ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

FOUNDED BY G.-C. ROTA

Volume 99

Solving Polynomial Equation Systems II

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

40 N. White (ed.) *Matroid Applications*
41 S. Sakai *Operator Algebras in Dynamical Systems*
42 W. Hodges *Basic Model Theory*
43 H. Stahl and V. Totik *General Orthogonal Polynomials*
45 G. Da Prato and J. Zabczyk *Stochastic Equations in Infinite Dimensions*
46 A Björner *et al.* *Oriented Matroids*
47 G. Edgar and L. Sucheston *Stopping Times and Directed Processes*
48 C. Sims *Computation with Finitely Presented Groups*
49 T. Palmer *Banach Algebras and the General Theory of *-Algebras I*
50 F. Borceux *Handbook of Categorical Algebra I*
51 F. Borceux *Handbook of Categorical Algebra II*
52 F. Borceux *Handbook of Categorical Algebra III*
53 V. F. Kolchin *Random Graphs*
54 A. Katok and B. Hasselblatt *Introduction to the Modern Theory of Dynamical Systems*
55 V. N. Sachkov *Combinatorial Methods in Discrete Mathematics*
56 V. N. Sachkov *Probabilistic Methods in Discrete Mathematics*
57 P. M. Cohn *Skew Fields*
58 R. Gardner *Geometric Tomography*
59 G. A. Baker, Jr., and P. Graves-Morris *Padé Approximants, 2nd edn*
60 J. Krajicek *Bounded Arithmetic, Propositional Logic, and Complexity Theory*
61 H. Groemer *Geometric Applications of Fourier Series and Spherical Harmonics*
62 H. O. Fattorini *Infinite Dimensional Optimization and Control Theory*
63 A. C. Thompson *Minkowski Geometry*
64 R. B. Bapat and T. E. S. Raghavan *Nonnegative Matrices with Applications*
65 K. Engel *Sperner Theory*
66 D. Cvetkovic, P. Rowlinson and S. Simic *Eigenspaces of Graphs*
67 F. Bergeron, G. Labelle and P. Leroux *Combinatorial Species and Tree-Like Structures*
68 R. Goodman and N. Wallach *Representations and Invariants of the Classical Groups*
69 T. Beth, D. Jungnickel, and H. Lenz *Design Theory I, 2nd edn*
70 A. Pietsch and J. Wenzel *Orthonormal Systems for Banach Space Geometry*
71 G. E. Andrews, R. Askey and R. Roy *Special Functions*
72 R. Ticciati *Quantum Field Theory for Mathematicians*
73 M. Stern *Semimodular Lattices*
74 I. Lasiecka and R. Triggiani *Control Theory for Partial Differential Equations I*
75 I. Lasiecka and R. Triggiani *Control Theory for Partial Differential Equations II*
76 A. A. Ivanov *Geometry of Sporadic Groups I*
77 A. Schinzel *Polymomials with Special Regard to Reducibility*
78 H. Lenz, T. Beth, and D. Jungnickel *Design Theory II, 2nd edn*
79 T. Palmer *Banach Algebras and the General Theory of *-Algebras II*
80 O. Stormark *Lie's Structural Approach to PDE Systems*
81 C. F. Dunkl and Y. Xu *Orthogonal Polynomials of Several Variables*
82 J. P. Mayberry *The Foundations of Mathematics in the Theory of Sets*
83 C. Foias *et al.* *Navier–Stokes Equations and Turbulence*
84 B. Polster and G. Steinke *Geometries on Surfaces*
85 R. B. Paris and D. Kaminski *Asymptotics and Mellin–Barnes Integrals*
86 R. McEliece *The Theory of Information and Coding, 2nd edn*
87 B. Magurn *Algebraic Introduction to K-Theory*
88 T. Mora *Solving Polynomial Equation Systems I*
89 K. Bichteler *Stochastic Integration with Jumps*
90 M. Lothaire *Algebraic Combinatorics on Words*
91 A. A. Ivanov and S. V. Shpectorov *Geometry of Sporadic Groups II*
92 P. McMullen and E. Schulte *Abstract Regular Polytopes*
93 G. Gierz *et al.* *Continuous Lattices and Domains*
94 S. Finch *Mathematical Constants*
95 Y. Jabri *The Mountain Pass Theorem*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Solving Polynomial Equation Systems II

Macaulay's Paradigm and Gröbner Technology

TEO MORA
University of Genoa

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521811562

First published 2005

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

ISBN-13 978-0-521-81156-9 hardback
ISBN-10 0-521-81156-2 hardback

In the beginning was the Word, and the Word was with God, and the Word was God.
St John (Authorized Version)

God bless the girl who refuses to study algebra. It is a study that has caused many a girl to lose her soul.
Superintendent Francis of the Los Angeles schools.

