nmid i$. Hence the polynomial f is of the form $f = \sum_{i \geq 0} a_{pi} x^{pi}$. Since the field K is perfect, there exist elements $b_i \in K$ such that $a_{pi} = b_i^p$ for all $i \geq 0$. Altogether, we find $f = \sum_{i \geq 0} (b_i x^i)^p = g^p$ for $g = \sum_{i \geq 0} b_i x^i$.

Finally we prove d). We decompose f into irreducible factors $f = f_1 \cdots f_t$ and note that $f' = \sum_{i=1}^{t} f_1 \cdots f_{i-1} f_i' f_{i+1} \cdots f_t$. Now we claim that every irreducible polynomial $f_i \in K[x]$ satisfies $f_i' \neq 0$. If $\mathrm{char}(K) = 0$, this is clear, and if $\mathrm{char}(K) = p > 0$, it follows from c). Thus we get $\gcd(f_i, f_i') = 1$. This implies $\gcd(f_i, f') = \gcd(f_i, f_i') = 1$, and therefore $\gcd(f, f') = 1$. $\square$

For the promised algorithm, we need one further ingredient. When we work over a perfect base field K of characteristic $p > 0$, Definition 3.7.7 requires that every element in K has a pth root. But of course we need to be able to *compute* that root. This observation motivates the following definition.

Definition 3.7.10. Let K be a perfect field of characteristic $p > 0$. We shall say that K has **effective p^{th} roots** if there exists an algorithm which computes the pth root of any element of K.

For instance, finite fields are perfect fields with effective p^{th} roots. Over perfect fields having effective p^{th} roots, we can extract the pth root of univariate polynomials with vanishing derivative as follows.

Remark 3.7.11. Let K be a perfect field of characteristic $\mathrm{char}(K) = p > 0$ which has effective p^{th} roots. Suppose that $f \in K[x]$ is a non-constant polynomial such that $f' = 0$. Then we can effectively compute the unique polynomial $g \in K[x]$ such that $f = g^p$. Namely, we saw in the proof of Proposition 3.7.9.c that f is of the form $f = \sum_{i \geq 0} a_{pi} x^{pi}$. By assumption, for every $i \geq 0$ such that $a_{pi} \neq 0$, we can compute the element $b_i \in K$ such that $b_i^p = a_{pi}$. Then $g = \sum_{i \geq 0} b_i x^i$ is the desired polynomial.

Finally, all the tools we need to compute squarefree parts of univariate polynomials in characteristic p are in place. Ready, steady, go! (American English: Ready, set, go!)

Proposition 3.7.12. (Squarefree Parts in Characteristic p)
Let K be a perfect field of characteristic $p > 0$ having effective p^{th} roots. Given a polynomial $f \in K[x] \setminus K$, consider the following sequence of instructions.

1) *Calculate $s_1 = \gcd(f, f')$. If $s_1 = 1$, then return f.*
2) *Check whether we have $s_1' = 0$. In this case, $s_1 = g^p$ for some uniquely determined polynomial $g \in K[x]$. Calculate g, replace f by $\frac{fg}{s_1} = \frac{f}{g^{p-1}}$, and continue with step 1).*
3) *Compute $s_{i+1} = \gcd(s_i, s_i')$ for $i = 1, 2, \ldots$ until $s_{i+1}' = 0$, i.e. until s_{i+1} is a pth power $s_{i+1} = g^p$ for some $g \in K[x]$. Then calculate g, replace f by $\frac{fg}{s_1}$, and continue with step 1).*

This is an algorithm which computes the squarefree part $\operatorname{sqfree}(f)$ of f.

Proof. If $\gcd(f, f') = 1$, the algorithm stops in step 1) and returns the correct result by Proposition 3.7.9.a. If $\gcd(f, f') \neq 1$, we write $f = c f_1^p f_2$ with $c \in K \setminus \{0\}$ and monic polynomials $f_1, f_2 \in K[x]$ such that no p^{th} power of an irreducible polynomial divides f_2. Then we calculate $f' = c f_1^p f_2'$ and $s_1 = \gcd(f, f') = f_1^p \gcd(f_2, f_2')$. We let $f_3 = \gcd(f_2, f_2')$ and find $s_1' = f_1^p f_3'$.

If now $s_1' = 0$, the algorithm executes the second part of step 2). In this case, $f_3' = 0$ implies $f_3 = 1$, because no p^{th} power of an irreducible polynomial divides f_2 and $f_3 = \gcd(f_2, f_2')$ divides f_2. Hence it follows that $s_1 = f_1^p$, and the polynomial g which is computed in step 2) equals f_1. Therefore we have $\frac{f}{g^{p-1}} = f_1 f_2$. Since $s_1 = f_1^p \neq 1$, we have $\deg(f_1) > 0$, and the algorithm is applied again to a polynomial of smaller degree.

If $s_1' \neq 0$, we calculate $s_2 = \gcd(s_1, s_1') = f_1^p \gcd(f_3, f_3')$, and so on, until $s_{i+1}' = 0$ for some $i \geq 1$. This case will eventually happen, since each iteration lowers the degree of the corresponding polynomial s_i. When $s_{i+1}' = 0$, we see as above that $s_{i+1} = f_1^p$. Thus the polynomial g calculated in step 3) equals f_1 again, and the algorithm is applied to the polynomial $\frac{f f_1}{s_1} = f_1 f_2 / \gcd(f_2, f_2')$ which has clearly a smaller degree than f.

Finally, the correctness of the algorithm in the case $s_1 \neq 1$ follows from

$$\begin{aligned}
\operatorname{sqfree}(f) = \operatorname{sqfree}(f_1^p f_2) &= \operatorname{sqfree}(f_1 \operatorname{sqfree}(f_2)) \\
&= \operatorname{sqfree}(f_1 f_2 / \gcd(f_2, f_2')) = \operatorname{sqfree}(f f_1 / f_1^p \gcd(f_2, f_2')) \\
&= \operatorname{sqfree}(f f_1 / s_1)
\end{aligned}$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

To improve our understanding of this algorithm, we shall now apply it in two non-trivial concrete cases.

Example 3.7.13. Let $K = \mathbb{Z}/(5)$, and let $f = x^{31} - 2x^{30} - x^6 + 2x^5 \in K[x]$. We apply the algorithm of Proposition 3.7.12 to compute the squarefree part of f.

1) Since $f' = x^{30} - x^5$, we get $s_1 = \gcd(f, f') = x^{30} - x^5 \neq 1$.
2) Since $s_1' = 0$, we see that $s_1 = g^5$, where $g = x^6 - x$. So we replace f by $f = fg/s_1 = x^7 - 2x^6 - x^2 + 2x$ and start again.
1) Since $f' = 2x^6 - 2x^5 - 2x + 2$, we get $s_1 = \gcd(f, f') = x^5 - 1 \neq 1$.
2) Since $s_1' = 0$, we see that $s_1 = g^5$, where $g = x - 1$. So we replace f by $f = fg/s_1 = x^3 + 2x^2 + 2x$ and start again.
1) Since $f' = -2x^2 - x + 2$, we get $s_1 = \gcd(f, f') = 1$. At this point the algorithm stops and returns $\mathrm{sqfree}(f) = x^3 + 2x^2 + 2x$.

Using a factorization algorithm, we can check $f = x^{31} - 2x^{30} - x^6 + 2x^5 = x^5(x - 1)^{25}(x - 2)$ and $\mathrm{sqfree}(f) = x^3 + 2x^2 + 2x = x(x - 1)(x - 2)$.

Example 3.7.14. Let $K = \mathbb{Z}/(3)$ and $f = x^6 + x^5 - x^4 + x^2 - x - 1 \in K[x]$. When we apply the algorithm of Proposition 3.7.12, we have to perform the following steps.

1) Since $f' = -x^4 - x^3 - x - 1$, we get $s_1 = \gcd(f, f') = x^4 + x^3 + x + 1 \neq 1$.
2) We calculate $s_1' = x^3 + 1 \neq 0$.
3) We calculate $s_2 = \gcd(s_1, s_1') = x^3 + 1$. Since $s_2' = 0$, we find $s_2 = g^3$, where $g = x + 1$. Thus we replace f by $\frac{fg}{s_1} = x^3 + x^2 - x - 1$.
1) Since $f' = -x - 1$, we have $s_1 = \gcd(f, f') = x + 1 \neq 1$.
2) We calculate $s_1' = 1 \neq 0$.
3) We calculate $s_2 = 1$ and $s_2' = 0$. Hence $s_2 = g^3$, where $g = 1$. We replace f by $\frac{fg}{s_1} = x^2 - 1$.
1) Since $f' = -x$, we get $s_1 = 1$. At this point the algorithm stops and returns $\mathrm{sqfree}(f) = x^2 - 1$.

Notice that in this case it is important that we divide fg by s_1 in the second execution of step 3), because $\frac{fg}{s_2} = f$.

Altogether, we may combine Proposition 3.7.9.b and Proposition 3.7.12 by saying that over fields of characteristic zero and over perfect fields of characteristic $p > 0$ having effective p^{th} roots, we can compute the squarefree part of a univariate polynomial effectively.

Our next proposition provides the key for reducing the computation of radicals of zero-dimensional ideals to the univariate case.

Proposition 3.7.15. (Seidenberg's Lemma)
Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $I \subseteq P$ be a zero-dimensional ideal. Suppose that, for every $i \in \{1, \ldots, n\}$, there exists a non-zero polynomial $g_i \in I \cap K[x_i]$ such that $\gcd(g_i, g_i') = 1$. Then I is a radical ideal.

Proof. By Proposition 3.7.9.a, the polynomials $g_1, \ldots, g_n$ are squarefree. We proceed by induction on n. For $n = 1$, the principal ideal $I \subseteq K[x_1]$ contains

a squarefree polynomial. Therefore it is generated by a squarefree polynomial, i.e. it is a radical ideal.

Now let $n > 1$. We write $g_1 = h_1 \cdots h_t$ with irreducible polynomials $h_1, \ldots, h_t \in K[x_1]$. We claim that $I = \cap_{i=1}^{t}(I + (h_i))$. For every polynomial $f \in \cap_{i=1}^{t}(I + (h_i))$ there are $r_i \in I$ and $q_i \in P$ such that $f = r_i + q_i h_i$ for $i = 1, \ldots, t$. Obviously, we have $f \cdot \prod_{j \neq i} h_j \in I$ for $i = 1, \ldots, t$, and because of $\gcd(\prod_{j \neq 1} h_j, \ldots, \prod_{j \neq t} h_j) = 1$ we find $\ell_1, \ldots, \ell_t \in K[x_1]$ such that $\ell_1 \prod_{j \neq 1} h_j + \cdots + \ell_t \prod_{j \neq t} h_j = 1$ (see Proposition 1.2.8.c). Altogether, $f = \sum_{i=1}^{t} \ell_i f \prod_{j \neq i} h_j \in I$ proves the claim.

Because of this claim and the fact that a finite intersection of radical ideals is again radical, it suffices to show that $I + (h_i)$ is radical for $i = 1, \ldots, t$. So we may assume that g_1 is irreducible. Hence the field $L = K[x_1]/(g_1)$ is a finite K-vector space, and the canonical surjective homomorphism $\varphi : K[x_1, \ldots, x_n] \longrightarrow L[x_2, \ldots, x_n]$ satisfies $\ker(\varphi) = (g_1) \subseteq I$. The ideal $J = \varphi(I)$ is again zero-dimensional, because $L[x_2, \ldots, x_n]/J \cong P/I$. For all $i = 2, \ldots, n$, the polynomials $\varphi(g_i) = g_i \in L[x_2, \ldots, x_n]$ satisfy $\gcd(g_i, g_i') = 1$ again. Therefore J is a radical ideal by the inductive hypothesis, i.e. we have no non-zero nilpotents in $L[x_2, \ldots, x_n]/J$. The above isomorphism shows that also P/I has no non-zero nilpotents, hence I is a radical ideal. $\qquad\square$

As a consequence of Seidenberg's Lemma, we can now prove the following straightforward algorithm for computing the radical of a zero-dimensional polynomial ideal.

Corollary 3.7.16. (Computation of Radicals of Zero-Dimensional Ideals)
Let K be a field of characteristic zero or a perfect field of characteristic $p > 0$ having effective p^{th} roots. Then the following algorithm computes the radical of a zero-dimensional ideal I in $K[x_1, \ldots, x_n]$.

1) For $i = 1, \ldots, n$ compute a generator $g_i \in K[x_i]$ of the elimination ideal $I \cap K[x_i]$.

2) Using Proposition 3.7.9.b or Proposition 3.7.12, compute $\mathrm{sqfree}(g_1), \ldots, \mathrm{sqfree}(g_n)$ and return the ideal $I + (\mathrm{sqfree}(g_1), \ldots, \mathrm{sqfree}(g_n))$.

Proof. By Proposition 3.7.1.c, the polynomials $g_1, \ldots, g_n$ are non-zero. Since the ideal $J = I + (\mathrm{sqfree}(g_1), \ldots, \mathrm{sqfree}(g_n))$ satisfies $I \subseteq J \subseteq \sqrt{I}$, we have $\sqrt{I} = \sqrt{J}$. For $i = 1, \ldots, n$, let $h_i = \mathrm{sqfree}(g_i)$. By Proposition 3.7.9.d, the polynomials h_i satisfy $\gcd(h_i, h_i') = 1$. Thus Seidenberg's Lemma yields the claim. $\qquad\square$

Notice that the ideal $J = I + (\mathrm{sqfree}(g_1), \ldots, \mathrm{sqfree}(g_n))$ returned by this algorithm satisfies $J \cap K[x_i] = (\mathrm{sqfree}(g_i))$ for $i = 1, \ldots, n$. Next, we want to see the above algorithm working in practice. It allows us to replace a system of polynomial equations by another one which has the same set of solutions, but corresponds to an ideal which is usually larger.

Example 3.7.17. Let us consider the following system $\mathcal{S}$ over the polyno-
mial ring $P = \mathbb{Q}[x, y, z]$.

$$
\begin{cases}
y^2 - \frac{2}{375}xz + \frac{22}{75}yz + \frac{29}{1500}z^2 + \frac{2}{75}x - \frac{7}{15}y - \frac{7}{150}z = 0 \\
xy + \frac{31}{150}xz - \frac{1}{5}yz - \frac{1}{50}z^2 - \frac{8}{15}x + y + \frac{1}{10}z = 0 \\
x^2 - \frac{7}{15}xz + 4yz + \frac{2}{5}z^2 + \frac{7}{3}x - 20y - 2z = 0 \\
z^3 + \frac{6}{5}xz + 24yz - \frac{38}{5}z^2 - 6x - 120y + 13z = 0 \\
yz^2 - \frac{3}{25}xz - \frac{47}{5}yz + \frac{3}{50}z^2 + \frac{3}{5}x + 22y - \frac{3}{10}z = 0 \\
xz^2 - 7xz + 10x = 0
\end{cases}
$$

The associated ideal $I \subseteq P$, i.e. the ideal generated by the left-hand sides of
the equations in $\mathcal{S}$, satisfies $\dim_{\mathbb{Q}}(P/I) = 7$, as we can compute for instance
using Buchberger's Algorithm 2.5.5 and Macaulay's Basis Theorem 2.4.11.
The upper bound for the number of solutions of $\mathcal{S}$ given by Proposition 3.7.5
is therefore 7.

Now we compute the three generators g_1, g_2, and g_3 of the elimination
ideals $I \cap \mathbb{Q}[x]$, $I \cap \mathbb{Q}[y]$, and $I \cap \mathbb{Q}[z]$. We obtain $g_1 = x^4 + 2x^3 - 3x^2$,
$g_2 = y^4 + \frac{4}{5}y^3 + \frac{1}{20}y^2 - \frac{1}{20}y$, and $g_3 = z^4 - 12z^3 + 45z^2 - 50z$. Then we
use Proposition 3.7.9.b to calculate $\mathrm{sqfree}(g_1) = x^3 + 2x^2 - 3x$, $\mathrm{sqfree}(g_2) =$
$y^3 + \frac{3}{10}y^2 - \frac{1}{10}y$, and $\mathrm{sqfree}(g_3) = z^3 - 7z^2 + 10z$.

By adding these three equations to the system, we obtain a larger system
of polynomial equations with the same set of solutions. Let us try to use
Proposition 3.7.5 again to bound the number of solutions. By computing a
Gröbner basis of the associated ideal, we see that the new system of equations
can be replaced by

$$
\begin{cases}
z^2 + \frac{6}{5}x + 24y - \frac{13}{5}z = 0 \\
x^2 + \frac{7}{5}x - 12y - \frac{6}{5}z = 0 \\
xy - \frac{3}{25}x + \frac{3}{5}y + \frac{3}{50}z = 0 \\
y^2 + \frac{7}{250}x + \frac{9}{25}y - \frac{7}{500}z = 0 \\
xz - 2x = 0 \\
yz - \frac{3}{25}x - \frac{22}{5}y + \frac{3}{50}z = 0
\end{cases}
$$

This time Macaulay's Basis Theorem yields $\dim_{\mathbb{Q}}(P/J) = 4$, i.e. we get a
better bound for the number of solutions. Is this a good bound? Our next
goal is to show that it is in fact optimal, i.e. that 4 is exactly the number of
solutions of $\mathcal{S}$.

For a system of equations $f_1 = \cdots = f_s = 0$ corresponding to a zero-
dimensional radical ideal $I = (f_1, \ldots, f_s)$, and for a perfect base field K,
the solutions of the system are *simple zeros* of I in the sense of the following
proposition. We note that a finite intersection of maximal ideals in P is
clearly a radical ideal.

Proposition 3.7.18. *Let I be a zero-dimensional radical ideal in P, let $\overline{K}$ be the algebraic closure of K, and let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$.*

a) *There are only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ of P containing I, and the ideal I is their intersection $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$.*

b) *If K is a perfect field, then also the ideal $I\overline{P}$ is a radical ideal. In particular, the ideal $I\overline{P}$ is again the intersection of the finite set of maximal ideals containing it.*

Proof. First we show claim a). Every maximal ideal $\mathfrak{m}$ containing I is zero-dimensional by Corollary 3.7.3.a. Therefore also $\mathfrak{m}\overline{P}$ is zero-dimensional by Corollary 3.7.3.c. By the Finiteness Criterion 3.7.1.a, this implies that $\mathcal{Z}(\mathfrak{m}\overline{P})$ is finite. So, there are finitely many maximal ideals $\overline{\mathfrak{m}}_1, \ldots, \overline{\mathfrak{m}}_u$ of $\overline{P}$ containing $\mathfrak{m}\,\overline{P}$, and for each of those we have $\overline{\mathfrak{m}}_i \cap P = \mathfrak{m}$. Using the same reasoning, we also see that $I\overline{P}$ is contained in only finitely many maximal ideals of $\overline{P}$, and then it follows that I is contained in only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ of P. Every element f of $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$ lies in all maximal ideals of $\overline{P}$ containing $I\overline{P}$. By Corollary 2.6.17, we therefore have $f \in \sqrt{I} = I$. Altogether, we get $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$.

