

# References

- [Act] F. Acton. *Numerical Methods That Work*, MAA, Washington DC, 1990.
- [AL] W. Adams and P. Loustanaunau. *An Introduction to Gröbner Bases*, AMS, Providence RI, 1994.
- [ASW] P. Alfeld, L. Schumaker and W. Whiteley. *The generic dimension of the space of  $C^1$  splines of degree  $d \geq 8$  on tetrahedral decompositions*, SIAM J. Numerical Analysis **30** (1993), 889–920.
- [AG] E. Allgower and K. Georg. *Numerical Continuation Methods*, Springer-Verlag, New York, 1990.
- [AMR] M. Alonso, T. Mora and M. Raimondo. *A computational model for algebraic power series*, J. Pure Appl. Algebra **77** (1992), 1–38.
- [AGK] B. Amrhein, O. Gloor and W. Küchlin. *On the walk*, Theoretical Computer Science **187** (1997), 179–202.
- [AGV] V. Arnold, S. Gusein-Zade and V. Varchenko. *Singularities of Differential Maps, Volumes 1 and 2*, Birkhäuser, Boston, 1985 and 1988.
- [Art] M. Artin. *Algebra*, Prentice-Hall, Englewood Cliffs NJ, 1991.
- [AS] W. Auzinger and H. J. Stetter. *An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations*, in: *Numerical Mathematics (Singapore 1988)*, Internat. Ser. Numer. Math., **86**, Birkhäuser, Basel, 1988, 11–30.
- [BGW] C. Bajaj, T. Garrity and J. Warren. *On the applications of multi-equational resultants*, Technical Report CSD-TR-826, Department of Computer Science, Purdue University, 1988.
- [BC] V. Batyrev and D. Cox. *On the Hodge structure of projective hypersurfaces*, Duke Math. J. **75** (1994), 293–338.
- [BaM] D. Bayer and I. Morrison. *Gröbner bases and geometric invariant theory I*, J. Symbolic Comput. **6** (1988), 209–217.
- [BW] T. Becker and V. Weispfenning. *Gröbner Bases*, Springer-Verlag, New York, 1993.
- [BKR] M. Ben-Or, D. Kozen and J. Reif. *The complexity of elementary algebra and geometry*, J. of Computation and Systems **32** (1986), 251–264.
- [Ber] D. Bernstein. *The number of roots of a system of equations*, Functional Anal. Appl. **9** (1975), 1–4.

- [Bet] U. Betke. *Mixed volumes of polytopes*, Archiv der Mathematik **58** (1992), 388–391.
- [BLR] A. Bigatti, R. LaScala and L. Robbiano. *Computing toric ideals*, J. Symbolic Comput. **27** (1999), 351–365.
- [BU] P. Bikker and A. Yu. Uteshev. *On the Bézout construction of the resultant*, J. Symbolic Comput. **28** (1999), 45–88.
- [Bil1] L. Billera. *Homology of smooth splines: Generic triangulations and a conjecture of Strang*, Trans. Amer. Math. Soc. **310** (1988), 325–340.
- [Bil2] L. Billera. *The algebra of continuous piecewise polynomials*, Adv. Math. **76** (1989), 170–183.
- [BR1] L. Billera and L. Rose. *Groebner Basis Methods for Multivariate Splines*, in: *Mathematical Methods in Computer Aided Geometric Design* (T. Lyche and L. Schumaker, eds.), Academic Press, Boston, 1989, 93–104.
- [BR2] L. Billera and L. Rose. *A Dimension Series for Multivariate Splines*, Discrete Comp. Geom. **6** (1991), 107–128.
- [BR3] L. Billera and L. Rose. *Modules of piecewise polynomials and their freeness*, Math. Z. **209** (1992), 485–497.
- [BS] L. Billera and B. Sturmfels, *Fiber polytopes*, Ann. of Math. **135** (1992), 527–549.
- [Bla] R. Blahut. *Theory and Practice of Error Control Codes*, Addison Wesley, Reading MA, 1984.
- [BMP] D. Bondyfalat, B. Mourrain and V. Y. Pan. *Solution of polynomial system of equations via the eigenvector computation*, Linear Algebra Appl. **319** (2000), 193–209.
- [BoF] T. Bonnesen and W. Fenchel. *Theorie der konvexen Körper*, Chelsea, New York, 1971 and Springer-Verlag, New York, 1974.
- [BH] W. Bruns and J. Herzog. *Cohen-Macaulay Rings*, Cambridge U. Press, Cambridge, revised edition, 1998.
- [Bry] V. Bryant. *Aspects of Combinatorics*, Cambridge U. Press, Cambridge, 1993.
- [BuM] B. Buchberger and H. M. Möller. *The construction of multivariate polynomials with preassigned zeros*, in: *Computer algebra (Marseille, 1982)*, Lecture Notes in Computer Science **144**, Springer, Berlin, New York, 1982, 24–31.
- [BE] D. Buchsbaum and D. Eisenbud. *Algebra structures for finite free resolutions and some structure theorems for ideals of codimension 3*, Amer. J. Math. **99** (1977), 447–485.
- [BZ] Yu. Burago and V. Zalgaller, *Geometric Inequalities*, Springer-Verlag, New York, 1988.
- [BuF] R. Burden and J. Faires. *Numerical Analysis*, 5th edition, PWS Publishing, Boston, 1993.
- [Bus] L. Busé. *Residual resultant over the projective plane and the implicitization problem*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 2001, 48–55.

- [BEM1] L. Busé, M. Elkadi and B. Mourrain. *Generalized resultants over unirational algebraic varieties*, J. Symbolic Comput. **29** (2000), 515–526.
- [BEM2] L. Busé, M. Elkadi and B. Mourrain. *Resultant over the residual of a complete intersection*, J. Pure Appl. Algebra **164** (2001), 35–57.
- [Can1] J. Canny. *Generalised characteristic polynomials*, J. Symbolic Comput. **9** (1990), 241–250.
- [Can2] J. Canny. *Some algebraic and geometric computations in PSPACE*, in: *Proc. 20th Annual ACM Symposium on the Theory of Computing*, ACM Press, New York, 1988, 460–467.
- [CE1] J. Canny and I. Emiris. *An efficient algorithm for the sparse mixed resultant*, in: *Applied Algebra, Algebraic Algorithms and Error-correcting codes (AAECC-10)* (G. Cohen, T. Mora and O. Moreno, eds.), Lecture Notes in Computer Science **673**, Springer-Verlag, New York, 1993, 89–104.
- [CE2] J. Canny and I. Emiris. *A subdivision-based algorithm for the sparse resultant*, J. ACM **47** (2000), 417–451.
- [CM] J. Canny and D. Manocha. *Multipolynomial resultant algorithms*, J. Symbolic Comput. **15** (1993), 99–122.
- [CKL] J. Canny, E. Kaltofen and Y. Lakshman. *Solving systems of nonlinear polynomial equations faster*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1989, 121–128.
- [CDS] E. Cattani, A. Dickenstein and B. Sturmfels. *Residues and resultants*, J. Math. Sci. Univ. Tokyo **5** (1998), 119–148.
- [Chi] E.-W. Chionh. *Rectangular corner cutting and Dixon A-resultants*, J. Symbolic Comput. **31** (2001), 651–669.
- [CK1] A. Chtcherba and D. Kapur. *Conditions for exact resultants using Dixon formulation*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 2000, 62–70.
- [CK2] A. Chtcherba and D. Kapur. *Extracting sparse resultant matrices from Dixon resultant formulation*, in: *Computer Algebra: Proceedings of the Seventh Rhine Workshop (RWCA'00)*, Bergen, Austria, 2000, 167–182.
- [CK3] A. Chtcherba and D. Kapur. *On the efficiency and optimality of Dixon-base resultant methods*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 2002.
- [ColKM] S. Collart, M. Kalkbrenner and D. Mall. *Converting bases with the Gröbner walk*, J. Symbolic Comput. **24** (1997), 465–469.
- [CT] P. Conti and C. Traverso. *Buchberger algorithm and integer programming*, in: *Applied Algebra, Algebraic Algorithms and Error-correcting codes (AAECC-9)* (H. Mattson, T. Mora and T. Rao, eds.), Lecture Notes in Computer Science **539**, Springer-Verlag, New York, 1991, 130–139.
- [Cox1] D. Cox. *The homogeneous coordinate ring of a toric variety*, J. Algebraic Geom. **4** (1995), 17–50.

- [Cox2] D. Cox. *Equations of parametric curves and surfaces via syzygies*, in: *Symbolic Computation: Solving Equations in Algebra, Geometry and Engineering* (E. L. Green, S. Hoşten, R. C. Laubenbacher and V. A. Powers, eds.), Contemporary Mathematics **286**, AMS, Providence, RI, 2001, 1–20.
- [Cox3] D. Cox. *Curves, Surfaces and Syzygies*, in: *Algebraic Geometry and Geometric Modeling* (R. Goldman and R. Krasauskas, eds.), Contemporary Mathematics **334**, AMS, Providence, RI, 2003, 131–150.
- [Cox4] D. Cox. *What is a toric variety?*, in: *Algebraic Geometry and Geometric Modeling* (R. Goldman and R. Krasauskas, eds.), Contemporary Mathematics **334**, AMS, Providence, RI, 2003, 203–223.
- [CoxKM] D. Cox, R. Krasauskas and M. Mustatǎ. *Universal rational parametrizations and toric varieties*, in: *Algebraic Geometry and Geometric Modeling* (R. Goldman and R. Krasauskas, eds.), Contemporary Mathematics **334**, AMS, Providence, RI, 2003, 241–265.
- [CLO] D. Cox, J. Little and D. O’Shea. *Ideals, Varieties, and Algorithms*, 2nd edition, Springer-Verlag, New York, 1997.
- [CSC] D. Cox, T. Sederberg and F. Chen. *The moving line ideal basis of planar rational curves*, Computer Aided Geometric Design **15** (1998), 803–827.
- [DKK] Y. Dai, S. Kim and M. Kojima. *Computing all nonsingular solutions of cyclic- $n$  polynomial using polyhedral homotopy continuation methods*, J. Comput. Appl. Math. **152** (2003), 83–97.
- [D’An] C. D’Andrea. *Macaulay style formulas for sparse resultants*, Trans. Amer. Math. Soc. **354** (2002), 2595–2629.
- [DD] C. D’Andrea and A. Dickenstein. *Explicit formulas for the multivariate resultant*, in: *Effective Methods in Algebraic Geometry (Bath, 2000)*, J. Pure Appl. Algebra **164** (2001), 59–86.
- [D’AE] C. D’Andrea and I. Emiris. *Computing sparse projection operators*, in: *Symbolic Computation: Solving Equations in Algebra, Geometry and Engineering* (E. L. Green, S. Hoşten, R. C. Laubenbacher and V. A. Powers, eds.), Contemporary Mathematics **286**, AMS, Providence, RI, 2001, 121–139.
- [dBP1] M. de Boer and R. Pellikaan. *Gröbner bases for codes*, in: *Some Tapas of Computer Algebra* (A. M. Cohen, H. Cuyppers, H. Sterk and H. Cohen, eds.), Springer-Verlag, Berlin, 1999, 237–259.
- [dBP2] M. de Boer and R. Pellikaan. *Gröbner bases for decoding*, in: *Some Tapas of Computer Algebra* (A. M. Cohen, H. Cuyppers, H. Sterk and H. Cohen, eds.), Springer-Verlag, Berlin, 1999, 260–275.
- [Dev] R. Devaney. *A First Course in Chaotic Dynamical Systems*, Addison-Wesley, Reading MA, 1992.
- [DS] P. Diaconis and B. Sturmfels. *Algebraic algorithms for sampling from conditional distributions*, Annals of Statistics **26** (1998), 363–397.

- [DE] A. Dickenstein and I. Emiris. *Multihomogeneous resultant formulae by means of complexes*, J. Symbolic Comput. **36** (2003), 317–342.
- [Dim] A. Dimca. *Singularities and Topology of Hypersurfaces*, Springer-Verlag, New York, 1992.
- [Dre] F. Drexler. *A homotopy method for the calculation of zeros of zero-dimensional ideals*, in: *Continuation Methods* (H. Wacker, ed.), Academic Press, New York, 1978.
- [DGH] M. Dyer, P. Gritzmann and A. Hufnagel. *On the complexity of computing mixed volumes*, SIAM J. Comput. **27** (1998), 356–400.
- [Eis] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1995.
- [EH] D. Eisenbud and C. Huneke, eds. *Free Resolutions in Commutative Algebra and Algebraic Geometry*, Jones and Bartlett, Boston, 1992.
- [EGSS] D. Eisenbud, D. Grayson, M. Stillman and B. Sturmfels (eds.). *Computations in Algebraic Geometry with Macaulay 2*, Springer-Verlag, Berlin, 2002.
- [EK] G. Elber and M.-S. Kim. *The bisector surface of rational space curves*, ACM Transactions on Graphics **17** (1998), 32–49.
- [EIM1] M. Elkadi and B. Mourrain. *Some applications of bezoutians in effective algebraic geometry*, Rapport de Recherche **3572**, INRIA, 1998.
- [EIM2] M. Elkadi and B. Mourrain. *Approche effective des résidus algébriques*, Rapport de Recherche **2884**, INRIA, 1996.
- [EIM3] M. Elkadi and B. Mourrain. *A new algorithm for the geometric decomposition of a variety*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1999, 9–16.
- [Emi1] I. Emiris. *On the complexity of sparse elimination*, Journal of Complexity **14** (1996), 134–166.
- [Emi2] I. Emiris. *A general solver based on sparse resultants*, in: *Proc. PoSSo (Polynomial System Solving) Workshop on Software*, Paris, 1995, 35–54.
- [Emi3] I. Emiris. *Matrix methods for solving algebraic systems*, in: *Symbolic Algebraic Methods and Verification Methods (Dagstuhl 1999)*, Springer-Verlag, Vienna, 2001, 69–78.
- [EC] I. Emiris and J. Canny. *Efficient incremental algorithms for the sparse resultant and the mixed volume*, J. Symbolic Comput. **20** (1995), 117–149.
- [EmM] I. Emiris and B. Mourrain. *Matrices in elimination theory*, J. Symbolic Comput. **28** (1999), 3–44.
- [ER] I. Emiris and A. Rege. *Monomial bases and polynomial system solving*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1994, 114–122.
- [Ewa] G. Ewald. *Combinatorial Convexity and Algebraic Geometry*, Springer-Verlag, New York, 1996.