The present state of our knowledge of the properties of Modular Systems is chiefly due to the fundamental theorems and processes of L. Kronecker, M. Noether, D. Hilbert, and E. Lasker, and above all to J. König's profound exposition and numerous extensions of Kronecker's theory. König's treatise might be regarded as in some measure complete if it were admitted that a problem is finished with when its solution has been reduced to a finite number of feasible operations. If however the operations are too numerous or too involved to be carried out in practice the solution is only a theoretical one; and its importance then lies not in itself, but in the theorems with which it is associated and to which it leads. Such a theoretical solution must be regarded as a preliminary and not the final stage in the consideration of the problem.
F. S. Macaulay, *The Algebraic Theory of Modular Systems*

Gauss is the perfect representative of the Thaurus mathematicians. Their style consists in performing long and numerous computations until this allows them to guess a conjecture, usually a correct one.
Theodyl Magus, *Astrology and Mathematics*

Contents

Preface		*page* xi
Setting		xiv
	Part three: Gauss, Euclid, Buchberger: Elementary Gröbner Bases	1
20	**Hilbert**	3
	20.1 Affine Algebraic Varieties and Ideals	3
	20.2 Linear Change of Coordinates	8
	20.3 Hilbert's Nullstellensatz	10
	20.4 *Kronecker Solver	15
	20.5 Projective Varieties and Homogeneous Ideals	22
	20.6 *Syzygies and Hilbert Function	28
	20.7 *More on the Hilbert Function	34
	20.8 Hilbert's and Gordan's Basissätze	36
21	**Gauss II**	46
	21.1 Some Heretical Notation	47
	21.2 Gaussian Reduction	51
	21.3 Gaussian Reduction and Euclidean Algorithm Revisited	63
22	**Buchberger**	72
	22.1 From Gauss to Gröbner	75
	22.2 Gröbner Basis	78
	22.3 Toward Buchberger's Algorithm	83
	22.4 Buchberger's Algorithm (1)	96
	22.5 Buchberger's Criteria	98
	22.6 Buchberger's Algorithm (2)	104
23	**Macaulay I**	109
	23.1 Homogenization and Affinization	110
	23.2 H-bases	114

23.3 Macaulay's Lemma 119
23.4 Resolution and Hilbert Function for Monomial Ideals 122
23.5 Hilbert Function Computation: the 'Divide-and-Conquer' Algorithms 136
23.6 H-bases and Gröbner Bases for Modules 138
23.7 Lifting Theorem 142
23.8 Computing Resolutions 146
23.9 Macaulay's Nullstellensatz Bound 152
23.10 *Bounds for the Degree in the Nullstellensatz 156
24 Gröbner I 170
24.1 Rewriting Rules 173
24.2 Gröbner Bases and Rewriting Rules 183
24.3 Gröbner Bases for Modules 188
24.4 Gröbner Bases in Graded Rings 195
24.5 Standard Bases and the Lifting Theorem 198
24.6 Hironaka's Standard Bases and Valuations 203
24.7 *Standard Bases and Quotients Rings 218
24.8 *Characterization of Standard Bases in Valuation Rings 223
24.9 Term Ordering: Classification and Representation 234
24.10 *Gröbner Bases and the State Polytope 247
25 Gebauer and Traverso 255
25.1 Gebauer–Möller and Useless Pairs 255
25.2 Buchberger's Algorithm (3) 264
25.3 Traverso's Choice 271
25.4 Gebauer–Möller's Staggered Linear Bases and Faugère's F_5 274
26 Spear 289
26.1 Zacharias Rings 291
26.2 Lexicographical Term Ordering and Elimination Ideals 300
26.3 Ideal Theoretical Operation 304
26.4 *Multivariate Chinese Remainder Algorithm 313
26.5 Tag-Variable Technique and Its Application to Subalgebras 316
26.6 Caboara–Traverso Module Representation 321
26.7 *Caboara Algorithm for Homogeneous Minimal Resolutions 329

	Part four: Duality		333
27	**Noether**		335
	27.1	Noetherian Rings	337
	27.2	Prime, Primary, Radical, Maximal Ideals	340
	27.3	Lasker–Noether Decomposition: Existence	345
	27.4	Lasker–Noether Decomposition: Uniqueness	350
	27.5	Contraction and Extension	356
	27.6	Decomposition of Homogeneous Ideals	364
	27.7	*The Closure of an Ideal at the Origin	368
	27.8	Generic System of Coordinates	371
	27.9	Ideals in Noether Position	374
	27.10	*Chains of Prime Ideals	378
	27.11	Dimension	380
	27.12	Zero-dimensional Ideals and Multiplicity	384
	27.13	Unmixed Ideals	390
28	**Möller I**		393
	28.1	Duality	393
	28.2	Möller Algorithm	401
29	**Lazard**		414
	29.1	The FGLM Problem	415
	29.2	The FGLM Algorithm	418
	29.3	Border Bases and Gröbner Representation	426
	29.4	Improving Möller's Algorithm	432
	29.5	Hilbert Driven and Gröbner Walk	440
	29.6	*The Structure of the Canonical Module	444
30	**Macaulay II**		451
	30.1	The Linear Structure of an Ideal	452
	30.2	Inverse System	456
	30.3	Representing and Computing the Linear Structure of an Ideal	461
	30.4	Noetherian Equations	466
	30.5	Dialytic Arrays of $M^{(r)}$ and Perfect Ideals	478
	30.6	Multiplicity of Primary Ideals	492
	30.7	The Structure of Primary Ideals at the Origin	494
31	**Gröbner II**		500
	31.1	Noetherian Equations	501
	31.2	Stability	502
	31.3	Gröbner Duality	504
	31.4	Leibniz Formula	508
	31.5	Differential Inverse Functions at the Origin	509
	31.6	Taylor Formula and Gröbner Duality	512