Now we prove b). We note that, for $i = 1, \ldots, n$, the Finiteness Criterion 3.7.1.c says that the ideal $I \cap K[x_i]$ is a principal ideal generated by a non-zero polynomial $g_i \in K[x_i]$. Because of the assumption that I is radical, the generator g_i of $I \cap K[x_i]$ has to be squarefree. Then we use the assumption that K is perfect and Proposition 3.7.9.d to see that $\gcd(g_i, g_i') = 1$. Hence, by Proposition 1.2.8.c, there exist polynomials $h_i, \tilde{h}_i \in K[x_i]$ such that $1 = h_i g_i + \tilde{h}_i g_i'$. This equation continues to hold in $\overline{K}[x_i]$. Thus we also have $\gcd(g_i, g_i') = 1$ if we view g_i and g_i' as elements of $\overline{P}$. Now we may apply Seidenberg's Lemma 3.7.15 to $I\overline{P}$, and the proof is complete. $\square$

If the system of polynomial equations $\mathcal{S}$ corresponds to a zero-dimensional radical ideal, and if the base field is perfect, the bound for the number of solutions given in Proposition 3.7.5 is sharp, i.e. we have the following formula for the exact number of solutions.

Theorem 3.7.19. (Exact Number of Solutions)
Let I be a zero-dimensional radical ideal in P, let $\overline{K}$ be the algebraic closure of K, and let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$. If K is a perfect field, the number of solutions of the system of equations $\mathcal{S}$ is equal to the number of maximal ideals of $\overline{P}$ containing $I\overline{P}$, and this number is precisely $\dim_K(P/I)$.

Proof. Using Proposition 3.7.18.a, we write $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$ with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ of P, and we write $\mathfrak{m}_i\,\overline{P} = \overline{\mathfrak{m}}_{i1} \cap \cdots \cap \overline{\mathfrak{m}}_{i\mu_i}$ with maximal ideals $\overline{\mathfrak{m}}_{i1}, \ldots, \overline{\mathfrak{m}}_{i\mu_i}$ of $\overline{P}$ for $i = 1, \ldots, t$. Then the Chinese Remainder Theorem 3.7.4.b and Corollary 3.7.3.c allow us to calculate

$$\dim_K(P/I) = \sum_{i=1}^{t} \dim_K(P/\mathfrak{m}_i) = \sum_{i=1}^{t} \dim_{\overline{K}}(\overline{P}/\mathfrak{m}\,\overline{P})$$

$$=\sum_{i=1}^{t} \sum_{j=1}^{\mu_i} \dim_{\overline{K}}(\overline{P}/\overline{\mathfrak{m}}_{ij}) = \sum_{i=1}^{t} \mu_i$$

The last equality follows from Corollary 2.6.9. The number $\sum_{i=1}^{t} \mu_i$ is exactly the number of maximal ideals of $\overline{P}$ containing $I\overline{P}$, i.e. the number of solutions of $\mathcal{S}$. $\qquad\square$

Now we know that the number of solutions of the system $\mathcal{S}$ in Example 3.7.17 is precisely 4. Can we find them?

Example 3.7.20. Consider the second system of polynomial equations contained in Example 3.7.17. Notice that the equation $xz - 2x = 0$ can be factored into $x(z - 2) = 0$. As in high school, we can split the system into two systems $\mathcal{S}_1$ and $\mathcal{S}_2$. After interreducing the generators, these systems are given by

$$\begin{cases} z - 2 = 0 \\ x + 20\,y - 1 = 0 \\ y^2 - \frac{1}{5}\,y = 0 \end{cases} \quad \text{and} \quad \begin{cases} x = 0 \\ y + \frac{1}{10}\,z = 0 \\ z^2 - 5\,z = 0 \end{cases}$$

Now it is easy to get the four solutions $(1, 0, 2)$, $(-3, \frac{1}{5}, 2)$, $(0, 0, 0)$, $(0, -\frac{1}{2}, 5)$.

Of course, most of the time we cannot use tricks like this one. Therefore we need a general strategy for finding the solutions. Such a strategy will be developed in the next subsection.

3.7.C   Solving Systems Effectively

As a consequence of the above discussions, we shall from now on assume that we want to solve a system of polynomial equations $f_1 = \ldots = f_s = 0$ such that $I = (f_1, \ldots, f_s)$ is a zero-dimensional radical ideal in $P = K[x_1, \ldots, x_n]$. Our next goal is to perform a linear change of coordinates in such a way that the resulting system of equations has the additional property that its solutions in $\overline{K}^n$ have pairwise distinct last coordinates. Let us introduce the following name for this property.

Definition 3.7.21. Suppose that I is a zero-dimensional ideal in P, and let $i \in \{1, \ldots, n\}$. We say that I is **in normal x_i-position** if any two zeros $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \overline{K}^n$ of I satisfy $a_i \neq b_i$.

To bring a given zero-dimensional ideal into normal x_n-position, we may have to extend the base field (if it is finite) and to perform a linear change of coordinates. Our next proposition gives a precise condition when this is possible.

Proposition 3.7.22. *Suppose that I is a zero-dimensional ideal in P, let $t = \dim_K(P/I)$, and assume that the field K contains more than $\binom{t}{2}$ elements. Then there exists a tuple $(c_1, \ldots, c_{n-1}) \in K^{n-1}$ such that*

$$c_1 a_1 + \cdots + c_{n-1} a_{n-1} + a_n \neq c_1 b_1 + \cdots + c_{n-1} b_{n-1} + b_n$$

for all pairs of zeros $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \overline{K}^n$ of I. Consequently the linear change of coordinates given by $x_1 \mapsto x_1, \ldots, x_{n-1} \mapsto x_{n-1}$, and by $x_n \mapsto x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}$ transforms I into an ideal in normal x_n-position.

Proof. Let $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ be two distinct zeros of I in $\overline{K}^n$. In choosing the tuple $(c_1, \ldots, c_{n-1}) \in K^{n-1}$, we have to avoid the solutions in K^{n-1} of the linear equation

$$(a_1 - b_1) x_1 + \cdots + (a_{n-1} - b_{n-1}) x_{n-1} = a_n - b_n$$

These solutions are obtained by adding all solutions of the corresponding homogeneous equation to one of them. Thus there are at most $(\#K)^{n-2}$ of them. Altogether, we have to avoid at most $\binom{t}{2} \cdot (\#K)^{n-2}$ tuples in K^{n-1}, which is clearly possible if $\#K > \binom{t}{2}$. $\qquad\square$

At this point it may be useful to remind the reader that the linear change of coordinates mentioned in this proposition transforms the ideal I into the ideal $J = (f(x_1, \ldots, x_{n-1}, x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}) \mid f \in I)$, and that a point $(a_1, \ldots, a_n) \in \overline{K}^n$ is a zero of I if and only if the point $(a_1, \ldots, a_{n-1}, a_n + c_1 a_1 + \cdots + c_{n-1} a_{n-1})$ is a zero of J (see also Exercise 6). To finish the discussion of how to bring a zero-dimensional ideal into normal x_n-position, it now suffices to explain how one can check whether it already is in normal x_n-position. For that, we shall have to pass to its radical ideal first. Then we use the following theorem.

Theorem 3.7.23. *Let K be a perfect field, let $P = K[x_1, \ldots, x_n]$, let $I \subseteq P$ be a zero-dimensional radical ideal, and let g_n be the monic generator of the ideal $I \cap K[x_n]$. Then the following conditions are equivalent.*

a) *The ideal I is in normal x_n-position.*
b) *The degree of g_n is equal to $\dim_K(P/I)$.*
c) *The injection $K[x_n] \hookrightarrow P$ induces an isomorphism of K-algebras $K[x_n]/(g_n) \cong P/I$.*

Proof. By construction, the injection $K[x_n] \hookrightarrow P$ induces an injective K-algebra homomorphism $K[x_n]/(g_n) \hookrightarrow P/I$. In particular, we have $\deg(g_n) = \dim_K(K[x_n]/(g_n)) \leq \dim_K(P/I)$. Now claim a) implies b), because the last component of every zero of I is a zero of g_n and g_n is squarefree. Hence we have $\deg(g_n) \geq \dim_K(P/I)$ by Theorem 3.7.19.

It is clear that b) implies c), because we have an injective K-algebra homomorphism $K[x_n]/(g_n) \hookrightarrow P/I$, and both algebras have the same

vector space dimension over K. Thus it remains to prove that c) implies a). We consider the reduced Gröbner basis G of I with respect to an elimination ordering σ for $\{x_1, \ldots, x_{n-1}\}$. By Theorem 3.4.5.c, we have $G \cap K[x_n] = \{g_n\}$. By Lemma 2.4.16.b, the set G is also the reduced σ-Gröbner basis of $I\overline{P} \cap \overline{K}[x_n]$, where $\overline{K}$ is the algebraic closure of K. Thus the canonical map $\overline{K}[x_n]/(g_n) \longrightarrow \overline{P}/I\overline{P}$ is injective. Using the hypothesis, we see that $\deg(g_n) = \dim_K(P/I)$, and Corollary 3.7.3.c shows $\dim_K(P/I) = \dim_{\overline{K}}(\overline{P}/I\overline{P})$. Hence the map $\overline{K}[x_n]/(g_n) \longrightarrow \overline{P}/I\overline{P}$ is bijective.

By Theorem 3.7.19, the degree of g_n equals the number of zeros of I. Let $d = \deg(g_n)$, and let $a_1, \ldots, a_d \in \overline{K}$ be the zeros of g_n. The maximal ideals of the quotient ring $\overline{K}[x_n]/(g_n)$ are the principal ideals generated by the residue classes of $x_n - a_i$ for $i = 1, \ldots, d$. Under the above isomorphism, they correspond to maximal ideals $\mathfrak{m}_i$ of $\overline{P}/I\overline{P}$. By Corollary 2.6.9, each ideal $\mathfrak{m}_i$ is the residue class ideal of an ideal of the form $(x_1 - \alpha_{i1}, \ldots, x_n - \alpha_{in})$ in $\overline{P}$, where $\alpha_{i1}, \ldots, \alpha_{in} \in \overline{K}$. Since we have $(x_1 - \alpha_{i1}, \ldots, x_n - \alpha_{in}) \cap \overline{K}[x_n] = (x_n - a_i)$ by construction, it follows that $\alpha_{in} = a_i$ for $i = 1, \ldots, d$. By Proposition 3.7.18.b, the squarefree polynomial g_n has pairwise distinct roots $a_1, \ldots, a_d$. Therefore we see that the last coordinates of the zeros $\{(\alpha_{i1}, \ldots, \alpha_{in}) \mid i = 1, \ldots, d\}$ of I are pairwise distinct. $\square$

This theorem can be viewed as a generalization of a well-known result in field theory.

Remark 3.7.24. Let L/K be a finite field extension, i.e. let $L \supseteq K$ be an extension field which is a finite dimensional K-vector space. Since every K-basis of L is also a system of generators of the K-algebra L, there exists a presentation $L \cong P/I$, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over K, and where $I \subseteq P$ is a maximal ideal.

Let $t = \dim_K(L)$. If the field K is perfect and has more than $\binom{t}{2}$ elements, we can use Proposition 3.7.22 to find a linear change of coordinates such that the transform of I is in normal x_n-position. Then condition c) of the theorem shows that L is of the form $L \cong K[x]/(g)$ with an irreducible polynomial $g \in K[x]$. In other words, viewed as a K-algebra, the field L is generated by a single element.

In field theory, this result is called the **Primitive Element Theorem**. Although we are not going to treat this subject in greater detail, let us mention that the assumption that K is a perfect field is essential for the Primitive Element Theorem to hold, whereas the assumption that K has more than $\binom{t}{2}$ elements can easily be dispensed with (see also Exercise 8).

The reason why we wanted to reduce our problem of solving a system of polynomial equations $f_1 = \cdots = f_s = 0$ to the case when $I = (f_1, \ldots, f_s)$ is a zero-dimensional radical ideal in normal x_n-position is the following theorem. It says that, in this situation, the reduced Lex-Gröbner basis of I has a

very special shape. That is why it is sometimes called the **Shape Lemma**. Moreover, the special shape of this Gröbner basis enables us to write down formulas for all solutions of $\mathcal{S}$ in terms of the roots of a generator g_n of $I \cap K[x_n]$.

Theorem 3.7.25. (The Shape Lemma)
Let K be a perfect field, let $I \subseteq P$ be a zero-dimensional radical ideal in normal x_n-position, let $g_n \in K[x_n]$ be the monic generator of the elimination ideal $I \cap K[x_n]$, and let $d = \deg(g_n)$.

a) *The reduced Gröbner basis of the ideal I with respect to* Lex *is of the form $\{x_1 - g_1, \ldots, x_{n-1} - g_{n-1}, g_n\}$, where $g_1, \ldots, g_{n-1} \in K[x_n]$.*

b) *The polynomial g_n has d distinct zeros $a_1, \ldots, a_d \in \overline{K}$, and the set of zeros of I is*

$$\mathcal{Z}(I) = \{(g_1(a_i), \ldots, g_{n-1}(a_i), a_i) \mid i = 1, \ldots, d\}$$

Proof. Since b) follows from a) by applying Theorem 3.7.19 to the zero-dimensional radical ideal $(g_n) \subseteq K[x_n]$, it suffices to prove claim a). From Theorem 3.7.23.c we deduce that, for each $i \in \{1, \ldots, n\}$, the residue class $x_i + I$ is a K-linear combination of $1 + I, \ldots, x_n^{d-1} + I$. Hence there exist $g_1, \ldots, g_{n-1} \in K[x_n]$ such that $x_i - g_i \in I$ for $i = 1, \ldots, n-1$. Now we show that $\{x_1 - g_1, \ldots, x_{n-1} - g_{n-1}, g_n\}$ is the reduced Lex-Gröbner basis of I. Since those polynomials are in I, we have $(x_1, \ldots, x_{n-1}, x_n^d) \subseteq \mathrm{LT}_{\mathtt{Lex}}(I)$, and Macaulay's Basis Theorem 1.5.7 implies that this is an equality. Therefore $\{\mathrm{LT}_{\mathtt{Lex}}(x_1 - g_1), \ldots, \mathrm{LT}_{\mathtt{Lex}}(x_{n-1} - g_{n-1}), \mathrm{LT}_{\mathtt{Lex}}(g_n)\}$ is a minimal system of generators of $\mathrm{LT}_{\mathtt{Lex}}(I)$. Furthermore, since $\deg(g_i) < d$ for $i = 1, \ldots, n-1$, the elements of this Gröbner basis are fully reduced. $\square$

The last result of this section, its highlight, and in some sense also its true beginning, is the following corollary. It combines everything we learned before and gives a detailed recipe for solving systems of polynomial equations effectively, albeit not necessarily efficiently.

Corollary 3.7.26. (Solving Systems Effectively)
Let K be a field of characteristic zero or a perfect field of characteristic $p > 0$ having effective p^{th} roots. Furthermore, let $f_1, \ldots, f_s \in P = K[x_1, \ldots, x_n]$, and let $I = (f_1, \ldots, f_s)$. Consider the following sequence of instructions.

1) *For $i = 1, \ldots, n$, compute a generator g_i of the elimination ideal $I \cap K[x_i]$. If $g_i = 0$ for some $i \in \{1, \ldots, n\}$, then return* "Infinite Solution Set" *and stop.*

2) *Depending on the characteristic of K, use Proposition 3.7.9.b or Proposition 3.7.12 to compute $h_i = \mathrm{sqfree}(g_i)$ for $i = 1, \ldots, n$. Then replace I by $I + (h_1, \ldots, h_n)$.*

3) *Compute $d = \#(\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\})$.*

4) *Check if $\deg(h_n) = d$. In this case, let $(c_1, \ldots, c_{n-1}) = (0, \ldots, 0)$ and continue with step 8).*

5) *If K is finite, enlarge it so that it has more than $\binom{d}{2}$ elements.*
6) *Choose $(c_1, \ldots, c_{n-1}) \in K^{n-1}$. Apply the coordinate transformation $x_1 \mapsto x_1, \ldots, x_{n-1} \mapsto x_{n-1}, x_n \mapsto x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}$ to I and get an ideal J.*
7) *Compute a generator of $J \cap K[x_n]$ and check if it has degree d. If not, repeat steps 6) and 7) until this is the case. Then rename J and call it I.*
8) *Compute the reduced Gröbner basis of I with respect to Lex. It has the shape $\{x_1 - g_1, \ldots, x_{n-1} - g_{n-1}, g_n\}$ with polynomials $g_1, \ldots, g_n \in K[x_n]$ and with $\deg(g_n) = d$. Return the tuples $(c_1, \ldots, c_{n-1})$ and $(g_1, \ldots, g_n)$ and stop.*

This is an algorithm which decides whether the system of polynomial equations $\mathcal{S}$ given by $f_1 = \cdots = f_s = 0$ has finitely many solutions. In that case, it returns tuples $(c_1, \ldots, c_{n-1}) \in K^{n-1}$ and $(g_1, \ldots, g_n) \in K[x_n]^n$ such that, after we perform the linear change of coordinates $x_1 \mapsto x_1, \ldots, x_{n-1} \mapsto x_{n-1}, x_n \mapsto x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}$, the transformed system of equations has the set of solutions $\{(g_1(a_i), \ldots, g_{n-1}(a_i), a_i) \mid i = 1, \ldots, d\}$, where $a_1, \ldots, a_d \in \overline{K}$ are the zeros of g_n.

In other words, the original system of equations has the set of solutions $\{(g_1(a_i), \ldots, g_{n-1}(a_i), a_i - c_1 g_1(a_i) - \cdots - c_{n-1} g_{n-1}(a_i)) \mid i = 1, \ldots, d\}$.

Proof. The fact that step 1) checks correctly whether $\mathcal{Z}(I)$ is finite follows from Proposition 3.7.1. By Corollary 3.7.16, the ideal I is replaced by its radical $\sqrt{I}$ in step 2). As we noticed after the proof of Corollary 3.7.16, we have $\sqrt{I} \cap K[x_i] = (h_i)$ for $i = 1, \ldots, n$. Now Theorem 3.7.19 and Macaulay's Basis Theorem 1.5.7 imply that the number d computed in step 3) is exactly the number of solutions of our system of equations.

The ideal I is in normal x_n-position if and only if the degree of a generator of $I \cap K[x_n]$ is d (see Theorem 3.7.23). This is checked in step 4). If it does not hold, we have to find a suitable linear change of coordinates. In step 5) we enlarge the field K if necessary so that the hypothesis of Proposition 3.7.22 is satisfied. Then this proposition says that we eventually find a tuple $(c_1, \ldots, c_{n-1}) \in K^{n-1}$ in step 6) such that the corresponding linear change of coordinates puts I into normal x_n-position. In step 7) we check whether this has happened, and if not, we repeat step 6). Finally we are in the situation of the Shape Lemma. It yields the correctness of step 8) and the claim of the corollary. $\square$

For more advanced readers we note that when we work over a finite field K and we arrive at step 6) of this algorithm, we can perform an exhaustive search of all tuples $(c_1, \ldots, c_{n-1}) \in K^{n-1}$, and Proposition 3.7.22 guarantees that we will eventually find a suitable coordinate transformation. In the case of an infinite base field K, choosing random tuples $(c_1, \ldots, c_{n-1}) \in K^{n-1}$ seems to yield only a probabilistic algorithm, but using more refined tools one could show that it is actually deterministic.

Of course, if $K = \mathbb{Q}$ and if the zeros of the polynomial g_n can be represented using radicals, then this corollary provides us with actual formulas for the solutions of our system of equations $\mathcal{S}$. More generally, if we accept the zeros $a_1, \ldots, a_d \in \overline{K}$ of g_n as *symbols* denoting certain algebraic numbers over K, we still get formulas for the solutions of $\mathcal{S}$ in terms of those symbols. If we want the minimal polynomials over K of the coordinates of those solutions, we can compute them using the methods described in Tutorial 17. We end this section with an example which shows how one can apply the preceding algorithm in a concrete case.

