Advanced Lectures in Mathematics
Volume XV

An Introduction to Groups and Lattices:

Finite Groups and Positive Definite Rational Lattices

by Robert L. Griess, Jr.

International Press
www.intlpress.com

高等教育出版社
HIGHER EDUCATION PRESS

Advanced Lectures in Mathematics, Volume XV
An Introduction to Groups and Lattices:
Finite Groups and Positive Definite Rational Lattices

by Robert L. Griess, Jr.

2010 Mathematics Subject Classification. 11H56, 20C10, 20C34, 20D08.

ISBN: 978-1-57146-206-0

Printed in the United States of America.

15 14 13 12 2 3 4 5 6 7 8 9

Advanced Lectures in Mathematics

Contents

1 Introduction

Rational lattices occur naturally in many areas of mathematics, such as number theory, geometry, combinatorics, representation theory, discrete mathematics, finite groups and Lie theory.

The main goal of this book is to explain methods for construction and analysis of positive definite rational lattices and their finite groups of isometries.

It seems that many lattices of great interest are related to finite groups and vice versa. One thinks of root lattices, the Barnes-Wall lattices, the Leech lattice and others which occur as sublattices or overlattices of these. The Leech lattice is closely related to twenty of the twenty-six sporadic simple groups. Many lattices with relatively high minimum norms have interesting finite isometry groups.

Materials in this book are similar to that in graduate courses we gave during the 2000s decade at the University of Michigan in Ann Arbor, USA and Zhejiang University in Hangzhou, China. We present group theory and lattice theory as closely interrelated subjects.

Many topics in the theory of lattices and the theory of groups shall be treated from first principles and proofs will be self-contained. Our presentation is more classroom style or conversational than encyclopedic. We try to provide clear introductions, give examples and indicate directions. If a full treatment would be long and is otherwise available in publications, we may refer to outside sources.

We shall assume the basic knowledge in graduate algebra and introduce more specialized results as we go along. Elementary linear algebra (Jordan and rational canonical forms, multilinear algebra and tensors, modules over a principal ideal domain) is necessary. Elementary representation theory for groups and algebras over fields is assumed, e.g., [23, 52]. Integral representation theory is less well-known, so we shall cover some basics on this topic. Group cohomology theory will be quoted as needed. The knowledge of root systems for the finite dimensional Lie algebras would be helpful but not absolutely necessary.

We thank the Center for Mathematical Research at Zhejiang University in Hangzhou, China, for an invitation to teach a course on Groups and Lattices in winter, 2008. Also, we thank the University of Michigan and the National Science Foundation of the United States for financial support during this period.

1.1 Outline of the book

The goal is an introduction to groups, positive definite rational lattices and their interactions.

Chapter 2 covers the basic algebra associated to rational lattices, such as integrality, the dual, Gram matrices and relations between a lattice and a sublattice. Definitions for quadratic spaces and their isometries are treated with some generality. Particular attention is paid to involutions.

Chapter 3 deals with rational lattices invariant under a given finite group and with finiteness of the isometry group of a given rational lattice. An orthogonal decomposition of a lattice into orthogonally indecomposable summands indicates certain decompositions of its isometry group.

Chapter 4 deals with root lattices of types ADE. These lattices and closely related ones occur widely and are an important part of basic vocabulary in this subject. We give detailed analysis of these lattices, their duals and isometry groups.

Chapter 5 discusses the two inequalities of Hermite and Minkowski which say that, given integers n and d, there is a number $f(n, d)$ so that a lattice of rank n and determinant d has a nonzero vector such that the absolute value of its norm is at most $f(n, d)$. This technique is important for starting structure analyses of lattices for which n and d are not too large. An application is given to uniqueness of the exceptional root lattices E_6, E_7 and E_8 and other cases.

Chapter 6 introduces elementary theory of error correcting codes and their role in building lattices. Applications are given to root lattices (e.g. several different constructions of E_8).

Chapter 7 begins with a review of representation theory of finite groups then specializes to extraspecial p-groups and groups obtained from them by extending upwards by subgroups of the outer automorphism group. In particular, we construct the Bolt-Room-Wall groups. Such groups play important roles in the theory of lattices, as explained in the next chapter.

Chapters 8 and 9 are about an inductive construction of the family of Barnes-Wall lattices, in ranks 2^d. We sketch how to get the rank 2^d case by starting with the rank 2^{d-1} case and using integral representation theory of a dihedral group of order 8. The concepts of 2/4-generation, 3/4-generation and commutator density are developed in generality then specialized to the Barnes-Wall constructions. Applications are given, including a description of minimal vectors and indication of how the Reed-Muller binary codes occur within the Barnes-Wall lattices.

Chapter 10 is about the even unimodular integral lattices in dimensions 8, 16 and 24. The number of isometry types are, respectively, 1, 2 and 24. We describe many of these and devote a lot of attention to the Golay code and the Leech lattice, the unique even unimodular integral lattices in dimension 24 which has no norm 2 vectors. Its isometry group is a remarkable finite groups whose quotient by the center is simple. We sample the rich combinatorics and group theory.

Chapter 11 gives a new treatment of existence and uniqueness for the Leech lattice. It has many logical advantages over the past treatments. For example, it implies existence and properties of the Golay code and Mathieu groups, rather than using these respective theories.

An appendix gives a table of orders for the finite simple groups.

Three articles of this author are reprinted (one in revised form) to supplement treatments in the text.

1.2 Suggestions for further reading

Chapter 2: Bilinear forms, quadratic forms and their isometry groups

For basics about integer quadratic forms, see [17, 55, 58].