- [Far] G. Farin. *Curves and Surfaces for Computer Aided Geometric Design*, 2nd edition, Academic Press, Boston, 1990.
- [FGLM] J. Faugère, P. Gianni, D. Lazard and T. Mora. *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. **16** (1993), 329–344.
- [FR] G.-L. Feng and T. Rao. *Decoding of algebraic geometric codes up to the designed minimum distance*, IEEE Trans. Inform. Theory **39** (1993), 743–751.
- [Fit1] P. Fitzpatrick. *On the key equation*, IEEE Trans. Inform. Theory **41** (1995), 1290–1302.
- [Fit2] P. Fitzpatrick. *Solving a multivariable congruence by change of term order*, J. Symbolic Comput. **24** (1997), 575–589.
- [FM] J. Fogarty and D. Mumford. *Geometric Invariant Theory*, Second Edition, Springer-Verlag, Berlin, 1982.
- [FIS] S. Friedberg, A. Insel and L. Spence. *Linear Algebra*, 3rd edition, Prentice-Hall, Englewood Cliffs, NJ, 1997.
- [Ful] W. Fulton. *Introduction to Toric Varieties*, Princeton U. Press, Princeton NJ, 1993.
- [GL1] T. Gao and T. Y. Li. *Mixed volume computation via linear programming*, Taiwanese J. Math. **4** (2000), 599–619.
- [GL2] T. Gao and T. Y. Li. *Mixed volume computation for semi-mixed systems*, Discrete Comput. Geom. **29** (2003), 257–277.
- [GLW] T. Gao, T. Y. Li and X. Wang. *Finding all isolated zeros of polynomial systems in  $\mathbb{C}^n$  via stable mixed volumes*, J. Symbolic Comput. **28** (1999), 187–211.
- [GS] A. Garcia and H. Stichtenoth. *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211–222.
- [GeP] O. Geil and R. Pellikaan. *On the Structure of Order Domains*, Finite Fields Appl. **8** (2002), 369–396.
- [GKZ] I. Gelfand, M. Kapranov and A. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, Boston, 1994.
- [GRRT] L. Gonzalez-Vega, F. Rouillier, M.-F. Roy and G. Trujillo. *Symbolic recipes for real solutions*, in: *Some Tapas of Computer Algebra* (A. M. Cohen, H. Cuyppers, H. Sterk and H. Cohen, eds.), Springer-Verlag, Berlin, 1999, 211–167.
- [Grä] H.-G. Gräbe. *Algorithms in Local Algebra*, J. Symbolic Comput. **19** (1995), 545–557.
- [GrP] G.-M. Greuel and G. Pfister. *A Singular Introduction to Commutative Algebra*, Springer-Verlag, Berlin, 2002.
- [GuS] L. Gurvits and A. Samorodnitsky. *A deterministic algorithm for approximating the mixed determinant and mixed volume, and a combinatorial corollary*, Discrete Comput. Geom. **27** (2002), 531–550.
- [HeS] C. Heegard and K. Saints. *Algebraic-geometric codes and multidimensional cyclic codes: Theory and algorithms for decoding using Gröbner bases*, IEEE Trans. Inform. Theory **41** (1995), 1733–1751.

- [HLS] C. Heegard, J. Little and K. Saints. *Systematic Encoding via Gröbner Bases for a Class of Algebraic-Geometric Goppa Codes*, IEEE Trans. Inform. Theory **41** (1995), 1752–1761.
- [Her] I. Herstein. *Topics in Algebra*, 2nd edition, Wiley, New York, 1975.
- [Hil] D. Hilbert. *Ueber die Theorie der algebraischen Formen*, Math. Annalen **36** (1890), 473–534.
- [Hir] H. Hironaka. *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann. of Math. **79** (1964), 109–326.
- [HP] T. Høholdt and R. Pellikaan. *On the Decoding of Algebraic Geometric Codes*, IEEE Trans. Inform. Theory **41** (1995), 1589–1614.
- [HvLP] T. Høholdt, J. van Lint and R. Pellikaan. *Algebraic geometry codes*, Chapter 10, in: *Handbook of Coding Theory* (V. Pless and W. Huffman, eds.), Elsevier, Amsterdam, 1998.
- [HT] S. Hoşten and R. Thomas. *Gröbner bases and integer programming*, in: *Gröbner Bases and Applications (Linz, 1998)* (B. Buchberger and F. Winkler, eds.), London Math. Soc. Lecture Notes Ser. **251**, Cambridge U. Press, (1998), 144–158.
- [HuS1] B. Huber and B. Sturmfels. *A Polyhedral Method for Solving Sparse Polynomial Systems*, Math. Comp. **64** (1995), 1541–1555.
- [HuS2] B. Huber and B. Sturmfels. *Bernstein’s theorem in affine space*, Discrete Comput. Geom. **17** (1997), 137–141.
- [HV] B. Huber and J. Verschelde. *Polyhedral end games for polynomial continuation*, Numer. Algorithms **18** (1998), 91–108.
- [Jac] N. Jacobson. *Basic Algebra I*, W. H. Freeman, San Francisco, 1974.
- [Jou1] J.-P. Jouanolou. *Le formalisme du résultant*, Adv. Math. **90** (1991), 117–263.
- [Jou2] J.-P. Jouanolou. *Formes d’inertie et résultant: un formulaire*, Adv. Math. **126** (1997), 119–250.
- [Kal] M. Kalkbrenner. *On the complexity of Gröbner bases conversion*, J. Symbolic Comput. **28** (1999), 265–273.
- [KSZ] M. Kapranov, B. Sturmfels and A. Zelevinsky. *Chow polytopes and general resultants*, Duke Math. J. **67** (1992), 189–218.
- [KS1] D. Kapur and T. Saxena. *Comparison of various multivariate resultant formulations*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1995.
- [KS2] D. Kapur and T. Saxena. *Sparsity considerations in Dixon resultants*, in: *Proceedings of the Symposium on the Theory of Computing*, ACM Press, New York, 1996, 184–191.
- [KSY] D. Kapur, T. Saxena and L. Yang. *Algebraic and geometric reasoning using Dixon resultants*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1994, 99–107.
- [Khe] A. Khetan. *Determinantal formula for the Chow form of a toric surface*, in: *Proceedings of International Symposium on Symbolic*

- and *Algebraic Computation*, ACM Press, New York, 2002, 145–150.
- [Kho] A.G. Khovanskii. *Newton polytopes and toric varieties*, Functional Anal. Appl. **11** (1977), 289–298.
- [Kir] F. Kirwan. *Complex Algebraic Curves*, Cambridge U. Press, Cambridge, 1992.
- [Kob] N. Koblitz. *Algebraic aspects of cryptography*, with an appendix by A. J. Menezes, Y.-H. Wu and R. J. Zuccherato, Algorithms and Computation in Mathematics **3**, Springer-Verlag, Berlin, 1998.
- [Kra] R. Krasauskas. *Toric surface patches*, Adv. Comput. Math. **17** (2002), 89–113.
- [KR] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1*, Springer-Verlag, Berlin, 2000.
- [KM] S. Krishnan and D. Manocha. *Numeric-symbolic algorithms for evaluating one-dimensional algebraic sets*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1995, 59–67.
- [Kus] A.G. Kushnirenko. *Newton polytopes and the Bézout theorem*, Functional Anal. Appl. **10** (1976), 233–235.
- [Laz] D. Lazard. *Résolution des systèmes d'équations algébriques*, Theor. Comp. Sci. **15** (1981), 77–110.
- [Lei] K. Leichtweiss. *Konvexe Mengen*, Springer-Verlag, Berlin, 1980.
- [Leo] D. Leonard. *A generalized Forney formula for AG codes*, IEEE Trans. Inform. Theory **46** (1996), 1263–1268.
- [Lew] R. Lewis. *Computer algebra system Fermat*, available at [www.bway.net/~lewis/](http://www.bway.net/~lewis/).
- [Li] T. Y. Li. *Solving polynomial systems by polyhedral homotopies*, Taiwanese J. Math. **3** (1999), 252–279.
- [LL] T. Y. Li and X. Li. *Finding mixed cells in the mixed volume computation*, Found. Comput. Math. **1** (2001), 161–181.
- [LW] T. Li and X. Wang. *The BKK root count in  $\mathbb{C}^n$* , Math. Comp. **65** (1996), 1477–1484.
- [Lit] J. Little. *A key equation and the computation of error values for codes from order domains*, preprint, 2003, arXiv math.AC/0303299.
- [LS] A. Logar and B. Sturmfels. *Algorithms for the Quillen-Suslin Theorem*, J. Algebra **145** (1992), 231–239.
- [Mac1] F. Macaulay. *The Algebraic Theory of Modular Systems*, Cambridge U. Press, Cambridge, 1916. Reprint with new introduction, Cambridge U. Press, Cambridge, 1994.
- [Mac2] F. Macaulay. *On some formulas in elimination*, Proc. London Math. Soc. **3** (1902), 3–27.
- [MS] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.
- [Man1] D. Manocha. *Algorithms for computing selected solutions of polynomial equations*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1994, 1–8.



- [Man2] D. Manocha. *Efficient algorithms for multipolynomial resultant*, The Computer Journal **36** (1993), 485–496.
- [Man3] D. Manocha. *Solving systems of polynomial equations*, IEEE Computer Graphics and Applications, March 1994, 46–55.
- [MMM1] M. Marinari, H. M. Möller and T. Mora. *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, Appl. Algebra Engrg. Comm. Comput. **4** (1993), 103–145.
- [MMM2] M. Marinari, H. M. Möller and T. Mora. *On multiplicities in polynomial system solving*, Trans. Amer. Math. Soc. **348** (1996), 3283–3321.
- [Mey] F. Meyer. *Zur Theorie der reducibeln ganzen Functionen von  $n$  Variabeln*, Math. Annalen **30** (1887), 30–74.
- [Mil] J. Milnor. *Singular Points of Complex Hypersurfaces*, Princeton U. Press, Princeton, 1968.
- [Mis] B. Mishra. *Algorithmic Algebra*, Springer-Verlag, New York, 1993.
- [Möl] H. Möller. *Systems of Algebraic Equations Solved by Means of Endomorphisms*, in: *Applied Algebra, Algebraic Algorithms and Error-correcting codes (AAECC-10)* (G. Cohen, T. Mora and O. Moreno, eds.), Lecture Notes in Computer Science **673**, Springer-Verlag, New York, 1993, 43–56.
- [MöS] H. M. Möller and H. J. Stetter. *Multivariate polynomial systems with multiple zeros solved by matrix eigenproblems*, Numer. Math. **70** (1995), 311–329.
- [MT] H. M. Möller and R. Tenberg. *Multivariate polynomial system solving using intersections of eigenspaces*, J. Symbolic Comput. **30** (2001), 1–19.
- [Mon] C. Monico. *Computing the primary decomposition of zero-dimensional ideals*, J. Symbolic Comput. **34** (2002), 451–459.
- [MR] T. Mora and L. Robbiano. *The Gröbner fan of an ideal*, J. Symbolic Comput. **6** (1988), 183–208.
- [MPT] T. Mora, G. Pfister and C. Traverso. *An introduction to the tangent cone algorithm*, Advances in Computing Research **6** (1992), 199–270.
- [Mor] C. Moreno. *Algebraic Curves over Finite Fields*, Cambridge U. Press, Cambridge, 1991.
- [Mou1] B. Mourrain. *Computing the isolated roots by matrix methods*, J. Symbolic Comput. **26** (1998), 715–738.
- [Mou2] B. Mourrain. *An introduction to algebraic and geometric methods for solving polynomial equations*, Technical Report ECG-TR-122102-01, INRIA Sophia-Antipolis, 2002.
- [O’Su1] M. O’Sullivan. *The key equation for one-point codes and efficient error evaluation*, J. Pure Appl. Algebra **169** (2002), 295–320.
- [O’Su2] M. O’Sullivan. *A generalization of the Berlekamp-Massey-Sakata algorithm*, preprint, 2001.
- [O’Su3] M. O’Sullivan. *New codes for the Berlekamp-Massey-Sakata algorithm*, Finite Fields Appl. **7** (2001), 293–317.
- [PW] H. Park and C. Woodburn. *An algorithmic proof of Suslin’s stability theorem for polynomial rings*, J. Algebra **178** (1995), 277–298.

- [Ped] P. Pedersen. Lecture at AMS-IMS-SIAM Summer Conference on Continuous Algorithms and Complexity, Mount Holyoke College, South Hadley, MA, 1994.
- [PS1] P. Pedersen and B. Sturmfels. *Mixed monomial bases*, in: *Algorithms in Algebraic Geometry and Applications* (L. Gonzalez-Vega and T. Recio, eds.), Birkhäuser, Boston, 1996, 307–316.
- [PS2] P. Pedersen and B. Sturmfels. *Product formulas for resultants and Chow forms*, *Math. Z.*, **214** (1993), 377–396.
- [PRS] P. Pedersen, M.-F. Roy and A. Szpirglas. *Counting real zeros in the multivariate case*, in: *Computational Algebraic Geometry* (F. Eyssette and A. Galligo, eds.), Birkhäuser, Boston, 1993, 203–224.
- [PR] H.-O. Peitgen and P. Richter. *The Beauty of Fractals*, Springer-Verlag, Berlin, 1986.
- [PH] A. Poli and F. Huguet. *Error correcting codes*. Prentice Hall International, Hemel Hempstead, 1992.
- [Qui] D. Quillen. *Projective modules over polynomial rings*, *Invent. Math.* **36** (1976), 167–171.
- [Rob] L. Robbiano. *Term orderings on the polynomial ring*, in: *Proceedings of EUROCAL 1985*, Lecture Notes in Computer Science **204**, Springer-Verlag New York, 513–517.
- [Roj1] J. M. Rojas. *A convex geometric approach to counting roots of a polynomial system*, *Theoretical Computer Science* **133** (1994), 105–140.
- [Roj2] J. M. Rojas. *Solving degenerate sparse polynomial systems faster*, *J. Symbolic Comput.* **28** (1999), 155–186.
- [Roj3] J. M. Rojas. *Toric intersection theory for affine root counting*, *J. Pure Appl. Algebra* **136** (1999), 67–100.
- [Roj4] J. M. Rojas. *Toric laminations, sparse generalized characteristic polynomials, and a refinement of Hilbert’s tenth problem*, in: *Foundations of Computational Mathematics, Rio de Janeiro, 1997* (F. Cucker and M. Shub, eds.), Springer-Verlag, Berlin, 1997, 369–381.
- [Roj5] J. M. Rojas. *Why polyhedra matter in non-linear equation solving*, in: *Algebraic Geometry and Geometric Modeling* (R. Goldman and R. Krasauskas, eds.), *Contemporary Mathematics* **334**, AMS, Providence, RI, 2003, 293–320.
- [RW] J. M. Rojas and X. Wang. *Counting affine roots of polynomial systems via pointed Newton polytopes*, *Journal of Complexity* **12** (1996), 116–133.
- [Ros] L. Rose. *Combinatorial and Topological Invariants of Modules of Piecewise Polynomials*, *Adv. Math.* **116** (1995), 34–45.
- [Rou] F. Rouillier. *Solving zero-dimensional systems through the rational univariate representation*, *Appl. Algebra Engrg. Comm. Comput.* **9** (1999), 433–461.
- [Sak] S. Sakata. *Extension of the Berlekamp-Massey algorithm to  $n$  dimensions*, *Inform. Comput.* **84** (1989), 207–239.
- [Sal] G. Salmon. *Lessons Introductory to the Modern Higher Algebra*, Hodges, Foster and Co., Dublin, 1876.

