Texts & Monographs in Symbolic Computation

Bernd Sturmfels

Algorithms in Invariant Theory

2nd Edition

SpringerWienNewYork

SpringerWienNewYork

Texts and Monographs in
Symbolic Computation

A Series of the
Research Institute for Symbolic Computation,
Johannes Kepler University, Linz, Austria

Edited by P. Paule

Bernd Sturmfels

Algorithms in Invariant Theory

Second edition

SpringerWienNewYork

Dr. Bernd Sturmfels
Department of Mathematics
University of California, Berkeley, California, U.S.A.

Printed in Germany
SpringerWienNewYork is a part of Springer Science + Business Media
springer.at

Typesetting by HD Ecker: TeXtservices, Bonn
Printed by Strauss GmbH, Mörlenbach, Deutschland
Printed on acid-free paper
SPIN 12185696

With 5 Figures

Library of Congress Control Number 2007941496

ISSN 0943-853X
ISBN 978-3-211-77416-8 SpringerWienNewYork
ISBN 3-211-82445-6 1st edn. SpringerWienNewYork

Preface

The aim of this monograph is to provide an introduction to some fundamental problems, results and algorithms of invariant theory. The focus will be on the three following aspects:

(i) *Algebraic algorithms* in invariant theory, in particular algorithms arising from the theory of Gröbner bases;
(ii) *Combinatorial algorithms* in invariant theory, such as the straightening algorithm, which relate to representation theory of the general linear group;
(iii) *Applications* to projective geometry.

Part of this material was covered in a graduate course which I taught at RISC-Linz in the spring of 1989 and at Cornell University in the fall of 1989. The specific selection of topics has been determined by my personal taste and my belief that many interesting connections between invariant theory and symbolic computation are yet to be explored.

In order to get started with her/his own explorations, the reader will find exercises at the end of each section. The exercises vary in difficulty. Some of them are easy and straightforward, while others are more difficult, and might in fact lead to research projects. Exercises which I consider "more difficult" are marked with a star.

This book is intended for a diverse audience: graduate students who wish to learn the subject from scratch, researchers in the various fields of application who want to concentrate on certain aspects of the theory, specialists who need a reference on the algorithmic side of their field, and all others between these extremes. The overwhelming majority of the results in this book are well known, with many theorems dating back to the 19th century. Some of the algorithms, however, are new and not published elsewhere.

I am grateful to B. Buchberger, D. Eisenbud, L. Grove, D. Kapur, Y. Lakshman, A. Logar, B. Mourrain, V. Reiner, S. Sundaram, R. Stanley, A. Zelevinsky, G. Ziegler and numerous others who supplied comments on various versions of the manuscript. Special thanks go to N. White for introducing me to the beautiful subject of invariant theory, and for collaborating with me on the topics in Chapters 2 and 3. I am grateful to the following institutions for their support: the Austrian Science Foundation (FWF), the U.S. Army Research Office (through MSI Cornell), the National Science Foundation, the Alfred P. Sloan Foundation, and the Mittag-Leffler Institute (Stockholm).

Ithaca, June 1993 Bernd Sturmfels

Preface to the second edition

Computational Invariant Theory has seen a lot of progress since this book was first published 14 years ago. Many new theorems have been proved, many new algorithms have been developed, and many new applications have been explored. Among the numerous interesting research developments, particularly noteworthy from our perspective are the methods developed by Gregor Kemper for finite groups and by Harm Derksen on reductive groups. The relevant references include

Harm Derksen, Computation of reductive group invariants, Advances in Mathematics 141, 366–384, 1999;
Gregor Kemper, Computing invariants of reductive groups in positive characteristic, Transformation Groups 8, 159–176, 2003.

These two authors also co-authored the following excellent book which centers around the questions raised in my chapters 2 and 4, but which goes much further and deeper than what I had done:

Harm Derksen and Gregor Kemper, Computational invariant theory (Encyclopaedia of mathematical sciences, vol. 130), Springer, Berlin, 2002.

In a sense, the present new edition of "Algorithms in Invariant Theory" may now serve the role of a first introductory text which can be read prior to the book by Derksen and Kemper. In addition, I wish to recommend three other terrific books on invariant theory which deal with computational aspects and applications outside of pure mathematics:

Karin Gatermann, Computer algebra methods for equivariant dynamical systems (Lecture notes in mathematics, vol. 1728), Springer, Berlin, 2000;
Mara Neusel, Invariant theory, American Mathematical Society, Providence, R.I., 2007;
Peter Olver, Classical invariant theory, Cambridge University Press, Cambridge, 1999.

Graduate students and researchers across the mathematical sciences will find it worthwhile to consult these three books for further information on the beautiful subject of classical invariant theory from a contempory perspective.

Berlin, January 2008 Bernd Sturmfels

Contents

1 Introduction

Invariant theory is both a classical and a new area of mathematics. It played a central role in 19th century algebra and geometry, yet many of its techniques and algorithms were practically forgotten by the middle of the 20th century.

With the fields of combinatorics and computer science reviving old-fashioned algorithmic mathematics during the past twenty years, also classical invariant theory has come to a renaissance. We quote from the expository article of Kung and Rota (1984):

"Like the Arabian phoenix rising out of its ashes, the theory of invariants, pronounced dead at the turn of the century, is once again at the forefront of mathematics. During its long eclipse, the language of modern algebra was developed, a sharp tool now at last being applied to the very purpose for which it was invented."

This quote refers to the fact that three of Hilbert's fundamental contributions to modern algebra, namely, the *Nullstellensatz*, the *Basis Theorem* and the *Syzygy Theorem*, were first proved as lemmas in his invariant theory papers (Hilbert 1890, 1893). It is also noteworthy that, contrary to a common belief, Hilbert's main results in invariant theory yield an explicit finite algorithm for computing a fundamental set of invariants for all classical groups. We will discuss Hilbert's algorithm in Chap. 4.

Throughout this text we will take the complex numbers $\mathbf{C}$ to be our ground field. The ring of polynomials $f(x_1, x_2, \ldots, x_n)$ in n variables with complex coefficients is denoted $\mathbf{C}[x_1, x_2, \ldots, x_n]$. All algorithms in this book will be based upon arithmetic operations in the ground field only. This means that if the scalars in our input data are contained in some subfield $K \subset \mathbf{C}$, then all scalars in the output also lie in K. Suppose, for instance, we specify an algorithm whose input is a finite set of $n \times n$-matrices over $\mathbf{C}$, and whose output is a finite subset of $\mathbf{C}[x_1, x_2, \ldots, x_n]$. We will usually apply such an algorithm to a set of input matrices which have entries lying in the field $\mathbf{Q}$ of rational numbers. We can then be sure that all output polynomials will lie in $\mathbf{Q}[x_1, x_2, \ldots, x_n]$.

