# Basic Quadratic Forms

#### Larry J. Gerstein

Graduate Studies in Mathematics Volume 90



**American Mathematical Society** 

# Basic Quadratic Forms

# Basic Quadratic Forms

Larry J. Gerstein

Graduate Studies in Mathematics

Volume 90



American Mathematical Society Providence, Rhode Island

#### **Editorial Board**

David Cox (Chair) Walter Craig N. V. Ivanov Steven G. Krantz

2000 Mathematics Subject Classification. Primary 11Exx, 12Exx, 15-XX.

For additional information and updates on this book, visit www.ams.org/bookpages/gsm-90

#### Library of Congress Cataloging-in-Publication Data

Gerstein, Larry J.
Basic quadratic forms / Larry J. Gerstein.
p. cm. — (Graduate studies in mathematics, ISSN 1065-7339 ; v. 90)
Includes bibliographical references and index.
ISBN 978-0-8218-4465-6 (alk. paper)
1. Forms, Quadratic. 2. Equations, Quadratic. 3. Number theory. I. Title.

2007062041

**Copying and reprinting.** Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

> © 2008 by the American Mathematical Society. All rights reserved. The American Mathematical Society retains all rights except those granted to the United States Government. Printed in the United States of America.
>  The paper used in this book is acid-free and falls within the guidelines

established to ensure permanence and durability.

Visit the AMS home page at http://www.ams.org/

10 9 8 7 6 5 4 3 2 1 13 12 11 10 09 08

To SUE, DAVID, and BENJY

### Contents

Preface		xi
Chapter	1. A Brief Classical Introduction	1
$\S{1.1.}$	Quadratic Forms as Polynomials	1
§1.2.	Representation and Equivalence; Matrix Connections; Discriminants	4
Exerc	ises	7
§1.3.	A Brief Historical Sketch, and Some References to the Literature	7
Chapter	2. Quadratic Spaces and Lattices	13
$\S{2.1.}$	Fundamental Definitions	13
$\S{2.2.}$	Orthogonal Splitting; Examples of Isometry and Non-isometry	16
Exercises		20
§2.3.	Representation, Splitting, and Isotropy; Invariants $u(F)$ and $s(F)$	21
$\S{2.4.}$	The Orthogonal Group of a Space	26
$\S{2.5.}$	Witt's Cancellation Theorem and Its Consequences	29
$\S{2.6.}$	Witt's Chain Equivalence Theorem	34
$\S{2.7.}$	Tensor Products of Quadratic Spaces; the Witt ring of a field	35
Exerc	ises	39
$\S{2.8.}$	Quadratic Spaces over Finite Fields	40
$\S{2.9.}$	Hermitian Spaces	44
Exercises		49

vii

Chapter 3	3. Valuations, Local Fields, and <i>p</i> -adic Numbers	51	
$\S{3.1.}$	Introduction to Valuations	51	
$\S{3.2.}$	Equivalence of Valuations; Prime Spots on a Field	54	
Exercis	Exercises 58		
§ <b>3.3</b> .	Completions, $\mathbb{Q}_p$ , Residue Class Fields	59	
$\S{3.4.}$	Discrete Valuations	63	
$\S{3.5.}$	The Canonical Power Series Representation	64	
$\S{3.6.}$	Hensel's Lemma, the Local Square Theorem, and Local Fields	69	
$\S{3.7.}$	The Legendre Symbol; Recognizing Squares in $\mathbb{Q}_p$	74	
Exercis	ses	76	
Chapter -	4. Quadratic Spaces over $\mathbb{Q}_p$	81	
$\S4.1.$	The Hilbert Symbol	81	
$\S4.2.$	The Hasse Symbol (and an Alternative)	86	
$\S4.3.$	Classification of Quadratic $\mathbb{Q}_p$ -Spaces	87	
$\S4.4.$	Hermitian Spaces over Quadratic Extensions of $\mathbb{Q}_p$	92	
Exercis	ses	94	
Chapter	5. Quadratic Spaces over $\mathbb{Q}$	97	
$\S{5.1.}$	The Product Formula and Hilbert's Reciprocity Law	97	
$\S{5.2.}$	Extension of the Scalar Field	98	
$\S{5.3.}$	Local to Global: The Hasse–Minkowski Theorem	99	
$\S{5.4.}$	The Bruck–Ryser Theorem on Finite Projective Planes	105	
$\S{5.5.}$	Sums of Integer Squares (First Version)	109	
Exercis	ses	111	
Chapter	6. Lattices over Principal Ideal Domains	113	
$\S6.1.$	Lattice Basics	114	
$\S6.2.$	Valuations and Fractional Ideals	116	
$\S6.3.$	Invariant factors	118	
$\S6.4.$	Lattices on Quadratic Spaces	122	
$\S6.5.$	Orthogonal Splitting and Triple Diagonalization	124	
$\S6.6.$	The Dual of a Lattice	128	
Exercis	ses	130	
$\S6.7.$	Modular Lattices	133	
$\S6.8.$	Maximal Lattices	136	
$\S6.9.$	Unimodular Lattices and Pythagorean Triples	138	