32 Gröbner III 517
- 32.1 Macaulay Bases 518
- 32.2 Macaulay Basis and Gröbner Representation 521
- 32.3 Macaulay Basis and Decomposition of Primary Ideals 522
- 32.4 Horner Representation of Macaulay Bases 527
- 32.5 Polynomial Evaluation at Macaulay Bases 531
- 32.6 Continuations 533
- 32.7 Computing a Macaulay Basis 542

33 Möller II 549
- 33.1 Macaulay's Trick 550
- 33.2 The Cerlienco–Mureddu Correspondence 554
- 33.3 Lazard Structural Theorem 560
- 33.4 Some Factorization Results 562
- 33.5 Some Examples 569
- 33.6 An Algorithmic Proof 574

Part five: Beyond Dimension Zero 583

34 Gröbner IV 585
- 34.1 Nulldimensionalen Basissätze 586
- 34.2 Primitive Elements and Allgemeine Basissatz 593
- 34.3 Higher-Dimensional Primbasissatz 598
- 34.4 Ideals in Allgemeine Positions 601
- 34.5 Solving 605
- 34.6 Gianni–Kalkbrener Theorem 608

35 Gianni–Trager–Zacharias 614
- 35.1 Decomposition Algorithms 615
- 35.2 Zero-dimensional Decomposition Algorithms 616
- 35.3 The GTZ Scheme 622
- 35.4 Higher-dimensional Decomposition Algorithms 631
- 35.5 Decomposition Algorithms for Allgemeine Ideals 634
  - 35.5.1 Zero-dimensional Allgemeine Ideals 634
  - 35.5.2 Higher-dimensional Allgemeine Ideals 637
- 35.6 Sparse Change of Coordinates 640
  - 35.6.1 Gianni's Local Change of Coordinates 641
  - 35.6.2 Giusti–Heintz Coordinates 645
- 35.7 Linear Algebra and Change of Coordinates 650
- 35.8 Direct Methods for Radical Computation 654
- 35.9 Caboara–Conti–Traverso Decomposition Algorithm 658
- 35.10 Squarefree Decomposition of a Zero-dimensional Ideal 660

36 Macaulay III 665
36.1 Hilbert Function and Complete Intersections 666
36.2 The Coefficients of the Hilbert Function 670
36.3 Perfectness 678
37 Galligo 686
37.1 Galligo Theorem (1): Existence of Generic Escalier 686
37.2 Borel Relation 697
37.3 *Galligo Theorem (2): the Generic Initial Ideal is Borel Invariant 706
37.4 *Galligo Theorem (3): the Structure of the Generic Escalier 710
37.5 Eliahou–Kervaire Resolution 714
38 Giusti 725
38.1 The Complexity of an Ideal 726
38.2 Toward Giusti's Bound 728
38.3 Giusti's Bound 733
38.4 Mayr and Meyer's Example 735
38.5 Optimality of Revlex 741

Bibliography 749
Index 758

Preface

If you HOPE that this second *SPES* volume preserves the style of the previous volume, you will not be disappointed: in fact it maintains a self-contained approach using only undergraduate mathematics in this introduction to elementary commutative ideal theory and to its computational aspects,[1] while my *horror vacui* compelled me to report nearly all the relevant results in computational algebraic geometry that I know about.

When the commutative algebra community was exposed, in 1979, to Buchberger's theory and algorithm (dated 1965) of Gröbner bases[2], the more alert researchers, mainly Schreyer and Bayer, immediately realized that this injection of Gröbner technology was all one needed to make effective Macaulay's paradigm for reducing computational problems for ideals either to the corresponding combinatorial problem for monomials[3] or to a more elementary linear algebraic computation.[4] This realization gave to researchers a straightforward approach which led them, within more or less fifteen years, to completely effectivize commutative ideal theory.

This second volume of *SPES* is an eyewitness report on this successful introduction of effective methods to algebraic geometry.

Part three, *Gauss, Euclid, Buchberger: Elementary Gröbner Bases*, introduces at the same time Buchberger's theory of Gröbner bases, his algorithm for computing them and Macaulay's paradigm.

While I will discuss in depth both of the classical main approaches to the introduction of Gröbner bases – their relation with rewriting rules and the

[1] Up to the point that some results whose proof requires knowldge in advanced commutative algebra are simply quoted, pointing only to the original proof.
[2] And to the independent discovery by Spear.
[3] The computation of the Hilbert function by means of Macaulay's Lemma (Corollary 23.4.3).
[4] Macaulay's notion of H-basis (Definition 23.2.1) and his related lifting theorem (Theorem 23.7.1) transformed by Schreyer as the tool for computing resolution.

Knuth–Bendix Algorithm, and their connection with Macaulay's H-bases and Hironaka's standard bases as tools for lifting properities to a polynomial algebra from its graded algebra – my presentation stresses the relation of both the notion and the algorithm to elementary linear algebra and Gaussian reduction; an added bonus of this approach is the ability to link Buchberger's algorithm with the most recent alternative linear algebra approach proposed by Faugère.