Chapter 3: General results on finite groups and invariant lattices

There are many good texts on basic representation theory of finite groups over fields, e.g. [1, 2, 23, 24, 25, 26, 29, 30, 52]. The term "modular representation theory" refers to representations of a finite group over fields of positive characteristic which divides the group order. In this case, the group algebra has a nonzero radical and finite dimensional modules are not completely reducible. Integral representation theory is not as widely treated as representation theory over fields. Aspects are treated in the abovementioned texts.

The text [59] studies many interesting integral lattices which have strong connections to Lie algebras and finite groups.

Chapter 4: Root lattices of types A, D, E

In this text, consider the classification of root systems as given. For an axiomatic treatment, see [11, 50]; the appendices in [11] are quite useful and have become a standard reference.

Chapter 5: Hermite and Minkowski functions

We emphasize the Hermite function because in low ranks, it gives better results than the Minkowski function. For larger ranks, the Minkowski function is much better than the Hermite function, but does not seem to be strong enough for practical use in classification results, such as the ones at the end of this chapter. For a proof of the Minkowski result, see [80].

We have wondered if there is a generalization of such functions to the following situation. We are given two rational lattices L and M, where $\mathrm{rank}(M) \leq \mathrm{rank}(L)$. For each integer $r \geq 1$, one would like some estimate of the number of embeddings of $\sqrt{r}\,M$ into L. Perhaps a sharper question would get a better answer, such as one about preferred bases of M: given a finite set of vectors with Gram matrix G can one estimate the number of embeddings in L of a set of vectors with Gram matrix rG, for $r \geq 1$. Some kinds of estimate in the case of L a rootless rank 24 even unimodular lattice and M the E_8-lattice might be useful for a new uniqueness proof of the Leech lattice along the lines of [38].

The problem of determining the minimum norm of a given lattice is generally hard. Some techniques are given in [21, 57].

Chapter 6: Constructions of lattices by use of codes

For basic coding theory, see [64, 68, 77, 79] and for an extensive report, see [69]. This text gives only the simplest constructions of lattices from sublattices and glue codes. For a greater range of such constructions, see the systematic expositions in [21].

Chapter 7: Group theory and representations

Extraspecial p-groups got a lot of attention from the work of [47] and they frequently played roles throughout the development of finite group theory and the classification of simple groups. For example, see [31, 37, 51]. In [74], Theorem B of [47] is used a lot.

The result on character values of an element in a BRW group (7.4.6) was reported in [35] but it may be older; we do not know the earliest references.

Chapter 8: Overview of the Barnes-Wall Lattices

This short exposition shows that the Barnes-Wall series involves some familiar lattices, covered earlier in the text. The commutator density theory from [40] seems to be new. There are homological issues for representations of a group over $\mathbb{Z}$ which are trivial for the corresponding rational representations. For background on homological algebra, see [6, 46, 49, 70].

Chapter 9: Construction and properties of the Barnes-Wall lattices

These lattices were first described in [5]. In fact, [5] describes more lattices than we consider in this book. Their lattices depend on a set of parameters. For each of those lattices, the isometry group has a subgroup G for which $G/O_2(G)$ is some $GL(m, 2)$. Certain values of the parameters give "the" Barnes-Wall lattices, the ones we treat in this book, and for these lattices, the BRW group is properly larger than the preceding group G. Shortly after [5] appeared, there came several articles describing lattices like Barnes-Wall for odd primes and their groups [7, 8, 9].

The Barnes-Wall lattices were discovered independently in [15], which defines each as an ascending chain of lattices, depending on a sequence of Reed-Muller binary error-correcting codes. The authors give a lot of group theoretic information. See also the earlier articles [12, 13, 14]. Their viewpoint is more group-theoretic than that of [5].

Chapter 10: Even unimodular lattices in small dimensions

The classifications of rank 2 lattices and even unimodular lattices of ranks 8, 16 and 24 are well known. In other low dimensions, there are a few results for cases of interest. See the books [21] and [58] and the article [44]. Some such characterizations are found in Subsection 5.3.

Chapter 11: Pieces of eight

The early constructions of the Leech lattice were done by first creating a Golay code, then using it to make glue vectors over a square lattice with minimum norm 4 [20, 62]. Uniqueness of the Leech lattice is deduced from uniqueness of the Golay code. In [37], this program is described in detail. The approach of Borcherds [10] is based on hyperbolic lattices and so is quite different. He proves existence of a rootless Niemeier lattice but his proof indicates no properties of such a lattice. Uniqueness is proven using analysis of roots in the hyperbolic overlattice of rank 26. The Pieces of Eight [38] approach gets structure theory of the Leech lattice and its isometry group by the uniqueness viewpoint. The ideas in [38] led this author to [40].

1.3 Notations, background, conventions

The conventions in this book will be similar to that of [31]. However, we shall use mostly left actions of groups and rings, though in a few situations we use right actions.

Since we use n-tuples a lot, it is often more convenient to write row vectors for arguments with linear combinations, whereas with matrix work, we may apply a matrix on the left to a column vector. Conjugation and commutation follow the style of [31], e.g. x^y means $y^{-1}xy$ and $[x,y] = x^{-1}y^{-1}xy$ so that $x^y = x[x,y]$.

We tend to write $A \leq B$ when A is a subobject of B in an algebraic category (groups, rings, etc.).

Set theoretic notations include $A \setminus B$ for set-theoretic difference, i.e., $\{x \in A \mid x \notin B\}$, $A + B$ for Boolean sum ($A + B := A \cup B \setminus A \cap B = A \setminus B \cup B \setminus A$) and $A \sqcup B$ for disjoint union.

See the book index for a list of notations which occur in the text.