$\S6.10.$	Remarks on Lattices over More General Rings	141
Exerc	ises	142
Chapter	7. Initial Integral Results	145
${}_{\S{7.1.}}$	The Minimum of a Lattice; Definite Binary Z-Lattices	146
§7.2.	Hermite's Bound on min L, with a Supplement for $k[x]$ -Latti	ices149
§7.3.	Djokovič's Reduction of $k[x]$ -Lattices; Harder's Theorem	153
§7.4.	Finiteness of Class Numbers (The Anisotropic Case)	156
Exerc	ises	158
Chapter	8. Local Classification of Lattices	161
§8.1.	Jordan Splittings	161
§8.2.	Nondyadic Classification	164
§8.3.	Towards 2-adic Classification	165
Exerc	ises	171
Chapter	9. The Local-Global Approach to Lattices	175
§9.1.	Localization	176
§9.2.	The Genus	178
§9.3.	Maximal Lattices and the Cassels–Pfister Theorem	181
$\S9.4.$	Sums of Integer Squares (Second Version)	184
Exerc	ises	187
$\S{9.5.}$	Indefinite Unimodular Z-Lattices	188
§9.6.	The Eichler–Kneser Theorem; the Lattice $\mathbb{Z}^n$	191
$\S{9.7.}$	Growth of Class Numbers with Rank	196
$\S 9.8.$	Introduction to Neighbor Lattices	201
Exerc	ises	205
Chapter	10. Lattices over $\mathbb{F}_q[x]$	207
$\S{10.1}.$	An Initial Example	209
§10.2.	Classification of Definite $\mathbb{F}_q[x]$ -Lattices	210
§10.3.	On the Hasse–Minkowski Theorem over $\mathbb{F}_q(x)$	218
$\S{10.4}.$	Representation by $\mathbb{F}_q[x]$ -Lattices	220
Exerc	ises	223
Chapter	11. Applications to Cryptography	225
§11.1.	A Brief Sketch of the Cryptographic Setting	225
$\S{11.2.}$	Lattices in $\mathbb{R}^n$	227

$\S{11.3.}$	LLL-Reduction	230
$\S{11.4.}$	Lattice Attacks on Knapsack Cryptosystems	235
$\S{11.5.}$	Remarks on Lattice-Based Cryptosystems	239
Appendix: Further Reading		241
Bibliography		245

\_\_\_\_\_

### Preface

The theory of quadratic forms has a long and glorious history: launched in ancient Babylonia between 1900 and 1600 BC, taken up again by Brahmagupta in the Seventh Century, and then—another thousand years later by the great genius Fermat, followed by a succession of extraordinary mathematicians, including Euler, Lagrange, and Gauss, who brought the subject closer to its modern form. The work of Minkowski in the late Nineteenth Century, coupled with the extension of his work by Hasse in the early Twentieth Century, led to a great broadening and deepening of the theory that has served as the foundation for an enormous amount of research that continues today.

Though the roots of the subject are in number theory of the purest sort, the last third of the Twentieth Century brought with it new links of quadratic forms to group theory, topology, and—most recently—to cryptography and coding theory. So there are now many members of the mathematical community who are not fundamentally number theorists but who find themselves needing to learn about quadratic forms, especially over the integers. There is thus a need for an accessible introductory book on quadratic forms that can lead readers into the subject without demanding a heavy background in algebraic number theory or previous exposure to a lot of sophisticated algebraic machinery. My hope is that this is such a book.

One of the special attributes of number theory that distinguishes it from most other areas of mathematics is that soon after a subject is introduced and objects are defined, questions arise that can be understood even by a newcomer to the subject, although the answers may have eluded the experts for centuries. Even though this is an introductory book, it contains a substantial amount of material that has not yet appeared in book form, and the reader will be exposed to topics of current research interest. I will be happy if the readers find themselves wanting to pursue some aspects of the subject in more detail than this book can provide; accordingly, I will offer some references to the literature and recommendations for further study.

Before 1937, quadratic forms were treated primarily as homogeneous polynomials of degree 2 acted on by transformations that could change a given quadratic form into certain other ones. (And a fundamental question was: into *which* other ones?) But a pioneering paper by Witt in 1937 brought a more geometric flavor to the subject, putting it on the border of linear algebra and number theory—roughly speaking, a theory of generalized inner products on modules. Our coefficient ring of interest will most often be the ring  $\mathbb{Z}$  of rational integers, though we will also give special attention to the polynomial rings  $\mathbb{F}_q[x]$ . (Here  $\mathbb{F}_q$  denotes a finite field with q elements.) We will see that before we can effectively explore quadratic forms over a given domain R, we may need to extend R, perhaps in many ways, to larger rings. The extended domains (specifically, the *p*-adic number fields, their rings of integers, and their function-field analogues) may possess complications of their own that require clarification before we can consider quadratic forms over them; but once we have achieved that clarification, we may find that quadratic forms over those extensions are far more tractable than over R. When that happens, the trick is to then bring that information down to Rand apply it to the original forms.

This book has evolved from lecture notes for introductory graduate courses on quadratic forms I have taught many times at the University of California, Santa Barbara, and once at Dartmouth College. Typically these courses have been populated by second-year graduate students who have already had a basic course in algebraic structures, and this is the primary audience I have had in mind during the writing process. But in fact the book should be readable by anyone with a strong undergraduate background in linear and abstract algebra who has also seen the construction of the real numbers from the rationals.

Naturally the contents of this book have been shaped by my own interests, experience, and tastes, and I have no doubt that some mathematicians will lament the absence of one or more of their favorite topics in the theory of quadratic forms. But I hope that their concerns will be eased by seeing in these pages some new perspectives—and occasionally something completely new—and that where the material is familiar they will experience the joy of revisiting old friends.

I thank Miklós Ajtai, Mark Gaulter, Arnold Johnson, Timothy O'Meara, Martin Scharlemann, Thomas Shemanske, and the anonymous referees for their helpful comments, and I especially thank Melissa Flora for her detailed reading—and numerous corrections—of nearly the entire manuscript. Of course any errors that remain are my own doing. I have appreciated TeXnical rescues from Caroline Johnson, Barbara Beeton, and Richard Spjut. Natalya Pluzhnikov's perceptive and thorough copy editing helped me put the manuscript in final form. And I thank editor Ina Mette of the AMS for her patience and encouragement, and for her thoughtful selection of excellent referees.

Finally, I thank my dear family for the inspiration, love, and encouragement that have sustained me throughout my work on this project.