Chapter 1 starts out with a discussion of the ring of symmetric polynomials, which is the simplest instance of a ring of invariants. In Sect. 1.2 we recall some basics from the theory of Gröbner bases, and in Sect. 1.3 we give an elementary exposition of the fundamental problems in invariant theory. Section 1.4 is independent and can be skipped upon first reading. It deals with invariants of algebraic tori and their relation to integer programming. The results of Sect. 1.4 will be needed in Sect. 2.7 and in Chap. 4.

1.1. Symmetric polynomials

Our starting point is the fundamental theorem on symmetric polynomials. This is a basic result in algebra, and studying its proof will be useful to us in three ways. First, we illustrate some fundamental questions in invariant theory with their solution in the easiest case of the symmetric group. Secondly, the main theorem on symmetric polynomials is a crucial lemma for several theorems to follow, and finally, the algorithm underlying its proof teaches us some basic computer algebra techniques.

A polynomial $f \in \mathbf{C}[x_1, \ldots, x_n]$ is said to be *symmetric* if it is invariant under every permutation of the variables $x_1, x_2, \ldots, x_n$. For example, the polynomial $f_1 := x_1x_2 + x_1x_3$ is not symmetric because $f_1(x_1, x_2, x_3) \neq f_1(x_2, x_1, x_3) = x_1x_2 + x_2x_3$. On the other hand, $f_2 := x_1x_2 + x_1x_3 + x_2x_3$ is symmetric.

Let z be a new variable, and consider the polynomial

$$\begin{aligned} g(z) &= (z - x_1)(z - x_2) \ldots (z - x_n) \\ &= z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \ldots + (-1)^n \sigma_n. \end{aligned}$$

We observe that the coefficients of g with respect to the new variable z,

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \ldots + x_n, \\ \sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n, \\ \sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n, \\ \ldots & \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \sigma_n &= x_1x_2x_3 \cdots x_n, \end{aligned}$$

are symmetric in the old variables $x_1, x_2, \ldots, x_n$. The polynomials $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathbf{C}[x_1, x_2, \ldots, x_n]$ are called the *elementary symmetric polynomials*.

Since the property to be symmetric is preserved under addition and multiplication of polynomials, the symmetric polynomials form a subring of $\mathbf{C}[x_1, \ldots, x_n]$. This implies that every polynomial expression $p(\sigma_1, \sigma_2, \ldots, \sigma_n)$ in the elementary symmetric polynomials is symmetric in $\mathbf{C}[x_1, \ldots, x_n]$. For instance, the monomial $c \cdot \sigma_1^{\mu_1} \sigma_2^{\mu_2} \ldots \sigma_n^{\mu_n}$ in the elementary symmetric polynomials is symmetric and homogeneous of degree $\mu_1 + 2\mu_2 + \ldots + n\mu_n$ in the original variables $x_1, x_2, \ldots, x_n$.

Theorem 1.1.1 (Main theorem on symmetric polynomials). Every symmetric polynomial f in $\mathbf{C}[x_1, \ldots, x_n]$ can be written uniquely as a polynomial

$$f(x_1, x_2, \ldots, x_n) = p\big(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)\big)$$

in the elementary symmetric polynomials.

Proof. The proof to be presented here follows the one in van der Waerden

(1971). Let $f \in \mathbf{C}[x_1, \ldots, x_n]$ be any symmetric polynomial. Then the following algorithm rewrites f uniquely as a polynomial in $\sigma_1, \ldots, \sigma_n$.

We sort the monomials in f using the *degree lexicographic order*, here denoted "$\prec$". In this order a monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ is smaller than another monomial $x_1^{\beta_1} \ldots x_n^{\beta_n}$ if it has lower total degree (i.e., $\sum \alpha_i < \sum \beta_i$), or if they have the same total degree and the first nonvanishing difference $\alpha_i - \beta_i$ is negative.

For any monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ occurring in the symmetric polynomial f also all its images $x_{\sigma 1}^{\alpha_1} \ldots x_{\sigma n}^{\alpha_n}$ under any permutation σ of the variables occur in f. This implies that the initial monomial $\operatorname{init}(f) = c \cdot x_1^{\gamma_1} x_2^{\gamma_2} \ldots x_n^{\gamma_n}$ of f satisfies $\gamma_1 \geq \gamma_2 \geq \ldots \geq \gamma_n$. By definition, the *initial monomial* is the largest monomial with respect to the total order "$\prec$" which appears with a nonzero coefficient in f.

In our algorithm we now replace f by the new symmetric polynomial $\tilde{f} := f - c \cdot \sigma_1^{\gamma_1 - \gamma_2} \sigma_2^{\gamma_2 - \gamma_3} \cdots \sigma_{n-1}^{\gamma_{n-1} - \gamma_n} \sigma_n^{\gamma_n}$, we store the summand $c \cdot \sigma_1^{\gamma_1 - \gamma_2} \sigma_2^{\gamma_2 - \gamma_3} \cdots \sigma_{n-1}^{\gamma_{n-1} - \gamma_n} \sigma_n^{\gamma_n}$, and, if $\tilde{f}$ is nonzero, then we return to the beginning of the previous paragraph.

Why does this process terminate? By construction, the initial monomial of $c \cdot \sigma_1^{\gamma_1 - \gamma_2} \sigma_2^{\gamma_2 - \gamma_3} \cdots \sigma_{n-1}^{\gamma_{n-1} - \gamma_n} \sigma_n^{\gamma_n}$ equals $\operatorname{init}(f)$. Hence in the difference defining $\tilde{f}$ the two initial monomials cancel, and we get $\operatorname{init}(\tilde{f}) \prec \operatorname{init}(f)$. The set of monomials m with $m \prec \operatorname{init}(f)$ is finite because their degree is bounded. Hence the above rewriting algorithm must terminate because otherwise it would generate an infinite decreasing chain of monomials.

It remains to be seen that the representation of symmetric polynomials in terms of elementary symmetric polynomials is unique. In other words, we need to show that the elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ are algebraically independent over $\mathbf{C}$.