- [Sche] H. Schenck. *A spectral sequence for splines*, Adv. in Appl. Math. **19** (1997), 183–199.
- [SS] H. Schenck and M. Stillman. *Local cohomology of bivariate splines*, J. Pure Appl. Algebra **117/118** (1997), 535–548.
- [Schre1] F.-O. Schreyer. *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstraßschen Divisionssatz*, Diplom Thesis, University of Hamburg, Germany, 1980.
- [Schre2] F.-O. Schreyer. *A Standard Basis Approach to syzygies of canonical curves*, J. reine angew. Math. **421** (1991), 83–123.
- [Schri] A. Schrijver. *Theory of Linear and Integer Programming*, Wiley-Interscience, Chichester, 1986.
- [Schu] L. Schumaker. *On the dimension of spaces of piecewise polynomials in two variables*, in: *Multivariate Approximation Theory (Proc. Conf., Math. Res. Inst., Oberwolfach, 1979)*, Internat. Ser. Numer. Math. **51**, Birkhäuser, Basel-Boston, 1979, 396–412.
- [SC] T. Sederberg and F. Chen. *Implicitization using moving curves and surfaces*, in: *Computer Graphics Proceedings, Annual Conference Series*, 1995, 301–308.
- [SSQK] T. Sederberg, T. Saito, D. Qi and K. Klimaszewski. *Curve implicitization using moving lines*, Computer Aided Geometric Design **11** (1994), 687–706.
- [Ser] J.-P. Serre. *Faisceaux algébriques cohérents*, Ann. of Math. **61** (1955), 191–278.
- [Sha] I. Shafarevich. *Basic Algebraic Geometry*, Springer-Verlag, Berlin, 1974.
- [SVW] A. Sommese, J. Verschelde and C. Wampler. *Numerical decomposition of the solution sets of polynomial systems into irreducible components*, SIAM J. Numer. Anal. **36** (2001), 2022–2046.
- [Sta1] R. Stanley. *Combinatorics and Commutative Algebra*, 2nd edition, Birkhäuser, Boston, 1996.
- [Sta2] R. Stanley. *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. **1** (1979), 475–511.
- [Ste] H. J. Stetter. *Multivariate polynomial equations as matrix eigenproblems*, in: *Contributions in Numerical Analysis* (R. P. Agarwal, ed.), Series in Applicable Analysis **2**, World Scientific, Singapore, 1993, 355–371.
- [Sti] H. Stichtenoth. *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.
- [Stu1] B. Sturmfels. *Algorithms in Invariant Theory*, Springer-Verlag, Vienna, 1993.
- [Stu2] B. Sturmfels. *Gröbner Bases and Convex Polytopes*, AMS, Providence RI, 1996.
- [Stu3] B. Sturmfels. *On the Newton polytope of the resultant*, J. Algebraic Comb. **3** (1994), 207–236.
- [Stu4] B. Sturmfels. *Sparse elimination theory*, in: *Computational Algebraic Geometry and Commutative Algebra* (D. Eisenbud and L. Robbiano, eds.), Cambridge U. Press, Cambridge, 1993, 264–298.
- [Stu5] B. Sturmfels. *Solving Systems of Polynomial Equations*, AMS, Providence, RI, 2002.

- [SZ] B. Sturmfels and A. Zelevinsky. *Multigraded resultants of Sylvester type*, J. Algebra **163** (1994), 115–127.
- [Sus] A. Suslin. *Projective modules over a polynomial ring are free*, Soviet Math. Dokl. **17** (1976), 1160–1164.
- [Tei] M. Teixidor i Bigas. *Green’s conjecture for the generic  $r$ -gonal curve of genus  $g \geq 3r - 7$* , Duke Math. J. **111** (2002), 195–222.
- [Tho1] R. Thomas. *A geometric Buchberger algorithm for integer programming*, Math. Operations Research **20** (1995), 864–884.
- [Tho2] R. Thomas. *Applications to integer programming*, in: *Applications of Computational Algebraic Geometry* (D. Cox and B. Sturmfels, eds.), Proc. Sympos. Appl. Math. **53**, AMS, Providence, RI, 1998, 119–142.
- [Tran] Q. N. Tran. *A fast algorithm for Gröbner basis conversion and its applications*, J. Symbolic Comput. **30** (2000), 451–467.
- [Trav] C. Traverso. *Hilbert functions and the Buchberger algorithm*, J. Symbolic Comput. **22** (1996), 355–376.
- [TVZ] M. Tsfasman, S. Vladut and T. Zink. *Modular Curves, Shimura Curves, and Goppa Codes Better than the Varshamov-Gilbert Bound*, Math. Nachr. **109** (1982), 21–28.
- [vdW] B. van der Waerden. *Moderne Algebra, Volume II*, Springer-Verlag, Berlin, 1931. English translations: *Modern Algebra, Volume II*, F. Ungar Publishing Co., New York, 1950; *Algebra, Volume 2*, F. Ungar Publishing Co., New York 1970; and *Algebra, Volume II*, Springer-Verlag, New York, 1991. The chapter on Elimination Theory is included in the first three German editions and the 1950 English translation, but all later editions (German and English) omit this chapter.
- [vLi] J. van Lint. *Introduction to Coding Theory*, 2nd edition, Springer-Verlag, Berlin, 1992.
- [vLvG] J. van Lint and G. van der Geer. *Introduction to Coding Theory and Algebraic Geometry*, Birkhäuser, Basel, 1988.
- [Vas] W. Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry*, Springer-Verlag, Berlin, 1998.
- [Ver1] J. Verschelde. *Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation*, ACM Trans. Math. Softw. **25** (1999), 251–276.
- [Ver2] J. Verschelde. *Toric Newton method for polynomial homotopies*, J. Symbolic Comput. **29** (2000), 777–793.
- [VGC] J. Verschelde, K. Gatermann and R. Cools. *Mixed volume computation by dynamic lifting applied to polynomial system solving*, Discrete Comput. Geom. **16** (1996), 69–112.
- [VVC] J. Verschelde, P. Verlinden and R. Cools. *Homotopies Exploiting Newton Polytopes for Solving Sparse Polynomial Systems*, SIAM J. Numer. Anal. **31** (1994), 915–930.
- [Voi] C. Voisin. *Green’s generic syzygy conjecture for curves of even genus lying on a  $K3$  surface*, J. Eur. Math. Soc. **4** (2002), 363–404.
- [WEM] A. Wallack, I. Emiris and D. Manocha. *MARS: A MAPLE/MATLAB/C resultant-based solver*, in: *Proceedings of International*

- Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 1998, 244–251.
- [Wei] V. Weispfenning. *Constructing universal Gröbner bases*, in: *Applied Algebra, Algebraic Algorithms and Error-correcting Codes (AAECC-5)* (L. Huguët and A. Poli, eds.), Lecture Notes in Computer Science **356**, Springer-Verlag, Berlin, 1989, 408–417.
- [WZ] J. Weyman and A. Zelevinski, *Determinantal formulas for multigraded resultants*, *J. Algebraic Geom.* **3** (1994), 569–597.
- [Wil] J. Wilkinson. *The evaluation of the zeroes of ill-conditioned polynomials, part 1*, *Numerische Mathematik* **1** (1959), 150–166.
- [YNT] K. Yokoyama, M. Noro and T. Takeshima. *Solutions of systems of algebraic equations and linear maps on residue class rings*, *J. Symbolic Comput.* **14** (1992), 399–417.
- [ZG] M. Zhang and R. Goldman. *Rectangular corner cutting and Sylvester  $\mathcal{A}$ -resultants*, in: *Proceedings of International Symposium on Symbolic and Algebraic Computation*, ACM Press, New York, 2000, 301–308.
- [Zie] G. Ziegler, *Lectures on Polytopes*, Springer-Verlag, New York, 1995.
- [Zub] S. Zubè. *The  $n$ -sided toric patches and  $\mathcal{A}$ -resultants*, *Computer Aided Geometric Design* **17** (2000), 695–714.

# Index

- Adapted order, *see* monomial order, adapted
- $\mathcal{A}$ -degree, 320
- adjacent cells or polytopes in a polyhedral complex, 408, 411–413, 417, 422
- $\mathcal{A}$ -homogeneous, 330
- $\mathcal{A}$ -resultant, *see* resultant, sparse
- Abel, N., 29
- Acton, F., 30, 35, 533
- Adams, W., vii, 4, 11, 14, 16, 18, 24, 27, 39, 185, 211, 213, 376, 533
- affine
- half-space, 408
  - Hilbert Function, *see* Hilbert function, affine
  - hyperplane, 308, 312, 379, 411, 413, 418
  - linear space, *see* affine, subspace
  - $n$ -dimensional space over  $\mathbb{C}$  ( $\mathbb{C}^n$ ), 90, 97, 105, 114, 125, 316, 327, 343, 344, 346, 352, 353, 357
  - $n$ -dimensional space over  $\mathbb{F}_q$  ( $\mathbb{F}_q^n$ ), 459ff, 468ff, 505, 510, 511
  - $n$ -dimensional space over  $k$  ( $k^n$ ), 19, 293, 294
  - $n$ -dimensional space over  $\mathbb{R}$  ( $\mathbb{R}^n$ ), 69ff, 305ff, 392ff, 426ff, 436ff
  - subspace, 312, 340, 388
  - variety, 20, 24, 45, 495, 501
- Agacy, R., xi
- alex*, 159, 161, 162, 171, 175, 177, 183, 187
- Alexandrov-Fenchel inequality, 362
- Alfeld, P., 420, 533
- algebra over a field  $k$ , 38, 71, 495
- finite-dimensional algebra, 37ff, 56ff, 96, 478
- algebraic
- coding theory, viii, ix, 451, 459ff, 468ff, 480ff, 494ff, 508ff, 522ff
  - curve, 494, 498, 501, 506
  - decomposition, *see* subdivision, algebraic (non-polyhedral)
- algebraically closed field, 23–25, 27, 42, 96, 148, 150–152, 157, 182, 262
- Allgower, E., 353, 533
- Alonso, M., 179, 184, 186, 533
- alphabet (of a code), 459, 471, 479
- Amrhein, B., 445, 446, 533
- analytic function, *see* convergent power series ring
- annihilator of  $N$  ( $\text{ann}(N)$ ), 203
- anti-graded
- lex order, *see alex*
  - revlex order, *see arevlex*
  - order, *see* degree-anticompatible order
- Archimedean order domain, *see* order domain, Archimedean
- Archimedean property (in  $\mathbb{Z}_{\geq 0}$ ), 502
- arevlex*, 159, 160, 175

- Arnold, V., 187, 533  
 Artin, M., 244, 533  
 ascending chain condition, 168, 176,  
     179, 215, 217, 222, 428  
 automorphism, *see* field,  
     automorphism  
 Auszinger, W., 65, 135, 533  
  
 Bajaj, C., 108, 533  
 base point (of a parametrization),  
     294  
 Basic Question of resultants, 85  
 basis  
     monomials, 38, 40, 45, 46, 50, 52,  
         53, 55, 57, 62, 65, 68–71, 74,  
         128, 496, 498, 499, 510, 515,  
         529  
     of an ideal, 4  
     of a free module, *see* module basis  
 Batyrev, V., 327, 328, 533  
 Bayer, D., 434, 533  
 BCH code, 471, 479, 480  
     designed distance of, 479  
 Becker, T., vii, 4, 11, 14–16, 18, 27,  
     39, 49, 55, 69, 75, 185, 441,  
     517, 533  
 Berlekamp, E. 480, 491  
 Berlekamp-Massey algorithm, 480,  
     488  
 Berlekamp-Massey-Sakata algorithm  
     (BMS), xi, 494, 505, 508ff,  
     522ff  
     FRMV procedure, 519, 520, 523ff,  
         530, 531  
     InfoUpdate procedure, 519, 520,  
         523, 526–528, 530  
     termination, 528, 529  
     *see also* BMS data structure  
 Berlekamp-Welch algorithm, 491  
 Ben-Or, M., 73, 533  
 Bernstein, D., 346, 351, 370, 533  
 Bernstein's Theorem, 343, 344,  
     346ff  
 Betke, U., 362, 534  
 Bézout bound, 346, 355  
     *see also* Bézout's Theorem  
 Bézout Formula, 100  
 Bézoutians, 110  
 Bézout matrix, 369, 370  
  
 Bézout's Theorem, 97, 114–116, 186,  
     286, 344–346, 352, 505  
 Bigatti, A., 391, 534  
 bihomogeneous polynomial, 331, 332  
 bijective mapping, 477, 501, 514, 522  
 Bikker, P., 369, 534  
 bilinear mapping, 467  
 bilinear surface parametrization, 313  
 Billera, L., ix, 363, 405, 414, 420,  
     423, 425, 534  
 binomial (= difference of two  
     monomials), 383, 391, 397  
     *see also* toric ideal  
 binomial coefficient, 104, 112, 256,  
     265, 280, 282, 283, 284, 290,  
     299, 302, 323, 328, 401, 402,  
     415–417, 420, 421, 423  
 binomial theorem, 59, 84, 149  
 bisector surface, 446, 447  
 bivariate splines, 405, 420  
 BKK bound, 351–353, 355, 357  
     *see also* Bernstein's Theorem  
 Blahut, R., ix, 459, 534  
 block length (of a code), 459, 463,  
     464, 470, 471, 477, 479, 504,  
     521  
 block matrix, 227, 228  
 blow-up, 320  
 BMS data structure  
     Info( $k$ ), 519, 522, 523, 525–528  
     Syn( $k$ ), 519, 527, 528  
     *see also* Berlekamp-Massey-Sakata  
         algorithm (BMS)  
 Bondyfalat, D., 135, 534  
 Bonnesen, T., ix, 332, 335, 339, 534  
 boundary of a cone, 432, 438  
 bracket ( $[i_0, \dots, i_n]$ ), 98, 99, 319  
 Briançon, J., 188  
 Bruns, W., 299, 534  
 Bryant, V., 403, 534  
 Buchsbaum, D., 302, 534  
 Buchberger, B., 54, 534  
 Buchberger-Möller algorithm, 54  
 Buchberger's Algorithm, 15, 16, 49,  
     167, 171, 175, 225, 383, 384,  
     441, 448, 476  
     in module case, 211, 215–218, 423,  
         487, 492  
     parallel (for Gröbner fan), 434

- Buchberger's Criterion, 16, 167, 175, 176, 180, 223, 236, 500  
 in module case, 215, 222, 236
- Burago, Yu., 332, 534
- Burden, R., ix, 30, 35, 534
- burst error-correcting, *see*  
 error-correcting, burst
- Busé, L., 320, 534, 535
- $\mathbb{C}^n$ , *see* affine,  $n$ -dimensional space  
 over  $\mathbb{C}$
- $(\mathbb{C}^*)^n$ , 315, 316, 318, 321–323,  
 327–329, 344, 346–348,  
 350–353, 357, 358, 367, 370,  
 372
- $C_G$  (cone corresponding to a marked  
 Gröbner basis), 430ff, 436,  
 437, 440
- $C^r$  function, 405, 406
- $C^r$  spline, 406–408, 411ff, 422–424
- $C^\infty$  function, 405
- CALI, *see* REDUCE
- Canny, J., 111, 112, 120, 121, 126,  
 339, 363, 367–369, 374, 375,  
 535, 537
- canonical curve, 286
- categorical quotient, 327
- Cattani, E., 370, 535
- Cayley-Hamilton Theorem, 58
- cell  
 of a polyhedral or mixed  
 subdivision, 359, 360, 363  
 of a polyhedral complex, 408,  
 410–413, 415  
 interior, of a polyhedral complex,  
 413–419, 421
- center of a blow-up, 320
- chain rule, 354
- chaos, 36
- characteristic function, 294  
*see also* Hilbert function
- characteristic polynomial, 60, 67,  
 71–74, 150, 151
- Chen, F., 287, 288, 292, 294, 536,  
 543
- Chinese Remainder Theorem, 111
- Chionh, E.-W., 320, 535
- Chow form, 323
- Chtcherba, A., 359, 370, 535
- class, *see* coset ( $[f] = f + I$ )
- closed ball, 461, 464
- CoCoA, 217, 231, 253  
*intprog* package, 391
- code, 459ff, 468ff, 480ff, 503ff  
 alphabet of, *see* alphabet (of a  
 code)  
 BCH, *see* BCH code  
 block length of, *see* block length  
 (of a code)  
 codimension of, *see* codimension of  
 a code  
 cyclic, *see* cyclic code  
 dimension of, *see* dimension, of a  
 code  
 dual, *see* dual code  
 error-correcting, *see*  
 error-correcting code  
 geometric Goppa, *see* geometric  
 Goppa code  
 Hamming, *see* Hamming code  
 linear, *see* linear code  
 MDS, *see* MDS code  
 minimum distance of, *see*  
 minimum distance (of a code)  
 parameters of, *see* parameters of a  
 code ( $[n, k, d]$ )  
 perfect, *see* perfect code  
 Reed-Muller, *see* Reed-Muller  
 code  
 Reed-Solomon, *see* Reed-Solomon  
 code  
*see also* algebraic coding theory
- codeword, 459, 463, 464, 467, 468,  
 471, 472, 474–476, 478, 489,  
 491, 495, 502, 506, 510
- codimension of a code, 480
- coding theory, *see* algebraic coding  
 theory
- Cohen-Macaulay ring, 262, 285, 298
- coherent  
 Minkowski sum, *see* Minkowski  
 sum of polytopes ( $P + Q$ ),  
 coherent  
 mixed subdivision, *see* mixed  
 subdivision, coherent  
 subdivision, *see* mixed  
 subdivision, coherent
- cokernel, 205, 248, 249