The discussion of Buchberger's algorithm aims to present what essentially is its 'standard' structure as can be found in most good implementations.

In the same mood, the discussion of Macaulay's paradigm is illustrated by showing how Gröbner bases can be applied in order to successfully compute the Hilbert function and the minimal resolution of a finitely generated polynomial ideal and to present the most effective algorithmic solutions.

This part also includes Spear's tag-variable technique, its application in effectively performing ideal operations (intersection, quotient, colon, saturation), Sweedler's application of them to the study of subalgebras, Erdos's characterization of term orderings, the Bayer–Morrison analysis of the state polytope and the Gröbner fan of an ideal.

The next chapter, *Noether*, is the keystone of the book: it introduces the terminology and preliminary results needed to discuss multivariate 'solving': the Lasker–Noether decomposition theory, extension/contraction of decomposition, the notions of dimension and multiplicity, the Kredel–Weispfenning algorithm for computing dimension.

Part four, *Duality*, discusses linear algebra tools for describing and computing the multiplicity of both $\mathfrak{m}$-primary and $\mathfrak{m}$-closed ideals, $\mathfrak{m}$ being the maximal at the origin; this includes Möller's algorithm, its application to solve the FGLM-problem, the Cerlienco–Mureddu algorithm, and the linear algebra structure of configurations of points; but the main section of this part is a careful presentation of Macaulay's results on inverse systems and a recent algorithm which computes the inverse system of any $\mathfrak{m}$-primary ideal given by any basis.

Part five, *Beyond Dimension Zero*, begins with a discussion of Gröbner's *Basissätze* which describe the structure of lexicographical Gröbner bases of prime, primary and radical ideals and their ultimate generalization, Gianni–Kalkbrener's Theorem; this allows us to specify what it means to 'solve' a multi-dimensional ideal and introduces the decomposition algorithms.

This part also discusses Macaulay's results on Hilbert functions and perfectness, Galligo's theorem, and Giusti's analysis of the complexity of Gröbner bases.

As *congedo* I chose the most elegant result within computational commutative algebra, the Bayer and Stillman proof of the optimality of degrevlex orderings.

It being my firm belief that the best way of understanding a theory and an algorithm is to verify it through a computation, as in the previous volume, the crucial points of the most relevant algorithms are illustrated by examples, all developed via paper-and-pencil computations; readers are encouraged to follow them and, better, to test their own examples.

In order to help readers to plan their journey through this book, some sections containing only some interesting digressions are indicated by asterisks in the table of contents.

A possible short cut which allows readers to appreciate the discussion, without becoming too bored by the details, is Chapters 20–23, 26–28, 34–35.

I wish to thank Miguel Angel Borges Tranard, Maria Pia Cavaliere, Francesca Cioffi and Franz Pauel for their help, but I feel strongly indebted to Maria Grazia Marinari for her steady support. Also I need to thank all the friends with whom I have shared this exciting adventure of algorithmizing commutative algebra.

Setting

1. Let k be an infinite, perfect field, where, if $p := \text{char}(k) \neq 0$, it is possible to extract pth roots,[1] and let k be the algebraic closure of k. Let us fix an integer value n and consider the polynomial ring

$$\mathcal{P} := k[X_1, \ldots, X_n]$$

and its k-basis

$$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}.$$

2. We also fix an integer value $r \leq n$ and consider

the ring $K := k(X_{r+1}, \ldots, X_n)$,
the polynomial ring $\mathcal{Q} := K[X_1, \ldots, X_r]$ and
its k-basis $\mathcal{W} := \{X_1^{a_1} \cdots X_r^{a_r} : (a_1, \ldots, a_r) \in \mathbb{N}^r\}$.

All the notation introduced will also be applied in this setting, substituting everywhere $n, k, \mathcal{P}, \mathcal{T}$ with, respectively, $r, K, \mathcal{Q}, \mathcal{W}$.

3. For each $d \in \mathbb{N}$ we will set

$$\mathcal{T}_d := \{t \in \mathcal{T} : \deg(t) = d\} \text{ and } \mathcal{T}(d) := \{t \in \mathcal{T} : \deg(t) \leq d\}.$$

4. Where we need to use the set of the terms generated by some subsets of variables, we denote for each $i, j, 1 \leq i < j \leq n, \mathcal{T}[i, j]$ the monomials generated by $X_i, \ldots, X_j$,

$$\mathcal{T}[i, j] = \left\{X_i^{a_i} \cdots X_j^{a_j} : (a_i, \ldots, a_j) \in \mathbb{N}^{j-i+1}\right\},$$

[1] This is the general setting considered in this the volume, except for Chapters 37 and 38 where moreover $\text{char}(k) = 0$.
These restrictions can be relaxed in most of the volume, but, knowing my absentmindedness, I consider it safer to leave to the reader the responsibility of doing so.

and $\mathcal{T}[i, j]_d$ (respectively $\mathcal{T}[i, j](d)$) denotes those terms whose degree is equal to (respectively bounded by) d.