Example 3.7.27. Let us consider the following system of equations over $K = \mathbb{Q}$. Let $f_1 = x_1^2 + x_2^2 + x_3^2 - 9$, $f_2 = 3x_1^2 - x_2^2 x_3$, and $f_3 = x_1^2 x_3 - 2x_2^2 + 2$ be three polynomials in $P = \mathbb{Q}[x_1, x_2, x_3]$ which define a system of polynomial equations $f_1 = f_2 = f_3 = 0$. We let $I = (f_1, f_2, f_3)$ and follow the steps of the algorithm in Corollary 3.7.26.

1) We compute $I \cap \mathbb{Q}[x_i] = (g_i)$ for $i = 1, 2, 3$ and get the polynomials $g_1 = x_1^6 + 12x_1^4 - 12x_1^2 - 32 \neq 0$, $g_2 = x_2^8 - 16x_2^6 - 9x_2^4 + 108x_2^2 + 108 \neq 0$, and $g_3 = x_3^4 - 15x_3^2 - 2x_3 + 48 \neq 0$.
2) Since $\gcd(g_i, g_i') = 1$ for $i = 1, 2, 3$, those polynomials are squarefree and I is a radical ideal.
3) We compute $d = \#(\mathbb{T}^3 \setminus \mathrm{LT}_{\mathtt{Lex}}(I)) = 16$. Thus the number of solutions is 16.
4) Since $\deg(g_3) = 4 < 16$, the ideal I is not yet in normal x_3-position.
5) Nothing has to be done, because $K = \mathbb{Q}$ is infinite.
6) We choose $(c_1, c_2) = (-1, -1)$ and apply the corresponding coordinate transformation $x_1 \mapsto x_1$, $x_2 \mapsto x_2$, $x_3 \mapsto x_1 + x_2 + x_3$ to compute J.
7) We compute a generator h_3 of $J \cap \mathbb{Q}[x_3]$ and get the polynomial $h_3 = x_3^{16} - 72x_3^{14} + 16x_3^{13} + \cdots - 338\,079\,047$. Therefore the ideal J is in normal x_3-position. We rename J and call it I.
8) We compute the reduced Gröbner basis of I with respect to $\mathtt{Lex}$ and get $\{x_1 - c_{15}x_3^{15} - \cdots - c_0, x_2 - d_{15}x_3^{15} - \cdots - d_0, h_3\}$ with numbers $c_0, \ldots, c_{15}, d_0, \ldots, d_{15} \in \mathbb{Q}$ which have approximately 30-digit numerators and denominators. Then we let $h_1 = c_0 + \cdots + c_{15}x^{15}$ and $h_2 = d_0 + \cdots + d_{15}x^{15}$, and we return the tuples $(-1, -1)$ and (h_1, h_2, h_3). *Hint:* If this calculation takes very long on your computer, you may want to first enlarge the system of generators of I by adding to it elements of other Gröbner bases, e.g. with respect to the various elimination orderings.

The meaning of this result is that we can write the 16 solutions of $\mathcal{S}$ as triples whose coordinates are polynomials in the zeros $a_1, \ldots, a_{16} \in \overline{\mathbb{Q}}$ of h_3. In this particular example, there exists a way to simplify the computation. Factoring g_3, we get $g_3 = (x_3 - 2)(x_3 + 3)(x_3^2 - x_3 - 8)$. Therefore, instead of $\mathcal{S}$, we can also solve the following two systems of polynomial equations.

1) If $x_3 = 2$, we have the new system of equations

$$\begin{cases} x_1^2 + x_2^2 - 5 = 0 \\ 3x_1^2 - 2x_2^2 = 0 \\ x_1^2 - x_2^2 + 1 = 0 \end{cases}$$

which easily yields the solutions $(\pm\sqrt{2}, \pm\sqrt{3}, 2)$ of the original system $\mathcal{S}$.

2) In the system of equations $f_1 = f_2 = f_3 = 0$ and $x_3^3 + 2x_3^2 - 11x_3 - 24 = 0$, the indeterminates x_1 and x_2 appear only quadratically. Thus we may substitute $y_1 = x_1^2$, $y_2 = x_2^2$, and $y_3 = x_3$, and solve the system of equations

$$\begin{cases} h_1 = y_1 + y_2 + y_3^2 - 9 = 0 \\ h_2 = 3y_1 - y_2 y_3 = 0 \\ h_3 = y_1 y_3 - 2y_2 + 2 = 0 \\ h_4 = y_3^3 + 2y_3^2 - 11y_3 - 24 = 0 \end{cases}$$

That system of equations simplifies in a straightforward way, and we get $y_1 = 4y_3^2 - 2y_3 - 40$ and $y_2 = -5y_3^2 + 2y_3 + 49$, so that the three solutions of $h_4 = 0$ each give rise to four solutions of our original system $\mathcal{S}$.

Exercise 1. Prove that a field K is perfect if and only if the following two conditions are equivalent for every polynomial $f \in K[x] \setminus K$.

a) The polynomial f is squarefree.
b) We have $\gcd(f, f') = 1$.

Exercise 2. Let p be a prime number, let $K = \mathbb{F}_p$ be the field with p elements, and let $f \in K[x]$.

a) Write a CoCoA function `IsPPower(...)` which checks whether f is of the form $f = g^p$ with a polynomial $g \in K[x]$ and returns the corresponding Boolean value.
b) Write a CoCoA function `PRoot(...)` which takes a polynomial f of the form $f = g^p$ such that $g \in K[x]$ and computes g.

Exercise 3. Prove that a zero-dimensional prime ideal of P is maximal.
Hint: Use Proposition 3.7.18.a.

Exercise 4. Find an example of a field K and a radical ideal $I \subseteq K[x]$ such that $I \cdot \overline{K}[x]$ is not radical, where $\overline{K}$ is the algebraic closure of K.
Hint: Look at the polynomial $x^p - y \in \mathbb{Z}/(p)(y)[x]$.

Exercise 5. Let $f = x^5 - 4x^4 + 10x^2 - x - 3 \in \mathbb{Q}[x]$. Using for instance the CoCoA function `Factor(...)`, check that its factorization in $\mathbb{Q}[x]$ is $f = f_1 \cdot f_2$, where $f_1 = x^3 - 3x^2 + 1$ and $f_2 = x^2 - x - 3$.

a) Let $g = x^3 + ax^2 + bx + c$ and $h = x^2 + dx + e$ be polynomials in $\mathbb{Q}[x, a, b, c, d, e]$. We set $f = g \cdot h$ and compare the coefficients for the different powers of x. Solve the corresponding system $\mathcal{S}$ of polynomial equations and recover the above factorization.

b) Let $K = \mathbb{Q}[e]/(e^3 - 3e - 1)$, and let ε be the image of e in K. By computing the reduced Lex-Gröbner basis of the ideal associated with the system $\mathcal{S}$, show that $g = x^3 + (\varepsilon^2 - 4)x^2 - \varepsilon^2 x - 3(\varepsilon^2 - 3)$ and $h = x^2 - \varepsilon^2 x + \varepsilon$ in $K[x]$ satisfy $f = g \cdot h$.

c) Do a) and b) contradict the unique factorization property of $K[x]$? *Hint:* Show that $h \mid f_1$ in $K[x]$.

d) Find the complete factorization of f in $K[x]$, and then in $\overline{\mathbb{Q}}[x]$.

Exercise 6. Let K be a field, let I be an ideal in $P = K[x_1, \ldots, x_n]$, let $(c_1, \ldots, c_{n-1}) \in K^{n-1}$, and let $\varphi : P \longrightarrow P$ be the linear change of coordinates which is defined by $x_1 \mapsto x_1, \ldots, x_{n-1} \mapsto x_{n-1}$, and by $x_n \mapsto x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}$.

a) Show that φ is a K-algebra isomorphism and describe $J = \varphi(I)$.

b) Prove that a tuple $(a_1, \ldots, a_n) \in \overline{K}^n$ is a zero of I if and only if the tuple $(a_1, \ldots, a_{n-1}, a_n + c_1 a_1 + \cdots + c_{n-1} a_{n-1})$ is a zero of J.

Exercise 7. Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, and let $I \subseteq P$ be a zero-dimensional radical ideal.

a) Write a CoCoA function `IsNormalPos(...)` which checks whether I is in normal x_n-position and returns the corresponding Boolean value.

b) Write a CoCoA function `NormalPosTrafo(...)` which computes a tuple of rational numbers $(c_1, \ldots, c_{n-1}) \in \mathbb{Q}^{n-1}$ such that the linear change of coordinates which is defined by $x_1 \mapsto x_1, \ldots, x_{n-1} \mapsto x_{n-1}$, and by $x_n \mapsto x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}$ transforms I into an ideal in normal x_n-position. (Of course, if I is already in normal x_n-position, your function should return the zero vector.)

Exercise 8. Let K be a perfect field, and let L/K be a finite field extension. Prove that there exists an irreducible polynomial $g \in K[x]$ and an isomorphism $L \cong K[x]/(g)$. (*Hint:* If K is finite, look at Tutorial 3.)

Tutorial 42: Strange Polynomials

Let us remind you of Section 0.10 in the introduction of this book. There we claimed that even polynomials in a single indeterminate over a field are not as simple as one would think. Of course, you are familiar with the phenomenon where one multiplies two polynomials, and a lot of cancellation occurs so the result is simpler than either of the factors. But what about the following claim? Given any $\varepsilon > 0$, there exists a polynomial $f \in \mathbb{Q}[x]$ such that the number of terms of $\operatorname{Supp}(f^2)$ is less than ε times the number of terms of $\operatorname{Supp}(f)$. Would you believe this? For instance, with $\varepsilon = 0.001$ we are talking about a polynomial which has a thousand times more terms than its square. If you doubt that such a polynomial could ever exist, do not worry. Below you will *prove* it.

In this tutorial, we shall show you how to construct some *strange* polynomials, i.e. some polynomials having unexpected properties. For a polynomial

$f \in \mathbb{Q}[x]$, we let $\ell(f) = \# \operatorname{Supp}(f)$. We shall say that f is a **dense** polynomial if $\ell(f) = \deg(f) + 1$. To get started, we treat the following question.

Is it possible that f is dense, but f^2 is not?

In the remainder of this tutorial, we let $f \in \mathbb{Q}[x]$ be a dense univariate polynomial of degree $d = \deg(f) > 0$. We let $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$, where $a_0, \ldots, a_d \in \mathbb{Q}$.

a) Show that if $\deg(f) = 1$, then f^2 is dense.

b) Show that if $\deg(f) \geq 2$, then $\ell(f^2) \geq 4$.

c) Let $a \in \mathbb{Q} \setminus \{0\}$. Show that the following maps $T_i : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]$ induce bijective maps on the set of dense polynomials which preserve both $\ell(f)$ and $\ell(f^2)$.

  1) $T_1(f) = af$
  2) $T_2(f) = f(ax)$
  3) $T_3(f) = x^d f(\frac{1}{x})$

d) Using T_1, show that, for answering our question, we may assume that f is monic.

e) Assume that f is monic, i.e. that we have $f = x^d + a_{d-1} x^{d-1} + \cdots + a_0$. Consider $a_0, \ldots, a_{d-1}$ as indeterminates over $\mathbb{Q}$. Next, write f^2 in the form $f^2 = x^{2d} + b_{2d-1} x^{2d-1} + \cdots + b_0$ with $b_0, \ldots, b_{2d-1} \in \mathbb{Q}[a_0, \ldots, a_{d-1}]$. Prove that $\deg(b_i) \leq 2$ for $i = 0, \ldots, 2d - 1$.

f) Prove that there exists a non-empty Zariski-open subset $U \subseteq \mathbb{A}_{\mathbb{Q}}^d$ such that, for every $(a_0, \ldots, a_{d-1}) \in U$, the corresponding monic polynomial f satisfies $\ell(f^2) = 2 \deg(f) + 1$, i.e. it has a dense square. (For the definition of the Zariski topology on $\mathbb{A}_{\mathbb{Q}}^d$, see Tutorial 27.)

g) For $f = x^2 + a_1 x + a_0$, describe the set U explicitly. Find an example such that $\ell(f^2) < 5 = 2 \deg(f) + 1$.

h) Show that if $\deg(f) = 2$ and f is dense, then $4 \leq \ell(f^2) \leq 5$. Hence quadratic polynomials satisfy $\ell(f) < \ell(f^2)$.

i) Show that 4 is the first degree for which there exists a dense polynomial $f \in \mathbb{Q}[x]$ with $\ell(f) = \ell(f^2)$. Exhibit such an example.

Altogether, we have shown that there exists a *maximum value* for $\ell(f^2)$, namely $2 \deg(f) + 1$, which is achieved by *most* polynomials, but there are examples where this maximum is not achieved. In fact, we have seen that $\ell(f^2) = \ell(f) = \deg(f) + 1$ is possible. Now we become even more ambitious and ask the following question.

Is it possible that f is dense and $\ell(f^2) < \ell(f)$?

Our next goal is to show that this question has a positive answer, too. But in order to find an example of such a polynomial, one has to go at least to degree 12. More precisely, we shall explain how you can prove that there are no examples of degree ≤ 11.

As before, we let $f = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Q}[x]$ be a dense polynomial. The first possibility for $\ell(f^2) < \ell(f) = d + 1$ occurs when $\ell(f^2) = d$. It turns out to be easiest to look for f such that $\ell(f^2) \le d$.

j) Consider the polynomial
$$f = (x^6 + \tfrac{2}{5}x^5 - \tfrac{2}{25}x^4 + \tfrac{4}{125}x^3 - \tfrac{2}{125}x^2 + \tfrac{2}{125}x + \tfrac{1}{125})(x^6 + \alpha)$$
where α is one of the six values $\alpha_1 = -\tfrac{1}{110}$, $\alpha_2 = -\tfrac{1}{253}$, $\alpha_3 = -\tfrac{2}{55}$, $\alpha_4 = \tfrac{1}{15625 \cdot \alpha_1} = -\tfrac{110}{15625}$, $\alpha_5 = \tfrac{1}{15625 \cdot \alpha_2} = -\tfrac{253}{15625}$, or $\alpha_6 = \tfrac{1}{15625 \cdot \alpha_3} = -\tfrac{11}{6250}$. Use CoCoA to check that $\ell(f) = 13$, while $\ell(f^2) = 12$. For instance, in the case $\alpha_1 = -\tfrac{1}{110}$, we obtain the example printed in Section 0.10.

k) Apply T_2 and T_1 to the above polynomial f to produce another dense polynomial g of degree 12 such that $g = x^{12} + x^{11} + \cdots$ and $\ell(g^2) = 12$.

l) Show that there exist finitely many systems of $d+2$ polynomial equations over the ring $\mathbb{Q}[a_0, \ldots, a_{d-2}, x]$ such that at least one of them has a solution if and only if there exists a dense polynomial f which satisfies $\ell(f^2) \le d$.

Hint: In view of part i), it suffices to consider the case $d \ge 4$. Using T_1 and T_2, we may assume that $a_d = a_{d-1} = 1$ and that the coefficients $b_{2d}, b_{2d-1}, b_1, b_0$ of f^2 are different from zero. Therefore at least $d + 1$ coefficients of f^2 among the remaining $2d - 3$ have to vanish. Finally, we need to add one equation which expresses the fact that the coefficients of f are non-zero (see Proposition 3.5.6).

m) Let $d = 5$. Write a CoCoA program $\texttt{StrangeSystems}(\ldots)$ which finds the ideals associated to the systems described in part l). Then use Corollary 2.6.14 and suitable Gröbner basis computations with CoCoA to show that there is no dense polynomial $f \in \overline{\mathbb{Q}}[x]$ of degree five such that $\ell(f^2) \le 5$.

n) Try to do the computation for $d = 6$ and higher. Be careful that, as the degree of f increases, the number of systems to be checked grows tremendously. Give an estimate of this number depending on $\deg(f)$.

In the last part of this tutorial, we shall show that even the following daring question has a positive answer.

For every $\varepsilon > 0$, is there a dense $f \in \mathbb{Q}[x]$ with $\ell(f^2) < \varepsilon \cdot \ell(f)$?

o) Let $f \in \mathbb{Q}[x]$ be a dense polynomial. Show that $g(x) = f(x) \cdot f(x^{2d+1})$ satisfies $\ell(g) = \ell(f)^2$. (*Hint:* Think of g as consisting of $d + 1$ copies of f, multiplied by various terms and scalars.)

p) In the situation of o), show that $\ell(g^2) = \ell(f^2)^2$. (*Hint:* Let $h = f^2$ and note that $g(x)^2 = h(x) \cdot h(x^{2d+1})$.)

q) Now let f be one of the polynomials in j), and let $g(x) = f(x) \cdot f(x^{25})$. Show that $\tfrac{\ell(g^2)}{\ell(g)} = \left(\tfrac{\ell(f^2)}{\ell(f)}\right)^2 = (\tfrac{12}{13})^2$. By repeating this process, prove that the above question has a positive answer.

Tutorial 43: Primary Decompositions

Although the computation of the primary decomposition of a polynomial ideal is one of the most advanced operations in Computational Commutative Algebra, we shall now try to perform the first few steps in this direction. Naturally, this tutorial requires somewhat higher algebraic skills than the ones before.

Given a ring R, an ideal $\mathfrak{q} \subset R$ is called a **primary ideal** if every zerodivisor in $R/\mathfrak{q}$ is a nilpotent element. Equivalently, we are asking that, for all $a, b \in R$ such that $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$, there exists a number $i \geq 1$ such that $b^i \in \mathfrak{q}$.

In the sequel we assume that R is a Noetherian ring.

a) Prove that the radical of a primary ideal $\mathfrak{q}$ is a prime ideal $\mathfrak{p}$. We shall say that the ideal $\mathfrak{q}$ is $\mathfrak{p}$**-primary**.

b) Prove that an ideal $\mathfrak{q}$ in R is $\mathfrak{p}$-primary if and only if there exists exactly one associated prime of $R/\mathfrak{q}$, namely the prime $\mathfrak{p}$. (For the definition of an associated prime, see Tutorial 31.e.)

c) An ideal $\mathfrak{q}$ in R is called **irreducible** if it cannot be written as the intersection of two ideals, both of which properly contain it. Show that every irreducible ideal $\mathfrak{q}$ in R is a primary ideal.
   Hint: Assume that there are two different associated primes of $R/\mathfrak{q}$ and deduce a contradiction.

d) Using c) and the fact that R is Noetherian, prove that every ideal in R can be written as a finite intersection of primary ideals. Such a representation is called a **primary decomposition** of the ideal.
   Hint: Consider the largest ideal in R which is not an intersection of finitely many irreducible ideals.

