Basic Quadratic Forms

Larry J. Gerstein

Graduate Studies
in Mathematics
Volume 90

American Mathematical Society

http://dx.doi.org/10.1090/gsm/090

Basic Quadratic Forms

This page intentionally left blank

Basic Quadratic Forms

Larry J. Gerstein

Graduate Studies
in Mathematics
Volume 90

American Mathematical Society
Providence, Rhode Island

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.

QA243.G47 2008
512.7′4–dc22 2007062041

---

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

To

SUE, DAVID, and BENJY

This page intentionally left blank

Contents

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 R and 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.

This page intentionally left blank

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, *Rational Quadratic Forms*, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[C3] J. W. S. Cassels, *Local Fields*, 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.

[Con2] J. H. Conway, *The Sensual (Quadratic) Form*, 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, *Sphere Packings, Lattices and Groups* (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, *Representation Theory of Finite Groups and Associative Algebras* (reprint of the 1962 original), AMS Chelsea Publishing, Providence, 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, *Lattices and Codes* (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, *Definite 4-manifolds*, J. Differential Geom. **28** (1988), 133–141.

[GJ] M. R. Garey and D. S. Johnson, *Computers and Intractability*, 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* $\mathbb{Z}$*-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.

[P] 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.

[Si] 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.

This page intentionally left blank

Index

This page intentionally left blank

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

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^{c}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

Photograph by David L. Roth

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 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.

ISBN 978-0-8218-4465-6

9 780821 844656

GSM/90

For additional information and updates on this book, visit

www.ams.org/bookpages/gsm-90

AMS *on the* Web
www.ams.org