5. Each polynomial $f \in k[X_1, \dots, X_n]$ is therefore a unique linear combination

$$f = \sum_{t \in \mathcal{T}} c(f, t)t$$

of the terms $t \in \mathcal{T}$ with coefficients $c(f, t)$ in k and can be uniquely decomposed, by setting

$$f_\delta := \sum_{t \in \mathcal{T}_\delta} c(f, t)t, \text{ for each } \delta \in \mathbb{N},$$

as $f = \sum_{\delta=0}^{d} f_\delta$ where each f_δ is homogeneous, $\deg(f_\delta) = \delta$ and $f_d \neq 0$ so that $d = \deg(f)$.

6. Since, for each i, $1 \le i \le n$,

$$\mathcal{P} = k[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i],$$

each polynomial $f \in \mathcal{P}$ can be uniquely expressed as

$$f = \sum_{j=0}^{D} h_j(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n)X_i^j, h_D \neq 0,$$

and

$$\deg_{X_i}(f) := \deg_i(f) := D$$

denotes its degree in the variable X_i.

In particular $(i = n)$

$$f = \sum_{j=0}^{D} h_j(X_1, \dots, X_{n-1})X_n^j, h_D \neq 0, D = \deg_n(f);$$

the *leading polynomial* of f is $\mathrm{Lp}(f) := h_d$, and its *trailing polynomial* is $\mathrm{Tp}(f) := h_0$.

7. The support $\{t \in \mathcal{T} : c(f, t) \neq 0\}$ of f being finite, once a term ordering $<$ on $\mathcal{T}$ is fixed, f has a unique representation as an ordered linear combination of terms:

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in k \setminus 0, t_i \in \mathcal{T}, t_1 > \cdots > t_s.$$

The *maximal term* of f is $\mathbf{T}(f) := t_1$, its *leading coefficient* is $\mathrm{lc}(f) := c(f, t_1)$ and its *maximal monomial* is $\mathbf{M}(f) := c(f, t_1)t_1$.

8. For any set $F \subset \mathcal{P}$ we denote

- $\mathbf{T}_<\{F\} := \{\mathbf{T}(f) : f \in F\}$;
- $\mathbf{T}_<(F) := \{\tau\mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\}$;
- $\mathbf{N}_<(F) := \mathcal{T} \setminus \mathbf{T}_<(F)$;
- $k[\mathbf{N}_<(F)] := \mathrm{Span}_k(\mathbf{N}_<(F))$

and we will usually omit the dependence on $<$ if there is no ambiguity.

9. Each series $f \in k[[X_1, \ldots, X_n]]$ is a unique (infinite) linear combination

$$f = \sum_{t \in \mathcal{T}} c(f, t)t$$

of the terms $t \in \mathcal{T}$ with coefficients $c(f, t)$ in k; for any subset $\mathbf{N} \subset \mathcal{T}$ we will also write the subring

$$k[[\mathbf{N}]] := \left\{ \sum_{t \in \mathbf{N}} c(f, t)t \right\} \subset k[[X_1, \ldots, X_n]].$$

10. For each $f, g \in \mathcal{P}$ such that $\mathrm{lc}(f) = 1 = \mathrm{lc}(g)$, we denote

$$S(g, f) := \frac{\mathrm{lcm}(\mathbf{T}(f), \mathbf{T}(g))}{\mathbf{T}(f)} f - \frac{\mathrm{lcm}(\mathbf{T}(f), \mathbf{T}(g))}{\mathbf{T}(g)} g.$$

For any enumerated set $\{g_1, \ldots, g_s\} \subset \mathcal{P}$, such that $\mathrm{lc}(g_i) = 1$ for each i, we write $\mathbf{T}(i) := \mathbf{T}(g_i)$ and, for each i, j, $1 \le i < j \le s$

$$\mathbf{T}(i, j) := \mathrm{lcm}\,(\mathbf{T}(i), \mathbf{T}(j))\,,$$
$$S(i, j) := S(g_i, g_j) := \frac{\mathbf{T}(i, j)}{\mathbf{T}(j)} g_j - \frac{\mathbf{T}(i, j)}{\mathbf{T}(i)} g_i.$$

11. For any field k the (n-dimensional) *affine space* over k, k^n, is the set

$$k^n := \{(a_1, \ldots, a_n), a_i \in k\};$$

and we will denote by $\mathbf{0} \in k^n$ the point $\mathbf{0} := (0, \ldots, 0)$ and $\mathsf{m} := (X_1, \ldots, X_n)$ the maximal ideal at $\mathbf{0}$.

12. We associate

- to any set $F \subset \mathcal{P}$, the algebraic affine variety $\mathcal{Z}(F)$ consisting of each common root of all polynomials in F:

$$\mathcal{Z}(F) := \{\mathsf{a} \in \mathsf{k}^n : f(\mathsf{a}) = 0, \text{ for all } f \in F\} \subset \mathsf{k}^n;$$

- and to any set $\mathsf{Z} \subset \mathsf{k}^n$, the ideal $\mathcal{I}(\mathsf{Z})$ of all the polynomials vanishing in Z:

$$\mathcal{I}(\mathsf{Z}) := \{f \in \mathcal{P} : f(\mathsf{a}) = 0, \text{ for all } \mathsf{a} \in \mathsf{Z}\} \subset \mathcal{P}.$$

13. For any finite set $F := \{f_1, \ldots, f_s\} \subset \mathcal{P}$ the ideal generated by F is denoted by (F) or $(f_1, \ldots, f_s)$ and is the set

$$(F) := (f_1, \ldots, f_s) := \left\{ \sum_{i=1}^{s} h_i f_i : h_i \in \mathcal{P} \right\}.$$

14. For an ideal $\mathfrak{f} \subset \mathcal{P}$,

$$\mathfrak{f} := \bigcap_{i=1}^{r} \mathfrak{q}_i$$

denotes an irredundant primary representation; for each i, $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ is the associated prime and $\delta(i) := \dim(\mathfrak{q}_i)$ is the dimension of the primary $\mathfrak{q}_i$.