- Collart, S., 436, 535  
 Colley, S., x  
 collinear points, 285, 286, 292  
 column operation, 242  
 column vector  $\mathbf{f}$  (in a free module),  
   *see* vector  $\mathbf{f}$  (in a free module)  
 comaximal ideals, 155  
 combinatorial data, *see* polyhedral  
   complex, combinatorial data  
   of  
 combinatorial enumeration problem,  
   376, 392  
   *see also* magic squares  
 combinatorics, viii, ix  
 Common Factor property of  
   resultants, 78  
 commutative algebra, viii, ix, 218,  
   294, 402  
 commutative diagram, 124, 150, 156,  
   273, 278  
 commutative ring, 2  
 compact disk, 470, 479  
 companion matrix, 83  
 compatibility property (of a  
   monomial order), 384, 386,  
   390  
 complete intersection, 286, 320, 446  
   local, 320  
 complex, *see* polyhedral complex  
 computational geometry, 320  
 computer-aided geometric design,  
   287, 405, 446  
 computer science, 377  
 computing determinants  
   numerically 110, 111  
   symbolically, 110, 111, 120  
 cone, 421, 429, 436ff, 448, 449  
   boundary of, *see* boundary of a  
   cone  
   interior of, *see* interior of a cone  
   *see also*  $C_G$  (cone corresponding  
   to a marked Gröbner basis)  
 congruence, 482, 483, 487–489  
 conic section, 279, 301  
 connected graph, *see* graph,  
   connected  
 Conti, P., 376, 380, 390, 391, 535  
 contingency table, 403  
   marginal distribution of, 403, 404  
 continuation system, 354  
 Contraction Mapping Theorem, 35  
 convergent power series ring  
   ( $k\{x_1, \dots, x_n\}$ ), 140–142, 144,  
   145, 153–155, 160, 167, 174,  
   177, 179, 180, 234  
 convex  
   combinations, 305  
   hull of a set  $S$  ( $\text{Conv}(S)$ ),  
     305–307, 309–313, 316ff,  
     324–327, 330–332, 335, 338,  
     340, 345, 358, 360, 363, 366,  
     408, 416, 435  
   polyhedral cone, 395, 427, 430, 435  
   polytope, *see* polytope  
   set, 305, 306  
 Cools, R., 353, 355, 363, 544  
 coset ( $[f] = f + I$ ), 37, 84, 193, 452,  
   456, 457, 465, 467, 469, 470,  
   512  
   leader, 465  
 Courant functions, 425  
 Cox, D., 288, 292, 294, 322, 327, 328,  
   533, 535, 536; *see also* *Ideals,*  
   *Varieties, and Algorithms*  
 Cramer's Rule, 101  
 cryptography, 459  
 cubic  
   curve, 505  
   spline, 406–408  
 curve  
   algebraic, *see* algebraic curve  
   canonical, *see* canonical curve  
   cubic, *see* cubic curve  
   divisor on, *see* divisor (on an  
   algebraic curve)  
   Hermitian, *see* Hermitian curve  
   Klein Quartic, *see* Klein Quartic  
   curve  
   level, *see* level curve  
   projective, *see* projective curve  
   rational normal, *see* rational  
   normal curve  
   rational quartic, *see* rational  
   quartic curve  
   smooth, *see* smooth curve  
 cycles (in a graph), 418, 419  
 cyclic  
   code, 451, 468ff, 521

- $m$ -dimensional code, 473ff, 480, 531
- group, 456, 457, 459
- permutation, 398, 468
- shift, 468, 470, 471, 473
- Dai, Y., 355, 536
- D'Andrea, C., 110, 125, 369, 536
- de Boer, M., 491, 536
- decoding, 460, 465, 470, 480ff, 508ff, 522ff
  - function, 460
  - nearest neighbor, *see* nearest neighbor decoding function
  - Reed-Solomon, *see* Reed-Solomon decoding
  - syndrome, *see* syndrome decoding
  - see also* Berlekamp-Massey-Sakata algorithm (BMS)
- degenerate special case, 182
- degree
  - of a polynomial, *see* total degree
  - of a variety, 284, 300–302, 508
- degree-anticompatible order, 159–162, 175, 176, 179, 180
- dehomogenize, 81, 114, 170, 172, 180, 293, 300
- delta-set 516–518, 522, 525, 529, 532
  - $\Delta_k$ , 516–518, 520, 521, 522ff
  - maximal elements in  $\Delta_k$  ( $\delta_k$ ), 517–521, 522ff
  - of an error vector ( $\Delta(e)$ ), 511–516, 518, 520, 525, 529, 532
- delta-set complement
  - minimal elements in  $\Sigma_k$  ( $\sigma_k$ ), 517, 518, 521, 522ff
  - $\Sigma(e)$ , 515, 520, 529, 532
  - $\Sigma_k$ , 516, 517, 522ff
  - $\sigma_k$ , algorithm for, 521, 527
- dense
  - polynomial, 332
  - resultant, *see* resultant, dense
  - start system, *see* start system, dense
  - system of equations, 355
- derogatory linear map, 66
- Descartes, R., 1
- Descartes Rule of Signs, 72, 73, 75
- designed distance, *see* BCH code, designed distance of
- design of experiments, 393, 402
- Devaney, R., 36, 536
- Devlin, K., x
- Diaconis, P., 404, 536
- diagonalizable matrix, 63
- Dickenstein, A., x, xi, 110, 125, 359, 370, 535–537
- Dickson's Lemma, 14, 52, 209, 497, 517
- difference of varieties ( $V \setminus W$ ), 25
- Dimca, A., 187, 537
- dimension
  - of an affine subspace, 312
  - of a linear code, 460, 463, 464, 467, 470, 471, 473, 476–480, 505
  - of a polytope, 306, 312, 358, 359, 361, 363
  - of a polyhedral complex, 408
  - of a variety, 92–94, 284, 292, 300–302, 447
- dimension theorem for a linear mapping, 257, 278
- direct sum of modules ( $M \oplus N$ ), 192, 204, 229, 232, 243, 256, 258, 418, 419
  - of graded modules, 267, 268, 275, 276, 281
- discrete Fourier transform, 477, 478, 480
- discrete valuation, 142, 143
- discriminant of a polynomial ( $\text{Disc}(f)$ ), 356
- distance function, 461
- Division Algorithm
  - in  $k[x]$ , 4, 11, 22, 48, 75, 451, 469, 481, 491, 492
  - in  $k[x_1, \dots, x_n]$ , 11, 13, 37, 163, 167, 169, 222, 223, 225, 344, 383, 400, 428, 473–476, 496, 500
  - in a free module, 211–214, 218
  - in a free module over a local ring, 236
  - in a local ring, 235, 236, *see also* Mora Normal Form Algorithm
- divisor (on an algebraic curve), 506, 508

- Dixon, A., 110, 321  
 Dixon matrices, 110, 369  
 Dixon resultant, 321, 331, 359, 370  
   software, 370  
 doubly stochastic matrix, 403  
 “downward” order (on standard  
   basis in  $R^m$ ), 211, 218–220  
 dual basis, 46  
 dual code, 467, 477, 495, 504, 505,  
   *see also* dual of evaluation  
   code  
 dual graph, *see* graph, dual  
 dual of evaluation code ( $C_a$ ), 508,  
   510, 511, 517–519, 521, 522,  
   529, 531, 532  
 dual space of a vector space  $V$  ( $V^*$ ),  
   45, 46  
 Drexler, F., 353, 537  
 Dürer, A., 393  
 Duursma, I., 531  
 Dyer, M., 363, 537
- Eagon-Northcott complex, 279  
 écart, 165, 172, 173  
 edge  
   of a cone, 435  
   of a graph, 417, 419  
   of a polyhedral complex, 409, 412  
   of a polytope, 307, 308, 360, 362  
   oriented, 418  
 eigenvalues, 56ff, 72–75, 80, 97,  
   128ff, 304  
   dominant, 60, 61  
   numerical techniques, 60, 61, 65,  
   133  
   real, 69ff  
 eigenspaces  
   generalized, 157  
   left, 64, 66  
   right, 68  
 eigenvectors, 63  
   generalized, 67, 151, 157  
   left, 63–66, 133, 134  
   right, 63, 66, 68, 133, 134  
 Eisenbud, D., 218, 262, 265, 276,  
   279, 286, 287, 299, 302, 534,  
   537  
 Ellber, G., 446, 537
- elementary row operations, *see* row  
   operations  
 elementary symmetric functions, 102  
 elimination  
   ideal, 5, 18, 26–28, 79, 184, 287,  
     291, 404, 446, 447, 506  
   order, 184, 185, 220, 396, 397, 448  
   property of a monomial order, 383,  
     384, 386, 387, 390, 396, 447  
   property of mixed orders, 162  
 Elimination property of resultants,  
   78, 79  
 Elimination Theorem, 18, 19, 26–28,  
   40, 184  
   *see also* Local Elimination  
   Theorem  
 Elkadi, M., 110, 153, 320, 373, 535,  
   537  
 Emiris, I., x, 110, 129, 131, 135, 320,  
   339, 359, 362, 363, 367–369,  
   371–375, 535–537, 544  
 encoding, 459, 460, 463, 464, 466,  
   474–476  
   function, 460, 466  
   systematic, *see* systematic,  
     encoder  
 engineering, 377  
 Equal Ideals have Equal Varieties  
   principle, 22  
 equivalent  
   analytic functions, 145  
   matrices, 207  
   modules, 229, 233  
 errata, x  
 error 459, 461, 463, 464, 481, 482  
   locations, 480, 483, 490, 511, 520  
   locator ideal ( $I_e$ ), 512–514, 520,  
     530  
   locator polynomial, 482, 490, 491,  
     511, 512  
   values, 480, 483, 490  
 error-correcting, 461–463, 465, 468  
   burst, 470, 479, 480  
   codes, 451, 459ff  
 error-detecting, 461–463, 468  
 Euclidean algorithm, 82, 480, 492  
 Euclidean geometry, 181  
 Euler characteristic, 424  
 Euler’s formula, 113

- evaluation code, 495, 502, 503, 508, 529
  - $E_a$ , 503–506, 510, 521
  - relation to Goppa code, 506
- evaluation mapping, 470, 495, 510, 511
- Ewald, G., 332, 335, 339, 362, 378, 537
- exact sequence, 247ff, 256, 257, 264, 275, 277, 278, 281, 289, 299, 300, 401, 423
  - split, 258
- exponent vector of a monomial, *see* monomial, exponent vector of
- Extension Theorem, 26, 27, 30, 62
- extraneous factor, 105–108, 369
- $\mathbb{F}_q^n$ , *see* affine,  $n$ -dimensional space over  $\mathbb{F}_q$  ( $\mathbb{F}_q^n$ )
- face
  - of a cone, 427, 433
  - of a polytope, 307, 308, 333, 334, 347, 348, 359, 360, 365, 408
  - ring, 425
- facet
  - of a polytope, 308, 309, 324, 326, 334, 335, 337, 339, 341, 342, 351
  - variable, 324–328, 330, 331
- fail of  $f$  ( $\text{fail}_e(f)$ ), 513ff, 522ff
  - see also*  $\text{fl}_e(s)$
- fan, 427
  - see also* polyhedral complex
- Farin, G., 405, 538
- Faires, J., ix, 30, 35, 534
- Faugère, C., 49, 53, 538; *see also* Gröbner conversion, FGLM algorithm
- feasible region, 378, 379, 381, 388, 389, 392
- Fenchel, W., ix, 332, 335, 339, 534
- Feng, G.-L., 531, 538
- Feng-Rao bound, 512, 518
- Feng-Rao majority voting (FRMV), 508, 512, 517, 519, 523ff
  - vote in, 525
  - see also* Berlekamp-Massey-Sakata algorithm, FRMV procedure
- Fermat system, 370
- FGLM algorithm, *see* Gröbner basis conversion, FGLM algorithm
- field
  - algebraically closed, *see* algebraically closed field
  - automorphism, 458
  - finite, *see* finite field
  - isomorphism of, 455, 458
  - of rational functions, *see* rational function field
  - prime, *see* prime field
  - residue, *see* residue field
- finite-dimensional algebra, *see* algebra
- finite element method, 405
- finite field, 110, 451ff, 459ff, 468ff, 480ff, 494ff, 508ff
- finite free resolution, 252–257, 259–262, 265
  - graded, 279, 283
  - minimal, *see* minimal graded resolution
  - see also* free resolution
- Finite Generation of Invariants, 295
- finite group, 294ff, 451
  - abelian, 456
- finite matrix group, *see* finite group
- Finiteness Theorem, 39, 44, 65, 290
  - in module case, 221, 484
- finitely generated module, 193, 199, 202, 206, 207, 215, 238–242, 247, 259, 260, 269, 271, 274, 281, 283, 296
- finitely generated monoid, 497, 508
  - see also* order domain, standing assumptions on
- First Fundamental Theorem of Invariant Theory, 98
- First Isomorphism Theorem, *see* Fundamental Theorem, of Homomorphisms
- first syzygy module, 255
  - see also* syzygy module
- Fitting
  - equivalent matrices, 207
  - ideal, *see* Fitting invariant
  - invariant ( $F_i(M)$ ), 241, 242, 245

- Fitzpatrick, P., x, 480, 484, 487, 488, 538
- fixed point iteration, 35, 36
- $\text{fl}_e(s)$ , 514, 522ff
- Fogarty, J., 327, 538
- follow generically, 183  
*see also* generic
- Formal Implicit Function Theorem, 143
- formal infinite product, 454
- formal power series, 295, 302, 422, 453, 481
- ring ( $k[[x_1, \dots, x_n]]$ ), 140–142, 153, 154, 160, 164, 167, 171, 174, 177, 179, 180, 186, 234, 238, 241
- Forney formula, 483, 490  
generalized, 520
- free module, 190, 196, 197, 202, 236, 237, 243, 245, 246, 249, 250, 257, 261, 264, 267, 274, 276, 277, 294, 298, 414, 415, 420, 484
- graded, *see* graded free module
- is isomorphic to  $R^m$ , 202
- over a local ring, 242
- twisted, *see* graded free module
- free resolution, viii, 218, 247ff, 258ff, 266ff, 298, 401
- finite, *see* finite free resolution
- graded, *see* graded, resolution
- isomorphism of, *see* isomorphic resolutions
- partial, 253; *see also* partial graded resolution
- trivial, *see* trivial resolution
- Friedberg, S., 157, 538
- Frobenius automorphism, 458, 459, 479
- Fulton, W., 322, 327, 332, 339, 351, 362, 538
- function field, *see* rational function, field
- fundamental lattice polytope, 334, 335, 338, 341
- Fundamental Theorem  
of Algebra, 23, 347  
of Homomorphisms, 57, 58, 148, 203, 458, 497
- of Discrete Subgroups of Euclidean Space, 334
- Galois, E., 29
- Galois group, 459
- Galois theory, 459, 479
- Gao, T., 363, 538
- Garcia, A., 538
- Garrity, T., x, 108, 533
- Gatermann, K., 355, 363, 544
- Gauss-Jordan elimination, 466
- GCD, 36, 41, 75, 107, 209, 287, 289, 290, 293, 294, 299, 300, 303, 364, 369, 374, 480, 492, 500
- Geil, O., 494, 495, 497, 500, 502, 515, 538
- Gelfand, I., 82, 86, 93, 95, 99, 100, 109, 316–318, 322, 323, 332, 351, 358, 359, 538
- generalized characteristic polynomial, 112, 121  
toric, 373
- generalized  
companion matrix, 134, 135  
eigenspace, *see* eigenspace, generalized  
eigenvector, *see* eigenvector, generalized
- generating function, 302, 453
- generator  
matrix (of a linear code), 460–463, 465–470, 477, 504–506  
polynomial (of a cyclic code), 469, 471, 472, 475, 477–479, 492, 521
- generic, 114–116, 121, 122, 125, 128, 129, 131, 132, 292, 356, 370, 371  
linear subspace, 284  
number of solutions, 347, 357  
polynomial in  $L(\mathcal{A})$ , 311  
system of equations, 343, 344, 346, 347, 350–354
- genus, 506, 508
- geometric Goppa code, xi, 494, 497, 506–508, 531
- geometric modeling, 294, 320, 328
- geometric series  
finite summation formula, 455