In the remaining part of this tutorial, we want to compute primary decompositions for zero-dimensional ideals in the ring $P = K[x_1, \ldots, x_n]$ over a perfect field K. If $\operatorname{char}(K) = p > 0$, we also assume that K has effective p^{th} roots. We have seen that one can compute $\sqrt{I}$ in this case, and that $\sqrt{I}$ is the intersection of finitely many maximal ideals in P.

e) Write a CoCoA function `ZeroDimRad(...)` which takes a zero-dimensional ideal $I \subseteq P$ and computes $\sqrt{I}$ using the method of Corollary 3.7.16.
   Hint: The base field K is $\mathbb{Q}$ or $\mathbb{F}_p$. You may want to use the function `SqFree(...)` from Tutorial 5.

f) Apply your function `ZeroDimRad(...)` to compute the radicals of the following zero-dimensional ideals.
   1) $I_1 = (x^3, x^2y + x, y^2)$ in $\mathbb{Q}[x, y]$
   2) $I_2 = (x^{27} + y^{27} + 1, x^{18} - x^9y^9 - x^9)$ in $\mathbb{Z}/(3)[x, y]$
   3) $I_3 = (z^2, y^2z + yz, xz + yz, y^4 + 2y^3 + y^2, xy^2 + y^3 + xy + y^2, x^2 + 2xy + y^2)$ in $\mathbb{Q}[x, y, z]$
   4) $I_4 = (z^7, y^{98} + y^{49}, x^{49} + y^{49})$ in $\mathbb{Z}/(7)[x, y, z]$

g) Suppose that $\sqrt{I} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$ with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ in P. For $i = 1, \ldots, t$, let $\mathfrak{q}_i = I :_P (I :_P \mathfrak{m}_i^\infty)$. Show that $\mathfrak{q}_i$ is a $\mathfrak{m}_i$-primary ideal for $i = 1, \ldots, t$, and that $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ is a primary decomposition of I.

Hint: Start with a primary decomposition $I = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_u$. Show that $u = t$ and that we can assume $\mathfrak{m}_i = \sqrt{\mathfrak{q}'_i}$ for $i = 1, \ldots, t$. Then apply the Chinese Remainder Theorem 3.7.4 to P/I and prove $\mathfrak{q}'_i = \mathfrak{q}_i$ for $i = 1, \ldots, t$.

Thus we can reduce the computation of a primary decomposition of a zero-dimensional ideal to the case of a zero-dimensional radical ideal. From now on, let I be a zero-dimensional radical ideal in P.

h) Write a CoCoA function `IsNormalPos(...)` which checks whether I is in normal x_i-position for some $i \in \{1, \ldots, n\}$ and returns `FALSE` or the corresponding i.

i) Apply your function `IsNormalPos(...)` to check whether the following zero-dimensional ideals are in normal x_i-position for some $i \in \{1, \ldots, n\}$.

1) $I_5 = (x^2 + y^2 - 1,\ 4xy - 2x - 2y + 1)$ in $\mathbb{Q}[x, y]$
2) $I_6 = (x^2 - y,\ x^2 - 3x + 2)$ in $\mathbb{Q}[x, y]$
3) $I_7 = (yz + z,\ y^2 + y,\ x + y + z,\ z^2 - z)$ in $\mathbb{Q}[x, y, z]$

j) Suppose that I is not in normal x_i-position for any $i \in \{1, \ldots, n\}$. Write a CoCoA function `NormalPosTrafo(...)` which computes an index $i \in \{1, \ldots, n\}$ and a tuple $(c_1, \ldots, c_{n-1}) \in K^{n-1}$ such that the linear change of coordinates which is defined by $x_j \mapsto x_j$ for $j \neq i$ and by $x_i \mapsto x_i - c_1 x_1 - \cdots - c_{i-1} x_{i-1} - c_i x_{i+1} - \cdots - c_{n-1} x_n$ transforms I into an ideal in normal x_i-position.

Hint: If $\mathrm{char}(K) = 0$ and if you did Exercise 7, you may use your results. If $\mathrm{char}(K) = p > 0$, try all possible coordinate changes. In case none of them works, exit the program with an error message.

k) Use your function `NormalPosTrafo(...)` to find transformations which bring the following ideals into normal x_i-position for some $i \in \{1, \ldots, n\}$.

1) $I_8 = (x^2 + y^2 + 3,\ x^2 - y^2 + 1)$ in $\mathbb{Q}[x, y]$
2) $I_9 = (xy,\ x^2 + x,\ y^3 + y^2 + y)$ in $\mathbb{Z}/(2)[x, y]$
3) $I_{10} = (x^3 - x,\ y^2 + y,\ z^2 - z)$ in $\mathbb{Z}/(3)[x, y, z]$

In view of the preceding results, we shall from now on assume that there exists an $i \in \{1, \ldots, n\}$ such that the ideal I is in normal x_i-position.

l) Using Theorem 2.6.6, prove that $I \cap K[x_j] \neq (0)$ for $j = 1, \ldots, n$.

m) Let $p_i \in K[x_i]$ be the monic generator of $I \cap K[x_i]$, and let $p_i = f_{i1} \cdots f_{it}$ be the decomposition of p_i into monic irreducible factors. Show that the polynomials $f_{i1}, \ldots, f_{it}$ are pairwise distinct, and that $I + (f_{ij})$ is a maximal ideal for $j = 1, \ldots, t$.

Hint: Let $\mathfrak{m}$ and $\mathfrak{m}'$ be two maximal ideal containing $I + (f_{ij})$. Show that $\mathfrak{m} \cap K[x_i] = \mathfrak{m}' \cap K[x_i] = (f_{ij})$, and that $\mathfrak{m}$ and $\mathfrak{m}'$ are in normal x_i-position. Conclude that $\mathfrak{m}$ and $\mathfrak{m}'$ have the same zeros in $\overline{K}^n$.

n) In this situation, let $\mathfrak{m}_j = I + (f_{ij})$ for $j = 1, \ldots, t$. Prove that we have $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$.
Hint: Proceed as in the proof of Seidenberg's Lemma 3.7.15.

o) Find an example of a zero-dimensional radical ideal $I \subseteq P$ such that $I \cap K[x_i]$ is a maximal ideal for $i = 1, \ldots, n$, but I is not a maximal ideal. Thus the assumption about the normal position is essential in the argument above.

p) Now combine the results achieved so far and develop an algorithm which computes the primary decomposition of a zero-dimensional radical ideal I. Implement this algorithm in a CoCoA function `RadicalDec(...)`.
Hint: Use the built-in CoCoA function `Factor(...)` to compute the factorization of the element p_i.

q) Apply your function `RadicalDec(...)` to compute the primary decomposition of the following zero-dimensional radical ideals.

1) $I_{11} = (y^3 - 2y^2 - 2y - 3,\ xy^2 + xy - 2y^2 + x - 2y - 2,\ 13x^2 - 5y^2 - 5y + 8)$ in $\mathbb{Q}[x, y]$
2) $I_{12} = (2y^2 - y,\ x - y,\ 2yz + z^2 - y - z,\ 2z^3 - z^2 + y - z)$ in $\mathbb{Q}[x, y, z]$
3) $I_{13} = (x^2 - x,\ y^2 - y,\ z^2 - z,\ xy,\ xz,\ yz)$ in $\mathbb{Z}/(3)[x, y, z]$

r) Finally, write a CoCoA function `PrimaryDec(...)` which checks whether a given ideal I is zero-dimensional and computes a primary decomposition of I in that case.
Hint: Use the Finiteness Criterion 3.7.1 and the functions you wrote before. For the computation of the saturation and the colon ideal in part g), you can use the built-in CoCoA functions or the results of Tutorials 31 and 37.

s) Apply your function `PrimaryDec(...)` to compute the primary decompositions of the ideals $I_1, \ldots, I_{13}$ and of the following ideals.

1) $I_{14} = (4xy^3 - 6xy^2 - 2y^3 - x^2 + 3y^2 + 2x - 1,\ 2x^2y + 2xy^2 - x^2 - 4xy - y^2 + 2x + 2y - 1)$ in $\mathbb{Q}[x, y]$
2) $I_{15} = (x^2 + y^2 + z^2 + 1,\ y^2z + yz^2 + yz,\ xy^2 + y^3 + yz^2 + xy + y,\ y^4 + y^2,\ z^4 + z^2,\ yz^3 + yz^2,\ xz^2 + yz^2 + z^3 + xz + yz + z,\ xyz)$ in $\mathbb{Z}/(2)[x, y, z]$
3) $I_{16} = (x^3 + y^3 - z^3 + xy - x - y,\ xz - yz,\ xy^2 - xy - y^2 + y,\ x^2y - x^2 - xy + x,\ y^4 - y^3)$ in $\mathbb{Z}/(3)[x, y, z]$

Tutorial 44: Modern Portfolio Theory

> *Bull Markets*
> *are born on pessimism,*
> *grow on skepticism,*
> *mature on optimism,*
> *and die on euphoria.*
> (John Templeton)

With this, the final, tutorial we venture where few algebraists have gone before. Indeed, we want to apply Computational Commutative Algebra to some problems of mathematical finance. Modern portfolio theory originated with the doctoral dissertation of H. Markowitz, has been studied extensively in economic circles, is widely believed and applied on Wall Street, and even earned its author a Nobel Prize. But no applications of Computational Commutative Algebra to this area were known to us. Thus is was time to invent something!

What is modern portfolio theory about?

Let us begin this journey by explaining the main problem of portfolio theory. Suppose we have a certain number of investments available, for instance stocks, bonds, real estate, cash, gold, etc. Moreover, suppose we know the prices of those investments at certain dates in the past, for instance at the end of each of the last 20 years. Now the problem of portfolio theory consists in distributing the available money in those investments in such a way that the expected future value of the portfolio is as high as possible, while at the same time the risk that this expectation is badly disappointed is held to a minimum.

How can one describe this problem mathematically?

To solve this problem, modern portfolio theory proposes to use the following mathematical model. Suppose that there exist n investments from which we can choose. Let $\{t_0, \ldots, t_N\}$ be the points in time at which we know the prices of these investments. For simplicity, we assume that t_i is, for every $i \in \{1, \ldots, N\}$, of the form $t_i = t_0 + i \cdot \Delta t$ with a fixed time period Δt. For $i = 1, \ldots, n$, let $A_i : \{t_0, \ldots, t_N\} \longrightarrow \mathbb{Q}_{>0}$ be the function whose values are the prices of the ith investment.

Next, we set $\Omega = \{t_1, \ldots, t_N\}$, and, for $i = 1, \ldots, n$, we consider the maps

$$X_i : \Omega \longrightarrow \mathbb{Q}_{>0} \qquad \text{defined by} \quad t_j \longmapsto \tfrac{A_i(t_j) + B_i(t_j)}{A_i(t_{j-1})}$$

where $B_i(t_j)$ is the income derived from the ith investment during the period $[t_{i-1}, t_i]$, for instance a stock dividend or an interest payment. The function X_i is called the **total return** of the ith investment.

Now a **portfolio** is a tuple $(a_1, \ldots, a_n) \in \mathbb{R}^n_{>0}$ such that $a_1 + \cdots + a_n = 1$. Here a_i represents the portion of the initial capital which is allocated to the

i^{th} investment. Consequently, the function $X = a_1 X_1 + \cdots + a_n X_n$ represents the total return of the portfolio.

And how does one recognize a "good" portfolio?

In order to define what we mean by a "high expected return" and a "low risk" of the portfolio, we now have to make Ω into a discrete probability space. Don't worry! We do not expect that you know what this is. For our purposes, the following definitions will be sufficient. (For experts we remark that the map p which assigns to each subset $S \subseteq \Omega$ the number $p(S) = \frac{\#S}{N}$ is used to define the uniform distribution on Ω.)

For $i = 1, \ldots, n$, the number $E(X_i) = \frac{1}{N} \sum_{k=1}^{N} X_i(t_k)$ is called the **expected return** of the ith investment. (In probability theory, one would say that $E(X_i)$ is the expected value of the random variable X_i.) Similarly, the number

$$E(X) = \tfrac{1}{N} \sum_{j=1}^{N} (a_1 X_1(t_j) + \cdots + a_n X_n(t_j)) = a_1 E(X_1) + \cdots + a_n E(X_n)$$

is called the expected return of the portfolio $(a_1, \ldots, a_n)$.

Furthermore, for $i = 1, \ldots, n$, the number $\mathrm{Var}(X_i) = \frac{1}{N} \sum_{k=1}^{N} (X_i(t_k) - E(X_i))^2$ is called the **variance** of X_i, and the number $\sigma(X_i) = \sqrt{\mathrm{Var}(X_i)}$ is called the **standard deviation** of X_i. For $i, j \in \{1, \ldots, n\}$, the number $\mathrm{Cov}(X_i, X_j) = \frac{1}{N} \sum_{k=1}^{N} (X_i(t_k) - E(X_i))(X_j(t_k) - E(X_j))$ is called the **covariance** of X_i and X_j, and if $\sigma(X_i)\sigma(X_j) \neq 0$, the number $\varrho(X_i, X_j) = \mathrm{Cov}(X_i, X_j)/(\sigma(X_i)\sigma(X_j))$ is called the **correlation coefficient** of X_i and X_j.

At this point, it is time for you to start working. But let us insert a few cautionary remarks here. The tasks we assign in this tutorial are generally less well-defined than in the tutorials before. Moreover, the level of difficulty is somewhat higher than usual. However, we think that the rewards you can reap by solving all parts make the effort worthwhile.

a) Suppose that the investments are given by the lists of values of their total return functions $X_i : \Omega \longrightarrow \mathbb{Q}_{>0}$. Write CoCoA functions `ExpRet(...)`, `VarRet(...)`, and `CovRet(...)` which take these lists and a number $d \geq 1$ and compute $E(X_i)$, $\mathrm{Var}(X_i)$, and $\mathrm{Cov}(X_i, X_j)$ up to d decimal places.

b) Apply these functions to the following lists $L_i = [X_i(t_1), \ldots, X_i(t_N)]$.

1) $L_1 = [0.935, 0.989, 1.132, 0.687, 0.648, 1.408, 1.083, 0.816, 0.902, 1.035,$ $1.429, 1.034, 1.229, 1.333, 1.144, 1.022, 0.907, 0.839, 1.208, 1.271]$

2) $L_2 = [0.713, 1.067, 1.133, 0.739, 1.014, 1.402, 0.904, 1.079, 1.047, 0.865,$ $0.966, 1.02, 1.127, 1.4, 1.061, 1.664, 1.048, 0.698, 1.328, 1.348]$

3) $L_3 = [1.078, 1.118, 1.609, 1.167, 0.702, 1.09, 1.046, 1.177, 1.181, 0.831,$ $1.461, 1.207, 1.032, 1.434, 1.331, 1.104, 1.43, 1.222, 1.53, 1.069]$

4) $L_4 = [0.981, 1.058, 1.063, 0.99, 0.992, 1.094, 1.056, 1.154, 1.083, 0.998,$ $0.999, 0.947, 1.137, 1.094, 1.079, 1.081, 1.071, 1.08, 1.04, 1.001]$

5) $L_5 = [0.992, 1.042, 1.456, 1.437, 1.532, 0.805, 0.872, 1.056, 1.161, 2.056,$
    $1.445, 0.79, 1.164, 0.988, 0.933, 0.815, 0.953, 1.029, 0.954, 0.957]$

c) For $i, j = 1, \ldots, n$, show that the following claims hold.

1) $\mathrm{Cov}(X_i, X_i) = \mathrm{Var}(X_i)$

2) $-1 \le \varrho(X_i, X_j) \le 1$

Hint: Without giving a proof, use the **Cauchy-Schwarz inequality**
$|\sum_{k=1}^{N} x_k y_k|^2 \le (\sum_{k=1}^{N} x_k^2)(\sum_{k=1}^{N} y_k^2)$ for $x_k, y_k \in \mathbb{R}$.

d) For the variance $\mathrm{Var}(X) = \frac{1}{N} \sum_{k=1}^{N}(X(t_k) - E(X))^2$, prove

$$\mathrm{Var}(X) = \sum_{i,j=1}^{N} a_i a_j \, \mathrm{Cov}(X_i, X_j)$$

$$= \sum_{i=1}^{n} a_i^2 \, \mathrm{Var}(X_i) + 2 \sum_{1 \le i < j \le n} a_i a_j \, \mathrm{Cov}(X_i, X_j)$$

Using these numbers, modern portfolio theory considers the expected return $E(X)$ of a portfolio as a measure of its "expected future value" and the standard deviation $\sigma(X)$ or the variance $\mathrm{Var}(X)$ as a measure for the "risk" associated with this portfolio. Thus a portfolio $(a_1, \ldots, a_n)$ is called **efficient** if every other portfolio $(b_1, \ldots, b_n)$ with the same variance satisfies $E(b_1 X_1 + \cdots + b_n X_n) \le E(a_1 X_1 + \cdots + a_n X_n)$, and if every other portfolio $(c_1, \ldots, c_n)$ with the same expected return satisfies $\mathrm{Var}(c_1 X_1 + \cdots + c_n X_n) \ge \mathrm{Var}(a_1 X_1 + \cdots + a_n X_n)$. The set of all efficient portfolios is called the **efficient frontier**.

Thus, altogether, we see that the main problem of portfolio theory becomes the computation of the efficient frontier when the available investments are given via their total return functions $X_1, \ldots, X_n : \Omega \longrightarrow \mathbb{Q}_{>0}$.

How can one compute the efficient frontier?

To simplify our notation, let $e_i = E(X_i)$, let $v_i = \mathrm{Var}(X_i)$, and let $c_{ij} = \mathrm{Cov}(X_i, X_j)$ for $i, j = 1, \ldots, n$. We shall suppose that the numbers e_i, v_i, and c_{ij} are given rational numbers. Given a portfolio $(a_1, \ldots, a_n)$, we let $e = E(X)$ and $v = \mathrm{Var}(X)$ be the expected return and the variance of the corresponding function $X = a_1 X_1 + \cdots a_n X_n$. Our discussion so far shows that the following equations hold.

(1) $0 = a_1 + \cdots + a_n - 1$

(2) $0 = a_1 e_1 + \cdots + a_n e_n - e$

(3) $0 = \sum_{i=1}^{n} a_i^2 v_i + 2 \sum_{1 \le i < j \le n} a_i a_j c_{ij} - v$

In order to compute one efficient portfolio, we may consider v as a given number ("risk level") and try to optimize e in (2) under the side conditions (1), (3). The method of **Lagrange multipliers** says that the maximum of e

occurs when the partial derivatives of (2) with respect to the indeterminates $a_1, \ldots, a_n$ are linear combinations of the partial derivatives of (1) and (3).

e) Using the method of Lagrange multipliers, show that the following additional equations have to be satisfied for certain $\ell, m \in \mathbb{Q}$.

$$(4) \qquad 0 = e_i - \ell - m \left(2 a_i v_i + \sum_{j \neq i} a_j c_{ij} \right) \qquad \text{for } i = 1, \ldots, n$$

f) Write a CoCoA function PFEqn(...) which computes an ideal I in the ring $\mathbb{Q}[a_1, \ldots, a_n, e, v, \ell, m]$ which is generated by $n + 3$ polynomials corresponding to equations (1), (2), (3), and (4).

g) Prove that, in general, the ideal $J = I \cap \mathbb{Q}[e, v]$ is a non-zero principal ideal generated by a quadratic polynomial of the form $v - q(e)$.
   Hint: Divide equation (4) by m and assume that all denominators and determinants are non-zero.

Every point on the parabola defined by $v = q(e)$ in the (v, e)-plane corresponds to a portfolio if the associated tuple $(a_1, \ldots, a_n)$ consists of non-negative numbers. By construction, such a portfolio satisfies the first property of an efficient portfolio. In fact, one can show that it is an efficient portfolio. Notice that, for every non-empty subset $S \subseteq \{1, \ldots, n\}$, we can repeat this construction for the corresponding subset of investments and get a parabola defined by an equation $v = q_S(e)$.

h) Write a CoCoA program AllParab(...) which computes the list of all $2^n - 1$ quadratic polynomials $v - q_S(e)$.

i) Implement a CoCoA function IntPoints(...) which calculates a matrix containing approximations of all points of intersection of the "upper halves" of the parabolas $\mathcal{Z}(v - q_S(e))$.
   Hint: To find approximations for the solutions of a quadratic equation in one indeterminate, you may use the functions Round(...) and Sqrt(...) explained in Appendix C.5.

j) Apply your functions AllParab(...) and IntPoints(...) in the case of the five investments of part b).

k) The points of intersection computed by IntPoints(...) subdivide the upper half of each parabola $\mathcal{Z}(v - q_S(e))$ into a number of segments. Show that on each parabola there exists at most one segment whose points correspond to portfolios.