### Bibliography

- [AjD] M. Ajtai and C. Dwork, A public-key cryptosystem with worst-case/average case equivalence, in Proceedings 29th Annual Assoc. Comput. Mach. Symposium on Theory of Computing, 284–293, ACM, 1997.
- [A] E. Artin, Geometric Algebra (reprint of the 1957 original), John Wiley & Sons, New York, 1988.
- [Ba] G. Bachman, Introduction to p-adic Numbers and Valuation Theory, Academic Press, New York-London 1964.
- [BHJP] R. Baeza, J. S. Hsia, B. Jacob, A. Prestel (editors), Algebraic and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics v. 344, American Mathematical Society, Providence, 2004.
- [BLR] E. Bayer-Fluckiger, D. Lewis, A. Ranicki (editors), Quadratic Forms and Their Applications, Contemporary Mathematics v. 272, American Mathematical Society, Providence, 2000.
- [Be] C. N. Beli, Representations of integral quadratic forms over dyadic local fields, Electron. Res. Announc. Amer. Math. Soc. 12 (2006), 100–112.
- [Bh] M. Bhargava, On the Conway-Schneeberger fifteen theorem, in Quadratic Forms and Their Applications, 27–37, Contemp. Math. 272, Amer. Math. Soc., Providence, RI, 2000.
- [Bl] F. van der Blij, An invariant of quadratic forms mod 8, Indag. Math. 21 (1959), 291–293.
- [Bo] C. B. Boyer, A History of Mathematics (revised by U. C. Merzbach), John Wiley & Sons, 1991.
- [BR] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, Canadian J. Math. 1 (1949), 88–93.
- [BV] J. Buchmann and U. Vollmer, Binary Quadratic Forms, Springer; Berlin, Heidelberg, New York, 2007.
- [Bu] J. E. Bureau, Representation properties of definite lattices in function fields, Ph.D. dissertation, Louisiana State University, December 2006.
- [Ca] R. Casse, Projective Geometry: An Introduction, Oxford University Press, Oxford, 2006.

[C1]	J. W. S. Cassels, On the representation of rational functions as sums of squares, Acta Arith. 9 (1964), 79–82.
[C2]	J. W. S. Cassels, <i>Rational Quadratic Forms</i> , Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.
[C3]	J. W. S. Cassels, <i>Local Fields</i> , London Mathematical Society, Cambridge University Press, Cambridge, 1986.
[ChD]	W. K. Chan and J. Daniels, Definite regular quadratic forms over $\mathbb{F}_q[T]$ , Proc. Amer. Math. Soc. 133 (2005), 3121–3131.
[Coh]	H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin, 1993.
[Con1]	J. H. Conway, A characterisation of Leech's lattice, Invent. Math. 7 (1969), 137–142.
$[\operatorname{Con2}]$	J. H. Conway, <i>The Sensual (Quadratic) Form</i> , Carus Math. Monographs 26, Mathematical Association of America, 1997.
[Con3]	J. H. Conway, Universal quadratic forms and the fifteen theorem, in Quadratic Forms and Their Applications, 23–26, Contemp. Math. 272, Amer. Math. Soc., Providence, RI, 2000.
[CS]	J. H. Conway and N. J. A. Sloane, <i>Sphere Packings, Lattices and Groups</i> (third edition), Springer-Verlag, New York, 1999.
[Cox]	D. A. Cox, Primes of the Form $x^2 + ny^2$ , John Wiley and Sons, New York, 1997.
[CR]	C.W. Curtis and I. Reiner, <i>Representation Theory of Finite Groups and Asso-</i> <i>ciative Algebras</i> (reprint of the 1962 original), AMS Chelsea Publishing, Prov- idence, RI, 2006.
[D]	L. E. Dickson, Lowest integers representing sides of a right triangle, Amer. Math. Monthly 1 (1894), 6–11.
[Dj]	D. Djoković, Hermitian matrices over polynomial rings, J. Algebra 43 (1976), 359–374.
[EN]	A. G. Earnest and G. Nipp, On the theta series of positive quaternary quadratic forms, C. R. Math. Rep. Acad. Sci. Canada 13 (1991), 33–38.
[Eb]	W. Ebeling, <i>Lattices and Codes</i> (second revised edition), Friedr. Vieweg & Sohn, Braunschweig, 2002.
[Ei1]	M. Eichler, Note zur Theorie der Kristallgitter, Math. Ann. 125 (1952), 51–55.
[Ei2]	M. Eichler, Quadratische Formen und Orthogonale Gruppen, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1952
[El1]	N. D. Elkies, A characterization of the $Z^n$ lattice, Math. Res. Lett. 2 (1995), 321–326.
[El2]	N. D. Elkies, Lattices and codes with long shadows, Math. Res. Lett. 2 (1995), 643–651.
[FS]	R. Fintushel and R. J. Stern, <i>Definite 4-manifolds</i> , J. Differential Geom. 28 (1988), 133–141.
[GJ]	M. R. Garey and D. S. Johnson, <i>Computers and Intractability</i> , W. H. Freeman and Company, 1979.
[Gar]	D. A. Garbanati, An algorithm for the representation of 0 by a quadratic form, J. Pure and Applied Algebra 13 (1978), 57–63.
[Ga]	M. Gaulter, Lattices without short characteristic vectors, Math. Res. Lett. 5 (1998), 353-362.