Suppose on the contrary that there is a nonzero polynomial $p(y_1, \ldots, y_n)$ such that $p(\sigma_1, \ldots, \sigma_n) = 0$ in $\mathbf{C}[x_1, \ldots, x_n]$. Given any monomial $y_1^{\alpha_1} \cdots y_n^{\alpha_n}$ of p, we find that $x_1^{\alpha_1 + \alpha_2 + \ldots + \alpha_n} x_2^{\alpha_2 + \ldots + \alpha_n} \cdots x_n^{\alpha_n}$ is the initial monomial of $\sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n}$. Since the linear map

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (\alpha_1 + \alpha_2 + \ldots + \alpha_n,\ \alpha_2 + \ldots + \alpha_n,\ \ldots,\ \alpha_n)$$

is injective, all other monomials $\sigma_1^{\beta_1} \ldots \sigma_n^{\beta_n}$ in the expansion of $p(\sigma_1, \ldots, \sigma_n)$ have a different initial monomial. The lexicographically largest monomial $x_1^{\alpha_1 + \alpha_2 + \ldots + \alpha_n} x_2^{\alpha_2 + \ldots + \alpha_n} \cdots x_n^{\alpha_n}$ is not cancelled by any other monomial, and therefore $p(\sigma_1, \ldots, \sigma_n) \neq 0$. This contradiction completes the proof of Theorem 1.1.1. $\lhd$

As an example for the above rewriting procedure, we write the bivariate symmetric polynomial $x_1^3 + x_2^3$ as a polynomial in the elementary symmetric polynomials:

$$\underline{x_1^3} + x_2^3 \longrightarrow \sigma_1^3 - \underline{3x_1^2 x_2} - 3x_1 x_2^2 \longrightarrow \sigma_1^3 - 3\sigma_1\sigma_2.$$

The subring $\mathbf{C}[\mathbf{x}]^{S_n}$ of symmetric polynomials in $\mathbf{C}[\mathbf{x}] := \mathbf{C}[x_1, \ldots, x_n]$ is the prototype of an invariant ring. The elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ are said to form a *fundamental system of invariants*. Such fundamental systems are generally far from being unique. Let us describe another generating set for the symmetric polynomials which will be useful later in Sect. 2.1. The polynomial $p_k(\mathbf{x}) := x_1^k + x_2^k + \ldots + x_n^k$ is called the *k-th power sum.*

Proposition 1.1.2. The ring of symmetric polynomials is generated by the first n power sums, i.e.,

$$\mathbf{C}[\mathbf{x}]^{S_n} = \mathbf{C}[\sigma_1, \sigma_2, \ldots, \sigma_n] = \mathbf{C}[p_1, p_2, \ldots, p_n].$$

Proof. A *partition* of an integer d is an integer vector $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ such that $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq 0$ and $\lambda_1 + \lambda_2 + \ldots + \lambda_n = d$. We assign to a monomial $x_1^{i_1} \ldots x_n^{i_n}$ of degree d the partition $\lambda(i_1, \ldots, i_n)$ which is the decreasingly sorted string of its exponents.

This gives rise to the following total order on the set of degree d monomials in $\mathbf{C}[\mathbf{x}]$. We set $x_1^{i_1} \ldots x_n^{i_n} \prec x_1^{j_1} \ldots x_n^{j_n}$ if the partition $\lambda(i_1, \ldots, i_n)$ is lexicographically larger than $\lambda(j_1, \ldots, j_n)$, or if the partitions are equal and $(i_1, \ldots, i_n)$ is lexicographically smaller than $(j_1, \ldots, j_n)$. We note that this total order on the set of monomials in $\mathbf{C}[\mathbf{x}]$ is *not* a monomial order in the sense of Gröbner bases theory (cf. Sect. 1.2). As an example, for $n = 3$, $d = 4$ we have $x_3^4 \prec x_2^4 \prec x_1^4 \prec x_2 x_3^3 \prec x_2^3 x_3 \prec x_1 x_3^3 \prec x_1 x_2^3 \prec x_1^3 x_3 \prec x_1^3 x_2 \prec x_2^2 x_3^2 \prec x_1^2 x_3^2 \prec x_1^2 x_2^2 \prec x_1 x_2 x_3^2 \prec x_1 x_2^2 x_3 \prec x_1^2 x_2 x_3$.

We find that the initial monomial of a product of power sums equals

$$\operatorname{init}(p_{i_1} p_{i_2} \ldots p_{i_n}) = c_{i_1 i_2 \ldots i_n} \cdot x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \quad \text{whenever } i_1 \geq i_2 \geq \ldots \geq i_n,$$

where $c_{i_1 i_2 \ldots i_n}$ is a positive integer.

Now we are prepared to describe an algorithm which proves Proposition 1.1.2. It rewrites a given symmetric polynomial $f \in \mathbf{C}[\mathbf{x}]$ as a polynomial function in $p_1, p_2, \ldots, p_n$. By Theorem 1.1.1 we may assume that f is one of the elementary symmetric polynomials. In particular, the degree d of f is less or equal to n. Its initial monomial $\operatorname{init}(f) = c \cdot x_1^{i_1} \ldots x_n^{i_n}$ satisfies $n \geq i_1 \geq \ldots \geq i_n$. Now replace f by $\tilde{f} := f - \frac{c}{c_{i_1 \ldots i_n}} p_{i_1} \ldots p_{i_n}$. By the above observation the initial monomials in this difference cancel, and we get $\operatorname{init}(\tilde{f}) \prec \operatorname{init}(f)$. Since both f and $\tilde{f}$ have the same degree d, this process terminates with the desired result. ◁

Here is an example for the rewriting process in the proof of Proposition 1.1.2. We express the three-variate symmetric polynomial $f := x_1 x_2 x_3$ as a polynomial function in p_1, p_2 and p_3. Using the above method, we get

$$\begin{aligned} x_1x_2x_3 &\longrightarrow \tfrac{1}{6}p_1^3 - \tfrac{1}{2}\sum_{i\neq j} x_i^2x_j - \tfrac{1}{6}\sum_k x_k^3 \\ &\longrightarrow \tfrac{1}{6}p_1^3 - \tfrac{1}{2}\big(p_1p_2 - \sum_k x_k^3\big) - \tfrac{1}{6}\sum_k x_k^3 \\ &\longrightarrow \tfrac{1}{6}p_1^3 - \tfrac{1}{2}p_1p_2 + \tfrac{1}{3}p_3. \end{aligned}$$

Theorem 1.1.1 and Proposition 1.1.2 show that the monomials in the elementary symmetric polynomials and the monomials in the power sums are both $\mathbf{C}$-vector space bases for the ring of symmetric polynomials $\mathbf{C}[\mathbf{x}]^{S_n}$. There are a number of other important such bases, including the *complete symmetric polynomials*, the *monomial symmetric polynomials* and the *Schur polynomials*. The relations between these bases is of great importance in algebraic combinatorics and representation theory. A basic reference for the theory of symmetric polynomials is Macdonald (1979).