Thus the parts of the efficient frontier are made up of segments of parabolas corresponding to portfolios where $a_i = 0$ for some indices $i \in \{1, \ldots, n\}$, i.e. to portfolios which involve only a proper subset of the set of available investments. Clearly, there exists one portfolio for which v attains the minimal possible value $v_{\min}$. We call it the **minimal risk portfolio**. The situation can be illustrated as follows.
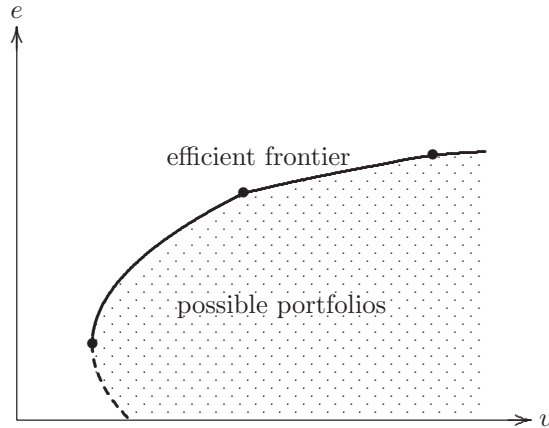
l) Write a CoCoA function `MinPF(...)` which computes the minimal risk portfolio $(a_1, \ldots, a_n)$.

m) Apply your function `MinPF(...)` to compute the minimal risk portfolio for the five investments of part b).

n) Implement a CoCoA function `Frontier(...)` which computes the different pieces of parabolas which constitute the efficient frontier and their points of intersection.

   Hint: Notice that you can easily decide which parabola is the "higher" one from their point of intersection onwards by comparing their leading coefficients.

o) Compute the efficient frontier for the five investments of part b).

What is the "best" efficient portfolio?

Naturally, the answer to this question depends partially on the type of investor for whom the portfolio is constructed. But, astonishingly, there is a nice rule which identifies one point on the efficient frontier which has the property that the corresponding portfolio has the highest return if one continues the investment process over many time periods.

To motivate this rule, we use some deeper results from probability theory. It is not necessary that you know them in order to solve this part of the tutorial, but the overall level of difficulty is somewhat higher than before. Let W_0 be the initial capital. The value of a portfolio $(a_1, \ldots, a_n)$ after i time periods is $W_i = W_0 \cdot \prod_{j=1}^{i} X(t_j)$, where $X = a_1 X_1 + \cdots + a_n X_n$. Thus we have $\ln(\frac{W_i}{W_0}) = \sum_{j=1}^{i} \ln(X(t_j))$. The **strong law of large numbers** now says that

$$\lim_{i \to \infty} \frac{1}{i} \sum_{j=1}^{i} (\ln(X(t_j)) - E(\ln X)) = 0$$

holds almost certainly, i.e. that it holds with probability one.

q) Let $(b_1, \ldots, b_n)$ be another portfolio, and let $Y = b_1 X_1 + \cdots + b_n X_n$. Furthermore, let W_i' be the value of the portfolio $(b_1, \ldots, b_n)$ after i time periods. Show that $W_i > W_i'$ holds almost certainly for large numbers i if and only if we have $E(\ln X) > E(\ln Y)$.

Hint: Assume that the limit $\lim_{i \to \infty} \frac{1}{i} \sum_{j=1}^{i} \ln(X(t_j))$ exists.

The **MEL-rule** ("maximum expected logarithm") says that a portfolio $(a_1, \ldots, a_n)$ is better than a portfolio $(b_1, \ldots, b_n)$ in the very long run if $E(\ln X) > E(\ln Y)$ for $X = a_1 X_1 + \cdots + a_n X_n$ and $Y = b_1 X_1 + \cdots + b_n X_n$. Thus we should choose that point on the efficient frontier for which $E(\ln X)$ attains its maximal value.

Above we computed segments of parabolas which constitute the efficient frontier. Since we can calculate $E(\ln X)$ for the portfolios corresponding to the points of intersection of those parabolas, it suffices to consider the case that the MEL-rule specifies a portfolio which corresponds to an interior point of one of those segments of parabolas.

r) Using the **Taylor expansion** of $\ln(x)$ at the point $x = e$, prove the approximation formula $E(\ln X) \approx \ln(E(X)) - \frac{1}{2} \frac{\text{Var}(X)}{E(X)^2}$.

s) Write $v = q(e)$ and form the derivative with respect to e of the above approximation formula. Conclude that the MEL-rule yields the following additional quadratic equation for the optimal portfolio on the efficient frontier.

$$(5) \qquad\qquad e^2 - \tfrac{1}{2} e\, q'(e) + q(e) = 0$$

t) Develop an algorithm for computing the portfolio which is specified by the MEL-rule. Implement this algorithm in a CoCoA function `MELPF(...)` and apply this function to the five investments of part b).

Hint: To compute $\ln(e)$, you can write $e = 1 + r$ and use the formula $\ln(1 + r) = r - \frac{1}{2} r^2 + \frac{1}{3} r^3 - + \cdots$.

How does this theory hold up in practice?

<div align="right">

Men, it has been well said, think in herds;
it will be seen that they go mad in herds,
while they only recover their senses slowly,
and one by one.
(Charles MacKay)

</div>

Nowadays, modern portfolio theory is widely believed and followed by professional money managers. As we have seen, it is possible to write programs which compute a suggested asset allocation in an automatic way. The economic justification for it is based on the assumption that financial markets are efficient. This means that if there was a theory which could produce reliable above-average gains in the financial world without taking above-average risks, everybody would immediately start to apply it, and it would necessarily stop functioning.

However, it has long been known that markets are not very efficient. As the world-wide stock market mania of the late 1990s showed once again, both private and institutional investors are influenced by crowd psychology. Moreover, many corporations and even governments do not hesitate to manipulate the stock and bond markets. And when a serious financial crisis develops, the market liquidity required by modern portfolio theory dries up completely, because there is no one willing or able to step in on the buy-side.

Another serious objection to modern portfolio theory is that the standard deviation or the variance of the total return of a portfolio is inadequate to measure the risk associated with this portfolio. Price volatility does not detect whether stocks or other investments are significantly over- or undervalued with respect to the assets they represent. If you invested money in the late 1920s or the late 1960s according to this theory, you would have had to put a significant portion into the US stock market, because it had a high expected return and a low volatility, and you would have lost it.

What should we do instead? Since CoCoA cannot really help us in this case, it may be useful to apply our common sense. When you invest money and buy something, it is important to pay a low price relative to the value of whatever you purchase. When your government dramatically increases the supply of money, it may be useful to convert some of your paper wealth to something of more lasting value such as real estate or gold. And when the people around you get carried away by their herd instincts, relax, recover your senses, get out of the markets while the going is good, and enjoy your life! We hope that in this way you will find the time to do some more of the tutorials in this book.

A. How to Get Started with CoCoA

A.1 Getting CoCoA

The computer algebra system CoCoA is available free of charge via the internet. You may download it from the WWW page

ftp://cocoa.dima.unige.it/cocoa/index.html

Choose the file corresponding to your machine and operating system, and do not forget to get a copy of the manual from the directory `/doc`. Then decompress the file ending in `.zip`, or `.tgz`, or `.hqx`. Depending on your system, you will have to use a command like `unzip` or `tar -zxvf`, or the graphical interface of a decompression tool like `Winzip`.

As a result you should have an appropriately named directory or folder, for instance `/usr/local/cocoa/`, which contains the executable file of the program (called `cocoa` or `cocoa.exe`), a file named `userinit.coc`, and a subdirectory called `lib`. If, instead, you find hundreds of files in your folder, you forgot to uncompress in such a way that all paths are restored!

A.2 Starting CoCoA

Now let us try the program. You can start it by simply typing

cocoa

while you are in the folder containing the executable file. Or, if you have a graphical operating system, you can also click on its icon. And if there is no icon, create a link or shortcut to the executable file first. Then the current version of CoCoA starts up and displays a screen like

```
 ---------------------------------------------------------
 ---            ___/        ___/         \            ---
 --            /     _ \  /      _ \     , \          --
 --            \    |   | \      |   |  ___  \        --
 ---            ____, __/  ____, __/ _/      _\       ---
 ---------------------------------------------------------
 --      Version     : 4.7                            --
 --      Online Help : type  ?   or   ?keyword        --
 --      Web site    : http://cocoa.dima.unige.it     --
 ---------------------------------------------------------


 -- The current ring is R ::= Q[x,y,z];
 -------------------------------
```

Below we shall explain how you can enter commands by going with you through a sample session. But first, let us show you how you can exit the program. Simply type

```
Quit;
```

hit `<Enter>`, and that's it! Or maybe not. If you are using the graphical interface of CoCoA under Unix or Windows, you can either send a line to CoCoA by typing `<Ctrl + Enter>` at the end of the line, or you can select a line or a group of lines and send it to CoCoA using `<Ctrl + Enter>`. And if you are using CoCoA on Macintosh, you should make sure you hit the `<Enter>` key, not the one marked `<Return>`. And if, by any chance, you are in a mediterranean mood, you can also leave CoCoA with a cordial

```
Ciao;
```

A.3   Using CoCoA Interactively

In fact, when you typed `Quit;` above, you entered your first CoCoA command. A CoCoA command has two notable features: it starts with a capital letter, and it ends with a semicolon. If you want to define a new object, you have to give it a name starting with a capital letter. Then you can assign it a value by using `:=` as in the following example.

```
F:=x^2+y^2-1;
```

This command defines a new polynomial `F` in the current ring which has the value $x^2 + y^2 - 1$. (We will be talking about rings later, but for the moment we assume that you just started CoCoA and that the current ring is the default ring `R = Q[x,y,z]`.) The value of the new polynomial `F` is `x^2+y^2-1`. As you can see, the indeterminates of a polynomial ring in CoCoA have lower-case letters as names and are raised to powers using the `^` key. Sometimes they

carry indices like `x[1]`,`x[2]`,`x[3]`. All other names of objects and functions in CoCoA start with a capital letter.

Now let us print out the value of our polynomial `F`. For this we could type `Print(F);` or simply

```
F;
```

Then CoCoA answers

```
x^2 + y^2 - 1
-------------------------------
```

We could also perform some calculation before typing its result, e.g.

```
F^2-F+1;
```

yields the output

```
x^4 + 2x^2y^2 + y^4 - 3x^2 - 3y^2 + 3
-------------------------------
```

Next we apply one of the built-in CoCoA functions.

```
Factor(F-2xy+1);
```

CoCoA replies

```
[[x - y, 2]]
-------------------------------
```

which means $F - 2xy + 1 = (x - y)^2$.

A.4   Getting Help

A moment ago we saw an example of the use of the CoCoA function `Factor()`. If you want to know more about this function, type

```
Man('Factor');
```

and CoCoA will display the page of its on-line manual describing the function `Factor()`. In this case, you may even type

```
Man('fac');
```

Since `fac` is not the name of a CoCoA command, CoCoA looks for all topics in its on-line manual containing that string. For more extensive information about how to use the manual, type

```
Man();
```

After that, you get a list of possible commands for getting help. For instance, `H.Toc();` will give you the table of contents of the online manual, `H.Tips();` will give you tips for using the online manual, and `H.Commands('Topic');` summarizes all commands associated with `'Topic'` (the quotes are needed to mark a string).

There are several other ways to access the CoCoA manual. In the directory `doc` on the ftp-server mentioned in Section A.1 you will find an html-version for reading with an internet browser, and a postscript-version for printing. Finally, if you use the graphical interface of CoCoA under Windows, you can also access the manual through the Windows help system.

Since this introduction to CoCoA has to be limited in space and scope, we strongly urge you to look up all the topics we discuss in the manual. There you will find more extensive and more detailed information. Moreover, there is a section of the manual called "Tutorial" which complements these appendices and should be studied as well.

A.5   Data Types

Let us get back to our example session. Suppose we now want to define a polynomial ideal. Using the manual, we find that the correct command is `Ideal()` and we can type

```
I:=Ideal(F,x-y);
J:=Ideal(x,y,z)^2;
Intersection(I,J);
```

CoCoA will not reply to the first two lines, since they are assignments. But it reacts to the last line by printing

```
Ideal(xz - yz, xy - y^2, y^2z^2 - 1/2z^2, y^3z - 1/2yz,
y^4 - 1/2y^2, x^2 - y^2)
-------------------------------
```

which means that the intersection of the ideals I and J has been computed. Sometimes it may be advisable to use the command `Set Indentation;` before typing out a list or an ideal. In our case, we'd get

```
Ideal(
  xz - yz,
  xy - y^2,
  y^2z^2 - 1/2z^2,
  y^3z - 1/2yz,
  y^4 - 1/2y^2,
  x^2 - y^2)
-------------------------------
```

Naturally, this behaviour can be reversed by entering `Unset Indentation;`

Many CoCoA objects like polynomials, ideals, and modules are defined over a base ring. The command `CurrentRing();` tells you the value of the current ring. E.g. in our example session we would get the answer `Q[x,y,z]`. A new ring can be defined by a command like

```
Use S::=Z/(5)[x,y,z];
```

Here `::=` is the instruction to create a new ring, `S` is its name, `Z/(5)` is its field of coefficients, and `x,y,z` are its indeterminates. After you have defined the new ring `S`, you are also making it the current base ring by invoking the command `Use <Ringname>;` You can switch back to your initial ring with the command `Use R;` and if you type `RingEnvs();` you get a list of all the base rings defined so far.

Whenever you create a new polynomial, ideal, or module, it is defined over the current ring. To see a list of all objects in the working memory, you can type `Memory();` and to see also the values of those objects you can use `Describe Memory();` At this point you may get a list of descriptions of objects of different types. Some of the most common data types in CoCoA are

INT, RAT	arbitrarily large integers resp. rational numbers
ZMOD	elements of a finite field $\mathbb{Z}/(p)$ where p is a prime number
POLY	polynomials
IDEAL	polynomial ideals
RING	polynomial rings
VECTOR	vectors whose entries are polynomials
MODULE	submodules of finite free modules over polynomial rings
LIST	Lists of objects of the form [Object1, Object2, Object3]
MAT	matrices of polynomials
STRING	strings (sequences of characters)
BOOL	Boolean variables (i.e. their value is either TRUE or FALSE)

In CoCoA, you usually do not have to specify the data types of the objects you create. Most sensible data type conversions are done automatically. The command `Type(Object)` displays the data type of an `Object`. If necessary, you can also force type conversions using `Cast()` e.g.

```
L:=[x,y,z];
Type(L);
```

shows that `L` is of type `LIST`, whereas

```
Cast(L,IDEAL);
```

leads to the answer

```
Ideal(x, y, z)
-------------------------------
```

For special type conversions, there are frequently individual commands, e.g. the above conversion could have been done by typing `I:=Ideal(L);` Then the ideal `I` can be converted back to a list by using `Gens(I);` which brings us to our next topic: What is a list?

A.6   Lists

In CoCoA, a list is a sequence of objects, separated by commas and enclosed in square brackets. Lists are very common and useful objects in CoCoA. Examples of lists are for instance `[1,2,3]` and `[x,y,z]`. The different components of a list do not necessarily have to have the same data type, e.g. as in the list `[1,TRUE,x]`. Given a list `L:=[x,y,z];` you can access its second component by typing

    L[2];

which yields the result `y`. Another way to achieve the same result is to type `Comp(L,2);` This is especially convenient if the list `L` is not directly given by its name but the result of some other evaluation, e.g. as in `Comp(Gens(I),1);` where `I` is an ideal.

Besides listing all the elements, there are other ways to create a list. Two simple ones are the range operator and the Cartesian product. The range operator `N..M` creates the list of all integers between `N` and `M`. For instance,

    1..5;

creates the list

    [1, 2, 3, 4, 5]

The range operator can also create a list of indeterminates of the current ring (in the current term ordering), e.g. if the current ring is `Q[x,y,z]`, then `x..z` creates the list `[x,y,z]`, and if the current ring is `Q[x[1..8]]`, then `x[1]..x[4]` creates the list `[x[1],x[2],x[3],x[4]]`. The Cartesian product of two lists is the list of all pairs, e.g. the product `[1,2,3] >< [x,y]` yields the list `[[1, x], [1, y], [2, x], [2, y], [3, x], [3, y]]`.

There are many built-in CoCoA function for dealing with lists. We invite you to print a list of them using `Man('Functions for Lists');` In our opinion, some of the most useful ones are

a) `Append(L,O)` to append an object `O` to a list `L`,
b) `Concat(L,M)` to combine two lists `L` and `M` into one,
c) `First(L,N)` and `Last(L,N)` to retrieve the list of the first and last `N` elements of a list `L`, respectively,
d) `Diff(L,M)` to create the list of all elements of the list `L` which are not in the list `M`, and
e) `Len(L)` to determine the number of elements of a list `L`.

If you want to build a new list by computing (or entering) its elements one by one, you can either apply commands such as `Append(L,x);` repeatedly, or you can first define a new "empty" list of a specified length `N` via `L:=NewList(N);` and then assign its entries using commands such as `L[1]:=x;`

Notice that, unlike other functions for lists, the command `Append(L,x)` does not return a value, but modifies the argument list `L`. CoCoA tries to be clever about operations with lists. For instance, if `L:=[x,y,z];` then `2L;` yields the list `[2x, 2y, 2z]`. But of course, it has to leave some thinking to you, and a construction like `[x,y,z]^3;` makes no unique sense.

Finally, we note that more advanced ways to construct lists will be discussed in Appendix B.5.

A.7   It

Finally, we would like to mention a special CoCoA variable called `It`. At each point in time it contains the last output. In particular, if you print the result of a computation and then discover that you still need it, you can assign it to a variable using `It`, e.g.

```
Factor(x^9-1);
[[x - 1, 1], [x^2 + x + 1, 1], [x^6 + x^3 + 1, 1]]
-------------------------------
L:=It;
L;
[[x - 1, 1], [x^2 + x + 1, 1], [x^6 + x^3 + 1, 1]]
-------------------------------
```

Of course, we encourage you to develop a habit of always assigning the result of a computation to a variable, e.g. using `L:=Factor(x^9-1);` and then to print it. As one CoCoA programmer put it:

<div align="center">Never use It!</div>

B. How to Program CoCoA

The code was willing.
It considered your request,
but the chips were weak.
(Anonymous)

B.1 Defining New CoCoA Functions

Apart from using CoCoA interactively as explained in Appendix A, the system also gives you the possibility to extend it by writing your own CoCoA functions. It has a fully-fledged programming language, called CoCoAL, and provides means for packaging, storing and reusing the functions you create.

A new CoCoA function is created using a command of the form

```
Define FunctionName(Arguments)
    <Commands>
EndDefine;
```

Here `FunctionName` is the name by which you later want to call your function, `Arguments` is the (possibly empty) list of arguments it takes, and `<Commands>` denotes a group of CoCoA commands.