- [G1] L. J. Gerstein, The growth of class numbers of quadratic forms, Amer. J. Math. 94 (1972), 221–236.
- [G2] L. J. Gerstein, A new proof of a theorem of Cassels and Pfister, Proc. Amer. Math. Soc. 41 (1973), 327–328.
- [G3] L. J. Gerstein, A remark on the quadratic analogue of the Quillen-Suslin theorem, J. Reine Angew. Math. 337 (1982), 166–170.
- [G4] L. J. Gerstein, Nearly unimodular quadratic forms, Annals of Math. 142 (1995), 597–610.
- [G5] L. J. Gerstein, Definite quadratic forms over  $\mathbb{F}_q[x]$ , J. Algebra 268 (2003), 252–263.
- [G6] L. J. Gerstein, On representation by quadratic  $\mathbb{F}_q[x]$ -lattices, Algebraic and Arithmetic Theory of Quadratic Forms, Contemp. Math. 344 (2004), 129–134, Amer. Math. Soc., Providence, RI.
- [G7] L. J. Gerstein, Characteristic elements of unimodular Z-lattices, Linear and Multilinear Algebra 52 (2004), 381–383.
- [GGH] O. Goldreich, S. Goldwasser, and S. Halevi, Public-key cryptosystems from lattice reduction problems, Advances in Cryptology—CRYPTO '97 (Santa Barbara, CA, 1997), 112–131, Lecture Notes in Comput. Sci. 1294, Springer, Berlin, 1997.
- [Gr] E. Grosswald, Representations of Integers as Sums of Squares, Springer-Verlag, New York, 1985.
- [Gro] L. C. Grove, *Classical Groups and Geometric Algebra*, American Mathematical Society, Providence, RI, 2002.
- [HO] A. J. Hahn and O. T. O'Meara, The Classical Groups and K-Theory, Springer-Verlag, New York, 1989.
- [H] M. Hall, Combinatorial Theory (reprint of the 1986 second ed.), John Wiley & Sons, Inc., New York, 1998.
- [HNK] F. Hirzebruch, W. D. Neumann, and S. S. Koh, Differentiable Manifolds and Quadratic Forms, Marcel Dekker, New York, 1971.
- [IR] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, 1982.
- [J] N. Jacobson, A note on hermitian forms, Bull. Amer. Math. Soc. 46 (1940), 264–268.
- [Jo] B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, by Burton W. Jones, Mathematical association of America, 1950.
- [Kap] I. Kaplansky Linear Algebra and Geometry, Dover Publications, 2003. (Reprint of the 1974 Edition by Chelsea Publications.)
- [KWX] M.-H. Kim, Y. Wang, and F. Xu, Universal quadratic forms over  $\mathbb{F}_q[T]$ , preprint, 2004.
- [KHKS] M.-H. Kim, J. S. Hsia, Y. Kitaoka, R. Schulze-Pillot (editors), Integral Quadratic Forms and Lattices, Contemporary Mathematics v. 249, American Mathematical Society, Providence, 1999.
- [Kit] Y. Kitaoka, Arithmetic of Quadratic Forms, Cambridge University Press, Cambridge, 1999.
- [Kb] M. Knebusch, Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. (1969/70), 93–157.

- [K1] M. Kneser, Zur Theorie der Kristallgitter, Math. Ann. 127 (1954), 105–106.
- [K2] M. Kneser, Klassenzahlen definiter quadratischer Formen, Arch. Math. 8 (1957), 241–250.
- [K3] M. Kneser, Quadratische Formen, Springer-Verlag, Berlin-Heidelberg-New York, 2002.
- [Knu] M.-A. Knus, Quadratic and Hermitian Forms over Rings, Springer-Verlag, Berlin-Heidelberg, 1991.
- [LO] J. C. Lagarias and A. M. Odlyzko, Solving low-density subset sum problems, J. Assoc. Comput. Mach. 32 (1985), 229–246.
- [Lam] T. Y. Lam, Introduction to Quadratic Forms over Fields, American Mathematical Society, Providence, RI, 2005.
- [Le] W. Leahey, Sums of squares of polynomials with coefficients in a finite field, Amer. Math. Monthly 74 (1967), 816–819.
- [Lp] D. Leep, *Editor's Endnotes*, Amer. Math. Monthly 112 (2005), 943–944; journal error corrected in vol. 113 (2006), 671.
- [LLL] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovasz, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), 515–534.
- [LN] R. Lidl and H. Niederrreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1986.
- [MB] S. MacLane and G. Birkhoff, *Algebra* (third edition), Chelsea Publishing Co., New York, 1988.
- [Mag] W. Magnus, Über die Anzahl der in einem Geschlecht enthaltenen Klassen von positiv-definiten quadratischen Formen, Math. Ann. 114 (1937), 465–475.
- [Mar] J. Martinet, *Perfect Lattices in Euclidean Space*, Springer-Verlag, Berlin-Heidelberg, 2003.
- [MeH] R. C. Merkle and M. Hellman, *Hiding information and signatures in trapdoor* knapsacks, IEEE Trans. Inform. Theory IT-24: 525–530, September, 1978.
- [MG] D. Micciancio and S. Goldwasser, Complexity of Lattice Problems, Kluwer Academic Publishers, Boston, MA, 2002.
- [MH] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer-Verlag, New York-Heidelberg, 1973.
- [N1] M. Newman, Integral Matrices, Academic Press, New York-London, 1972.
- [N2] M. Newman, Tridiagonal matrices, Linear Algebra Appl. 201 (1994), 51–55.
- [NS] P. Q. Nguyen and J. Stern, The two faces of lattices in cryptology, in Cryptography and Lattices, 146–180, Lecture Notes in Comput. Sci. 2146, Springer, Berlin, 2001.
- [Od] A. M. Odlyzko, The rise and fall of knapsack cryptosystems, in Cryptology and Computational Number Theory, 75–88, Proc. Sympos. Appl. Math., 42, Amer. Math. Soc., Providence, RI, 1990.
- [O'M1] O. T. O'Meara, Introduction to Quadratic Forms (reprint of the 1973 edition), Springer-Verlag, Berlin, 2000.
- [O'M2] O. T. O'Meara, The automorphisms of the orthogonal groups and their congruence subgroups over arithmetic domains, J. Reine Angew. Math. 238 (1969), 169-206.
- [O] T. Ono, Variations on a Theme of Euler, Plenum Press, New York and London, 1994.

