

ALM 15

Advanced Lectures in Mathematics

An Introduction to Groups and Lattices:

Finite Groups and Positive Definite Rational Lattices

群与格引论：有限群与正定有理格

Robert L. Griess, Jr.

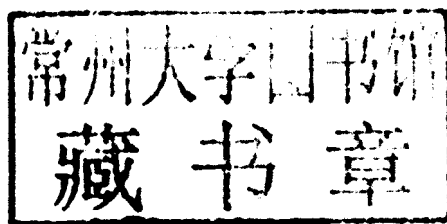
An Introduction to Groups and Lattices:

Finite Groups and Positive Definite Rational Lattices

群与格引论：有限群与正定有理格

Qun Yu Ge Yinlun: Youxianqun Yu Zhengding Youlige

Robert L. Griess, Jr.



高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING



International Press

图书在版编目 (CIP) 数据

群与格引论: 有限群与正定有理格 = An

Introduction to Groups and Lattices: Finite Groups

and Positive Definite Rational Lattices: 英文/

(美) 格里斯 (Griess, R. L.) 著. —北京: 高等教育出

版社, 2010.5

ISBN 978 - 7 - 04 - 029205 - 3

I. ①群… II. ①格… III. ①有限群-英文②格-英
-英文 IV. ①O152.1②O153.1

中国版本图书馆 CIP 数据核字 (2010) 第 069836 号

Copyright © 2010 by

Higher Education Press

4 Dewai Dajie, Beijing 100120, P. R. China, and

International Press

387 Somerville Ave, Somerville, MA, U. S. A

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without permission.

策划编辑 王丽萍 责任编辑 李 鹏 封面设计 张申申
责任校对 杨雪莲 责任印制 毛斯璐

出版发行 高等教育出版社
社 址 北京市西城区德外大街 4 号
邮政编码 100120
总 机 010-58581000

经 销 蓝色畅想图书发行有限公司
印 刷 北京中科印刷有限公司

开 本 787 × 960 1/16
印 张 16.5
字 数 370 000

购书热线 010-58581118

免费咨询 400-810-0598

网 址 <http://www.hep.edu.cn>

<http://www.hep.com.cn>

网上订购 <http://www.landaco.com>

<http://www.landaco.com.cn>

畅想教育 <http://www.widedu.com>

版 次 2010 年 5 月第 1 版

印 次 2010 年 5 月第 1 次印刷

定 价 58.00 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 29205 - 00

ADVANCED LECTURES IN MATHEMATICS

ADVANCED LECTURES IN MATHEMATICS

(Executive Editors: Shing-Tung Yau, Kefeng Liu, Lizhen Ji)

1. Superstring Theory
(Editors: Shing-Tung Yau, Kefeng Liu, Chongyuan Zhu)
2. Asymptotic Theory in Probability and Statistics with Applications
(Editors: Tze Leung Lai, Lianfen Qian, Qi-Man Shao)
3. Computational Conformal Geometry
(Authors: Xianfeng David Gu, Shing-Tung Yau)
4. Variational Principles for Discrete Surfaces
(Authors: Feng Luo, Xianfeng David Gu, Junfei Dai)
5. Proceedings of The 4th International Congress of Chinese Mathematicians
Vol. I — Vol. III
(Editors: Lizhen Ji, Kefeng Liu, Lo Yang, Shing-Tung Yau)
6. Geometry, Analysis and Topology of Discrete Groups
(Editors: Lizhen Ji, Kefeng Liu, Lo Yang, Shing-Tung Yau)
7. Handbook of Geometric Analysis Vol. I
(Editors: Lizhen Ji, Peter Li, Richard Schoen, Leon Simon)
8. Recent Developments in Algebra and Related Areas
(Editors: Chongying Dong, Fu-an Li)
9. Automorphic Forms and the Langlands Program
(Editors: Lizhen Ji, Kefeng Liu, Shing-Tung Yau)
10. Trends in Partial Differential Equations
(Editors: Baojun Bian, Shenghong Li, Xu-Jia Wang)
11. Recent Advances in Geometric Analysis
(Editors: Yng-Ing Lee, Chang-Shou Lin, Mao-Pei Tsui)
12. Cohomology of Groups and Algebraic K -theory
(Editors: Lizhen Ji, Kefeng Liu, Shing-Tung Yau)
13. Handbook of Geometric Analysis Vol. II
(Editors: Lizhen Ji, Peter Li, Richard Schoen, Leon Simon)
14. Handbook of Geometric Analysis Vol. III
(Editors: Lizhen Ji, Peter Li, Richard Schoen, Leon Simon)
15. An Introduction to Groups and Lattices
(Author: Robert L. Griess, Jr.)