Let us look at an example. We want to write a function which computes the ideal generated by the pth powers of the generators a given ideal, where the prime number p is the characteristic of the base field.

```
Define Frobenius(I)
    P:=Characteristic();
    L:=Gens(I);
    For N:=1 To Len(L) Do
        L[N]:=L[N]^P;
    EndFor;
    Return Ideal(L);
EndDefine;
```

Note that in order to enter this function definition on a version of CoCoA having a graphical interface, you should highlight all lines using the mouse

and then evaluate this selection. Afterwards we can use our new function like any built-in CoCoA function. For instance, we can type

```
Use S::=Z/(5)[x,y,z];
I:=Ideal(xy,yz,x-y);
Frobenius(I);
```

and we get the answer

```
Ideal(x^5y^5, y^5z^5, x^5-y^5)
-------------------------------
```

After the execution of this function, your original ideal `I` is unchanged, although it has been tampered with inside the function! The reason for this is that the ideal `I` inside the function `Frobenius(I)` is just a "local" object to which CoCoA passed the value of your original ideal `I`. Instead, if you want the function to operate directly on the original ideal, you should type `Define Frobenius(Var I)` in the first line of the function definition.

B.2   Program Development

As soon as you start to write CoCoA functions more frequently, you will feel the need to develop some techniques for doing this. Since the available methods vary considerably from one operating system to another, and since almost every CoCoA programmer has his own favourite procedures, we shall restrict ourselves to pointing out the most common ways.

Many CoCoA users work with a text-based CoCoA interface inside a graphical operating system environment, e.g. inside X-Windows or Windows. In this case we recommend the "Copy and Paste" technique for creating CoCoA functions:

- Open two windows, one for CoCoA and one for a text editor. The editor should be able to save pure ASCII files.
- Create the CoCoA function inside the editor.
- Use "Copy" and "Paste" to transfer the definition to CoCoA, so that CoCoA can check it for syntax errors.
- Repeat the previous steps until the program is correct. Then you can save it using the editor in a file whose file name extension is customarily taken to be `.coc`.

Another possibility for Unix users is to run CoCoA in a shell of a suitable editor program like Emacs. (Some useful files for doing this are on the CoCoA website.) If you run a text-based version of CoCoA under a text-based operating system like DOS, you will have to revert to a more primitive technique:

• Create the function using a text editor and save it in a file, e.g. in `myfile.coc`.

• Modify the file `userinit.coc` to include a source command which reads your file at startup, i.e. include the line

```
<< 'myfile.coc';
```

• Now start CoCoA. It reads and checks your program. If there is still an error, you have to quit CoCoA and return to the editor.

A much more advanced way of using CoCoA is possible if you are able to use one of the CoCoA versions with a graphical user interface, e.g. the new graphical interface for X-Windows and Windows, or CoCoA on a Macintosh. In this case you can edit your function inside the lower window, select it and send it to CoCoA until it is correct. Probably you may not want to do this in the interactive window, but rather in a file window which you can create using `<File> + <New>`. When you are content with your function, you can then save it to a file. And don't forget to write some documentation for your functions, or else you will soon be unable to reuse them!

B.3   Input and Output

In Section B.1 we saw an example of how a CoCoA function can pass the result of its computations back to the system. The command

```
Return <Object>;
```

exits the function and returns the value of `<Object>` to the place from where the function was called.

Passing objects to a CoCoA function is obviously achieved through its argument or list of arguments. Notice that the name which you give to a function argument in the function definition does not have to agree with the name of the object on which you call the function. Moreover, the argument name in the function definition denotes a variable for which you do not have to specify a data type and which is local to the function, i.e. it may agree with the name of an object elsewhere and it will be deleted after the function has been executed. Finally, it is important to remember that objects outside the CoCoA function which are not passed to it through the list of arguments are not known inside the function. For instance, if we have

```
I:=Ideal(x^2,y^2);
Define IdealSquare(J)
   I:=J^2;
   Return I;
EndDefine;
```

then the ideal `I:=Ideal(x^2,y^2);` is not destroyed or changed during the execution of `IdealSquare(Ideal(z));` and we can call `IdealSquare(I);` without getting into trouble.

Another way of obtaining feedback from a CoCoA function, for instance during its execution, is to have it write output on the screen. This can be achieved by using the commands

```
Print <Object>,...,<Object>;
PrintLn <Object>,...,<Object>;
```

The first command is used to print a sequence of objects to the screen, and the second one does the same thing but adds a line break afterwards. For example, to print out the value of `F:=x^2+y^2-1`, we could write

```
Print 'The value of F is F = ',F;
The value of F is F = x^2 + y^2 - 1
-------------------------------
```

Finally, using CoCoA you can also write data to files and read them again. We have already mentioned the source command `<<` which allows you to read a file containing function definitions, e.g. `<< 'myfile.coc';` For reading and writing other data, you need to open an input or an output file and to write to such a "device". Since this is a very advanced use of CoCoA, we refer you to `Man('Print On');` for details about printing on a file.

B.4   Program Flow Control

Our next topic is to discuss methods for controlling the way in which a sequence of commands is executed within a CoCoA function. In order to repeat a certain sequence of commands a prescribed number of times, you can use a construction like

```
N:=10;
For I:=1 To N Do
    <Commands>
EndFor;
```

Here `I` is the name of an integer variable which is initially one, is increased by one each time the `<Commands>` have been executed, and is `N` (or an expression having an integer value) when the loop ends. For instance, the following function creates a random vector over the base field whose length is the number of indeterminates of the base ring.

```
Define RandomVector()
    N:=NumIndets();
    L:=NewList(N);
    For I:=1 To N Do
```

```
        L[I]:=Rand();
    EndFor;
    Return Vector(L);
EndDefine;
```

Another way to create a loop is provided by the command

```
ForEach M In L Do
    <Commands>
EndForEach;
```

where `M` is an object name which you can choose and `L` is a list. Here the `<Commands>` are executed for each element of the list (whose elements are examined in the obvious order), and during that execution the element is the value of the "read-only" object `M`. This loop construction is particularly useful if you do not know beforehand how many elements `L` is going to have, i.e. how often the `<Commands>` have to be performed. For example, the function

```
Define TermProduct(D)
    L:=Support(DensePoly(D));
    Result:=1;
    ForEach M In L Do
        Result:=Result*M;
    EndForEach;
    Return Result;
EndDefine;
```

computes the product of all terms of degree `D` in the current ring. Even more common is the situation that a loop has to be repeated until a certain logical condition is satisfied. This can be achieved by using

```
While <logical condition> Do
    <Commands>
EndWhile;
```

Here the `<logical condition>` is some expression which evaluates to a Boolean value. If this Boolean value is `TRUE`, then the `<Commands>` are executed, otherwise the loop ends. For instance, the following example computes the largest power of two dividing a given natural number.

```
Define MaxPower(N)
    I:=1;
    While Mod(N,2)=0 Do
        I:=I*2;
        N:=N/2;
    EndWhile;
    Return I;
EndDefine;
```

Finally, CoCoA also provides methods for executing one sequence of commands or another, depending on the value of some logical condition. The two most frequently used methods are

```
If <logical condition> Then <Commands> EndIf;
If <logical condition> Then <Cmds1> Else <Cmds2> EndIf;
```

In the first case, the `<Commands>` are executed only if `<logical condition>` evaluates to `TRUE`. Otherwise they are skipped and program execution continues after the `EndIf;` In the second case, the commands `<Cmds1>` are executed if the `<logical condition>` is `TRUE`, and the commands `<Cmds2>` are executed if it is `FALSE`. For instance, the function

```
Define MaxOdd(N)
    If Mod(N,2)=1 Then
        Return N;
    Else
        M:=MaxPower(N)
    EndIf;
    Return N/M;
EndDefine;
```

computes the largest odd divisor of a natural number `N`. Notice that the command `Return N;` leads to an immediate termination of this function if it is encountered.

Should these hints be not sufficient to solve your specific program flow control problem, or should you intend to get the "CoCoA bug", we invite you to study the CoCoA manual which contains several more possibilities and a host of examples.

B.5   List Constructions

The creators of CoCoA spent a lot of effort to make the system as user-friendly as possible. In particular, CoCoA allows you define lists of objects in ways which are very similar to the usual mathematical definition of sets in books or on the blackboard. This list construction can take a number of different forms, the most important of which are

```
[ <Object> | X In <List> ]
[ <Object> | X In <LIST> And <logical condition> ]
[X In <List> | <logical condition>]
```

In the first form, `<Object>` is a CoCoA expression which usually depends on the variable `X` and evaluates to a CoCoA object. Thus this form constructs the list of all such objects such that `X` is an element of the `<List>`. The second form does essentially the same thing, except that only those elements `X` of `<List>` are used to construct objects for which the `<logical condition>`

evaluates to `TRUE`. The third form creates the sublist of `<List>` consisting of all of its elements `X` for which the `<logical condition>` is `TRUE`.

Let us see some examples of list constructions. The first function returns a list of `N` random linear forms in the current ring, where `N` is a specified natural number.

```
Define RandomLinear(N)
   L:=[Randomized(DensePoly(1)) | I In 1..N];
   Return L;
EndDefine;
```

Notice that in this case `I` is not used in the definition of the created list elements, and observe the use of the range operator `1..N` which generates the list `[1,2,3,...,N]`. An example for the second form of list constructions is

```
Define EvenIntegers(N)
   L:=[I | I In 1..N And Mod(I,2)=0];
   Return L;
EndDefine;
```

a function which returns the list of even integers between 1 and `N`. Finally, the function

```
Define IrrePolys(L)
   Irre:=[F In L | Len(Factor(F))=1];
   Irre:=[F In Irre | Comp(Factor(F),1,2)=1];
   Return Irre
EndDefine;
```

computes the sublist of a given list of monic polynomials consisting of the irreducible ones.

Maybe you have also noticed that in this example program we have a command which does not end in a semicolon, apparently contradicting what we said in Appendix A. Without falling into the abyss of computer jargon, let us just say that you can drop the semicolon if it immediately precedes

<div align="center">the <code>End;</code></div>

of some command.

B.6   Recursive Programming

Next we show you the perfect way for creating CoCoA programs which run into an infinite loop. More seriously, CoCoA allows a function to call itself. Of course, if you use this feature you have to make sure that the process terminates eventually. For example, a compact implementation of the computation of the factorial of a natural number is

```
Define Factorial(N)
    If N=0 Then
        Return 1;
    Else
        Return N*Factorial(N-1);
    EndIf;
EndDefine;
```

In this example finiteness is achieved by checking whether N=0 before the recursive function call which applies to a smaller integer N-1. Clearly, recursive function calls are both powerful and dangerous. Let us give one more example. The following function recursively computes the nondecreasing list of prime factors of a natural number.

```
Define FactorList(N)
    If N=1 Then
        Return [];
    EndIf;
    I:=2;
    While Mod(N,I)<>0 Do
        I:=I+1;
    EndWhile;
    L:=FactorList(N/I);
    Return Concat([I],L);
EndDefine;
```

And now off to your own experiments!

B.7   Improving Your Programs

To end our whirlwind tour of CoCoA, let us show you some ways to improve and manage your CoCoA programs. The command

```
Set Timer;
```

turns on an automatic timing mechanism. Every time you enter a command, CoCoA displays the CPU time that was consumed for its execution, e.g.

```
Set Timer;
Factor(x^233-3x^223+x^222-7x^12+x^11+21x^2-10x+1);
[[x^11 - 3x + 1, 1], [x^222 - 7x + 1, 1]]
-------------------------------
Cpu time = 1.81, User time = 1
-------------------------------
```

You can use this feature to test various versions of your programs and optimize them for fastest performance. If you get sick of those timing messages,

you can turn them off again by typing (guess what?) `Unset Timer`; To time a single command, you can also use `Time <Command>`; For instance, above we could have written

```
Time L:=Factor(x^233-3x^223+x^222-7x^12+x^11+21x^2-10x+1);
```

After a while, you will have a number of CoCoA functions, and if you do not use them regularly, you will forget their exact names, syntax, etc. To find their names again after you loaded the file containing them, you can use the CoCoA command

```
Starting( <String> );
```

It displays a list of the names of all CoCoA functions starting with `<String>`, including you own creations. Do not forget to enclose the string in quotes, though! And if you have a hard time remembering the syntax of the functions you wrote, we suggest that you write a help function for each of them. If the function is called `MyFunction()`, you should create a new function like

```
Define Help_MyFunction()
   <Commands>
EndDefine;
```

Then this function is executed every time you type `Help('MyFunction')`; Of course, the `<Commands>` it contains will usually be commands to print some help text.

After another long while, you will have so many CoCoA functions that it becomes difficult to keep track of all their names, etc. If you come this far, you can get out of trouble by collecting your functions in packages. A CoCoA package is a file containing a lot of CoCoA functions. Usually it has a name ending with `.pkg`. Its content is of the shape

```
Package <Packagename>
   <Function Definitions>
EndPackage;
```

Later you can share your package with others, e.g. people in the CoCoA User Group or other students in your class sweating over the same homework. As this is again a very advanced way of using CoCoA, we suggest that you look at `Man('Package')`; for details.

In the next appendix you can see some examples in which the previous hints are applied. If you need more precise information, we suggest that you look carefully at the CoCoA manual mentioned in Appendix A. And if all else fails, you may write an e-mail to

```
cocoa@dima.unige.it
```

But for the time being, we wish you good luck and say

```
Ciao;
-- Bye
```

C. A Potpourri of CoCoA Programs

Bugs come in through open Windows.
(Anonymous)

C.1 Some Hints for Tutorial 1

In this appendix we shall frequently see that the same algorithm can be
turned into CoCoA functions in many ways. Part a) of Tutorial 1 is a case in
point. For a beginning programmer, the following solution should not be too
difficult to find.

```
Define ReprUniv(F,X)
    L:=NewList(Deg(F)+1);
    For I:=0 To Deg(F) Do
        L[I+1]:=CoeffOfTerm(X^I,F);
    EndFor;
    Return L;
EndDefine;
```

In the second line, we define a new list `L` of the appropriate length. Then a
`For`-loop is used to fill that list with the coefficients of the given polynomial.
The identifier `X` holds the name of the indeterminate with respect to which
the polynomial `F` is univariate. Notice how we had to change the indices, since
in CoCoA the elements of a list are numbered starting with "1".

An elegant solution is based on the CoCoA function `Coefficients(...)`.

```
Define ReprUniv(F,X)
    Return Reversed(Coefficients(F,X));
EndDefine;
```

As for the function `ListToPoly(...)`, we only give you the solution in-
volving the list construction, in order to make you feel more comfortable with
this style of programming. (We trust you can do the `For`-loop by now, can't
you?)

```
Define ListToPoly(L)
    Return Sum([L[I] x^(I-1) | I In 1..Len(L)]);
EndDefine;
```

For part c), we leave the implementation of `AddUniv(...)` to you. A very explicit and down-to-earth solution for the multiplication could look as follows.

```
Define MultUniv(L,M)
   D:=Len(L)+Len(M)-2;
   For I:=Len(L)+1 To D+1 Do
      Append(L,0);
   EndFor;
   For I:=Len(M)+1 To D+1 Do
      Append(M,0);
   EndFor;
   N:=NewList(D+1,0);
   For I:=0 To D Do
      N[I+1]:=Sum([L[J+1]*M[I+1-J] | J In 0..I]);
   EndFor;
   Return N;
EndDefine;
```

In the second line, we determine the degree `D` of the product. Then we append zeros to the lists `L` and `M` until both of them have length `D+1`. Finally, we construct another list `N` which will contain the final result. Its entries are computed using the formula for the coefficients of the product given in the hint. The list construction creates the list of all $a_j b_{i-j}$.

The following CoCoA program removes the trailing zeros of a list. It may be useful for solving part d) of the tutorial. Notice how we were able to exploit the `While`-loop.

```
Define Shorten(L)
   N:=Len(L);
   While L[N]=0 Do
      N:=N-1;
   EndWhile;
   Return First(L,N);
EndDefine;
```

There is also an elegant solution to part d) based on `Coefficients(...)` and the list construction. Although we do not expect you to be able to write such programs (yet!), it is well worth studying.

```
Define ReprPoly(F)
   Return [Reversed(Coefficients(G,x))|G In
          Reversed(Coefficients(F,y))];
EndDefine;
```

By now, you should begin to see the picture of how the other parts of the tutorial can be solved. For instance, for the function `AddPoly(...)` you should

again switch the summands such that the one with the higher y-degree comes first, and then add the second one onto the first one using `AddUniv(...)`. And by the time you are doing `MultPoly(...)`, you will find that the hardest part of programming is usually to get your mathematics right. We end these hints with a *master solution* of the `PolyToList` conversion in the general case.

```
Define PolyToList(F)
   Return RecPolyToList(F,1);
EndDefine;

Define RecPolyToList(F,N)
   If N=NumIndets() Then
      Return Reversed(Coefficients(F,Indet(N)));
   EndIf;
   Return [RecPolyToList(G,N+1)|G In
           Reversed(Coefficients(F,Indet(N)))];
EndDefine;
```

C.2   Different Styles of CoCoA Programming

> *Computers are not intelligent.*
> *They only think they are.*
> (Anonymous)

Let us show you some different programming styles using a very elementary example. We want to create an $n \times n$-matrix whose entries are random integers between 0 and 100. A quick look at the on-line manual, and you should be able to locate the function `Rand(0,100)` which generates such a random integer.

A very explicit first way to solve our task is to create a new matrix of the desired size and then to fill it using a double `For`-loop.

```
Define RandomMatrix(N)
   M:=NewMat(N,N);
   For I:=1 To N Do
      For J:=1 To N Do
         M[I,J]:=Rand(0,100);
      EndFor;
   EndFor;
   Return M;
EndDefine;
```

Another possibility which is sometimes preferred by beginners is to create the necessary lists by starting with an empty list and using the `Append(...)` command, for instance

```
Define RandomMatrix(N)
   M:=[];
   For I:=1 To N Do
      L:=[];
      For J:=1 To N Do
         Append(L,Rand(0,100));
      EndFor;
      Append(M,L);
   EndFor;
   Return Mat(M);
EndDefine;
```

Both of these double loops tend to be rather slow in practice. Try
`RandomMatrix(100)`! A more efficient way is to use the list constructions
advertised in Appendix B.6. In our example, we could write

```
Define RandomMatrix(N)
   M:=[[Rand(0,100) | I In 1..N] | J In 1..N];
   Return Mat(M);
EndDefine;
```

This would produce the same result. Even more compressed code can be
generated using the short form for defining one-line functions.

```
RandomMatrix(N):=Mat[[Rand(0,100)|I In 1..N]|J In 1..N];
```

But don't overdo it! We would consider this bad programming style. If you
squeeze too much into those list constructions, your program code becomes
difficult to read. And the one who has to suffer most because of this is usually
yourself, when you want to reuse your code (or parts of it) at a later stage.

C.3.   Hints for Other Tutorials in Chapter 1

When all else fails,
read the instructions.
(Anonymous)

In order to make the tutorials accessible to inexperienced CoCoA pro-
grammers, we now provide some additional hints for selected tutorials in
Chapter 1. We strongly urge you to first try those tutorials on your own. If
all else fails, you may look for some inspiration here. But keep in mind that
CoCoA programming is only 10% inspiration and 90% perspiration.