- formal summation formula, 141, 142, 154, 302, 422, 453, 454, 481
- Geometry Center at the University of Minnesota, 365
- Georg, K., 353, 533
- germ of an analytic function, 145
- getform** (Maple procedure), *see* Maple, **getform**
- getmatrix** (Maple procedure), *see* Maple, **getmatrix**
- Gianni, P., 49, 53, 538; *see also* Gröbner conversion, FGLM algorithm
- Gilbert-Varshamov bound, 464
- $GL(2, R)$ , 296, 297
- $GL(m, R)$ , 207, 295, 298
- Gloor, O., 445, 446, 533
- Goldman, R., 320, 545
- Gonzalez-Vega, L., 73, 538
- Goppa, V.D., 494
- Gorenstein codimension 3 ideal, 302
- Gorenstein duality, 153
- Gräbe, H., 166, 284, 538
- graded
  - free resolution, *see* graded, resolution
  - homomorphism, 269ff, 281, 295
  - isomorphism, 272, 275
  - matrix, 269, 270, 272
  - minimal resolution, *see* minimal, graded resolution
  - module, 255, 266ff, 280, 282, 283, 297, 302, 303, 422, 423
  - resolution, 270ff, 280ff, 295, 299, 300, 302
  - ring, 266, 290, 296, 303
  - submodule, 267, 268, 271
  - subring, 295
  - twisted module, *see* twist of a graded module
- graded free module, 267, 423
  - standard structure ( $R^m$ ), 267
  - twisted structure
    - $(R(d_1) \oplus \cdots \oplus R(d_m))$ , 268–271, 275, 277, 280, 282, 283, 290, 297, 299, 300, 302, 303, 423
- Graded Hilbert Syzygy Theorem, *see* Hilbert Syzygy Theorem, Graded
- graded reverse lex order, *see* *grevlex*
- graph
  - connected, 418, 419
  - dual, 417–419
  - edge of, *see* edge, of a graph
  - oriented edge of, *see* edge, oriented
  - vertex of, *see* vertex, of a graph
- Grayson, D., xi, 218, 537
- greatest common divisor, *see* GCD
- Green, M., 286
- Greuel, G.-M., x, 165, 166, 173, 176, 177, 538
- grevlex*, 8–13, 38, 41, 44, 45, 49, 51, 61, 74, 216, 218–221, 255, 261–263, 388, 426, 430–433, 443, 447, 448, 501, 503
- Gritzmann, P., 363, 537
- grlex*, 8–10, 219, 432, 433, 503, 504, 518
- Gröbner basis, vii–ix, 4, 14, 16–19, 27–30, 33, 37–41, 43, 45, 49ff, 61, 62, 67, 74, 82, 87, 128, 137, 145, 171, 174–177, 180, 181, 184, 189, 208, 223, 226, 232, 237, 251, 253, 255, 261–263, 267, 287, 291, 345, 353, 384, 387, 390, 393, 396, 397, 400, 426ff, 436ff, 473, 475, 476, 496, 500, 501, 512, 520, 530
  - applied to contingency tables, 404
  - in integer programming, 376, 383ff
  - for modules, 207, 211, 214ff, 231, 233, 234, 253, 259, 260, 376, 405, 413, 414, 416, 417, 421, 423, 480, 484–488, 490–492
  - for modules over local rings, 234ff
  - marked, 428ff, 436–438, 440, 444, 445
  - minimal, 441
  - monic 17, 215, 218, 232, 263, 426, 428, 438, 439; *see also* Uniqueness of Monic Gröbner Bases

- Gröbner basis (*cont.*)  
 reduced, 17, 18, 40, 55, 68, 215,  
 225, 233, 267, 343, 441, 449,  
 474, 485  
 specialization of, 343  
 universal, 429  
*see also* standard basis
- Gröbner basis conversion, 49ff, 435,  
 436ff  
 applied to Reed-Solomon  
 decoding, 488–490  
 FGLM algorithm, 49ff, 61, 376,  
 435, 436, 487, 488  
 FGLM Main Loop, 50–53  
 FGLM Main Loop, Restated, 54  
 FGLM Next Monomial, 50–53, 55  
 FGLM Termination Test, 50–52, 55  
 Gröbner Walk algorithm, xi, 436ff  
 Gröbner Walk algorithm,  
 modified, 445, 449  
 Gröbner Walk Interreduce, 441,  
 442  
 Gröbner Walk Lift, 441, 442  
 Gröbner Walk NextCone, 441,  
 442, 444, 445  
 Hilbert function-driven, 53  
 Gröbner fan, xi, 376, 426ff, 436, 437,  
 442, 443, 448  
 restricted, 434  
 Gröbner Walk algorithm, *see*  
 Gröbner basis conversion,  
 Gröbner Walk algorithm
- group  
 cyclic, *see* cyclic group  
 finite, *see* finite group  
 finite matrix, *see* finite group  
 Galois, *see* Galois group  
 invariant theory of, *see* invariant  
 theory, of finite groups  
 multiplicative, *see* multiplicative  
 group
- Gurvits, L., 363, 538  
 Gusein-Zade, S., 187, 533
- Half-space, *see* affine, half-space  
 Hall's marriage theorem, 403  
 Hamming  
 code, 462, 463, 465, 467, 468  
 distance, 461
- Hasse-Weil bound, 507  
 Serre's improvement, 507  
 Heegard, C., 480, 538, 539  
 hereditary complex, 408, 410, 412,  
 414, 418, 419, 422  
 Hermitian curve, 501, 506, 507, 520  
 Herstein, I., 71, 539  
 Herzog, J., 299, 534  
 hidden variables, 121ff, 134, 152  
 higher syzygies, *see* free resolution  
 and syzygy module  
 Hilbert, D., ix, 258, 277, 294, 539  
 Hilbert basis, 395–398, 401, 402  
 Gröbner basis algorithm for, 395,  
 396, 402  
 Hilbert Basis Theorem, 4, 14, 174,  
 179, 427  
 Hilbert-Burch Theorem, 261, 262,  
 278, 285, 292–294, 300  
 Hilbert function viii, ix, 186, 218,  
 280ff, 292, 295, 296, 299–302,  
 393, 399, 400, 425  
 Hilbert polynomial, 277, 280ff, 290,  
 292, 294, 299–302, 420, 423  
 Hilbert-Samuel multiplicity, 146  
 Hilbert series, 296, 297, 302, 422  
 Hilbert Syzygy Theorem, 258ff, 294,  
 298  
 Graded, 271, 272, 274, 277  
 Hironaka, H., 179, 539  
 Høholdt, T., 494, 508, 531, 539  
 hold generically, 345  
*see also* generic
- homogeneous coordinates, 94, 96,  
 279, 301, 322–324, 328, 329,  
 421  
 homogeneous element of a graded  
 module, 266, 267, 269  
 homogeneous ideal, 253, 266, 267,  
 281–284, 290, 301, 302, 399  
 Homogeneous Mora Normal Form  
 Algorithm, *see* Mora Normal  
 Form Algorithm, Homogeneous
- homogeneous polynomial, 2, 80, 81,  
 84–88, 91, 93, 95, 113, 114,  
 127, 166–168, 176, 180,  
 267–270, 277, 280, 290, 291,  
 295, 297, 301, 315, 317, 323,  
 399, 421, 423

- weighted, *see* weighted
  - homogeneous polynomial
- homogeneous syzygy, 210, 232
- homogenize, 81, 166, 167, 170, 180, 289, 290, 293, 300, 314, 316, 344, 358, 422
  - a resolution, 271, 276
  - in the sparse or toric context, 324, 325, 327, 330, 331
- homomorphism
  - Fundamental Theorem of, *see* Fundamental Theorem, of Homomorphisms
  - graded, *see* graded, homomorphism
  - localization of, *see* localization, of a homomorphism
  - module, *see* module homomorphism
  - ring, *see* ring homomorphism
- homotopy continuation method, 342, 353–355
  - PHCpack software, 355, 363
- homotopy system, *see* continuation system
- Hoşten, S., xi, 376, 539
- Huber, B., 339, 351, 353, 355, 361–363, 539
- Hufnagel, A., 363, 537
- Huguet, F., 458, 542
- Huneke, C., 286, 299, 537
- hyperplane, 338, 340
  - at infinity, 96, 507
- hypersurface, 69
- ideal, 2, 192, 469, 473, 478, 495
  - basis of, *see* basis, of an ideal
  - comaximal, *see* comaximal ideals
  - elimination, *see* elimination ideal
  - error locator, *see* error, locator ideal
  - generated by  $f_1, \dots, f_s$  ( $(f_1, \dots, f_s)$ ), 2, 22
  - Gorenstein codimension 3, *see* Gorenstein codimension 3 ideal
  - homogeneous, *see* homogeneous ideal
  - intersection, *see* intersection, of ideals
  - maximal, *see* maximal ideal
  - membership problem, 6, 174, 208
  - monomial, *see* monomial ideal
  - of a set of points, 54, 262, 263, 284ff, 302
  - of a variety ( $\mathbf{I}(V)$ ), 22, 23, 25
  - of initial forms ( $(\text{in}_w(I))$ ), 439–441
  - of  $i$ th minors ( $I_i(A)$ ), 241, 242, 245
  - of leading terms ( $(\text{LT}(I))$ ), 14, 38, 145, 158, 168, 174, 175, 177–179, 281, 399, 400, 427, 428, 439, 440, 448, 499, 516
  - primary, *see* primary, ideal
  - primary decomposition of, *see* primary, decomposition
  - prime, *see* prime, ideal
  - principal, *see* principal ideal
  - product, *see* product, of ideals
  - quotient, *see* quotient ideal
  - radical, *see* radical, ideal
  - radical of, *see* radical, of an ideal
  - sum, *see* sum, of ideals
  - variety of, *see* variety, of an ideal
  - zero-dimensional, *see* zero-dimensional ideal
- Ideals, Varieties, and Algorithms* (Cox, Little, O’Shea), vii–ix, 4, 11, 13, 15, 16, 18, 19, 22, 24, 25, 27, 36, 37, 39, 41, 52, 58, 78, 79, 87, 91, 92, 152, 156, 157, 171, 176, 180–183, 185, 187, 209, 210, 213, 223, 232, 266, 267, 281, 283, 287, 295, 296, 298, 299, 304, 316, 343, 344, 356, 383, 385–387, 399, 400, 421, 449, 458, 469, 473, 475, 492, 497, 536
- Ideal-Variety Correspondence, 23, 25
- image, 148, 190, 195, 203, 247, 248, 250–253, 255–257, 271–275, 289, 322, 324, 382, 423, 506, 508, 510
- Implicit Function Theorem, 354
- implicitization, 86, 287, 294, 314, 436
  - via resultants, 82, 87, 291, 320
  - via Gröbner Walk, 446–450



- information
  - positions, 463, 474–476
  - rate, 464
- initial form of  $f$  ( $\text{in}_{\mathbf{w}}(f)$ ), 438ff
- initial value problem, 354
- injective, 248, 256, 273, 300, 329, 357, 400, 458, 459
- inner product, 467, 477
- Insel, A., 157, 538
- Integer Polynomial property of resultants, 78, 79
- integer programming, viii, ix, 376ff
- integer programming problem, 376ff, 393, 430
  - Gröbner basis algorithm for solving, 385, 386, 391
  - Gröbner basis software for, *see* CoCoA, `intprog` package *and* Singular, `intprog` package
  - standard form of, *see* standard form
- integer row operation, 356, 357
- integral domain, 143, 144, 495
- interior cell of a polyhedral complex, *see* cell, interior, of a polyhedral complex
- interior of a cone, 432, 433
- Intermediate Value Theorem, 33
- interpolation, 66, 68, 112, 134
  - cubic spline, 407
  - dense, 112
  - Lagrange interpolation formula, 43, 46
  - probabilistic, 112
  - sparse, 112
  - Vandermonde, 112
- intersection
  - of ideals ( $I \cap J$ ), 6, 18, 25, 45, 155, 156, 186, 230, 231, 261
  - of submodules ( $M \cap N$ ), 202, 203, 230, 231, 256
  - of varieties ( $V \cap W$ ), 20, 21, 24, 25
- interval arithmetic, 69
- invariant of a group action, 294ff
- invariant theory
  - First Fundamental Theorem of, *see* First Fundamental Theorem of Invariant Theory
  - of finite groups, 280, 294ff, 383
  - relation to combinatorics, 392
  - Second Fundamental Theorem of, *see* Second Fundamental Theorem of Invariant Theory
- inversion problem, 315
- inward normal, *see* inward pointing normal
- inward pointing facet normal, *see* inward pointing normal
- inward pointing normal, 308, 324, 325, 336, 337, 339, 341, 348, 351
  - primitive, 309, 324, 334, 335, 342, 347
- irreducible
  - component of a variety, 92, 181–183, 373
  - factor, 106, 151
  - polynomial, 86, 90, 92, 105, 157, 316, 451–456, 458
  - variety, 25, 92, 94, 184, 505, 507
- isobaric polynomial, 106, 114
- isolated singularity, *see* singularity, isolated
- isolated solution, 146, *see also* singularity, isolated
- isomorphic resolutions, 272, 273
- isomorphism
  - field, *see* field, isomorphism of
  - graded, *see* graded, isomorphism of
  - module, *see* module isomorphism of resolutions, *see* isomorphic resolutions
  - ring, *see* ring, isomorphism of
  - see also* First, Second, and Third Isomorphism Theorems
- Jacobian matrix or determinant, 88, 113, 157, 354
- Jacobson, N., 474, 539
- Jouanolou, J., 95, 96, 98, 100, 101, 108, 110, 539
- Julia set, 36
- $k^n$ , *see* affine,  $n$ -dimensional space over  $k$  ( $k^n$ )
- Kalkbrenner, M., 436, 446, 535, 539
- Kaltofen, E., 111, 535