We close this section with the definition of the Schur polynomials. Let A_n denote the *alternating group*, which is the subgroup of S_n consisting of all even permutations. Let $\mathbf{C}[\mathbf{x}]^{A_n}$ denote the subring of polynomials which are fixed by all even permutations. We have the inclusion $\mathbf{C}[\mathbf{x}]^{S_n} \subseteq \mathbf{C}[\mathbf{x}]^{A_n}$. This inclusion is proper, because the polynomial

$$D(x_1,\ldots,x_n) := \prod_{1\le i<j\le n} (x_i - x_j)$$

is fixed by all even permutations but not by any odd permutation.

Proposition 1.1.3. Every polynomial $f \in \mathbf{C}[\mathbf{x}]^{A_n}$ can be written uniquely in the form $f = g + h\cdot D$, where g and h are symmetric polynomials.

Proof. We set

$$\begin{aligned} g(x_1,\ldots,x_n) &:= \tfrac{1}{2}\big[f(x_1,x_2,x_3,\ldots,x_n) + f(x_2,x_1,x_3,\ldots,x_n)\big] \quad \text{and} \\ \tilde{h}(x_1,\ldots,x_n) &:= \tfrac{1}{2}\big[f(x_1,x_2,x_3,\ldots,x_n) - f(x_2,x_1,x_3,\ldots,x_n)\big]. \end{aligned}$$

Thus f is the sum of the symmetric polynomial g and the antisymmetric polynomial $\tilde{h}$. Here $\tilde{h}$ being *antisymmetric* means that

$$\tilde{h}(x_{\sigma_1},\ldots,x_{\sigma_n}) = \operatorname{sign}(\sigma)\cdot\tilde{h}(x_1,\ldots,x_n)$$

for all permutations $\sigma \in S_n$. Hence $\tilde{h}$ vanishes identically if we replace one of the variables x_i by some other variable x_j. This implies that $x_i - x_j$ divides $\tilde{h}$, for all $1 \le i < j \le n$, and therefore D divides $\tilde{h}$. To show uniqueness, we suppose that $f = g + hD = g' + h'D$. Applying an odd permutation π, we get $f\circ\pi = g - hD = g' - h'D$. Now add both equations to conclude $g = g'$ and therefore $h = h'$. $\triangleleft$

With any partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n)$ of an integer d we associate the homogeneous polynomial

$$a_\lambda(x_1, \ldots, x_n) = \det \begin{pmatrix} x_1^{\lambda_1+n-1} & x_2^{\lambda_1+n-1} & \cdots & x_n^{\lambda_1+n-1} \\ x_1^{\lambda_2+n-2} & x_2^{\lambda_2+n-2} & \cdots & x_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_n} & x_2^{\lambda_n} & \cdots & x_n^{\lambda_n} \end{pmatrix}.$$

Note that the total degree of $a_\lambda(x_1, \ldots, x_n)$ equals $d + \binom{n}{2}$.

The polynomials a_λ are precisely the nonzero images of monomials under antisymmetrization. Here by *antisymmetrization* of a polynomial we mean its canonical projection into the subspace of antisymmetric polynomials. Therefore the a_λ form a basis for the $\mathbf{C}$-vector space of all antisymmetric polynomials. We may proceed as in the proof of Proposition 1.1.3 and divide a_λ by the discriminant. The resulting expression $s_\lambda := a_\lambda / D$ is a symmetric polynomial which is homogeneous of degree $d = |\lambda|$. We call $s_\lambda(x_1, \ldots, x_n)$ the *Schur polynomial* associated with the partition λ.

Corollary 1.1.4. The set of Schur polynomials s_λ, where $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n)$ ranges over all partitions of d into at most n parts, forms a basis for the $\mathbf{C}$-vector space $\mathbf{C}[\mathbf{x}]_d^{S_n}$ of all symmetric polynomials homogeneous of degree d.

Proof. It follows from Proposition 1.1.3 that multiplication with D is an isomorphism from the vector space of symmetric polynomials to the space of antisymmetric polynomials. The images of the Schur polynomials s_λ under this isomorphism are the antisymmetrized monomials a_λ. Since the latter are a basis, also the former are a basis. $\triangleleft$

Exercises

(1) Write the symmetric polynomials $f := x_1^3 + x_2^3 + x_3^3$ and $g := (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$ as polynomials in the elementary symmetric polynomials $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, and $\sigma_3 = x_1x_2x_3$.

(2) Study the complexity of the algorithm in the proof of Theorem 1.1.1. More precisely, find an upper bound in terms of $\deg(f)$ for the number of steps needed to express a symmetric $f \in \mathbf{C}[x_1, \ldots, x_n]$ as a polynomial in the elementary symmetric polynomials.

(3) Write the symmetric polynomials $\sigma_4 := x_1x_2x_3x_4$ and $p_5 := x_1^5 + x_2^5 + x_3^5 + x_4^5$ as polynomials in the first four power sums $p = x_1 + x_2 + x_3 + x_4$, $p_2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $p_3 = x_1^3 + x_2^3 + x_3^3 + x_4^3$, $p_4 = x_1^4 + x_2^4 + x_3^4 + x_4^4$.

(4) Consider the vector space $V = \mathbf{C}[x_1, x_2, x_3]_6^{S_3}$ of all symmetric

polynomials in three variables which are homogeneous of degree 6. What is the dimension of V? We get three different bases for V by considering Schur polynomials $s_{(\lambda_1,\lambda_2,\lambda_3)}$, monomials $\sigma_1^{i_1}\sigma_2^{i_2}\sigma_3^{i_3}$ in the elementary symmetric polynomials, and monomials $p_1^{i_1}p_2^{i_2}p_3^{i_3}$ in the power sum symmetric polynomials. Express each element in one of these bases as a linear combination with respect to the other two bases.