In Tutorial 2 you should not have severe problems to convert the given
steps into workable CoCoA programs. But for `PolyExtEuclid(...)`, let us
show you how to implement the crucial step 4). We suppose that the tuple
(c_0, d_0, e_0) is stored in `T0` and (c_1, d_1, e_1) in `T1`.

```
While T1[3] <> 0 Do
   Q:=DivAlg(T0[3],[T1[3]]);
   Q1:=Comp(Q.Quotients,1);
   T:=T0-Q1*T1; T0:=T1; T1:=T;
EndWhile;
```

The following program computes all monic univariate polynomials of a specified degree over a finite field.

```
Define MonicPoly(D)
   If D=0 Then
      Return [1];
   EndIf;
   If D=1 Then
      Return [x+N | N In 0..(Characteristic()-1)];
   EndIf;
   Pre:=MonicPoly(D-1);
   Return ConcatLists([[x*F+N | N In
      0..(Characteristic()-1)] | F In Pre]);
EndDefine;
```

You can use it in Tutorial 3 for writing the function `IrredPoly(...)`. Loop through all monic polynomials of some degree and check whether they are divisible by any irreducible polynomial of smaller degree. The remainder of the division of `F` by `G` can be found by calling `NR(F,[G])`.

Clearly, the function `GaussFactor(...)` in Tutorial 4 is a tough nut to crack. So, let us help you. Suppose a Gaußian number $z = a + ib \in \mathbb{Z}[i]$ is represented in CoCoA by the list $[a, b]$. Using the function `Sqrt(...)` from Appendix C.5, we can create a list of possible divisors of $z = a+ib$ as follows.

```
Define PossibleDivisors(Z)
   Norm:=Z[1]^2+Z[2]^2;
   N:=Sqrt(Norm,0);
   L:=Diff((-N..N) >< (-N..N), [[0,0]]);
   Return [X In L | Mod(Norm,X[1]^2+X[2]^2)=0];
EndDefine;
```

While nothing special needs to be said about Tutorial 5, the following function does part of the work in Tutorial 6. In fact, it provides a quick way to compute the matrix Q.

```
Define MatQ(F)
   P:=Characteristic();
   Q:=NewMat(Deg(F),Deg(F),0%P);
   Q[1,1]:=1%P;
   XP:=NR(x^P,[F]);
   XI:=1;
```

```
      For I:=1 To Deg(F)-1 Do
         XI:=NR(XI*XP,[F]);
         Q[I+1]:=[CoeffOfTerm(x^J,XI) | J In 0..(Deg(F)-1)];
      EndFor;
      Return Q;
   EndDefine;
```

Notice that the expression `1%P` gives you the residue class of `1` in the field $Z/(P)$, independent of what the current ring is.

Tutorials 7 and 8 are again easy, but since there are so many small functions you have to write in Tutorial 8, let us do two of them for you. (The very desperate among you can even use those programs to reverse-engineer a hint for the proof!)

```
   Define MonIntersection(I,J)
      L:=[LCM(G[1],G[2]) | G In Gens(I) >< Gens(J)];
      Return Ideal(Interreduced(L));
   EndDefine;

   Define MonColon(I,J)
      K:=Ideal(1);
      ForEach G In Gens(J) Do
         L:=[LCM(F,G)/G | F In Gens(I)];
         K:=MonIntersection(K,Ideal(L));
      EndForEach;
      Return K;
   EndDefine;
```

For Tutorials 9 and 10, it is important that you know about CoCoA's sorting facilities. For instance, suppose we have a list of pairs of integers, and we want to sort them into lexicographically increasing order. The first step consists of defining a Boolean-valued function of two arguments which returns TRUE if the first argument is smaller than the second one.

```
   Define MyLex(A,B)
      Return A[1]<B[1] Or (A[1]=B[1] And A[2]<=B[2]);
   EndDefine;
```

Now we can sort any list `L` of pairs of integers with respect to our comparison function `MyLex(A,B)` by typing

```
   NewL:=SortedBy(L,Function('MyLex'));
```

In view of the extensive help we offered for Tutorial 1, we hope that you can manage to do Tutorial 11 essentially on your own. In order to check the correctness of your results, you can also use the inverse transformation

```
   Define ListToPoly(L)
      Return Sum([X[1]*LogToTerm(X[2]) | X In L]);
   EndDefine;
```

If you somehow got stuck writing the function `ElSym(...)` in Tutorial 12, but you would like to try your luck with the last parts of the tutorial, you can use the following alternative solution. It is based on the formula

$$(y - x_1)(y - x_2) \cdots (y - x_n) = \sum_{i=0}^{n} (-1)^{n-i} s_{n-i}\, y^i$$

Furthermore, you can learn from this function how to use a different base ring inside a CoCoA function and how to move polynomials from one ring to another.

```
Define AltElSym(N,I)
   P:=Characteristic();
   If P=0 Then
      NewR::=Q[x[1..N],y];
   Else
      NewR::=Z/(P)[x[1..N],y];
   EndIf;
   Using NewR Do
      F:=Product([y-x[I] | I In 1..N]);
      S:=Coefficients(F,y);
      SI:=(-1)^I * S[I+1];
   EndUsing;
   Phi:=RMap(Concat(First(Indets(),N),[0]));
   Return Image(SI,Phi);
EndDefine;
```

In Tutorial 13 there is nothing to program, and in Tutorials 14 and 15 the stated algorithms should easily convert into CoCoA programs on a step-by-step basis. Nevertheless, let us offer you the following subprograms which may aid you in implementing step 2) of the Division Algorithm 1.6.4.

```
Define Reducer(M,G)
   For I:=1 To Len(G) Do
      If LPos(G[I])=LPos(M) And Type(LPP(M)/LPP(G[I]))=POLY
      Then
         Return I;
      EndIf;
   EndFor;
   Return 0;
EndDefine;

Define DivisionLT(M,G)
   Q:=NewList(Len(G),0);
   I:=Reducer(M,G);
   While I<>0 Do
      Q[I]:=Q[I]+LPP(M)/LPP(G[I]);
```

```
        M:=M-LPP(M)/LPP(G[I])*G[I];
        I:=Reducer(M,G);
    EndWhile;
    Return [Q,M];
  EndDefine;
```

Finally, in Tutorial 16 no programming is required. What a pity, we were just getting the knack of it!

C.4   Optimizing CoCoA Functions

How do you make Windows faster?
Throw it harder.
(Anonymous)

When you start to write more complicated CoCoA programs, you will soon discover cases where the execution of the program seems to be unduly slow. There is a simple rule-of-thumb which says that most computer programs spend more than 90% of the execution time in less then 10% of the program code. Hence, if you want to improve the performance of your CoCoA programs, you have to find the lines corresponding to those 10% of the code, and to optimize them carefully.

Let us explain this process using a very easy example. In Appendix B.6 we showed you the program `FactorList(N)` which uses recursive programming and computes the list of prime numbers dividing a given integer `N`. First we measure the time it needs to factorize a few numbers.

```
Time FactorList(123456789);
[3, 3, 3607, 3803]
Cpu time = 7.31, User time = 7
-------------------------------
Time FactorList(1111111);
[239, 4649]
Cpu time = 4.51, User time = 5
-------------------------------
```

These answers mean that, on a modest computer, it took 7.3 and 4.5 seconds to factor the two numbers. If we look at the source code of our program, it is clear that the most time consuming part is the `While`-loop. If we didn't know that, we could put a `Time` command in front of every suspicious line of the program. For the moment, let us just put a `Time` command in front of the `While`-loop. (We also added a `PrintLn;` command before `Return [];` in order to improve the appearance of the output.)

```
FactorList(123456789);
Cpu time = 0.00, User time = 0
Cpu time = 0.00, User time = 0
Cpu time = 3.35, User time = 3
Cpu time = 3.57, User time = 4
[3, 3, 3607, 3803]
-------------------------------
FactorList(1111111);
Cpu time = 0.22, User time = 0
Cpu time = 4.34, User time = 4
[239, 4649]
-------------------------------
```

The data confirm that almost all of the time is spent searching for the large prime divisors. For this task, several obvious improvements are at hand. For instance, we can start the search for a new divisor with the last one, and after we have reduced N to an odd number we can look for odd divisors only. The following function incorporates these optimizations.

```
Define FactorList2(N)
    If N=1 Then
        Return [];
    EndIf;
    If Mod(N,2)=0 Then
        Return Concat([2],FactorList2(N/2));
    EndIf;
    L:=[];
    I:=1;
    While I<=N Do
        I:=I+2;
        If Mod(N,I)=0 Then
            Append(L,I);
            N:=Div(N,I);
            I:=I-2;
        EndIf;
    EndWhile;
    Return L;
EndDefine;
```

The result is a noticeable speeding up of our factorizations.

```
Time FactorList2(123456789);
[3, 3, 3607, 3803]
Cpu time = 2.14, User time = 2
-------------------------------
```

```
Time FactorList2(1111111);
[239, 4649]
Cpu time = 2.59, User time = 2
-------------------------------
```

But more difficult examples still take too long.

```
Time FactorList2(111111111);
[3, 3, 37, 333667]
Cpu time = 184.50, User time = 185
-------------------------------
```

Sometimes alternative ways of implementing the same function can influence the execution time. For instance, in Appendix C.2 the versions of the program `RandomMatrix(N)` which are based on list constructions are significantly faster than the ones based on `For`-loops. But usually we can achieve the best program improvements by working on the underlying mathematics. Our third and final version of `FactorList(N)` is a case in point. It applies the function `Sqrt(XRat,N)` introduced in the next section to restrict the search for prime divisors of `N` to numbers less than or equal to the square root of `N`.

```
Define FactorList3(N)
   If N=1 Then
      Return [];
   EndIf;
   If Mod(N,2)=0 Then
      Return Concat([2],FactorList3(N/2));
   EndIf;
   L:=[];
   S:=Sqrt(N,0);
   I:=3;
   Repeat
      If Mod(N,I)=0 Then
         Append(L,I);
         N:=Div(N,I);
         S:=Sqrt(N,0);
         I:=I-2;
      EndIf;
      I:=I+2;
   Until I>S;
   Append(L,N);
   Return L;
EndDefine;
```

This time the factorization of the more difficult example above is found in a split second!

```
Time FactorList3(111111111);
[3, 3, 37, 333667]
Cpu time = 0.17, User time = 0
-------------------------------
```

C.5   How To Do Calculus Using CoCoA

Ask not what your country can do for you.
Ask what you can do for your country.
(John F. Kennedy)

Most computer algebra systems have been designed and developed by people who had certain applications or functionalities in mind. Thus each of them has its strengths and its weaknesses. As a user, you will sooner or later discover that your favourite computer algebra system was not designed to do precisely what you want it to do. Should you then switch to another one? Maybe. But frequently it is just as useful and instructive to teach your old dog a new trick.

For instance, CoCoA was clearly not designed for applications in calculus. In the current version, there are no floating point numbers available, and not a single transcendental function (sin, log, exp,...) is implemented. Nevertheless, in several situations above we needed an approximation for the square root of a rational number. Let us show you how you can extend the scope of CoCoA to include such a function. First we need the possibility to round a rational number to a given number of digits after the decimal point. (Our function always rounds the number downwards. We leave it to you to find the appropriate change in order to get the usual rule.)

```
Define Round(XRat,N)
    XR:=Cast(XRat*10^N,RAT);
    Return Div(XR.Num,XR.Den)/10^N;
EndDefine;
```

Next, we scour some calculus books and come up with an algorithm for computing square roots. It is based on the method used by the ancient Babylonians. Namely, given a real number $r > 0$, the sequence $x_0 = r$ and $x_i = \frac{1}{2}\left(x_{i-1} + \frac{r}{x_{i-1}}\right)$ for $i \geq 1$ converges to $\sqrt{r}$.

```
Define Babylon(XRat,N)
    Last:=XRat;
    New:=(XRat+1)/2;
    While Abs(New-Last)>(0.1)^(N+1) Do
        Last:=New;
        New:=(Last+XRat/Last)/2;
    EndWhile;
    Return Round(New,N);
EndDefine;
```

Unfortunately, this method converges too slowly if we start with a large number. Hence our final function first reduces the problem to a number $r/10^i < 1$ and then applies the Babylonian algorithm.

```
Define Sqrt(XRat,N)
   I:=0;
   While 10^I<Abs(XRat) Do
      I:=I+1;
   EndWhile;
   If Mod(I,2)=1 Then
      I:=I+1;
   EndIf;
   Return Babylon(XRat/10^I,N+I/2)*10^(I/2);
EndDefine;
```

It is clear that endless further possibilities exist for extending the functionality of CoCoA. So, do not ask what CoCoA can do for you, but what you can do for CoCoA!

D. Hints for Selected Exercises

D.1   Hints for Exercises in Chapter 1

Exercise 1.1.1. Show that $x^2 - d$ generates a maximal ideal in $\mathbb{Q}[x]$. Then prove that $K \cong \mathbb{Q}[x]/(x^2 - d)$.

Exercise 1.1.4. Let $\{v_1, ..., v_n\}$ be a $\mathbb{Z}$-basis of $\mathbb{Z}^n$. Show that the $\mathbb{Z}$-module homomorphism $\varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ is an isomorphism, where φ is defined by $\varphi(e_i) = v_i$ for $i = 1, \ldots, n$. Therefore there exists a matrix $\mathcal{B} \in \mathrm{Mat}_n(\mathbb{Z})$ such that $\mathcal{AB} = \mathcal{I}$.

Conversely, let $\boldsymbol{x} = (x_1, \ldots, x_n)^{\mathrm{tr}}$. Then $\det(\mathcal{A}) \in \{1, -1\}$ implies that $\mathcal{A}$ is invertible in $\mathrm{Mat}_n(\mathbb{Z})$, and that the system of linear equations $\mathcal{A} \cdot \boldsymbol{x} = v$ has the unique solution $\mathcal{A}^{-1} \cdot v$.

Exercise 1.1.6. Let $B = \{r_\lambda \mid \lambda \in \Lambda\}$ be an R-basis of the non-zero ideal I. If it contains two elements r_{λ_1}, r_{λ_2}, then $r_{\lambda_2} r_{\lambda_1} - r_{\lambda_1} r_{\lambda_2} = 0\, r_{\lambda_1} - 0\, r_{\lambda_2}$. If it contains one element r which is a zero-divisor, then there exists a non-zero element $s \in R$ such that $sr = 0r = 0$.

Conversely, if $I = (r)$ and r is a non-zero divisor, then the multiplication by r yields an isomorphism of R-modules between R and I.

Exercise 1.1.7. We give a hint on c) $\Leftrightarrow$ a). Every non-zero element r generates a principal ideal. Since this is a cyclic R-module, the element r is a non-zero divisor. Conversely, assume that there exists a non-zero non-invertible element r. Then the cyclic R-module $R/(r)$ is not free.

Exercise 1.2.3. To prove a), use the fact that the canonical images of monic polynomials have the same degree.

Exercise 1.2.5. By assumption, there exists an element $a \in \mathfrak{p} \setminus \{0\}$. Obviously, the element a is not a unit. Then at least one of its irreducible factors, say p, is in $\mathfrak{p}$. The factoriality of R implies that (p) is prime. Hence we have $(p) = \mathfrak{p}$.

Exercise 1.2.7. We extend the hint on the proof of c) given at the end of the exercise. We see that $f_1 = 2 + 2\sqrt{-5} = 2(1 + \sqrt{-5})$ and that $f_2 = 6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$. Let $g = \gcd(f_1, f_2)$. Then there exist $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $g = 2(a_1 + b_1\sqrt{-5}) = (1 + \sqrt{-5})(a_2 + b_2\sqrt{-5})$. Define $\varphi(a + b\sqrt{-5}) = a^2 + 5b^2$. Show that φ is compatible with the product and evaluate $\varphi(g)$. In this way, you get $2(a_1^2 + 5b_1^2) = 3(a_2^2 + 5b_2^2)$ in $\mathbb{N}$. Hence $6 \mid \varphi(g)$. On the other hand, we have $\varphi(g) \mid \varphi(2 - 2\sqrt{-5})$ and $\varphi(g) \mid \varphi(6)$, so that $\varphi(g) \mid 12$. Now we combine

$g = (1+\sqrt{-5})(a_2+b_2\sqrt{-5})$ and $6 \mid \varphi(g) \mid 12$ and get $g = 1+\sqrt{-5}$. Together with $g = 2(a_1 + b_1\sqrt{-5})$, this yields a contradiction.

Exercise 1.2.9. To prove a), use Exercise 1.2.8. We give a hint on how to prove that $x_1 + (f)$ is irreducible in $P/(f)$. Suppose that there exist $g, h \in P$ such that $x_1+(f) = (g+(f))(h+(f))$. Then there exists a polynomial r such that $x_1 = gh+rf$ holds in P. Now use considerations about the degrees of the polynomials involved in this equation.

Exercise 1.2.11. We give a hint on c). To prove 1) $\Rightarrow$ 2), you may assume that $f = x(x - a)(x - b)$ and then use a). For the converse implication, you may use $f = x(x-1)(x+1)$ to show that 3 is a square, and then use b) to get the conclusion.

Exercise 1.3.3. To prove d), look at the cardinality of the sets under consideration.

Exercise 1.3.5. Imitate the proof of Proposition 1.3.11.b.

Exercise 1.3.6. Let $\{\delta_1, ..., \delta_s\}$ be a finite system of generators of Δ, and let $B = \{b_i \mid i \in I\}$ be a system of generators of Δ. Then, for every $k \in \{1, ..., s\}$, there exist $\gamma_k \in \Gamma$ and $b_{i_k} \in B$ such that $\delta_k = \gamma_k \circ b_{i_k}$. Therefore $\{b_{i_1}, ..., b_{i_s}\}$ generates Δ.

Exercise 1.3.8. Use Dickson's Lemma 1.3.6.

Exercise 1.3.9. Use the fact that $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle = \cup_{i=1}^r \mathbb{T}^n e_i$.

Exercise 1.4.5. Use the observation made after Proposition 1.4.14 that

$$t_1 \geq_{\mathtt{Ord}(V)} t_2 \iff V \cdot (\log(t_1) - \log(t_2)) \geq_{\mathtt{Lex}} 0$$

Exercise 1.4.6. We have $\mathtt{DegLex} = \mathtt{Ord}(V)$, where

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Exercise 1.5.3. Observe that $\mathrm{LT}_\sigma(x_2 f_2 - x_1 f_3) = x_1 x_3 \notin (x_1^4 x_2, x_1^3 x_2^3, x_1^2 x_2^4)$.

Exercise 1.5.4. Let $\sigma = \mathtt{Lex}$, let $a, b \in K[x_1, x_2, x_3]$, let $f_1 = a(x_1 - x_3^3)$, let $f_2 = b(x_2 - x_3^4)$, and let $f = f_1 + f_2$. First, examine the cases where a or b are zero. Then assume that both are non-zero polynomials, and examine the case where $\mathrm{LM}_\sigma(ax_1)+\mathrm{LM}_\sigma(bx_2) \neq 0$. Finally, assume that $\mathrm{LM}_\sigma(ax_1)+\mathrm{LM}_\sigma(bx_2) = 0$. Show that in every case $\mathrm{LT}_\sigma(f)$ is a multiple of x_1 or x_2.

Exercise 1.6.3. The process of replacing a power product in x_1 with smaller power products in x_1, and the process of replacing a power product in x_2 with smaller power products in x_2 are independent.

Exercise 1.7.8. To prove a), use the fact that, for $r, r' \in R_\gamma \setminus \{0\}$, we have $r' = (r^{-1}r')r$. To prove d), use Corollary 1.7.11.