15. For any field k and any $n \in \mathbb{N}$ we will denote by $C(n, k)$ the n-tuples of non-zero elements in k:

$$C(n, k) := \{(c_1, \ldots, c_n) \in k^n, c_i \neq 0, \text{ for each } i\}.$$

For each $\mathsf{c} := (c_1, \ldots, c_\nu) \in C(\nu, k)$, we denote by

$$L_{\mathsf{c}} : k[X_1, \ldots, X_\nu] \to k[X_1, \ldots, X_\nu]$$

the map defined by

$$L_{\mathsf{c}}(X_i) := \begin{cases} X_i + c_i X_\nu & \text{if } i < \nu, \\ c_\nu X_\nu & \text{if } i = \nu. \end{cases}$$

16. A term ordering[2] of the semigroup $\mathcal{T}$ is called *degree compatible* if for each $t_1, t_2 \in \mathcal{T}$

$$\deg(t_1) < \deg(t_2) \implies t_1 < t_2.$$

The semigroup $\mathcal{T}$ will be usually well-ordered by means of

- the *lexicographical ordering* induced by $X_1 < X_2 < \cdots < X_n$, which is defined by:

$$X_1^{a_1} \ldots X_n^{a_n} < X_1^{b_1} \ldots X_n^{b_n} \iff \exists j : a_j < b_j \text{ and } a_i = b_i \text{ for } i > j;$$

- the *degrevlex ordering* induced by $X_1 < X_2 < \cdots < X_n$, which is the degree-compatible term ordering under which any two terms having the same degree are compared according to

$$X_1^{a_1} \ldots X_n^{a_n} < X_1^{b_1} \ldots X_n^{b_n} \iff \exists j : a_j > b_j \text{ and } a_i = b_i \text{ for } i < j.$$

[2] That is a well-ordering and a semigroup ordering.

17. Let $<$ be a term ordering on $\mathcal{T}$, and $\mathsf{I} \subset \mathcal{P}$ an ideal, and $\mathsf{A} := \mathcal{P}/\mathsf{I}$.
Then, since $\mathsf{A} \cong k[\mathbf{N}_<(\mathsf{I})]$, for each $f \in \mathcal{P}$, there is a unique

$$g := \mathrm{Can}(f, \mathsf{I}, <) = \sum_{t \in \mathbf{N}_<(\mathsf{I})} \gamma(f, t, <)t$$

such that

$$g \in k[\mathbf{N}(\mathsf{I})] \text{ and } f - g \in \mathsf{I}.$$

18. More generally, if $\mathsf{I} \subset \mathcal{P}$ is an ideal, and $\mathbf{q} = \{q_1, \ldots, q_s\}$ is a linearly independent set such that $\mathcal{P}/\mathsf{I} = \mathrm{Span}_k(\mathbf{q})$, then, for each $f \in \mathcal{P}$, there is a unique vector

$$\mathbf{Rep}(f, \mathbf{q}) := (\gamma(f, q_1, \mathbf{q}), \ldots, \gamma(f, q_s, \mathbf{q})) \in k^s$$

which satisfies

$$f - \sum_j \gamma(f, q_j, \mathbf{q}) q_j \in \mathsf{I}.$$

In particular, if $\mathbf{N}_<(\mathsf{I}) = \{\tau_1, \ldots, \tau_s\}$, we have, for each $f \in \mathcal{P}$,

$$\gamma(f, t, \mathbf{N}_<(\mathsf{I})) = \gamma(f, t, <), \text{ for each } t \in \mathbf{N}_<(\mathsf{I}),$$

$$\mathbf{Rep}(f, \mathbf{N}_<(\mathsf{I})) := (\gamma(f, \tau_1, <), \ldots, \gamma(f, \tau_s, <)) \in k^s.$$

19. In the same setting,

$$\mathcal{M}(\mathbf{q}) := \left\{ \left(a_{lj}^{(h)}\right) \in k^{s^2}, 1 \le h \le n \right\}$$

denotes the set of the square matrices defined by the equalities

$$X_h q_l = \sum_j a_{lj}^{(h)} q_j, \text{ for each } l, j, h, \ 1 \le l, \ j \le s, \ 1 \le h \le n,$$

in $\mathcal{P}/\mathsf{I} = \mathrm{Span}_k(\mathbf{q})$.