- S. Parimala, Failure of a quadratic analogue of Serre's conjecture, Bull. Amer. Math. Soc. 82 (1976), 962–964.
- [Pf] A. Pfister, Zur Darstellung von -1 als Summe von Quadraten in einem Körper, J. London Math. Soc. 40 (1965), 159–165.
- [Pf2] A. Pfister, Quadratic Forms with Applications to Algebraic Geometry and Topology, Cambridge University Press, 1995.
- [PZ] M. Pohst and H. Zassenhaus, Algorithmic Algebraic Number Theory, Cambridge University Press, 1997.
- [PD] H. Pollard and H. G. Diamond, The Theory of Algebraic Numbers (third edition), Dover Publications, Inc., Mineola, NY, 1998.
- [Ra] A. R. Rajwade, *Squares*, Cambridge University Press, 1993.
- [Ri] C. Riehm, On the integral representation of quadratic forms over local fields, Amer. J. Math. 86 (1964), 25–62.
- [R] M. Rosen, Number Theory in Function Fields, Springer-Verlag, New York, 2002.
- [Rog] C. A. Rogers, *Packing and Covering*, Cambridge University Press, 1964.
- [SO] W. Scharlau and H. Opolka, From Fermat to Minkowski: Lectures on the Theory of Numbers and Its Historical Development, Springer-Verlag, New York, 1985.
- [Scha] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag, Berlin 1985.
- [Schn] W. A. Schneeberger, Arithmetic and Geometry of Integral Lattices, Ph.D. dissertation, Princeton University, November 1997.
- [SE] C.-P. Schnorr and M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems, Math. Programming 66 (1994), no. 2, Ser. A, 181–199.
- [Sen] M. Senechal, Quasicrystals and Geometry, Cambridge University Press, Cambridge, 1995.
- [Se] J.-P. Serre, A Course in Arithmetic, Springer-Verlag, New York-Heidelberg, 1973.
- J. Silverman (editor), Cryptography and Lattices, Lecture Notes in Computer Science 2146, Springer-Verlag, Berlin, 2001.
- [Sin] S. Singh, *The Code Book*, Doubleday, New York, 1999.
- [Sz] K. Szymiczek, *Bilinear Algebra*, Gordon and Breach, Amsterdam, 1997.
- [W1] G. L. Watson, Integral Quadratic Forms, Cambridge University Press, 1960.
- [W2] G. L. Watson, The class-number of a positive quadratic form, Proc. London Math. Soc. (3) 13 (1963), 549–576.
- [We] A. Weil, Number Theory, An Approach Through History, From Hammurapi to Legendre, Birkhäuser Boston, Boston, MA, 1984.
- [Y] S. Y. Yan, Number Theory for Computing (second edition), Springer-Verlag, New York-Heidelberg-Berlin, 2002.

### Index

 $(\varphi)^{\mathbb{B}'}_{\mathbb{B}}, 114$  $(a,b)_p, (a,b), 81$  $A_n, 125$  $F_{\mathfrak{p}}, 61$ I(R), 117 $K_n, \, 151$  $L^{\alpha}, 123$  $L^{\sharp}, 129$  $L^{(\alpha)}, 136$  $L_p, 176$  $N(\alpha), 45$ O(V), 26 $O^+(V), 26$ O'(V), 29 $R_{(p)}, 120$  $S_pV, 86$  $T(\alpha), 45$ U(V), 46 $V^* = \operatorname{Hom}(V, F), 21$  $V_E, 99$  $V_a, 31$ W(F), 38 $X \xrightarrow[R]{} Y, 2, 16$  $X^{\perp}, 16$ [V], 35  $\Sigma(A), 118$  $\Sigma_p(\cdot), 120$  $\cong$ , 14, 16 **P** | **p**, 60  $\mathfrak{m}(\mathfrak{p}), 62$  $\mathfrak{o}(\mathfrak{p}), 62$ p-adic valuation, 117 u(p), 62  $\delta, 40$  $\langle A \rangle$ , 14

 $\langle \alpha_1, \ldots, \alpha_n \rangle$ , 18  $\left(\frac{a}{p}\right), 74$  $\mathbb{F}_q, 2$  $\mathbb{Q}_p, 25, 61$  $\mathbb{Z}_p, 66$  $\mu L, 199$  $\mu_p L$ , 198  $\nu_p(\alpha), 52$  $\operatorname{cls} L$ , 181 gen L, 180 $\operatorname{spn} L, 202$  $\overline{F}, \, 62$  $\partial, 2, 152$  $\tau_y, 27$  $\operatorname{ind}^+ V, 31$  $ind^{-}V, 31$  $\operatorname{ord}_p \alpha, 52$ sig V, 31 $\theta(\sigma), 29$  $\underset{R}{\sim}$ , 118  $|\cdot|_{\infty}, 51, 52$  $|\cdot|_{p}, 52$ dM, 15dV, 46h(L), 181nL , 123 p(-), 192 $r(\alpha, V), 42$ s(F), 25 $s(\mathbb{Q}_p), 91$  $sL,\,123$ u(F), 25 $vL,\,123$  $v_i^{\sharp}, \, 128$ 