(5) Prove the following explicit formula for the elementary symmetric polynomials in terms of the power sums (Macdonald 1979, p. 20):

$$\sigma_k = \frac{1}{k\,!} \det \begin{pmatrix} p_1 & 1 & 0 & \dots & 0 \\ p_2 & p_1 & 2 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \dots & p_1 & k-1 \\ p_k & p_{k-1} & \dots & \dots & p_1 \end{pmatrix}.$$

1.2. Gröbner bases

In this section we review background material from computational algebra. More specifically, we give a brief introduction to the theory of Gröbner bases. Our emphasis is on how to use Gröbner bases as a basic building block in designing more advanced algebraic algorithms. Readers who are interested in "how this black box works" may wish to consult either of the text books Cox et al. (1992) or Becker et al. (1993). See also Buchberger (1985, 1988) and Robbiano (1988) for additional references and details on the computation of Gröbner bases.

Gröbner bases are a general-purpose method for multivariate polynomial computations. They were introduced by Bruno Buchberger in his 1965 dissertation, written at the University of Innsbruck (Tyrolia, Austria) under the supervision of Wolfgang Gröbner. Buchberger's main contribution is a finite algorithm for transforming an arbitrary generating set of an ideal into a Gröbner basis for that ideal.

The basic principles underlying the concept of Gröbner bases can be traced back to the late 19th century and the early 20th century. One such early reference is P. Gordan's 1900 paper on the invariant theory of binary forms. What is called *"Le système irréductible N"* on page 152 of Gordan (1900) is a Gröbner basis for the ideal under consideration.

Buchberger's Gröbner basis method generalizes three well-known algebraic algorithms:

- the Euclidean algorithm (for univariate polynomials)
- Gaussian elimination (for linear polynomials)
- the Sylvester resultant (for eliminating one variable from two polynomials)

So we can think of Gröbner bases as a version of the Euclidean algorithm which works also for more than one variable, or as a version of Gaussian elimination which works also for higher degree polynomials. The basic algorithms are implemented in many computer algebra systems, e.g., MAPLE, REDUCE, AXIOM, MATHEMATICA, MACSYMA, MACAULAY, COCOA[1], and playing with one of these systems is an excellent way of familiarizing oneself with Gröbner bases. In MAPLE, for instance, the command "gbasis" is used to compute a Gröbner basis for a given set of polynomials, while the command "normalf" reduces any other polynomial to normal form with respect to a given Gröbner basis.

The mathematical setup is as follows. A total order "$\prec$" on the monomials $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ in $\mathbf{C}[x_1, \dots, x_n]$ is said to be a *monomial order* if $1 \preceq m_1$ and $(m_1 \prec m_2 \Rightarrow m_1 \cdot m_3 \prec m_2 \cdot m_3)$ for all monomials $m_1, m_2, m_3 \in \mathbf{C}[x_1, \dots, x_n]$. Both the degree lexicographic order discussed in Sect. 1.1 and the *(purely) lexicographic order* are important examples of monomial orders. Every linear order on the variables $x_1, x_2, \dots, x_n$ can be extended to a lexicographic order on the monomials. For example, the order $x_1 \prec x_3 \prec x_2$ on three variables induces the (purely) lexicographic order $1 \prec x_1 \prec x_1^2 \prec x_1^3 \prec x_1^4 \prec \dots \prec x_3 \prec x_3x_1 \prec x_3x_1^2 \prec \dots \prec x_2 \prec x_2x_1 \prec x_2x_1^2 \prec \dots$ on $\mathbf{C}[x_1, x_2, x_3]$.

We now fix any monomial order "$\prec$" on $\mathbf{C}[x_1, \dots, x_n]$. The largest monomial of a polynomial $f \in \mathbf{C}[x_1, \dots, x_n]$ with respect to "$\prec$" is denoted by $\mathrm{init}(f)$ and called the *initial monomial* of f. For an ideal $I \subset \mathbf{C}[x_1, \dots, x_n]$, we define its *initial ideal* as $\mathrm{init}(I) := \langle\{\mathrm{init}(f) : f \in I\}\rangle$. In other words, $\mathrm{init}(I)$ is the ideal generated by the initial monomials of all polynomials in I. An ideal which is generated by monomials, such as $\mathrm{init}(I)$, is said to be a *monomial ideal*. The monomials $m \notin \mathrm{init}(I)$ are called *standard*, and the monomials $m \in \mathrm{init}(I)$ are *nonstandard*.

A *finite* subset $\mathcal{G} := \{g_1, g_2, \dots, g_s\}$ of an ideal I is called a *Gröbner basis* for I provided the initial ideal $\mathrm{init}(I)$ is generated by $\{\mathrm{init}(g_1), \dots, \mathrm{init}(g_s)\}$. One last definition: the Gröbner basis $\mathcal{G}$ is called *reduced* if $\mathrm{init}(g_i)$ does not divide any monomial occurring in g_j, for all distinct $i, j \in \{1, 2, \dots, s\}$. Gröbner bases programs (such as "gbasis" in MAPLE) take a finite set $\mathcal{F} \subset \mathbf{C}[\mathbf{x}]$ and they output a reduced Gröbner basis $\mathcal{G}$ for the ideal $\langle\mathcal{F}\rangle$ generated by $\mathcal{F}$. They are based on the Buchberger algorithm.

The previous paragraph is perhaps the most compact way of defining Gröbner bases, but it is not at all informative on what Gröbner bases theory is all about. Before proceeding with our theoretical crash course, we present six concrete examples $(\mathcal{F}, \mathcal{G})$ where $\mathcal{G}$ is a reduced Gröbner basis for the ideal $\langle\mathcal{F}\rangle$.

Example 1.2.1 (Easy examples of Gröbner bases). In (1), (2), (5), (6) we also give examples for the *normal form reduction* versus a Gröbner bases $\mathcal{G}$ which rewrites every polynomial modulo $\langle\mathcal{F}\rangle$ as a $\mathbf{C}$-linear combination of standard monomials (cf. Theorem 1.2.6). In all examples the used monomial order is specified and the initial monomials are underlined.

(1) For any set of univariate polynomials $\mathcal{F}$, the reduced Gröbner basis $\mathcal{G}$ is

[1] Among software packages for Gröbner bases which are current in 2008 we also recommend MACAULAY 2, MAGMA and SINGULAR.

always a singleton, consisting of the greatest common divisor of $\mathcal{F}$. Note that $1 \prec x \prec x^2 \prec x^3 \prec x^4 \prec \ldots$ is the only monomial order on $\mathbf{C}[x]$.

$\mathcal{F} = \{\underline{12x^3} - x^2 - 23x - 11,\ \underline{x^4} - x^2 - 2x - 1\}$

$\mathcal{G} = \{\underline{x^2} - x - 1\}$

Normal form: $x^3 + x^2 \rightarrow_{\mathcal{G}} 3x + 2$

Here x^2 generates the initial ideal, hence 1 and x are the only standard monomials.