D.2   Hints for Exercises in Chapter 2

Exercise 2.1.2. To prove $a) \Rightarrow b)$, argue by contradiction. Assume that $x_{i_1} = x_{i_2}$ and consider the polynomial $\frac{1}{\mathrm{LC}_\sigma(g_1)} g_1 - \frac{1}{\mathrm{LC}_\sigma(g_2)} g_2$. To prove $b) \Rightarrow a)$, we suggest an anticipation of a method which will be used later in Section 2.3. For a pair $(a_1, a_2) \in P^2 \setminus \{(0,0)\}$, we define $\deg(a_1, 0) = \mathrm{LT}_\sigma(a_1)$, $\deg(0, a_2) = \mathrm{LT}_\sigma(a_2)$, and $\deg(a_1, a_2) = \max\{\mathrm{LT}_\sigma(a_1), \mathrm{LT}_\sigma(a_2)\}$ if both a_1 and a_2 are non-zero. Given $g = a_1 g_1 + a_2 g_2$, we say that g has a representation via (a_1, a_2), and that $\deg(a_1, a_2)$ is the degree of the representation. Show that every element in the ideal (g_1, g_2) has a representation of minimal degree. Then prove that such a representation satisfies Condition A_2).

Exercise 2.1.3. Use $K[x, y]$, $g_1 = x + 1$, and $g_2 = y + 1$.

Exercise 2.1.4. Use $g_3 = (x_1 + 1)g_1 - x_2 g_2 = x_2^2 - x_2$.

Exercise 2.1.5. Use the suggestion given for Exercise 2.1.2 above, and the fact that x^3 and y^3 are coprime.

Exercise 2.2.4. To prove $a) \Rightarrow b)$, show that there exists a term ordering τ such that $t_1 >_\tau t_2$.

Exercise 2.3.7. To show a), use Theorem 2.3.7.b.

Exercise 2.4.8. Use Proposition 1.3.11.

Exercise 2.5.5. Show that every reduction step transforms a binomial into a binomial.

Exercise 2.6.1. Suppose there exists $i \in \{1, \ldots, n\}$ such that $\mathfrak{m} \cap K[x_i] = (0)$. Then show that there exists a K-algebra homomorphism $K[x_i] \hookrightarrow P/\mathfrak{m}$ which is injective.

D.3   Hints for Exercises in Chapter 3

Exercise 3.1.1. Use the fact that P is a factorial domain.

Exercise 3.1.3. We have $\Sigma = \{\sigma_{12}, \sigma_{13}, \sigma_{23}\}$, where $\sigma_{12} = x\varepsilon_1 - y\varepsilon_2$, where $\sigma_{13} = x\varepsilon_1 - z\varepsilon_3$, and where $\sigma_{23} = y\varepsilon_2 - z\varepsilon_3 = \sigma_{13} - \sigma_{12}$. Then consider the set $\mathbb{B}' = \{(1,2), (1,3)\}$.

Exercise 3.2.9. To prove $b) \Rightarrow a)$, use the fact that $ab(c, d) = bc(a, b)$.

Exercise 3.3.4. To show a), use the fact that $fx + gy = (f - y)x + (g + x)y$.

Exercise 3.4.6. Show that $\{g_1, \ldots, g_n\}$ is a Gröbner basis with respect to a suitable module term ordering.

Exercise 3.4.7. Prove that $B \cong \widehat{P}/(I \cap \widehat{P})$.

Exercise 3.4.11. Use Proposition 3.4.6.

Exercise 3.5.2. Consider the ideal $\mathfrak{p}R_S$.

Exercise 3.5.4. Prove that there is an isomorphism between P_S and P_f.

Exercise 3.5.7. To find an example with the required property, you may consider the polynomial ring $K[x]$ and the following exact sequence of P-modules.

$$0 \longrightarrow P \xrightarrow{\ x\ } P \longrightarrow P/(x)P \longrightarrow 0$$

Exercise 3.5.9. If you do not find a proof, use CoCoA to show that $d_1^2, d_2^2 \in J$ in the case $K = \mathbb{Q}$. Then verify that the representations of d_1^2 and d_2^2 obtained with CoCoA are valid for every field K.

Exercise 3.6.4. Consider the K-algebra homomorphism $\varphi : K[x_1, \ldots, x_s] \longrightarrow R$ which is defined by $\varphi(x_i) = f_i + I$ for $i = 1, \ldots, s$.

Exercise 3.6.9. Prove that the Jacobian determinant of the composition of two K-algebra homomorphisms from P to P is the product of the two Jacobian determinants.

Exercise 3.7.1. One important step in the proof is to show that if K is not a perfect field, then there exists a squarefree polynomial f such that $\gcd(f, f') = 1$. Let $a \in K$ be such that it has no p^{th} root in K. Then show that $f = x^p - a$ is irreducible. To do this, you may consider f as an element of $\overline{K}[x]$.

Ich habe fertig.
(Giovanni Trapattoni)

Notation

1. Special Sets

$\mathbb{N}$	set of natural numbers, $\mathbb{N} = \{0, 1, 2, \ldots\}$
$\mathbb{Z}$	set of integers
$\mathbb{Q}$	set of rational numbers
$\mathbb{Q}_{>0}$	set of positive rational numbers
$\overline{\mathbb{Q}}$	set of algebraic numbers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{F}_q$	finite field with q elements
$\mathbb{Z}[i]$	ring of Gaußian numbers
$\mathbb{I}$	set of irrational numbers, $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$
$\mathfrak{S}_n$	symmetric group on n elements
$\mathbb{A}_K^n$	n-dimensional affine space over a field K
$\mathbb{B}$	set of pairs $\mathbb{B} = \{(i, j) \mid 1 \le i < j \le s,\ \gamma_i = \gamma_j\}$
$\mathbb{T}^n$ or $\mathbb{T}(x_1, \ldots, x_n)$	set of terms in the indeterminates $x_1, \ldots, x_n$
$\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$	set of terms in $K[x_1, \ldots, x_n]^r$, i.e. the set of all te_i such that $t \in \mathbb{T}^n$ and $1 \le i \le r$
$\mathbb{S}(\mathcal{C})$	set of all $\mathcal{C}$-splines
$\mathbb{P}(V)$	projective space associated to a vector space V
$\mathbb{P}_K^n$	projective space associated to K^{n+1}
$\mathbb{E}^n$	set of extended terms $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$

2. Sets and Maps

$A \subseteq B$	set A is a (not necessarily proper) subset of set B
$A \subset B$	set A is a proper subset of set B
$A \setminus B$	set difference of A and B, i.e. the set of all elements of A which are not contained in B
$\#A$	number of elements of a finite set A
$\psi \circ \varphi$	composition of two maps $\varphi : A \longrightarrow B$ and $\psi : B \longrightarrow C$
$\mathrm{Im}(\varphi)$	image of a map $\varphi : A \longrightarrow B$
$\mathrm{Ker}(\varphi)$	kernel of a homomorphism $\varphi : A \longrightarrow B$

$\operatorname{Coker}(\varphi)$ cokernel of a homomorphism $\varphi : A \longrightarrow B$, i.e. $\operatorname{Coker}(\varphi) = B/\operatorname{Im}(\varphi)$

id_A identity map on a set A

$A \longrightarrow\!\!\!\!\!\rightarrow B$ a surjective map $A \longrightarrow B$

$A \lhook\joinrel\longrightarrow B$ an injective map $A \longrightarrow B$

$\varphi^{\smallsmile}$ dual of a linear map

$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ exact sequence of homomorphisms, i.e. a sequence such that φ is injective, ψ is surjective, and $\operatorname{Im}(\varphi) = \operatorname{Ker}(\psi)$

$\operatorname{LM} : P^r \longrightarrow P^r$ map defined by $\operatorname{LM}(m) = \operatorname{LM}_\sigma(m)$ for $m \neq 0$ and $\operatorname{LM}(0) = 0$

$\operatorname{LF} : P^s \longrightarrow P^s$ map defined by $\operatorname{LF}(m) = \operatorname{LF}_{\sigma,\mathcal{G}}(m)$ for $m \neq 0$ and $\operatorname{LF}(0) = 0$

$\mathcal{Z}_L(f)$ set of zeros of a polynomial

$\mathcal{Z}_L(I)$ set of zeros of an ideal

$\overline{p_1 p_2}$ line through two points p_1 and p_2

$(p_0 : \ldots : p_n)$ point in an n-dimensional projective space

$\operatorname{Hyp}(\mathbb{P}_K^n)$ set of hyperplanes in $\mathbb{P}_K^n$

$\operatorname{Lin}(\mathbb{P}_K^n)$ set of lines in $\mathbb{P}_K^n$

$(\mathbb{P}_K^n)^{\smallsmile}$ dual projective space

$\operatorname{Grass}_m(\mathbb{P}_K^n)$ Graßmannian of m-dimensional subspaces of $\mathbb{P}_K^n$

3. Orderings

$\geq_\sigma$ monoid ordering or module ordering

`Lex`   lexicographic term ordering

`DegLex`   degree-lexicographic term ordering

`DegRevLex`   degree-reverse-lexicographic term ordering

`RevLex`   reverse-lexicographic ordering

`Elim`(L) elimination ordering for L

`Ord`(V) ordering associated to the matrix V

4. Polynomials and Vectors

$\deg(f)$ degree of a polynomial

$\operatorname{Supp}(v)$ support of a vector of polynomials

$\gcd(f_1, \ldots, f_m)$ greatest common divisor of $f_1, \ldots, f_m$

$\operatorname{lcm}(f_1, \ldots, f_m)$ least common multiple of $f_1, \ldots, f_m$

$\operatorname{sqfree}(f)$ squarefree part of f

$\operatorname{cont}(f)$ content of a univariate polynomial f

f' derivative of a univariate polynomial f

$\operatorname{Newton}(f)$ Newton polytope of a polynomial

$[v_1 v_2]$ line segment from v_1 to v_2

$\mathrm{LT}_\sigma(v)$	leading term of a vector of polynomials
$\mathrm{LC}_\sigma(v)$	leading coefficient of a vector of polynomials
$\mathrm{LM}_\sigma(v)$	equals $\mathrm{LC}_\sigma(v) \cdot \mathrm{LT}_\sigma(v)$
$\mathrm{NR}_{\sigma,\mathcal{G}}(v)$	normal remainder of a vector
$\mathrm{LM}_\sigma(\mathcal{G})$	defined by $\mathrm{LM}_\sigma(\mathcal{G}) = (\mathrm{LM}_\sigma(g_1),\ldots,\mathrm{LM}_\sigma(g_s))$ for a tuple $\mathcal{G} = (g_1,\ldots,g_s)$
$\deg_{\sigma,\mathcal{G}}(v)$	σ-degree of a vector
$\mathrm{LF}_{\sigma,\mathcal{G}}(v)$	σ-leading form of a vector
t_{ij}	defined by $t_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{t_i}$ for terms t_i, t_j
σ_{ij}	fundamental syzygy, $\sigma_{ij} = \mathrm{LC}_\sigma(g_i)^{-1}t_{ij}\varepsilon_i - \mathrm{LC}_\sigma(g_j)^{-1}t_{ji}\varepsilon_j$
S_{ij}	S-vector of g_i and g_j, defined by $S_{ij} = \mathrm{LC}_\sigma(g_i)^{-1}t_{ij}g_i - \mathrm{LC}_\sigma(g_j)^{-1}t_{ji}g_j$
$\mathrm{NF}_{\sigma,M}(v)$	normal form of a vector w.r.t. a submodule
$\det(\frac{\partial f_i}{\partial x_j})$	Jacobian determinant of a system of polynomials

5. Rings and Fields

$\mathrm{char}(K)$	characteristic of the field K
$Q(R)$	field of fractions of an integral domain R
$K[x_1,\ldots,x_n]$	polynomial ring in the indeterminates $x_1,\ldots,x_n$ over K
$K(x_1,\ldots,x_n)$	field of rational functions in the indeterminates $x_1,\ldots,x_n$ over K
$K[[x]]$	power series ring in one indeterminate
$K[x_1,\ldots,x_n,x_1^{-1},\ldots,x_n^{-1}]$	Laurent polynomial ring
$K[x_1,\ldots,x_n]^G$	ring of invariants of G
$\prod_{i=1}^n R_i$	direct product of the rings $R_1,\ldots,R_n$

6. Ideals and Modules

$\mathrm{rk}(M)$	rank of a free module
$\{e_1,\ldots,e_r\}$	canonical basis of a finitely generated free module
$M_1 \oplus M_2$	direct sum of two groups or modules
$I \cdot M$	submodule of M generated by products fm, where $f \in I$ and $m \in M$
$v + M$	residue class of a vector v modulo M
$\langle m_\lambda \mid \lambda \in \Lambda \rangle$	module generated by the set $\{m_\lambda \mid \lambda \in \Lambda\}$
$(f_\lambda \mid \lambda \in \Lambda)$	ideal (or monoideal) generated by the set $\{f_\lambda \mid \lambda \in \Lambda\}$
$\mathrm{LT}_\sigma(M)$	leading term module of M
$\mathrm{LT}_\sigma\{M\}$	monomodule of terms in M
$\mathrm{Syz}_R(\mathcal{G})$	syzygy module of a tuple $\mathcal{G}$
$\sqrt{I}$	radical of an ideal
$\mathcal{I}(S)$	vanishing ideal of a set of points
$\mathrm{Ann}_R(M)$	annihilator of a module

$N :_R M$ colon ideal of N by M
$N :_M I$ colon module of N by I in M
$\mathrm{Hom}_R(M, N)$ Hom-module of linear maps $\varphi : M \longrightarrow N$
$\mathrm{Ext}_R^i(R/I, M)$ i^{th} Ext-module of R/I with values in M
M_S localization of a module M at a multiplicatively closed set S
M_f localization of a module at an element f
$N :_M I^\infty$ saturation of a module N by an ideal I in M
$I_{\mathcal{L}}$ lattice ideal associated to $\mathcal{L}$

7. Matrices

$\mathrm{Mat}_n(R)$ set of $n \times n$-matrices over R
$\mathrm{Mat}_{m,n}(R)$ set of $m \times n$-matrices over R
$\mathrm{GL}_n(R)$ set of invertible $n \times n$-matrices over R
$\mathcal{A}^{\mathrm{tr}}$ transposed matrix of $\mathcal{A}$
$\mathcal{I}_s$ identity matrix of size $s \times s$
$\mathcal{A}_\varphi$ matrix associated to a linear map φ
$\Lambda_{r,s}$ homomorphism mapping a linear map to its associated matrix
$\mathrm{Fl}_{s,r}$ flattening isomorphism
$\Phi_{r,s}$ isomorphism defined by $\Phi_{r,s} = \mathrm{Fl}_{s,r} \circ \Lambda_{r,s}$
$\mathcal{A} \otimes \mathcal{B}$ tensor product of $\mathcal{A}$ and $\mathcal{B}$

8. Mathematical Operators

$\dim_K(V)$ dimension of a K-vector space V
$\log(t)$ logarithm of a term, $\log(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = (\alpha_1, \ldots, \alpha_n)$
$\mathrm{conv}(S)$ convex hull of a set
$\mathrm{Vert}(P)$ set of vertices of a polytope
$\max_\sigma(A)$ maximum of the set A w.r.t. the relation σ
$\inf(A)$ infimum of a set A of real numbers
$\sup(A)$ supremum of a set A of real numbers
$\xrightarrow{g}$ reduction step using an element g
$\xrightarrow{G}$ rewrite relation defined by a set of vectors
$\xleftrightarrow{G}$ equivalence relation defined by $\xrightarrow{G}$
$\mathrm{Top}_{K,L}$ relative Zariski topology
$\mathrm{depth}_I(M)$ I-depth of a module
$\mathrm{IP}(\mathcal{A}, b, \mathcal{C})$ integer programming problem
ϱ_G Reynolds operator of G
$\ell(f)$ number of terms in the support of a polynomial f
$E(X)$ expected value of a random variable X
$\mathrm{Var}(X)$ variance of a random variable X
$\sigma(X)$ standard deviation of a random variable X
$\mathrm{Cov}(X, Y)$ covariance of two random variables X, Y
$\varrho(X, Y)$ correlation coefficient of two random variables X, Y

Bibliography

[AL94]   W. Adams and P. Loustaunau, An introduction to Gröbner bases, Graduate Studies in Math. **3**, Amer. Math. Soc., Providence 1994

[BW93]   T. Becker and V. Weispfenning, Gröbner bases, Springer, New York 1993

[Bu65]   B. Buchberger, On finding a vector space basis of the residue class ring modulo a zero dimensional polynomial ideal (in German), PhD Thesis, Universität Innsbruck, Innsbruck 1965

[BW98]   B. Buchberger and F. Winkler, Gröbner bases and applications, London Math. Soc. Lect. Note Ser. **251**, Cambridge University Press, Cambridge 1998

[CLS92] D. Cox, J. Little, and D. O'Shea, Ideals, varieties, and algorithms, Springer, New York 1992

[Ei95]   D. Eisenbud, Commutative algebra with a view toward algebraic geometry, Springer, New York 1995

[Fr97]   R. Fröberg, An introduction to Gröbner bases, John Wiley & Sons, Chichester 1997

[Ku80]   E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhäuser, Boston 1985

[La70]   S. Lang, Algebra, Addison-Wesley, Reading 1970

[Mi93]   B. Mishra, Algorithmic algebra, Springer, New York 1993

[Va98]   W. Vasconcelos, Computational methods in commutative algebra and algebraic geometry, Algorithms and Computation in Math. **2**, Springer, Berlin 1998

[Wi96]   F. Winkler, Polynomial algorithms in computer algebra, Springer, Wien 1996

Index

affine
– algebra, 134
– set, 144
– space, 144
– variety, 138, 144
algebra, 18
– affine, 134
– automorphism, 231
– finitely generated, 23
– fundamental theorem of, 137
– presentation, 23
algebraic closure of a field, 137
algebraic element, 227
algebraic relation, 23, 227
algebraically closed field, 137
algorithm
– Berlekamp, 38
– Buchberger, 123
– division, 71
– Euclidean, 26
– extended Buchberger, 125
– extended Euclidean, 27
– for solving systems effectively, 257
– normal remainder, 75
alternating group, 237
annihilator, 166
– computation, 167
– of a cyclic module, 167
– of a module, 166
antisymmetry, 50, 54
associated
– elements, 31
– matrix, 182
– prime, 175
– projective space, 204
– toric ideal, 222
automorphism
– of a polynomial ring, 232
– of an algebra, 231

basis
– canonical, 20
– of a module, 19
Berlekamp algorithm, 38
binomial, 127
– ideal, 127
Buchberger triple, 131
Buchberger's algorithm, 123
– extended version, 125
– optimization, 124, 131
Buchberger's criterion, 122, 128

CoCoA, 11
– introduction, 275
– programming, 283
cancellation law, 42
– left, 42
– right, 42
canonical basis, 20
Cauchy-Schwarz inequality, 269
characterization
– of Gröbner bases, 111, 122
– of homogeneous prime ideals, 80
– of Noetherian modules, 112
– of Noetherian monoids, 42
– of DegRevLex, 65
– of Lex, 63
– of RevLex, 64
Chinese remainder theorem, 39, 245
coefficient, 22
– leading, 60
cogenerator, 47
colon ideal, 48, 166
– computation, 167, 175, 204
colon module, 169
– computation, 170, 175
– using elimination, 199
comaximal ideals, 245
commutative monoid, 17
complete relation, 50
complex of linear maps, 194