- Kapranov, M., 82, 86, 93, 95, 99,  
100, 109, 316–318, 322,  
323, 332, 351, 358, 359,  
538, 539
- Kapur, D., 110, 359, 370, 535, 539
- kbasis** (Maple procedure), *see*  
Maple, **kbasis**
- kernel, 54, 148, 149, 190, 195, 197,  
198, 203, 204, 246–248, 250,  
252, 253, 255–258, 272–279,  
289, 394–397, 402, 404, 413,  
414, 423, 425, 497, 511
- key equation, 482–484, 486–489, 491,  
493
- Khetan, A., 359, 539
- Khovanskii, A.G., 351, 352, 540
- Kim, M.-S., 446, 537
- Kim, S., 355, 536
- Kirwan, F., 152, 540
- Klein Quartic curve, 507, 508
- Klimaszewski, K., 287, 543
- known syndromes, 511, 512, 530
- Koblitz, N., 459, 540
- Kögl, C., xi
- Kojima, M., 355, 536
- Koszul  
  complex, 265, 289, 299, 300  
  relations, 241
- Kozen, D., 73, 533
- Krasauskas, R., 328, 536, 540
- Kreuzer, M., 217, 540
- Krishnan, S., 373, 540
- Küchlin, W., 445, 446, 533
- Kushnirenko, A.G., 351, 540
- $L(\mathcal{A})$ , 311, 315, 321, 322, 331, 345,  
358, 366  
  *see also* Laurent polynomial
- $L_a$  subspace of an order domain,  
503, 504, 510–512, 515, 518,  
519, 524
- Lagrange’s Theorem, 471
- LaScala, R., 391, 534
- Lakshman, Y., 111, 535
- lattice, 334, 340
- lattice polytope, 306, 309, 319, 333,  
336
- Laurent  
  monomial, 311, 348, 357  
  polynomial ( $k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ ), 311,  
313, 315, 345, 346, 352, 357,  
370, 371, 373, 376, 388, 389,  
395  
  *see also*  $L(\mathcal{A})$
- Lazard, D., 49, 53, 60, 165, 166, 180,  
538, 540; *see also* Gröbner  
  conversion, FGLM algorithm
- LCM, 15, 209, 210, 222, 223, 259,  
479
- leading  
  coefficient ( $LC(f)$ ), 11, 161, 163,  
172, 212  
  monomial ( $LM(f)$ ), 11, 161, 163,  
172, 212, 259, 496, 500, 509  
  term ( $LT(f)$ ), 10, 11, 15, 53, 55,  
161, 163, 167–173, 175, 176,  
178, 187, 212–216, 218, 219,  
223, 224, 259, 264, 427, 428,  
435, 436, 439, 440, 486, 487,  
494
- Leonard, D., 520, 540
- least common multiple, *see* LCM
- Leichtweiss, K., 332, 335, 339, 540
- length of a finite free resolution, 252,  
259–265, 271, 272, 277
- level curve, 379
- Lewis, R., 110, 370, 540
- lex*, 8, 9, 11–14, 17, 18, 27, 29, 33,  
40, 41, 49–56, 62, 67, 68, 128,  
145, 158, 161, 183, 211–214,  
225, 232, 251, 259, 343, 384,  
387, 426, 443, 449, 476, 496,  
498, 500, 501, 503
- lexicographic order, *see lex*
- Li, T.Y., 353, 355, 363, 538, 540
- Li, X., 363, 540
- lift of a polytope  $Q$  ( $\widehat{Q}$ ), 362, 363,  
366
- lifting initial forms (in Gröbner  
Walk) 441, 444; *see also*  
Gröbner basis conversion,  
Gröbner Walk algorithm
- line at infinity, *see* hyperplane, at  
infinity
- linear code, 451, 460, 462, 464, 466,  
468, 470, 471, 473, 495, 510
- linear programming, 376, 379
- linear system, 508

- linearly independent set in a module,
  - 191, 195, 196
  - see also* module, basis of
- Little, J., 509, 536, 539, 540; *see also*
  - Ideals, Varieties, and Algorithms*
- Local Division Algorithm, *see*
  - Division Algorithm, in a local ring
- Local Elimination Theorem, 184, 185
- local intersection multiplicity, 146
- local order, 159, 160, 162–167, 171,
  - 172, 174, 176, 177, 179, 180
  - for a module over a local ring, 235
- local ring, viii, 137, 139–141, 143,
  - 146, 153, 155, 156, 158, 184, 234ff, 264
- localization, 138–141, 143, 144,
  - 146–148, 152, 154, 160, 162, 164, 167, 171, 174, 177, 178, 180, 182, 184–187, 192, 234, 237, 239, 247
  - at a point  $p$ , 183, 234, 235, 245
  - of an exact sequence, 264
  - of a homomorphism, 264
  - of a module, 234–237, 239, 240, 243, 245, 261, 264
  - with respect to  $>$ 
    - $(\text{Loc}_{>}(k[x_1, \dots, x_n]))$ ,
    - 161–163, 166, 167, 170–172, 174, 175
- Loehr, N., xi
- Logar, A., 197, 540
- logarithmic derivative, 454
- long exact sequence, 256
- Loustaunau, P., vii, 4, 11, 14, 16, 18,
  - 24, 27, 39, 185, 211, 213, 376, 533
- lower facet, 363, 366
- $\mu$ -basis, 288, 289, 291–293, 298, 303
- $\mu$ -constant, 188;
  - see also* Milnor number
- $\mu^*$ -constant, 188; *see also* Teissier
  - $\mu^*$ -invariant
- Macaulay 2*, xi, 41, 217–219, 231,
  - 253, 254, 271, 384, 397, 423, 476
- gb**, 219
  - gens**, 219
  - hilbertSeries**, 423
  - ideal**, 254
  - matrix**, 219
  - resolution**, 253, 254, 271
  - syz**, 231
  - web site, 218
- Macaulay, F., ix, 106–108, 110, 369, 540
- MacMahon, P., 402
- MacWilliams, F., 459, 471, 540
- Madden, J., xi
- magic squares, 328, 393ff
  - symmetric, 403
- Magma, 448
- Mall, D., 436, 535
- Manocha, D., 110, 112, 120, 121,
  - 126, 135, 369, 373, 535, 540, 541, 544
- Maple, xi, 10, 12, 16, 17, 20, 24,
  - 27–34, 39–43, 46–48, 60–63, 69, 74, 75, 79, 118, 120, 126, 176, 217, 221, 343, 344, 388, 447, 448, 456, 457, 466, 475, 476, 489, 490
  - alias**, 456, 466, 475
  - array**, 466
  - CASA package**, 448
  - charpoly**, 74
  - collect**, 221, 475
  - Digits**, 31, 32
  - eigenvals**, 63
  - expand**, 32
  - Expand**, 475
  - factor**, 28, 29, 118, 151
  - fsolve**, 31–34, 120, 126
  - Gaussjord**, 466
  - gbasis**, 17, 27, 29, 62, 221, 448, 476
  - getform**, 74, 75
  - getmatrix**, 69, 74, 80, 98
  - Groebner package**, 10, 12, 16, 27, 41, 221, 388, 447, 448, 476
  - implicitplot3d**, 20, 24
  - is\_finite**, 47, 48
  - kbasis**, 46–48, 62
  - lexdeg** “bug”, 221
  - minpoly**, 60
  - mod**, 457, 466, 475, 476, 489, 490

- MR package, 110
- MulMatrix, 63, 69
- normal, 457
- Normal, 457, 489, 490
- normalf, 12, 39, 74
- Ore\_algebra package, 221, 476
- poly\_algebra, 221, 476
- Rem, 475, 489
- resultant, 79
- RootOf, 29, 30, 118, 457, 466, 475
- SetBasis, 46–48, 62, 69
- simplify, 43, 48
- solve, 29
- subs, 28, 31, 32, 489, 490
- termorder, 221, 476
- univpoly, 41, 47, 48
- zdimradical, 48
- Marinari, M., 54, 153, 541
- marked Gröbner basis, *see* Gröbner basis, marked
- Massey, J., 480
- Mathematica*, 61, 176, 217, 388, 448
- matrix order ( $>_M$ ), 9, 10, 12, 13, 160, 161, 173, 176, 388, 429ff, 437ff, 498, 503
- Matsumoto, R., 499
- maximal ideal, 5, 42, 45, 138–140, 143, 144, 146, 148, 149, 155, 237–239, 244, 264, 452
- maximum distance separable code, 471
- $m$ -dimensional cyclic code, *see* cyclic,  $m$ -dimensional code
- MDS code, *see* maximum distance separable code
- Melancholia*, 393
- Mereb, M., 49
- metric, 461
- Meyer, F., 294, 541
- Milnor, J., 154, 541
- Milnor number ( $\mu$ ), 145, 154, 155, 158, 180, 181, 186, 187
- Minimair, M., 110
- minimal
  - element (with respect to a monomial order), 486–488, 490, 492
  - graded resolution, 271–274, 276, 277, 297
  - number of generators of a module ( $\mu(M)$ ), 236ff
  - polynomial (of a linear map), 58–60, 67
  - polynomial (of a primitive element), 458
  - presentation, 240ff
  - resolution, *see* minimal, graded resolution
  - set of generators of a module, 191, 198, 203, 236ff, 240, 247, 271, 272
  - set of generators of a monoid, *see* Hilbert basis
  - set of generators of a monomial ideal, 499, 500
- minimum distance (of a code), 462–468, 471, 473, 479, 480, 504, 505, 508, 517, 518, 520
- Feng-Rao ( $d_{FR}$ ), 518, 520, 525, 529, 532
- Minkowski sum of polytopes ( $P + Q$ ), 332–334, 337–342, 347, 359–362, 364–368, 371, 372, 374, 375
  - coherent, 366, 374
- minor of a matrix, 241, 242, 245, 261, 262, 265, 293, 300
- Mishra, B., 69, 541
- Miura, S., 499
- mixed cell of a mixed subdivision, 360–362, 368, 371
- mixed elimination-weight monomial order, 391
- mixed monomial basis, *see* monomial basis, mixed
- mixed order, 162, 176, 183
- mixed sparse resultant, *see* resultant, mixed sparse
- mixed subdivision, 339, 358, 360–363
  - coherent, 363–367, 371, 372, 375
- mixed volume, viii, 337, 338, 340, 341, 343, 345, 346, 348, 350–354, 355, 357, 358, 360–362, 367, 368, 370–372, 375
  - computing, 339, 363
  - normalized, 338, 339, 347, 350, 352, 357
  - software, 363

- Möbius inversion formula, 454
- module, viii, ix, 189ff, 247ff, 258ff, 266ff, 288, 296, 413ff, 484ff
- basis of, 195, 196, 198, 203, 204, 214, 226, 236, 244, 249, 414; *see also* free module
  - direct sum of, *see* direct sum of modules
  - equivalent, *see* equivalent modules
  - finitely generated, *see* finitely generated module
  - free, *see* free module
  - graded, *see* graded module
  - graded free, *see* graded free module
  - Gröbner basis of, *see* Gröbner basis, for modules
  - homomorphism of, *see* module homomorphism
  - isomorphism, *see* module isomorphism
  - localization of, *see* localization, of a module
  - of leading terms ( $\langle \text{LT}(M) \rangle$ ), 214, 221, 423, 484–486
  - over a local ring, 234ff, 255
  - presentation of, *see* presentation of a module
  - projective, *see* projective module
  - quotient, *see* quotient module
  - quotient of, *see* quotient of modules
  - rank of, *see* rank, of a module
  - syzygy, *see* syzygy module
  - twisted free, *see* graded free module, twisted structure
- module homomorphism, 193, 194, 197, 201, 202, 205, 207, 247ff, 279, 282, 419
- graded, *see* graded, homomorphism
  - $\text{hom}(M, N)$ , 202
  - localization of, *see* localization, of a homomorphism
- module isomorphism, 195, 200, 202–205, 220, 229, 235, 242, 248–250, 275, 278, 288, 300, 419
- graded, *see* graded, isomorphism
  - molecular structure, 320
  - Molien series, 295–298, 303
  - Molien’s Theorem, 298, 303, 304
  - Möller, H.M., 54, 60, 66, 153, 534, 541
  - $\text{Mon}(I)$  (set of ideals of leading terms), 427–429, 435, 448
  - monic polynomial, 453–455, 458
  - Monico, C., 153, 541
  - monoid, 295, 398, 401, 404, 495, 505, 506, 532
    - finitely generated, *see* finitely generated monoid
    - isomorphism of, 509
    - of pole orders, 507
  - monoid divisibility order on  $\mathbb{Z}_{\geq 0}$  ( $\gg$ ), 509, 510, 516, 517, 522ff
  - monoid operation on  $\mathbb{Z}_{\geq 0}$  ( $\oplus$ ), 509, 510, 513–515, 517, 518, 522ff
  - monoid ring ( $\mathbb{F}_q[\Gamma]$ ), 506
  - monomial, 1
    - exponent vector of, 306, 307
    - Laurent, *see* Laurent, monomial
    - relation to integer programming, 382–384, 389
  - monomial in a free module, 208ff
    - belongs to  $f \in R^m$ , 208
    - contains a basis vector, 208
    - quotient of monomials, 209
  - monomial basis, 470
    - determined by a monomial order, *see* basis monomials
    - for generic polynomials, 128, 132
    - mixed, 371, 373
  - monomial ideal, 14, 158, 209, 281, 427, 501
  - monomial order, xi, 7–10, 17, 61, 160, 162, 163, 167, 173, 176, 224, 225, 306, 399, 426ff, 448, 496, 503–505
    - adapted, 384, 385, 387, 390
    - associated to an order domain ( $\succ_{(\rho, \succ, \tau)}$ ), 498–501, 509, 512, 516, 520
    - in  $R^m$ , 207, 211, 484, 485
    - see also* matrix order ( $\succ_M$ ), ordering monomials, product order, weight order
  - monomial submodule, 209, 210, 217

- Mora, T., 49, 53, 54, 153, 164–166, 168, 172, 179, 184, 186, 427, 433, 434, 533, 538, 541; *see also* Gröbner conversion, FGLM algorithm
- Mora’s algorithm for modules, 236
- Mora Normal Form Algorithm, xi, 166, 167, 170, 171, 173–176, 179, 184, 185
- Homogeneous, 167, 170, 172, 173
- Moreno, C., 507, 541
- Morley forms, 110
- Morrison, I., 434, 533
- Mourrain, B., 66, 110, 135, 153, 320, 369, 370, 373, 534, 535, 537, 541
- moving
  - hyperplane, 293, 301
  - line, 287, 288, 301
  - line basis, *see*  $\mu$ -basis
- multidegree (multideg( $f$ )), 161, 163
- multiplication map ( $m_f$ ), 56ff, 70, 71, 80, 83, 84, 96, 97, 101, 102, 118, 123, 124, 132, 150, 151, 156, 157, 373
- multiplicative group, 452, 456, 457
- multiplicity, ix, 36, 41, 44, 71, 100, 114–116, 118, 119, 121, 129, 137, 145ff, 180, 181, 186, 262, 344, 347, 356, 371
- multipolynomial resultant, *see* resultant, multipolynomial
- multires** package, *see* resultant, mixed sparse, software
- multivariable factorization, 106, 119, 120
- multivariate splines, 405, 408ff
- Mumford, D., 327, 538
- Mustăţă, M., 328, 536
- Nakayama’s Lemma, 237, 238
- National Science Foundation, x
- nearest neighbor decoding function, 462, 465
- Newton polytope of  $f$  (NP( $f$ )), 310, 311, 313, 320, 332, 333, 335, 336, 344–348, 351, 355, 358, 374, 430, 435
- Newton-Raphson method, 30, 31, 35, 36, 61, 69, 354
- Newton’s method, *see* Newton-Raphson method
- Noetherian ring, 199, 206, 207
- nonderogatory linear map, 66
- noncollinear points, 284–286, 292
- non-generic equations, 120, 121, 135, 136
- (non-standard) degree, *see* weight of a variable
- nonstandard monomial, 401, 474, 475
  - see also* standard monomial
- nontrivial solution, 81, 85–87, 90–93, 95, 97, 105
  - in sparse context, 322, 324, 326, 327, 329–331
- nontrivial splines, 411, 415, 416
- normal form, 15; *see also* remainder
- normal vector, *see* inward pointing normal
- normalized basis (of an order domain), 515, 519, 524–529
- normalized volume, *see* volume of a polytope, normalized
- Noro, M., 153, 545
- NP-complete decision problem, 363, 380
- Nullstellensatz, *see* Strong Nullstellensatz
- numerical methods, 30, 34, 72, 354
  - accumulated errors, 32, 62
  - homotopy continuation, *see* homotopy continuation method
  - Newton-Raphson, *see* Newton-Raphson method
  - root-finding, 342, 353, 354
- octahedron, 392, 422, 423
- one-to-one, *see* injective
- one variable splines, *see* univariate splines
- onto, *see* surjective
- operations research, 377
- optimization, 376, 394