20. In general, when we need to discuss homogenization of polynomials, we will use the notation ${}^h\mathcal{P} := k[X_0, X_1, \ldots, X_n]$ and

$${}^h\mathcal{T} := \left\{ X_0^{a_0} X_1^{a_1} \cdots X_n^{a_n} : (a_0, a_1, \ldots, a_n) \in \mathbb{N}^{n+1} \right\}.$$

The homogenization/affinization maps are denoted

$${}^h- : \mathcal{P} \to {}^h\mathcal{P} \text{ and } {}^a- : {}^h\mathcal{P} \to \mathcal{P}$$

and defined by

$$
\begin{aligned}
{}^h f(X_1, \ldots, X_n) &:= X_0^{\deg(f)} f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right), \\
{}^a f(X_0, X_1, \ldots, X_n) &:= f(1, X_1, \ldots, X_n).
\end{aligned}
$$

For any term ordering $<$ on $\mathcal{T}$ the *homogenization* of $<$ is the term-ordering $<_h$ on ${}^h\mathcal{T}$ defined by

$$t_1 <_h t_2 \iff \deg(t_1) < \deg(t_2) \text{ or } \deg(t_1) = \deg(t_2) \text{ and } {}^a t_1 < {}^a t_2.$$

21. For an ideal $\mathsf{I} \subset \mathcal{P}$ we will denote $H(T; \mathsf{I})$ its Hilbert function; $H_{\mathsf{I}}(T)$ its Hilbert polynomial, which we will represent as

$$H_{\mathsf{I}}(T) = k_0(\mathsf{I})\binom{T+d}{d} + k_1(\mathsf{I})\binom{T+d-1}{d-1} + \cdots + k_{d-1}(\mathsf{I})(T+1) + k_d(\mathsf{I});$$

and $\mathfrak{H}(\mathsf{I}, T)$ its Hilbert series.

22. For a free-module $\mathcal{P}^m$, we usually denote $\{e_1, \ldots, e_m\}$ its canonical basis and

$$
\begin{aligned}
\mathcal{T}^{(m)} &= \{te_i, t \in \mathcal{T}, 1 \le i \le m\} \\
&= \{X_1^{a_1} \cdots X_n^{a_n} e_i, (a_1, \ldots, a_n) \in \mathbb{N}^n, 1 \le i \le m\}
\end{aligned}
$$

its monomial k-basis.

23. The free-module $\mathcal{P}^m$ is transformed into an $\mathbb{N}$-graded module by assigning, for each i, a degree $\deg(e_i) := d_i$ and considering each element $(g_1, \ldots, g_m) \in \mathcal{P}^m$ to be homogeneous of degree R if and only if each g_i will be either 0 or a homogeneous polynomial of degree $R - d_i$.

Therefore each element $f \in \mathcal{P}^m$ can be uniquely decomposed as $f = \sum_{i=1}^d f_i$ where each $f_i \in \mathcal{P}^m$ is homogeneous of degree i and $d = \deg(f)$

In a similar way, $\mathcal{P}^m$ is also transformed into a $\mathcal{T}$-graded module by

- assigning a term ordering $<$ on $\mathcal{T}$ and a term $\omega_i \in \mathcal{T}$ to each e_i,
- defining

$$\mathcal{T}\text{-deg} : \mathcal{T}^{(m)} \to \mathcal{T} \text{ by } \mathcal{T}\text{-deg}(te_i) = t\omega_i,$$

- and $\mathcal{T}$-deg : $\mathcal{P}^{(m)} \to \mathcal{T}$ as

$$\mathcal{T}\text{-deg}(f) := \max_{<}\{\mathcal{T}\text{-deg}(\tau) : c(f, \tau) \neq 0\}$$

for each $f = \sum_{\tau \in \mathbf{T}^{(m)}} c(f, \tau)\tau \in \mathcal{P}^{(m)}$,

- considering $\mathcal{T}$-homogeneous of $\mathcal{T}$-degree ω any element $(\gamma_1, \ldots, \gamma_m) \in \mathcal{P}^m$ such that for each i

$$\gamma_i \in \mathcal{T}, \text{ and } \gamma_i \omega_i = \omega \text{ unless } \gamma_i = 0.$$

Each element $f \in \mathcal{P}^m$ can therefore be uniquely decomposed as $f = \sum_{t \in \mathcal{T}} f_t$ where each $f_t \in \mathcal{P}^m$ is $\mathcal{T}$-homogeneous of $\mathcal{T}$-degree t.

If we fix a well-ordering $\prec$ on $\mathcal{T}^{(m)}$ which is compatible with a term-ordering $<$ on $\mathcal{T}$ that is satisfying

$$t_1 \leq t_2, \tau_1 \preceq \tau_2 \implies t_1 \tau_1 \preceq t_2 \tau_2,$$

for each $t_1, t_2 \in \mathcal{T}$, $\tau_1, \tau_2 \in \mathcal{T}^{(m)}$ then for each $f = \sum_{\tau \in \mathbf{T}^{(m)}} c(f, \tau)\tau \in \mathcal{P}^{(m)}$, its *maximal term* is the term $\mathbf{T}(f) := \max_{\prec}\{\tau : c(f, \tau) \neq 0\}$; its *leading coefficient* is $\operatorname{lc}(f) := c(f, \mathbf{T}(f))$ and its *maximal monomial* is $\mathbf{M}(f) := \operatorname{lc}(f)\mathbf{T}(f)$.