affine encryption, 226 algebraic coding theory, 10 algebraic function fields, 73 algebraic integers, 141 algebraic number field, 73, 141 algebraically closed field, 22 anisotropic part, 32 anisotropic quadratic module, 14 anisotropic vector, 14 archimedean spot, 56 archimedean valuation, 51 Artin, Emil, 9, 73, 181 attack on a cryptosystem, 225 automorph, 26 Beli, Constantin N., 9 bilinear form, 13 Bruck-Ryser Theorem, 107, 108 Bureau, Jean, 223 canonical power series representation, 64, 66 Cartan-Dieudonné Theorem, 28 Cassels, J. W. S., 181 Cassels-Pfister Theorem, 182, 220 Cauchy sequence, 55 characteristic vector in a lattice, 193 Chinese Remainder Theorem, 100 class, 5, 123, 181 class number, 148, 156, 181, 199, 200 class number growth, 200 classification of definite  $\mathbb{F}_q[x]$ -lattices, 214 classification of indefinite unimodular Z-lattices, 190 closest vector problem, 12, 239 complete field, 59 completion, 60 congruent matrices, 6 convergence, 54 Conway, John, 10, 223 coset-minimal vector, 195 cryptosystem, 225 CVP, 239 cyphertext, 225 decryption functions, 226 definite lattice, 146, 210 definite space, 146, 210 density of a weight set, 238 determinant, 6 determinantal divisors, 119 Dirichlet's theorem on primes, 101, 218 discrete logarithm problem, 227 discrete valuation, 63 discrete valuation ring, 63

discriminant, 6, 15, 36

discriminant (Hermitian), 46

divides, 117 divides (for spots), 60 Djoković, Dragomir, 153 dominant diagonal, 153 dual basis of  $V^*$ , 21 dual lattice, 129, 213 dual of a basis of a quadratic space, 128 dyadic local field, 73 Eichler, Martin, 191 Eichler-Kneser Theorem, 191, 192 Eisenstein, Gotthold, 156 El Gamal cryptosystem, 227 elementary divisors, 119 Elkies, Noam, 195 encryption functions, 225 equivalent matrices, 118 equivalent quadratic (polynomial) forms, 5 equivalent valuations, 56 Euler, Leonhard, 2, 3 even lattice, 151, 188 extending the field of scalars, 99 Fermat's Two-Square Theorem, 2, 109, 185 Fermat, Pierre de, 2 Fifteen Theorem, 223 finite fields, 22, 40 finite projective plane, 106 finite spots, 56 Fintushel, Robert, 195 formal derivative, 69 formally real field, 25, 183 Four Conjecture, 223 four-manifold, 10 fractional ideal, 63, 117 Freshman Dream I, 60 Freshman Dream II, 69 fundamental region, 129, 228 Gaulter, Mark, 195 Gauss's Three-Square Theorem, 110, 186 generator matrix, 228 genus, 180 GGH cryptosystem, 239 global field, 73 Goldbach Conjecture, 3 Gram matrix, 2, 14, 46 Gram-Schmidt procedure, 17 Hadamard's inequality, 228, 229 Harder's Theorem, 155, 183 Hardy, Godfrey Harold, 204 Hasse symbol, 86 Hasse symbol (alternate), 87 Hasse, Helmut, 8 Hasse-Minkowski Theorem, 102, 104, 178, 220

Hensel's Lemma, 69 Hensel, Kurt, 8 Hermite's inequality, 149, 202, 228, 235 Hermite, Charles, 8, 149, 156 Hermite-type inequality over k[x], 152, 158 Hermitian form, 45 Hermitian space, 45, 92 hexagonal lattice, 20, 21 hidden hyperplanes, 240 Hilbert symbol, 81, 83, 84, 208 Hilbert's Reciprocity Law, 98, 103, 219 hyperbolic pair, 15 hyperbolic plane, 15, 23 hyperbolic space, 24 incidence matrix, 107 indecomposable lattice, 125 indefinite lattice, 146, 210 indefinite space, 31, 104, 146, 210 induced bilinear form, 46 induced quadratic form, 46 infinite spot, 56 integral lattice, 197 Invariant Factor Theorem, 122 invariant factors, 118 involution, 27, 44 irreducible vector, 191 isometry, 16, 122 isometry (Hermitian), 46 isometry class, 123 isometry over  $\mathbb{Q}_p$ , 90 isospectral lattices, 124 isotropic quadratic module, 14 isotropic vector, 14 isotropy over  $\mathbb{Q}_p$ , 90 Izhboldin, Oleg, 25 Jacobi, Carl G. J., 126, 161 Jacobson's Theorem, 47 Jacobson, Nathan, 44 Jones, Burton, 9 Jordan chain, 171 Jordan splitting, 162, 163 Kaplansky, Irving, 9 keys for a cryptosystem, 225 knapsack cryptosystems, 11, 236 knapsack problem, 235 Kneser's Theorem, 202 Kneser, Martin, 10, 152, 191, 202 Kronecker product of matrices, 36  $L^3$ -reduced, 230 Lagrange's Four-Square Theorem, 110, 185 Lagrange, Joseph-Louis, 3, 4, 110

lattice, 13, 114

lattice reduction over k[x], 153

Leahey, William, 2, 221 Leech lattice, 10 Leep, David, 178 Legendre symbol, 74, 208 level (stufe) s(F), 25, 91, 183 light cone, 14 line at infinity, 106 LLL-algorithm, 10, 148, 231, 232 LLL-reduced, 230 local field, 71 local ring, 58, 62 Local Square Theorem, 70 local-global, 8 local-global (for matrix equivalence), 120 localization at p, 99 localization of a fractional ideal, 175 localization of a lattice, 176 Magnus, Wilhelm, 204 mass, 204 Mass Formula, 204 maximal anisotropic  $\mathbb{Q}_p$ -space, 91 maximal lattice, 136, 182 Merkuriev, Alexander S., 25 Meyer's Theorem, 104 minimal vector, 146 minimum, 8 minimum of a lattice, 146, 211 Minkowski space, 14 Minkowski, Hermann, 8 modular lattice, 133 Motzkin polynomial, 183 *n*-ary quadratic form, 1 natural numbers of a field, 53 negative definite space, 31 negative index, 31 neighbor lattice, 10, 202 Newman, Morris, 127 nonarchimedean spot, 56 nonarchimedean valuation, 51 nondegenerate, 7 nondyadic local field, 73 norm, 123 norm mapping, 45 normalized valuation, 52 NP class of problems, 236 NP-complete class of problems, 236 O'Meara, O. Timothy, 9, 10, 142, 170, 171 odd lattice, 188 on (a lattice "on" a space), 114 open disk, 54 order of a finite projective plane, 106 orthogonal basis, 17 orthogonal complement, 16 orthogonal component, 16