- order
  - of a pole, *see* pole, order of
  - of a polynomial ( $\text{ord}(g)$ ), 172
- order domain, xi, 496ff, 508ff, 522ff
  - Archimedean, 502ff, 508ff
  - $L_a$  subspace, *see*  $L_a$  subspace of an order domain
  - normalized basis of, *see* normalized basis (of an order domain)
  - standing assumptions on, 497, 503, 508, 522
  - value monoid of, *see* value monoid of an order domain
- order function on a ring, 495ff; *see also* order domain
- ordering monomials
  - $>_r$ , 485ff
  - adapted, *see* monomial order, adapted
  - alex*, *see alex*
  - anti-graded, *see* degree-anticompatible order
  - arevlex*, *see arevlex*
  - degree-anticompatible, *see* degree-anticompatible order
  - grevlex*, *see grevlex*
  - grlex*, *see grlex*
  - in  $R^m$ , *see* monomial order, in  $R^m$
  - lex*, *see lex*
  - local, *see* local order
  - matrix, *see* matrix order ( $>_M$ )
  - mixed, *see* mixed order
  - POT, *see* POT order
  - product, *see* product order
  - semigroup, *see* semigroup order
  - TOP, *see* TOP order
  - weight, *see* weight order
  - see also* monomial order
- ordinary differential equations (ODEs), 354
- ordinary double point, *see* singularity, ordinary double point
- oriented edge, *see* edge, oriented
- O’Shea, D., 536; *see also Ideals, Varieties, and Algorithms*
- O’Sullivan, M., xi, 494, 497, 502, 503, 508, 529, 531, 541
- Ostebee, A., x
- outward normal, 309, 363
  - see also* inward pointing normal
- #P-complete enumerative problem, 363
- $\mathbb{P}^n$ , *see* projective,  $n$ -dimensional space
- Pan, V.Y., 135, 534
- parallelogram, 181, 182
- parameters of a code ( $[n, k, d]$ ), 463, 464, 467, 495
- parametrization, 82, 86–88, 93, 139, 140, 143, 279, 280, 287ff, 299–301, 313, 315, 321, 437, 445, 448
- parametrized solution, 354
- parity check
  - equations, 510
  - matrix, 460, 461, 463, 466–468, 504
  - position, 463, 474–476
- Park, H., 197, 541
- partial differential equations, 405
- partial graded resolution, 253, 276, 277
- partial ordering, 509
- partial solution, 27, 28
- partition (of an interval), 407, 408
- path perturbation (in Gröbner Walk), 445, 446 ; *see also* Gröbner basis conversion, Gröbner Walk algorithm
- Pedersen, P., x, 69, 70, 72, 73, 129, 319, 363, 370, 371, 542
- Peitgen, H.-O., 35, 542
- Pellikaan, R., 491, 494, 495, 497, 500, 502, 508, 515, 531, 536, 538, 539
- perfect code, 463, 468
- permutation matrix, 397–399, 402, 403
- Pfister, G., x, 165, 166, 173, 176, 177, 179, 538, 541
- PHCpack, *see* homotopy continuation method, PHCpack
- PID, 41

- piecewise polynomial function, 376, 405; *see also* splines  
 pigeonhole principle, 427, 428  
 Poisson Formula, 98  
 Poli, A., 458, 542  
 polyhedral complex, 408–410, 422, 424, 427  
   cell of, *see* cell, of a polyhedral complex  
   combinatorial data of, 416, 417, 420, 423  
   dimension of, *see* dimension, of a polyhedral complex  
   edge of, *see* edge, of a polyhedral complex  
   hereditary, *see* hereditary complex  
   pure, *see* pure complex  
   pure, hereditary, *see* pure, hereditary complex  
   simplicial, *see* simplicial complex  
   vertex of, *see* vertex, of a polyhedral complex  
 polyhedral region, 376, 378, 379, 392–394, 408  
   unbounded, 378, 394  
 polyhedral subdivision, 359, 405  
   *see also* mixed subdivision and polyhedral complex  
 polynomial, 2  
   relation to polytopes, 305, 309–311  
 polynomial ring ( $k[x_1, \dots, x_n]$ ), 2, 173, 174, 197, 204, 234, 239, 243–247, 258, 280, 295, 298, 382, 452, 495  
 polynomial splines, *see* splines  
 polytope, viii, ix, 305ff, 324, 328, 332ff, 355, 376, 378, 408  
   convex, *see* polytope  
   dimension of, *see* dimension, of a polytope  
   edge of, *see* edge, of a polytope  
   face of, *see* face, of a polytope  
   facet of, *see* facet, of a polytope  
   fundamental lattice, *see* fundamental lattice polytope  
   lattice, *see* lattice polytope  
   lift of, *see* lift of a polytope  
   Minkowski sum of, *see* Minkowski sum of polytopes ( $P + Q$ )  
   Newton, *see* Newton polytope of  $f$  ( $\text{NP}(f)$ )  
   relation to homogenizing sparse equations  
   relation to integer programming, 376, 378  
   relation to sparse resultants, 316ff, 358, 359  
   supporting hyperplane of, *see* supporting hyperplane  
   vertex of, *see* vertex, of a polytope  
   volume of, *see* volume of a polytope  
 “position-over-term”, *see* POT order  
 positive orthant ( $(\mathbb{R}^n)^+$ ), 429ff, 436, 437, 448  
 POT order, 211–215, 218, 220, 221, 232, 233, 235, 485  
 power method, *see* eigenvalues, numerical techniques  
 presentation matrix, 199–201, 204, 206–208, 227, 228, 234, 235, 239–241, 243, 249, 250  
   of  $\text{hom}(M, N)$ , 202  
   *see also* minimal, presentation  
 presentation of a module, 249–251, 257, 260  
 primary  
   decomposition, 54, 151, 153, 156, 157  
   ideal, 156  
 prime  
   field, 451  
   ideal, 5, 25, 143, 144, 147, 184  
 primitive  
   element (of a field extension), 456, 458, 470, 476, 479, 480, 489, 504  
   inward pointing normal, *see* inward pointing normal, primitive  
   vector in  $\mathbb{Z}^n$ , 309, 339, 348, 356  
 principal axis theorem, 71  
 principal ideal, 5, 261, 469, 501  
 Principal Ideal Domain, *see* PID  
 prism, 341  
 product  
   of ideals, 25, 155  
   of rings, 46, 148, 149, 156



- product order, 18, 184
- projection, 304
- projective
  - closure, 506
  - dimension of a module, 262
  - embedding, 508
  - module, 204, 242ff, 258
  - $n$ -dimensional space ( $\mathbb{P}^n$ ), 91, 96, 97, 114, 125, 266, 279, 280, 282–286, 290, 292, 300, 301, 303, 315, 320, 322–324, 327–329, 467
  - plane, 507, 508
- Projective
  - Extension Theorem, 92, 120
  - Images principle, 323
  - Varieties in Affine Space principle, 96
- projective variety, 20, 91, 266, 283, 284, 327, 328, 401
  - affine part ( $\mathbb{C}^n \cap V$ ), 96
  - part at infinity ( $\mathbb{P}^n \cap V$ ), 96
- Puiseux expansion, 346
- pure complex, 408, 410, 417
- pure, hereditary complex, 411ff
  
- qhull, 366
- Qi, D., 287, 543
- QR algorithm, 61
- quadratic formula, 115
- quadratic splines, 406, 407, 419
- quadric surface, 301
- Quillen, D., 197, 204, 243, 542
- Quillen-Suslin Theorem, 197, 204, 244
- quintic del Pezzo surface, 302
- quotient ideal ( $I : J$ ). 6, 19, 25, 186, 232
  - see also* stable quotient of  $I$  with respect to  $f$
- quotient of modules ( $M/N$ ), 193, 200, 202, 203, 217, 221, 238–240, 248, 250, 256, 257, 268, 484
- quotient of modules ( $M : N$ ), 203
- quotient ring ( $k[x_1, \dots, x_n]/I$ ), 37, 38, 115, 123, 128, 137, 144–148, 150, 152, 154, 155, 157, 177–180, 185, 186, 192, 262, 281, 290, 292, 313, 345, 371, 389, 393, 395, 399, 402, 425, 436, 451, 453, 455, 460, 469, 471, 472, 474–477, 495–502, 506, 507, 511, 512, 520
- $\mathbb{R}^n$ , *see* affine,  $n$ -dimensional space over  $\mathbb{R}$  ( $\mathbb{R}^n$ )
- radical
  - ideal, 4, 24, 25, 42–46, 48, 49, 67, 68, 71, 128, 150
  - membership test, 182
  - of an ideal  $I$  ( $\sqrt{I}$ ), 4, 23, 25, 41, 44, 45, 48, 64
- Radical Ideal Property, 4
- Raimondo, M., 179, 184, 186, 533
- Ramshaw, L., xi, 375
- rank
  - of a matrix, 71, 94, 239, 244, 245, 329
  - of a module, 244, 245
  - of a symmetric bilinear form over  $\mathbb{R}$ , 71, 72, 74
- Rao, T.R.N., 531, 538
- rational function, 2, 265, 287, 288, 294, 481, 498, 506–508
  - field ( $k(x_1, \dots, x_n)$ ), 2, 265, 278, 343, 356
  - field of transcendence degree one, 494
- rational mapping, 302, 508
- rational point over  $\mathbb{F}_q$  ( $X(\mathbb{F}_q)$ ), 495, 502, 504–507, 510, 511
- rational
  - normal curve, 279, 301
  - normal scroll, 301
  - quartic curve, 253, 300
- received word, 461, 465, 480, 482, 483, 489–491, 511, 518, 520
- recurrence relation, 481, 491
- REDUCE, 41
  - CALI package, 176, 217, 231, 236, 253, 255
- reduced Gröbner basis, *see* Gröbner basis, reduced
- reduced monomial, 107, 108
  - in toric context, 331
- reducible variety, 182

- reduction of  $f$  by  $g$  ( $\text{Red}(f, g)$ ),  
163–165, 167, 170, 172, 213
- Reed-Muller code, 504, 505
- Reed-Solomon  
code, 470–472, 475–479, 480ff,  
494, 495, 502, 521  
decoding, 480ff, 510, 511
- Rege, A., 129, 371, 373, 537
- Reif, J., 73, 533
- Reisner, G., 425
- relations among generators, 194,  
198, 199, 204; *see also* syzygy
- remainder, 11–13, 15, 16, 18, 37–39,  
48, 50, 52, 57, 75, 80, 83, 383,  
387, 389, 391, 400, 451, 469,  
473–475, 481, 488, 491, 496,  
497, 500; *see also* Division  
Algorithm  
in local case, 167, 174, 175,  
178–180; *see also* Moral  
Normal Form Algorithm  
in module case, 212ff, 225, 236  
remainder arithmetic, 37, 38  
Uniqueness of Remainders, 15
- removable singularity, 36
- residue classes, 238; *see also* coset
- residue field ( $k = Q/m$ ), 238
- Research Institute in Symbolic  
Computation (RISC), at  
University of Linz, 448
- resolution  
finite free, *see* finite free resolution  
free, *see* free resolution  
graded, *see* graded, resolution  
homogenization of, *see*  
homogenize, a resolution  
isomorphism of, *see* isomorphic  
resolutions  
length of, *see* length of a finite free  
resolution  
minimal, *see* minimal resolution  
minimal graded, *see* minimal,  
graded resolution  
partial graded, *see* partial graded  
resolution  
trivial, *see* trivial resolution
- resultant, viii, ix, 77ff, 313ff, 357ff  
 $\mathcal{A}$ -resultant, *see* resultant, sparse  
and multiplicities, 151, 152  
computing, 102ff, 357ff  
degree of, 95, 106, 107, 317, 358,  
367, 374  
dense, 317, 369  
geometric meaning, 90ff  
mixed Bézout–Sylvester, 370  
mixed, *see* resultant, mixed sparse  
mixed sparse, 357ff  
mixed sparse, software, 369  
multipolynomial, vii, 17, 84ff, 95ff,  
102ff, 114ff, 152, 313–319,  
322–324, 345, 358, 359, 364,  
367  
properties of, 78, 95ff  
of two polynomials, 77ff  
residual, 320  
solving equations via, *see* solving  
polynomial equations  
sparse, viii, 88, 112, 121, 135,  
313ff, 322–325, 327, 329–331,  
345, 357, 359, 374  
Sylvester determinant for, 77, 292,  
369  
(unmixed) sparse resultant, 358  
 $u$ -resultant, *see*  $u$ -resultant
- Reynolds operator, 303
- Richter, P., 35, 542
- Riemann-Roch Theorem, 508
- ring  
Cohen-Macaulay, *see*  
Cohen-Macaulay ring  
commutative, *see* commutative  
ring  
convergent power series, *see*  
convergent power series ring  
formal power series, *see* formal  
power series, ring  
homomorphism of, 57, 148, 289,  
295, 382, 395, 425, 458, 497  
integral domain, *see* integral  
domain  
isomorphism of, 46, 49, 144, 148,  
152, 153, 156–158, 313, 389,  
395, 474–476, 497, 501, 506,  
507  
localization of, *see* localization  
Noetherian, *see* Noetherian ring  
of fractions, 139, 144, 162  
of invariants ( $S^G$ ), 295ff, 303, 304

ring (*cont.*)

- polynomial, *see* polynomial ring
- product of, *see* product, of rings
- quotient, *see* quotient ring
- valuation, *see* valuation ring
- $R^m$ , *see* free module
- $R$ -module, *see* module
- Robbiano, L., 10, 217, 391, 427, 433, 434, 534, 540–542
- robotics, 446
- Rojas, J.M., x, 351, 353, 357, 369, 373, 542
- Rose, L., 405, 414, 417, 418, 429, 534, 542
- Rouillier, F., 73, 153, 538, 542
- row operation, 206
  - integer, *see* integer row operation
- row reduction, 466
- Roy, M.-F., 69, 70, 72, 73, 538, 542
- Ruffini, P., 29
  
- Saints, K., 480, 538, 539
- Saito, K., 287, 543
- Sakata, S., 480, 531, 542
- Salmon, G., 89, 109, 542
- Samorodnitsky, A., 363, 538
- Saxena, T., 110, 370, 539
- Schenck, H., xi, 405, 420, 543
- Schmale, W., x
- Schreyer, F.-O., 223, 286, 289, 543
- Schreyer's Theorem, 224, 236, 251, 253, 255, 259–261, 263, 414
- Schrijver, A., 377, 534
- Schumaker, L., 418, 420, 533, 543
- Second Fundamental Theorem of Invariant Theory, 99
- Second Isomorphism Theorem, 203
- second syzygies, 247, 251, 252, 255; *see also* syzygy module
- Sederberg, T., 234, 287, 288, 292, 294, 536, 543
- Segre map, 324
- semidefinite programming, 73
- semigroup, 496; *see also* monoid
  - order, 160–163, 166, 167, 170, 171, 173–176, 180, 184; *see also* matrix order ( $>_M$ )
- Serre, J.-P., 197, 204, 243, 507, 543