24. Usually a free resolution of a $\mathcal{P}$-module M will be denoted

$$0 \to \mathcal{P}^{r_\rho} \xrightarrow{\delta_\rho} \mathcal{P}^{r_{\rho-1}} \xrightarrow{\delta_{\rho-1}} \ldots \mathcal{P}^{r_{i+1}} \xrightarrow{\delta_{i+1}} \mathcal{P}^{r_i} \xrightarrow{\delta_i} \mathcal{P}^{r_{i-1}} \ldots \mathcal{P}^{r_1} \xrightarrow{\delta_1} \mathcal{P}^{r_0} \xrightarrow{\delta_0} M \tag{0.1}$$

25. We will denote

- by $GL(n, k)$ the *general linear group*, that is the set of all invertible $n \times n$ square matrices with entries in k,
- by $B(n, k) \subset GL(n, k)$ the *Borel group* of the upper triangular matrices $\mathsf{M} := (c_{ij})$, that is those such that $i > j \implies c_{ij} = 0$,
- by $N(n, k) \subset B(n, k)$ the subgroup of the upper triangular unipotent matrices $\mathsf{M} := (c_{ij})$, that is those such that

$$i > j \implies c_{ij} = 0, \quad \text{and} \quad i = j \implies c_{ij} = 1.$$

We will use the shorthand $k[X_{ij}]$ and $k(X_{ij})$ to denote, respectively, the polynomial ring generated over k by the variables

$$\{X_{ij}, 1 \leq i \leq n, 1 \leq j \leq n\}$$

and its rational function field.

Any matrix

$$M := (c_{ij}) \in GL(n, k)$$

describes the linear transformation

$$M : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]$$

defined by

$$M(X_i) = \sum_j c_{ij} X_j \text{ for each } i.$$

If we also write for each i,

$$Y_i := M(X_i) = \sum_j c_{ij} X_j,$$

we obtain a system of coordinates $\{Y_1, \ldots, Y_n\}$ and a corresponding change of coordinates

$$k[Y_1, \ldots, Y_n] = k[X_1, \ldots, X_n]$$

which is defined by

$$f(X_1, \ldots, X_n) = f\left(\sum_i d_{1i} Y_i, \ldots, \sum_i d_{ni} Y_i\right) \in k[Y_1, \ldots, Y_n],$$

where

$$\left(d_{ij}\right) = M^{-1} \in GL(n, k),$$

denotes the inverse of M.

26. The module $\mathcal{P}^* := \mathrm{Hom}_k(\mathcal{P}, k)$ denotes the k-vector space of all k-linear functionals $\ell : \mathcal{P} \to k$.

Each k-linear functional $\ell : \mathcal{P} \to k$ can be encoded by means of the series

$$\sum_{t \in \mathcal{T}} \ell(t)t \in k[[X_1, \ldots, X_n]]$$

in such a way that to each such series $\sum_{t\in\mathcal{T}} \gamma(t)t \in k[[X_1, \ldots, X_n]]$ is associated the k-linear functional $\ell \in \mathcal{P}^*$ defined, on each polynomial $f = \sum_{t\in\mathcal{T}} c(f, t)t$, by

$$\ell(f) := \sum_{t \in \mathbf{T}} c(f, t)\gamma(t).$$

Module $\mathcal{P}^*$ has a natural structure as $\mathcal{P}$-module, which is obtained by defining, for each $\ell \in \mathcal{P}^*$ and $f \in \mathcal{P}$, $(\ell \cdot f) \in \mathcal{P}^*$ as

$$(\ell \cdot f)(g) := \ell(fg), \text{ for each } g \in \mathcal{P}.$$

27. For each k-vector subspace $L \subset \mathcal{P}^*$, let

$$\mathfrak{P}(L) := \{g \in \mathcal{P} : \ell(g) = 0, \forall \ell \in L\}$$

and for each k-vector subspace $P \subset \mathcal{P}$, let

$$\mathfrak{L}(P) := \{\ell \in \mathcal{P}^* : \ell(g) = 0, \forall g \in P\}.$$

28. For each $\tau \in \mathcal{W}$, $M(\tau) : \mathcal{Q} \to K$ denotes the morphism defined by

$$M(\tau) = c(f, \tau) \text{ for each } f = \sum_{t \in \mathcal{W}} c(f, t)t \in \mathcal{Q}$$

and set

$$\mathbb{M} := \{M(\tau) : \tau \in \mathcal{W}\} \subset \mathcal{Q}^*,$$

and

$$\nabla_\rho := \mathrm{Span}_K \left(M(\tau)(\cdot) : \tau \in \mathcal{W}(\rho)\right),$$

for each $\rho \in \mathbb{N}$.

For each K-vector subspace $\Lambda \subset \mathrm{Span}_K(\mathbb{M})$, let

$$\mathfrak{I}(\Lambda) := \mathfrak{P}(\Lambda) = \{f \in \mathcal{Q} : \ell(f) = 0, \text{ for each } \ell \in \Lambda\}$$

and, for each K-vector subspace $P \subset \mathcal{Q}$, let

$$\mathfrak{M}(P) := \mathfrak{L}(P) \cap \mathrm{Span}_K(\mathbb{M}) = \{\ell \in \mathrm{Span}_K(\mathbb{M}) : \ell(f) = 0, \text{ for each } f \in P\}.$$