(2) This ideal in two variables corresponds to the intersection of the unit circle with a certain hyperbola. We use the purely lexicographic order induced from $x \prec y$.

$\mathcal{F} = \{\underline{y^2} + x^2 - 1,\ \underline{3xy} - 1\}$

$\mathcal{G} = \{\underline{y} + 3x^3 - 3x,\ \underline{9x^4} - 9x^2 + 1\}$

Normal form: $y^4 + y^3 \rightarrow_{\mathcal{G}} 27x^3 + 9x^2 - 24x - 8$

The Gröbner basis is triangularized, and we can easily compute coordinates for the intersection points of these two curves. There are four such points and hence the residue ring $\mathbf{C}[x, y]/\langle\mathcal{F}\rangle$ is a four-dimensional $\mathbf{C}$-vector space. The set of standard monomials $\{1, x, x^2, x^3\}$ is a basis for this vector space because the normal form of any bivariate polynomial is a polynomial in x of degree at most 3.

(3) If we add the line $y = x + 1$, then the three curves have no point in common. This means that the ideal equals the whole ring. The Gröbner basis with respect to any monomial order consists of a nonzero constant.

$\mathcal{F} = \{\underline{y^2} + x^2 - 1,\ \underline{3xy} - 1,\ \underline{y} - x - 1\}$

$\mathcal{G} = \{\underline{1}\}$

(4) The three bivariate polynomials in (3) are algebraically dependent. In order to find an algebraic dependence, we introduce three new "slack" variables f, g and h, and we compute a Gröbner basis of

$\mathcal{F} = \{\underline{y^2} + x^2 - 1 - f,\ \underline{3xy} - 1 - g,\ \underline{y} - x - 1 - h\}$

with respect to the lexicographic order induced from $f \prec g \prec h \prec x \prec y$.

$\mathcal{G} = \{\underline{y} - x - h - 1,\ \underline{3x^2} + 3x - g + 3hx - 1,\ \underline{3h^2} + 6h + 2g - 3f + 2\}$

The third polynomial is an algebraic dependence between the circle, the hyperbola and the line.

(5) We apply the same slack variable computation to the elementary symmetric polynomials in $\mathbf{C}[x_1, x_2, x_3]$, using the lexicographic order induced from $\sigma_1 \prec \sigma_2 \prec \sigma_3 \prec x_1 \prec x_2 \prec x_3$.

$\mathcal{F} = \{x_1 + x_2 + \underline{x_3} - \sigma_1,\ x_1x_2 + x_1x_3 + \underline{x_2x_3} - \sigma_2,\ \underline{x_1x_2x_3} - \sigma_3\}$

$\mathcal{G} = \{\underline{x_3} + x_2 + x_1 - \sigma_1,\ \underline{x_2^2} + x_1x_2 + x_1^2 - \sigma_1x_2 - \sigma_1x_1 + \sigma_2,\ \underline{x_1^3} - \sigma_1x_1^2 + \sigma_2x_1 - \sigma_3\}$

The Gröbner basis does not contain any polynomial in the slack variables $\sigma_1, \sigma_2, \sigma_3$ because the elementary symmetric polynomials are algebraically independent. Here the standard monomials are $1, x_1, x_1^2, x_2, x_2x_1, x_2x_1^2$ and all their products with monomials of the form $\sigma_1^{i_1}\sigma_2^{i_2}\sigma_3^{i_3}$.

Normal form: $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 \rightarrow_{\mathcal{G}}$
$-27\sigma_3^2 + 18\sigma_3\sigma_2\sigma_1 - 4\sigma_3\sigma_1^3 - 4\sigma_2^3 + \sigma_2^2\sigma_1^2$

(6) This is a special case of a polynomial system which will be studied in detail in Chap. 3, namely, the set of $d \times d$-subdeterminants of an $n \times d$-matrix (x_{ij}) whose entries are indeterminates. We apply the slack variable computation to the six 2×2-minors of a 4×2-matrix, using the lexicographic order induced from the variable order $[12] \prec [13] \prec [14] \prec [23] \prec [24] \prec [34] \prec x_{11} \prec x_{12} \prec x_{21} \prec x_{22} \prec x_{31} \prec x_{32} \prec x_{41} \prec x_{42}$. In the polynomial ring in these $14 = 6 + 8$ variables, we consider the ideal generated by

$$\begin{aligned}\mathcal{F} = \{&\underline{x_{11}x_{22}} - x_{12}x_{21} - [12],\ \underline{x_{11}x_{32}} - x_{12}x_{31} - [13],\\ &\underline{x_{11}x_{42}} - x_{12}x_{41} - [14],\ \underline{x_{21}x_{32}} - x_{22}x_{31} - [23],\\ &\underline{x_{21}x_{42}} - x_{22}x_{41} - [24],\ \underline{x_{31}x_{42}} - x_{32}x_{41} - [34]\}\end{aligned}$$

The Gröbner basis equals

$$\begin{aligned}\mathcal{G} = \mathcal{F} \cup \{&\underline{[12][34]} - [13][24] + [14][23],\ \ldots\ \ldots\ \ldots \text{ (and}\\ &\text{many more) } \ldots\}\end{aligned}$$

This polynomial is an algebraic dependence among the 2×2-minors of any 4×2-matrix. It is known as the *(quadratic) Grassmann–Plücker syzygy*. Using the Gröbner basis $\mathcal{G}$, we can rewrite any polynomial which lies in the subring generated by the 2×2-determinants as a polynomial function in $[12], [13], \ldots, [34]$.

$$\begin{aligned}\text{Normal form: } & x_{11}x_{22}x_{31}x_{42} + x_{11}x_{22}x_{32}x_{41} + x_{12}x_{21}x_{31}x_{42} +\\ & x_{12}x_{21}x_{32}x_{41} - 2x_{11}x_{21}x_{32}x_{42} - 2x_{12}x_{22}x_{31}x_{41} \rightarrow_{\mathcal{G}}\\ & [14][23] + [13][24]\end{aligned}$$

Before continuing to read any further, we urge the reader to verify these six examples and to compute at least fifteen more Gröbner bases using one of the computer algebra systems mentioned above.

We next discuss a few aspects of Gröbner bases theory which will be used in the later chapters. To begin with we prove that every ideal indeed admits a finite Gröbner basis.

Lemma 1.2.2 (Hilbert 1890, Gordan 1900). Every monomial ideal $\mathcal{M}$ in $\mathbf{C}[x_1, \ldots, x_n]$ is finitely generated by monomials.