orthogonal group, 26 orthogonal splitting, 16 orthogonal sum, 16 orthogonal vectors, 16 P class of problems, 236 p-adic integers, 66 p-adic numbers, 25, 61 p-adic order, 52 p-adic spot, 56, 175 p-adic valuation, 52, 175 Pall, Gordon, 9 Parimala, Raman, 156 parity of a lattice, 188 partition function, 192, 200, 204 Pfister form, 50 Pfister, Albrecht, 9, 181, 183 place, 56 plaintext, 225 polar lattice, 129 positive definite space, 31 positive index, 31 prime (or uniformizing) element, 64 prime spot, 56 primitive element of  $\mathbb{Z}_p^n$ , 83 primitive lattice, 197 primitive Pythagorean triple, 138 primitive sublattice, 134 primitive vector, 114, 116 principle of domination, 54 private key, 226 Product Formula, 97 product of fractional ideals, 63 projective plane, 105 public key, 226 public key cryptography, 226 public key encryption, 11 Pythagorean triple, 1, 2, 138 quadratic form, 13 quadratic module, 13 Quadratic Reciprocity, 75, 218 quadratic space, 13 radical, 17, 46 radical splitting, 17 Ramanujan, Srinivasa, 204 rank, 114 real projective plane, 105 reciprocal lattice, 129 reduced basis, 145, 147, 153 reduced form, 147 reduced matrix, 153 reducible vector, 191 reduction, 7 regular, 46

regular quadratic space, 17

representation, 16, 22, 24, 122 representation numbers (over finite fields), 42 representative set, 62 representattion, 16 represents, 2 residue class field at a spot, 62 Riehm, Carl, 9 ring of integers at p, 62 rotation group, 26 RSA cryptosystem, 227 RSA encryption, 11 scale, 123 scaling a lattice, 123 scaling a space, 33 Schneeberger, William, 223 secret key, 226 sesqilinear form, 45 shortest vector problem, 11, 239 Siegel, Carl Ludwig, 8, 204 signature, 31 signature of a lattice, 189 similar quadratic spaces, 35 similarity class, 35 size reduction, 229 Smith normal form, 118, 119 Smith-McMillan form, 119 special orthogonal group, 26 sphere packing, 11 spinor genus, 201 spinor norm, 29, 201 spinorial kernel, 29 spot, 56 stereographic projection, 59 Stern, Ronald, 195 Strong Approximation Theorem, 100, 101 strong triangle inequality, 51 subset sum problem, 235 successive minima, 212 sums of four squares, 110 sums of integer squares, 109, 184 sums of three squares, 110 sums of two squares in  $\mathbb{F}_q[x]$ , 221 superincreasing sequence, 236 SVP, 239 Sylvester's Law of Inertia, 30 Sylvester, James Joseph, 8 symmetry, 27

tensor product of matrices, 36 tensor product of quadratic spaces, 37, 38 totally isotropic quadratic module, 14 trace mapping, 45 transition matrix, 114 triangle inequality, 51 triple-diagonal matrix, 126, 161 trivial quadratic module, 14 trivial spot, 56 trivial valuation, 52 Twin Prime Conjecture, 3 type I lattice, 188 type II lattice, 188 u-invariant, 25, 155 unimodular lattice, 127, 134 unimodular matrix, 5, 114 unitary group, 46 universal  $\mathbb{F}_q[x]$ -lattice, 220, 221 universal quadratic space, 23 valuation, 51 valuation ring, 58, 62 value group, 51 volume, 123 Watson, George L., 196 Weak Approximation Theorem, 99 weights in a knapsack problem, 235 Whaples, George, 73 Witt decomposition, 31, 35 Witt group, 36 Witt index, 31 Witt ring, 38 Witt ring of  $\mathbb{Q}_p$ , 92 Witt ring of a finite field, 41 Witt's Cancellation Theorem, 30 Witt's Chain Equivalence Theorem, 34, 86 Witt's Isometry Extension Theorem, 33 Witt, Ernst, 9