- Serre's conjecture, *see* Serre's problem
- Serre's problem, 197, 204, 243; *see also* Quillen-Suslin Theorem
- Shafarevich, I., 92, 94, 96, 97, 100, 543
- Shannon's Theorem, 464
- Shape Lemma, 67, 128, 426
- shifted module, *see* twist of a graded module  $M$
- short exact sequence, 256, 257
- Shurman, J., x
- signature of a symmetric bilinear form over  $\mathbb{R}$ , 71, 72, 74
- simple root, 36
- simplex, 307, 309, 312, 340, 346, 363
- simplicial complex, 420, 421, 423
- Singer, M., x
- Singleton bound, 464, 471
- Singular**, 41, 165, 176, 177, 182, 183, 187, 188, 217, 219, 220, 231, 232, 253, 255, 263, 384, 387, 388, 476
  - homepage, 176
  - ideal, 177, 183, 255, 263, 388
  - intprog package, 391
  - milnor package, 187
  - module, 220
  - poly, 183, 388
  - reduce, 183, 388
  - res, 255
  - ring, 177, 183, 219, 232, 387
  - sres, 263
  - std, 177, 183, 220, 388
  - syz, 231
  - vdim, 177
  - vector, 220
- singular point, *see* singularity
- singularity, 137, 154
  - isolated, 154, 155, 187, 188
  - ordinary double point, 158
- skew-symmetric matrix, 302
- slack variable, 381–383
- Sloane, N., 459, 471, 540
- smooth curve, 507
- software
  - for Dixon resultants, *see* Dixon resultant, software

- for mixed volumes, *see* mixed volumes, software
- for sparse resultants, *see* resultant, mixed sparse, software
- see also* CoCoA, Fermat system, *Macaulay 2*, Magma, Maple, REDUCE, Singular
- solutions at  $\infty$ , 115, 118, 121, 151, 344, 345
- see also* projective variety, part at infinity
- solving polynomial equations, viii, ix, 49, 66, 342
- generic number of solutions, *see* Bezout's Theorem, Bernstein's Theorem
- real solutions, 69ff
- via eigenvalues, 56ff, 128ff, 371
- via eigenvectors, 63ff, 128ff, 371
- via elimination, 26ff, 49, 353
- via homotopy continuation, *see* homotopy continuation method
- via resultants, 114ff, 320, 344, 345, 353, 358, 370ff
- via toric and unirational varieties, 320
- see also* numerical methods
- Sommese, A., 373, 543
- span of  $f$  ( $\text{span}_e(f)$ ), 513ff, 520ff
- see also*  $\text{sp}_e(s)$
- sparse Bézout's Theorem, *see* Bernstein's Theorem
- sparse polynomial, 313, 344
- see also*  $L(\mathcal{A})$
- sparse resultant, *see* resultant, sparse
- special position (curve in), 507, 508
- spectral theorem, 71
- Speder, J.-P., 188
- $\text{sp}_e(s)$ , 514, 522ff
- Spence, L., 157, 538
- splines, viii, ix, 376, 405ff
  - bivariate, *see* bivariate splines
  - $C^r$ , *see*  $C^r$  splines
  - cubic, *see* cubic, spline
  - multivariate, *see* multivariate splines
  - nontrivial, *see* nontrivial splines
  - one variable, *see* univariate splines
  - quadratic, *see* quadratic splines
  - trivial, *see* trivial splines
  - univariate, *see* univariate splines
  - see also* piecewise polynomial functions
- split exact sequence, *see* exact sequence, split
- $S$ -polynomial, 15, 16, 175, 217, 222, 251, 383, 434
- square-free part of  $p$  ( $p_{red}$ ), 41–43, 157
- stable quotient of  $I$  with respect to  $f$  ( $I : f^\infty$ ), 185, 186
- standard basis
  - of an ideal, viii, 174ff, 180ff
  - of a module over a local ring, 236
  - of  $R^m$ , 194, 196, 200, 217, 230, 233, 259, 260, 264, 268, 269, 271, 274, 279, 485–487, 492
  - of  $\mathbb{R}^m$ , 309, 422, 435
- standard form
  - of an integer programming problem, 381, 382, 384, 387, 390
  - of a polynomial 402; *see also* remainder
- standard monomial, 38, 177–180, 399, 400, 474, 475, 499, 510
- basis, 179
- see also* basis monomials
- Stanfield, M., x
- Stanley, R., 297, 298, 392, 425, 543
- starting order (for Gröbner Walk), 436, 443, 447
- start system (in homotopy continuation), 354, 355
- dense, 355
- state polytope, 435
- statistics, 393, 402
- Steinwandt, R., xi
- Sterk, H., xi
- Stetter, H.J., 54, 60, 65, 66, 135, 153, 533, 541, 543
- Stichtenoth, H., 506, 507, 538, 543
- Stillman, M., xi, 218, 405, 537, 543
- Strang, G., 420, 423
- Strong Nullstellensatz, 23, 42, 44, 45, 59, 67, 90, 105, 148, 155, 156, 182

- Sturmfels, B., ix–xi, 73, 88, 98, 99, 110, 125, 129, 153, 197, 218, 298, 319, 321–323, 339, 351, 355, 359, 361–363, 370, 371, 373, 377, 392, 395, 396, 401, 404, 429, 433, 434, 506, 534–537, 539, 540, 542–544
- Sturm sequence, 76
- Sturm's Theorem, 75, 76
- subdivision
  - algebraic (non-polyhedral), 424, 425
  - coherent, *see* mixed subdivision, coherent
  - mixed, *see* mixed subdivision
  - polyhedral, *see* polyhedral complex *and* polyhedral subdivision
- subfield, 457
- submatrix, 470
- submodule, 190, 192, 193, 197, 199
  - generated by a set  $(\langle \mathbf{f}_1, \dots, \mathbf{f}_s \rangle)$ , 190, 192, 193
  - graded, *see* graded, submodule of  $R^m$  via ideals, 217, 218
- Submodule Membership Problem, 207, 208, 210, 214
- submonoid, 395, 396
  - generated by a set  $(\langle m_1, \dots, m_t \rangle)$ , 497, 498, 500
- subpolytope, 341
- subring
  - generated by  $f_1, \dots, f_n$  ( $k[f_1, \dots, f_n]$ ), 382, 383, 385, 506
  - membership test, 382, 383, 389, 390
- sudden death approach (in Gröbner Walk) ; 445, 446, 448; *see also* Gröbner basis conversion, Gröbner Walk algorithm
- sum
  - of ideals  $(I + J)$ , 6, 24, 25
  - of squares, 73
  - of submodules  $(M + N)$ , 201–203, 256
- supporting
  - hyperplane of a polytope, 308, 309, 324, 340
  - line, 379
- surjective, 248, 249, 258, 271, 278, 295, 327, 328, 357, 382, 400, 458
- Suslin, A., 197, 204, 243, 544
- $S$ -vector ( $S(\mathbf{f}, \mathbf{g})$ ), 215, 216, 224, 225
  - over a local ring, 236
- Swanson, I., xi
- Sweedler, M., x
- Sylvester determinant, *see* resultant, Sylvester determinant for
- Sylvester matrices, 369
- symbolic
  - computation, 61, 72
  - parameter, 343
- symmetric
  - bilinear form, 70, 71, 74
  - magic square, *see* magic square, symmetric
- syndrome, 465, 468, 480, 490, 510–512, 521
  - decoding, 465, 480, 491
  - known, *see* known syndromes
  - mapping, 510–513, 518, 519, 524–528, 530, 532
  - polynomial, 481, 483, 491
- systematic
  - encoder, 463, 474
  - generator matrix, 463, 466, 467
- syzygy, viii, 186, 199, 206, 208, 210, 218, 222ff, 239, 240, 252, 277, 285
  - among invariants, 296, 297
  - homogeneous, *see* homogeneous syzygy
  - over a local ring, 235, 236
- syzygy module ( $\text{Syz}(f_1, \dots, f_t)$ ), 176, 199, 200, 204, 208, 210, 222ff, 234, 236, 240, 243, 245–247, 249, 250, 252, 253, 257, 259, 260, 262, 264, 265, 270, 277, 285, 288–291, 293, 294, 300, 413, 414, 416, 417, 423
- Syzygy Problem, 208
- Syzygy Theorem, *see* Hilbert Syzygy Theorem
- Szpirglas, A., 69, 70, 72, 73, 542
- Takeshima, T., 153, 545
- tangent cone, 181, 187

- target order (for Gröbner Walk),  
436, 437, 443, 445, 447
- Taylor series, 145
- Tenberg, R., 66, 541
- term, 2  
in a free module, 208, 209
- term orders (in local case), 158ff  
*see also* ordering monomials
- “term-over-position”, *see* TOP order
- ternary quadric, 88, 89
- Teissier  $\mu^*$ -invariant, 188
- Teixidor i Bigas, M., 286, 544
- tetrahedron, 422
- Third Isomorphism Theorem, 203
- third syzygy, 247, 251, 252; *see also*  
syzygy module
- Thomas, R., 376, 539, 544
- Tjurina number, 145, 155, 180, 181,  
186
- TOP order, 211, 212, 214, 218, 221,  
235, 485
- toric  
GCP, *see* generalized  
characteristic polynomial,  
toric  
ideal, 401, 506  
variety, viii, 320, 322ff, 346, 351,  
376, 392, 401, 402, 505, 506
- total degree of a polynomial  $f$   
( $\deg(f)$ ), 2, 80, 172, 317, 505
- total ordering, 7, 495
- trace of a matrix  $M$  ( $\text{Tr}(M)$ ), 70, 71,  
304
- Tran, Q.-N., 446, 544
- transform, *see* discrete Fourier  
transform
- translate of a subset of  $\mathbb{R}^n$ , 312, 313,  
330, 338, 341, 347, 364–366,  
368
- transpose of a matrix  $M$  ( $M^T$ ), 132,  
192
- Traverso, C., 53, 165, 179, 376, 380,  
390, 391, 535, 541, 544
- tree, 420
- triangulation of a polytope, 319,  
320
- trivial resolution, 276
- trivial solution, 87, 89
- trivial splines, 405, 414, 416, 419
- Trujillo, G., 73, 538
- Tsfasman, M., 494, 544
- twist of a graded module  $M$  ( $M(d)$ ),  
268, 281, 282
- twisted  
cubic, 261, 282, 284, 303, 435,  
447  
free module, *see* graded free  
module
- Using Algebraic Geometry* web site,  
x
- unbounded polyhedral region, *see*  
polyhedral region, unbounded
- unimodular row, 197, 204, 246
- union of varieties ( $V \cup W$ ), 22, 25
- Uniqueness of Monic Gröbner Bases,  
17
- Uniqueness of Remainders, *see*  
remainder
- unirational variety, 320
- unit cube in  $\mathbb{R}^n$ , 307
- unit in a ring, 138, 139, 144, 149,  
162, 163, 165–167, 170, 183,  
184, 237
- univariate splines, 405–408, 410
- universal categorical quotient, 327
- universal polynomials, 91, 101, 107,  
108
- University of Kaiserslautern, 176
- University of Linz, 448
- University of Minnesota, 365
- unshortenable, 236, 237
- “upward” order (on standard basis  
in  $R^m$ ), 218–220, 231
- $u$ -resultant, 116, 119–121, 152, 370
- Uteshev, A. Yu., 369, 534
- valuation, 502, 515; *see also* discrete  
valuation
- valuation ring, 142, 143
- value monoid of an order domain,  
496, 497, 499, 500, 502,  
505, 506, 508, 512
- van der Geer, G., 544
- van der Waerden, B., 79, 86, 116,  
544
- Vandermonde determinant, 470, 478
- van Lint, J., 459, 464, 471, 494, 539,  
544
- Varchenko, V., 187, 533

- variety, 20
  - affine, *see* affine, variety
  - degree, *see* degree, of a variety
  - dimension of, *see* dimension, of a variety
  - ideal of, *see* ideal, of a variety
  - irreducible, *see* irreducible, variety
  - irreducible component of, *see* irreducible, component of a variety
  - of an ideal  $(\mathbf{V}(I))$ , 22, 23, 25
  - reducible, *see* reducible, variety
  - toric, *see* toric, variety
  - unirational, *see* unirational variety
- Vasconcelos, W., 218, 544
- vector  $\mathbf{f}$  (in a free module), 190
- Verlinden, P., 353, 355
- Veronese
  - map, 323, 328, 329
  - surface, 301, 302
- Verschelde, J., 353, 355, 363, 373, 539, 543, 544
- vision, 320
- Vladut, S., 494, 544
- vertex
  - of a cone, 395, 422, 427
  - of a graph, 417–419
  - of a polyhedral complex, 409, 416, 425
  - of a polytope, 307–309, 326, 365, 435
- vertex monomial, 326, 327, 331
- Voisin, C., 286, 544
- volume of a polytope  $Q$  ( $\text{Vol}_n(Q)$ ), 307, 319, 321, 334ff, 358, 361, 362, 368
  - normalized, 334–338, 342
  - relation to sparse resultants, 317, 318
  - relation to mixed volume, 337, 338
- Wallack, A., 110, 369, 544
- Wampler, C., 373, 543
- Wang, X., 353, 357, 363, 538, 540, 542
- Warren, J., 108, 533
- Weierstrass Gap Theorem, 506
- weighted homogeneous components of a polynomial, 439
- weighted homogeneous polynomial, 386, 387, 439, 440, 448, 449
- weight
  - of a monomial, 498, 500, 501
  - of a variable, 106, 114, 296, 303
  - of a vector in  $\mathbb{F}_q^n$ , 461, 511, 517, 520, 525, 526, 530, 532; *see also* error-correcting, error-detecting
  - order, 10, 18, 386, 426, 433, 437, 443, 485
- weight vector, 431–433, 437ff, 448
  - compatible with a monomial order, 439, 440, 448
- Weispfenning, V., vii, 4, 11, 14–16, 18, 27, 39, 49, 55, 69, 75, 185, 429, 441, 517, 533, 545
- Welch, L., 491
- well-ordering, 7, 159, 160, 162, 163, 175, 211, 386, 495, 497
- Weyman, J., 110, 125, 359, 545
- White, J., x
- Whiteley, W., 420, 533
- Wilkinson, J., 32, 33, 545
- Woodburn, C., 197, 541
- words, *see* codewords
- Yang, L., 110, 370, 539
- Yokoyama, K., 153, 545
- Zalgaller, V., 332, 534
- Zariski closure, 25, 316, 317, 322, 324, 329, 358, 401, 506
- zdimradical**, *see* Maple, **zdimradical**
- Zelevinsky, A., 82, 86, 93, 95, 99, 100, 109, 110, 125, 316–318, 322, 323, 332, 351, 358, 359, 538, 539, 544, 545
- zero-dimensional ideal, 39–44, 47–49, 52–54, 56, 58–60, 64, 67–71, 137, 145, 148, 150, 153, 154, 157, 158, 180, 186, 435, 436
- Zero Function, 19, 22
- zeroes of a cyclic code, 478, 521
- Zhang, M., 320, 545
- Ziegler, G., 306, 545
- Zink, T., 494, 544
- Zubé, S., 328, 545