Proof. We proceed by induction on n. By definition, a monomial ideal $\mathcal{M}$ in $\mathbf{C}[x_1]$ is generated by $\{x_1^j : j \in J\}$, where J is some subset of the nonnegative integers. The set J has a minimal element j_0, and $\mathcal{M}$ is generated by the singleton $\{x_1^{j_0}\}$. This proves the assertion for $n = 1$.

Suppose that Lemma 1.2.2 is true for monomial ideals in $n - 1$ variables. For every nonnegative integer $j \in \mathbf{N}$ consider the $(n - 1)$-variate monomial ideal $\mathcal{M}_j$ which is generated by all monomials $m \in \mathbf{C}[x_1, \ldots, x_{n-1}]$ such that $m \cdot x_n^j \in \mathcal{M}$. By the induction hypothesis, $\mathcal{M}_j$ is generated by a finite set S_j of monomials. Next observe the inclusions $\mathcal{M}_0 \subseteq \mathcal{M}_1 \subseteq \mathcal{M}_2 \subseteq \ldots \subseteq \mathcal{M}_i \subseteq \mathcal{M}_{i+1} \subseteq \ldots$. By the induction hypothesis, also the monomial ideal $\bigcup_{j=0}^{\infty} \mathcal{M}_j$ is finitely generated. This implies the existence of an integer r such that $\mathcal{M}_r = \mathcal{M}_{r+1} = \mathcal{M}_{r+2} = \mathcal{M}_{r+3} = \ldots$. It follows that a monomial $x_1^{\alpha_1} \ldots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n}$ is contained in $\mathcal{M}$ if and only if $x_1^{\alpha_1} \ldots x_{n-1}^{\alpha_{n-1}}$ is contained in $\mathcal{M}_t$, where $t = \min\{r, \alpha_n\}$. Hence the finite monomial set $\bigcup_{i=0}^{r} S_i \cdot x_n^i$ generates $\mathcal{M}$. ◁

Corollary 1.2.3. Let "$\prec$" be any monomial order on $\mathbf{C}[x_1, \ldots, x_n]$. Then there is no infinite descending chain of monomials $m_1 \succ m_2 \succ m_3 \succ m_4 \succ \ldots$.

Proof. Consider any infinite set $\{m_1, m_2, m_3, \ldots\}$ of monomials in $\mathbf{C}[x_1, \ldots, x_n]$. Its ideal is finitely generated by Lemma 1.2.2. Hence there exists an integer j such that $m_j \in \langle m_1, m_2, \ldots, m_{j-1} \rangle$. This means that m_i divides m_j for some $i < j$. Since "$\prec$" is a monomial order, this implies $m_i \prec m_j$ with $i < j$. This proves Corollary 1.2.3. $\lhd$

Theorem 1.2.4.
(1) Any ideal $I \subset \mathbf{C}[x_1, \ldots, x_n]$ has a Gröbner basis $\mathcal{G}$ with respect to any monomial order "$\prec$".
(2) Every Gröbner basis $\mathcal{G}$ generates its ideal I.

Proof. Statement (1) follows directly from Lemma 1.2.2 and the definition of Gröbner bases. We prove statement (2) by contradiction. Suppose the Gröbner basis $\mathcal{G}$ does not generate its ideal, that is, the set $I \setminus \langle \mathcal{G} \rangle$ is nonempty. By Corollary 1.2.3, the set of initial monomials $\{\text{init}(f) : f \in I \setminus \langle \mathcal{G} \rangle\}$ has a minimal element $\text{init}(f_0)$ with respect to "$\prec$". The monomial $\text{init}(f_0)$ is contained in $\text{init}(I) = \langle \text{init}(\mathcal{G}) \rangle$. Let $g \in \mathcal{G}$ such that $\text{init}(g)$ divides $\text{init}(f_0)$, say, $\text{init}(f_0) = m \cdot \text{init}(g)$.

Now consider the polynomial $f_1 := f_0 - m \cdot g$. By construction, $f_1 \in I \setminus \langle \mathcal{G} \rangle$. But we also have $\text{init}(f_1) \prec \text{init}(f_0)$. This contradicts the minimality in the choice of f_0. This contradiction shows that $\mathcal{G}$ does generate the ideal I. $\lhd$

From this we obtain as a direct consequence the following basic result.

Corollary 1.2.5 (Hilbert's basis theorem). Every ideal in the polynomial ring $\mathbf{C}[x_1, x_2, \ldots, x_n]$ is finitely generated.

We will next prove the normal form property of Gröbner bases.

Theorem 1.2.6. Let I be any ideal and "$\prec$" any monomial order on $\mathbf{C}[x_1, \ldots, x_n]$. The set of (residue classes of) standard monomials is a $\mathbf{C}$-vector space basis for the residue ring $\mathbf{C}[x_1, \ldots, x_n]/I$.

Proof. Let $\mathcal{G}$ be a Gröbner basis for I, and consider the following algorithm which computes the normal form modulo I.

Input: $p \in \mathbf{C}[x_1, \ldots, x_n]$.

1. Check whether all monomials in p are standard. If so, we are done: p is in normal form and equivalent modulo I to the input polynomial.
2. Otherwise let $\text{hnst}(p)$ be the highest nonstandard monomial occurring in p. Find $g \in \mathcal{G}$ such that $\text{init}(g)$ divides $\text{hnst}(p)$, say, $m \cdot \text{init}(g) = \text{hnst}(p)$.
3. Replace p by $\tilde{p} := p - m \cdot g$, and go to 1.

We have $\text{init}(\tilde{p}) \prec \text{init}(p)$ in Step 3, and hence Corollary 1.2.3 implies that this algorithm terminates with a representation of $p \in \mathbf{C}[x_1, \ldots, x_n]$ as a $\mathbf{C}$-linear combination of standard monomials modulo I. We conclude the proof of Theorem 1.2.6 by observing that such a representation is necessarily unique because, by definition, every polynomial in I contains at least one nonstandard monomial. This means that zero cannot be written as nontrivial linear combination of standard monomials in $\mathbf{C}[x_1,\ldots,x_n]/I$. $\triangleleft$

Sometimes it is possible to give an a priori proof that an explicitly known "nice" subset of a polynomial ideal I happens to be a Gröbner basis. In such a lucky situation there is no need to apply the Buchberger algorithm. In order to establish the Gröbner basis property, tools from algebraic combinatorics are particularly useful. We illustrate this by generalizing the above Example (5) to an arbitrary number of variables.