#### Titles in This Series

- 90 Larry J. Gerstein, Basic quadratic forms, 2008
- 89 Anthony Bonato, A course on the web graph, 2008
- 88 Nathanial P. Brown and Narutaka Ozawa, C\*-algebras and finite-dimensional approximations, 2008
- 87 Srikanth B. Iyengar, Graham J. Leuschke, Anton Leykin, Claudia Miller, Ezra Miller, Anurag K. Singh, and Uli Walther, Twenty-four hours of local cohomology, 2007
- 86 Yulij Ilyashenko and Sergei Yakovenko, Lectures on analytic differential equations, 2007
- 85 John M. Alongi and Gail S. Nelson, Recurrence and topology, 2007
- 84 Charalambos D. Aliprantis and Rabee Tourky, Cones and duality, 2007
- 83 Wolfgang Ebeling, Functions of several complex variables and their singularities (translated by Philip G. Spain), 2007
- 82 Serge Alinhac and Patrick Gérard, Pseudo-differential operators and the Nash-Moser theorem (translated by Stephen S. Wilson), 2007
- 81 V. V. Prasolov, Elements of homology theory, 2007
- 80 Davar Khoshnevisan, Probability, 2007
- 79 William Stein, Modular forms, a computational approach (with an appendix by Paul E. Gunnells), 2007
- 78 Harry Dym, Linear algebra in action, 2007
- 77 Bennett Chow, Peng Lu, and Lei Ni, Hamilton's Ricci flow, 2006
- 76 Michael E. Taylor, Measure theory and integration, 2006
- 75 Peter D. Miller, Applied asymptotic analysis, 2006
- 74 V. V. Prasolov, Elements of combinatorial and differential topology, 2006
- 73 Louis Halle Rowen, Graduate algebra: Commutative view, 2006
- 72 R. J. Williams, Introduction the the mathematics of finance, 2006
- 71 S. P. Novikov and I. A. Taimanov, Modern geometric structures and fields, 2006
- 70 Seán Dineen, Probability theory in finance, 2005
- 69 Sebastián Montiel and Antonio Ros, Curves and surfaces, 2005
- 68 Luis Caffarelli and Sandro Salsa, A geometric approach to free boundary problems, 2005
- 67 T.Y. Lam, Introduction to quadratic forms over fields, 2004
- 66 Yuli Eidelman, Vitali Milman, and Antonis Tsolomitis, Functional analysis, An introduction, 2004
- 65 S. Ramanan, Global calculus, 2004
- 64 A. A. Kirillov, Lectures on the orbit method, 2004
- 63 Steven Dale Cutkosky, Resolution of singularities, 2004
- 62 T. W. Körner, A companion to analysis: A second first and first second course in analysis, 2004
- 61 Thomas A. Ivey and J. M. Landsberg, Cartan for beginners: Differential geometry via moving frames and exterior differential systems, 2003
- 60 Alberto Candel and Lawrence Conlon, Foliations II, 2003
- 59 Steven H. Weintraub, Representation theory of finite groups: algebra and arithmetic, 2003
- 58 Cédric Villani, Topics in optimal transportation, 2003
- 57 Robert Plato, Concise numerical mathematics, 2003
- 56 E. B. Vinberg, A course in algebra, 2003
- 55 C. Herbert Clemens, A scrapbook of complex curve theory, second edition, 2003

#### TITLES IN THIS SERIES

- 54 Alexander Barvinok, A course in convexity, 2002
- 53 Henryk Iwaniec, Spectral methods of automorphic forms, 2002
- 52 Ilka Agricola and Thomas Friedrich, Global analysis: Differential forms in analysis, geometry and physics, 2002
- 51 Y. A. Abramovich and C. D. Aliprantis, Problems in operator theory, 2002
- 50 Y. A. Abramovich and C. D. Aliprantis, An invitation to operator theory, 2002
- 49 John R. Harper, Secondary cohomology operations, 2002
- 48 Y. Eliashberg and N. Mishachev, Introduction to the h-principle, 2002
- 47 A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi, Classical and quantum computation, 2002
- 46 Joseph L. Taylor, Several complex variables with connections to algebraic geometry and Lie groups, 2002
- 45 Inder K. Rana, An introduction to measure and integration, second edition, 2002
- 44 Jim Agler and John E. M<sup>c</sup>Carthy, Pick interpolation and Hilbert function spaces, 2002
- 43 N. V. Krylov, Introduction to the theory of random processes, 2002
- 42 Jin Hong and Seok-Jin Kang, Introduction to quantum groups and crystal bases, 2002
- 41 Georgi V. Smirnov, Introduction to the theory of differential inclusions, 2002
- 40 Robert E. Greene and Steven G. Krantz, Function theory of one complex variable, third edition, 2006
- 39 Larry C. Grove, Classical groups and geometric algebra, 2002
- 38 Elton P. Hsu, Stochastic analysis on manifolds, 2002
- 37 Hershel M. Farkas and Irwin Kra, Theta constants, Riemann surfaces and the modular group, 2001
- 36 Martin Schechter, Principles of functional analysis, second edition, 2002
- 35 James F. Davis and Paul Kirk, Lecture notes in algebraic topology, 2001
- 34 Sigurdur Helgason, Differential geometry, Lie groups, and symmetric spaces, 2001
- 33 Dmitri Burago, Yuri Burago, and Sergei Ivanov, A course in metric geometry, 2001
- 32 Robert G. Bartle, A modern theory of integration, 2001
- 31 Ralf Korn and Elke Korn, Option pricing and portfolio optimization: Modern methods of financial mathematics, 2001
- 30 J. C. McConnell and J. C. Robson, Noncommutative Noetherian rings, 2001
- 29 Javier Duoandikoetxea, Fourier analysis, 2001
- 28 Liviu I. Nicolaescu, Notes on Seiberg-Witten theory, 2000
- 27 Thierry Aubin, A course in differential geometry, 2001
- 26 Rolf Berndt, An introduction to symplectic geometry, 2001
- 25 Thomas Friedrich, Dirac operators in Riemannian geometry, 2000
- 24 Helmut Koch, Number theory: Algebraic numbers and functions, 2000
- 23 Alberto Candel and Lawrence Conlon, Foliations I, 2000
- 22 Günter R. Krause and Thomas H. Lenagan, Growth of algebras and Gelfand-Kirillov dimension, 2000
- 21 John B. Conway, A course in operator theory, 2000
- 20 Robert E. Gompf and András I. Stipsicz, 4-manifolds and Kirby calculus, 1999
- 19 Lawrence C. Evans, Partial differential equations, 1998

For a complete list of titles in this series, visit the AMS Bookstore at **www.ams.org/bookstore**/.

The arithmetic theory of quadratic forms is a rich branch of number theory that has had important applications to several areas of pure mathematics—particularly group theory and topology—as well as to cryptography and coding theory. This book is a self-contained introduction to quadratic forms that is based on graduate courses the author has taught many times. It leads the reader from foundation material up to topics of current research interest—with



Photograph by David L. Roth

special attention to the theory over the integers and over polynomial rings in one variable over a field—and requires only a basic background in linear and abstract algebra as a prerequisite. Whenever possible, concrete constructions are chosen over more abstract arguments. The book includes many exercises and explicit examples, and it is appropriate as a textbook for graduate courses or for independent study. To facilitate further study, a guide to the extensive literature on quadratic forms is provided.



For additional information and updates on this book, visit

www.ams.org/bookpages/gsm-90