Let I denote the ideal in $\mathbf{C}[\mathbf{x},\mathbf{y}] = \mathbf{C}[x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n]$ which is generated by the polynomials $\sigma_i(x_1,\ldots,x_n) - y_i$ for $i = 1,2,\ldots,n$. Here σ_i denotes the i-th elementary symmetric polynomial. In other words, I is the ideal of all algebraic relations between the roots and coefficients of a generic univariate polynomial.

The i-th *complete symmetric polynomial* h_i is defined to be the sum of all monomials of degree i in the given set of variables. In particular, we have $h_i(x_k,\ldots,x_n) = \sum x_k^{\nu_k} x_{k+1}^{\nu_{k+1}} \cdots x_n^{\nu_n}$ where the sum ranges over all $\binom{n-k+i}{i}$ nonnegative integer vectors $(\nu_k,\nu_{k+1},\ldots,\nu_n)$ whose coordinates sum to i.

Theorem 1.2.7. The unique reduced Gröbner basis of I with respect to the lexicographic monomial order induced from $x_1 \succ x_2 \succ \ldots \succ x_n \succ y_1 \succ y_2 \succ \ldots \succ y_n$ equals

$$\mathcal{G} = \left\{ h_k(x_k,\ldots,x_n) + \sum_{i=1}^{k} (-1)^i \, h_{k-i}(x_k,\ldots,x_n) y_i \; : k = 1,\ldots,n \right\}.$$

Proof. In the proof we use a few basic facts about symmetric polynomials and Hilbert series of graded algebras. We first note the following symmetric polynomial identity

$$h_k(x_k,\ldots,x_n) + \sum_{i=1}^{k} (-1)^i \, h_{k-i}(x_k,\ldots,x_n)\, \sigma_i(x_1,\ldots,x_{k-1},x_k,\ldots,x_n) = 0.$$

This identity shows that $\mathcal{G}$ is indeed a subset of the ideal I.

We introduce a grading on $\mathbf{C}[\mathbf{x},\mathbf{y}]$ by setting degree$(x_i) = 1$ and degree$(y_j) = j$. The ideal I is homogeneous with respect to this grading. The quotient ring $R = \mathbf{C}[\mathbf{x},\mathbf{y}]/I$ is isomorphic as a graded algebra to $\mathbf{C}[x_1,\ldots,x_n]$, and hence the Hilbert series of $R = \bigoplus_{d=0}^{\infty} R_d$ equals $H(R,z) = \sum_{d=0}^{\infty} \dim_{\mathbf{C}}(R_d) z^d = (1-z)^{-n}$. It follows from Theorem 1.2.6 that the quotient $\mathbf{C}[\mathbf{x},\mathbf{y}]/\operatorname{init}_{\prec}(I)$ modulo the initial ideal has the same Hilbert series $(1-z)^{-n}$.

Consider the monomial ideal $J = \langle x_1, x_2^2, x_3^3, \ldots, x_n^n \rangle$ which is generated by the initial monomials of the elements in $\mathcal{G}$. Clearly, J is contained in the initial ideal $\mathrm{init}_\prec(I)$. Our assertion states that these two ideals are equal. For the proof it is sufficient to verify that the Hilbert series of $R' := \mathbf{C}[\mathbf{x}, \mathbf{y}]/J$ equals the Hilbert series of R.

A vector space basis for R' is given by the set of all monomials $x_1^{i_1} \cdots x_n^{i_n} y_1^{j_1} \cdots y_n^{j_n}$ whose exponents satisfy the constraints $i_1 < 1, i_2 < 2, \ldots, i_n < n$. This shows that the Hilbert series of R' equals the formal power series

$$H(R', z) = \left(\sum z^{i_1+i_2+\ldots+i_n}\right)\left(\sum z^{j_1+2j_2+\ldots+nj_n}\right).$$

The second sum is over all $(j_1, \ldots, j_n) \in \mathbf{N}^n$ and thus equals $[(1-z)(1-z^2)\cdots(1-z^n)]^{-1}$. The first sum is over all $(i_1, \ldots, i_n) \in \mathbf{N}^n$ with $i_\mu < \mu$ and hence equals the polynomial $(1+z)(1+z+z^2)\cdots(1+z+z^2+\ldots+z^{n-1})$. We compute their product as follows:

$$\begin{aligned} H(R', z) &= \left(\frac{1}{1-z}\right)\left(\frac{1+z}{1-z^2}\right)\left(\frac{1+z+z^2}{1-z^3}\right)\cdots\left(\frac{1+z+z^2+\ldots+z^{n-1}}{1-z^n}\right) \\ &= \left(\frac{1}{1-z}\right)\left(\frac{1}{1-z}\right)\left(\frac{1}{1-z}\right)\cdots\left(\frac{1}{1-z}\right) = H(R, z). \end{aligned}$$

This completes the proof of Theorem 1.2.7. $\triangleleft$

The normal form reduction versus the Gröbner basis $\mathcal{G}$ in Theorem 1.2.7 provides an alternative algorithm for the Main Theorem on Symmetric Polynomials (1.1.1). If we reduce any symmetric polynomial in the variables $x_1, x_2, \ldots, x_n$ modulo $\mathcal{G}$, then we get a linear combination of standard monomials $y_1^{i_1} y_2^{i_2} \cdots y_n^{i_n}$. These can be identified with monomials $\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$ in the elementary symmetric polynomial.

Exercises

(1) Let "$\prec$" be a monomial order and let I be any ideal in $\mathbf{C}[x_1, \ldots, x_n]$. A monomial m is called *minimally nonstandard* if m is nonstandard and all proper divisors of m are standard. Show that the set of minimally nonstandard monomials is finite.

(2) Prove that the reduced Gröbner basis $\mathcal{G}_{\mathrm{red}}$ of I with respect to "$\prec$" is unique (up to multiplicative constants from $\mathbf{C}$). Give an algorithm which transforms an arbitrary Gröbner basis into $\mathcal{G}_{\mathrm{red}}$.

(3) Let $I \subset \mathbf{C}[x_1, \ldots, x_n]$ be an ideal, given by a finite set of generators. Using Gröbner bases, describe an algorithm for computing the *elimination ideals* $I \cap \mathbf{C}[x_1, \ldots, x_i]$, $i = 1, \ldots, n-1$, and prove its correctness.

(4) Find a characterization for all monomial orders on the polynomial ring $\mathbf{C}[x_1, x_2]$. (Hint: Each variable receives a certain "weight" which behaves additively under multiplication of variables.) Generalize your result to n variables.