ADVANCED LECTURES IN MATHEMATICS

EXECUTIVE EDITORS

Shing-Tung Yau
Harvard University
Cambridge, MA. USA

Lizhen Ji
University of Michigan
Ann Arbor, MI. USA

Kefeng Liu
University of California, Los Angeles
Los Angeles, CA. USA
Zhejiang University
Hangzhou, China

EXECUTIVE BOARD

Chongqing Cheng
Nanjing University
Nanjing, China

Tatsien Li
Fudan University
Shanghai, China

Zhong-Ci Shi
Institute of Computational Mathematics
Chinese Academy of Sciences (CAS)
Beijing, China

Zhiying Wen
Tsinghua University
Beijing, China

Zhouping Xin
The Chinese University of Hong Kong
Hong Kong, China

Lo Yang
Institute of Mathematics
Chinese Academy of Sciences (CAS)
Beijing, China

Weiping Zhang
Nankai University
Tianjin, China

Xiangyu Zhou
Institute of Mathematics
Chinese Academy of Sciences (CAS)
Beijing, China

Xiping Zhu
Sun Yat-sen University
Guangzhou, China

Contents

1	Introduction	1
1.1	Outline of the book	2
1.2	Suggestions for further reading	3
1.3	Notations, background, conventions	5
2	Bilinear Forms, Quadratic Forms and Their Isometry Groups	7
2.1	Standard results on quadratic forms and reflections, I	9
2.1.1	Principal ideal domains (PIDs)	10
2.2	Linear algebra	11
2.2.1	Interpretation of nonsingularity	11
2.2.2	Extension of scalars	13
2.2.3	Cyclicity of the values of a rational bilinear form	13
2.2.4	Gram matrix	14
2.3	Discriminant group	16
2.4	Relations between a lattice and sublattices	18
2.5	Involutions on quadratic spaces	19
2.6	Standard results on quadratic forms and reflections, II	20
2.6.1	Involutions on lattices	20
2.7	Scaled isometries: norm doublers and triplers	23
3	General Results on Finite Groups and Invariant Lattices	25
3.1	Discreteness of rational lattices	25
3.2	Finiteness of the isometry group	25
3.3	Construction of a G -invariant bilinear form	26
3.4	Semidirect products and wreath products	27
3.5	Orthogonal decomposition of lattices	28
4	Root Lattices of Types A, D, E	31
4.1	Background from Lie theory	31
4.2	Root lattices, their duals and their isometry groups	32
4.2.1	Definition of the A_n lattices	33

4.2.2	Definition of the D_n lattices	34
4.2.3	Definition of the E_n lattices	34
4.2.4	Analysis of the A_n root lattices	34
4.2.5	Analysis of the D_n root lattices	37
4.2.6	More on the isometry groups of type D_n	39
4.2.7	Analysis of the E_n root lattices	41
5	Hermite and Minkowski Functions	49
5.1	Small ranks and small determinants	51
5.1.1	Table for the Minkowski and Hermite functions	52
5.1.2	Classifications of small rank, small determinant lattices	53
5.2	Uniqueness of the lattices E_6, E_7 and E_8	54
5.3	More small ranks and small determinants	57
6	Constructions of Lattices by Use of Codes	61
6.1	Definitions and basic results	61
6.1.1	A construction of the E_8 -lattice with the binary $[8, 4, 4]$ code	62
6.1.2	A construction of the E_8 -lattice with the ternary $[4, 2, 3]$ code	64
6.2	The proofs	64
6.2.1	About power sets, boolean sums and quadratic forms	64
6.2.2	Uniqueness of the binary $[8, 4, 4]$ code	65
6.2.3	Reed-Muller codes	66
6.2.4	Uniqueness of the tetracode	67
6.2.5	The automorphism group of the tetracode	67
6.2.6	Another characterization of $[8, 4, 4]_2$	69
6.2.7	Uniqueness of the E_8 -lattice implies uniqueness of the binary $[8, 4, 4]$ code	69
6.3	Codes over $\mathbb{F}_7$ and a (mod 7)-construction of E_8	70
6.3.1	The A_6 -lattice	71
7	Group Theory and Representations	73
7.1	Finite groups	73
7.2	Extraspecial p -groups	75
7.2.1	Extraspecial groups and central products	75
7.2.2	A normal form in an extraspecial group	77
7.2.3	A classification of extraspecial groups	77
7.2.4	An application to automorphism groups of extraspecial groups	79
7.3	Group representations	79
7.3.1	Representations of extraspecial p -groups	80
7.3.2	Construction of the BRW groups	82
7.3.3	Tensor products	85
7.4	Representation of the BRW group G	86
7.4.1	BRW groups as group extensions	88

8	Overview of the Barnes-Wall Lattices	91
8.1	Some properties of the series	91
8.2	Commutator density	93
8.2.1	Equivalence of 2/4-, 3/4-generation and commutator density for Dih_8	93
8.2.2	Extraspecial groups and commutator density	96
9	Construction and Properties of the Barnes-Wall Lattices	99
9.1	The Barnes-Wall series and their minimal vectors	99
9.2	Uniqueness for the BW lattices	101
9.3	Properties of the BRW groups	102
9.4	Applications to coding theory	103
9.5	More about minimum vectors	104
10	Even unimodular lattices in small dimensions	107
10.1	Classifications of even unimodular lattices	107
10.2	Constructions of some Niemeier lattices	108
10.2.1	Construction of a Leech lattice	109
10.3	Basic theory of the Golay code	111
10.3.1	Characterization of certain Reed-Muller codes	111
10.3.2	About the Golay code	112
10.3.3	The octad Triangle and dodecads	113
10.3.4	A uniqueness theorem for the Golay code	116
10.4	Minimal vectors in the Leech lattice	116
10.5	First proof of uniqueness of the Leech lattice	117
10.6	Initial results about the Leech lattice	118
10.6.1	An automorphism which moves the standard frame	118
10.7	Turyn-style construction of a Leech lattice	119
10.8	Equivariant unimodularizations of even lattices	121
11	Pieces of Eight	125
11.1	Leech trios and overlattices	125
11.2	The order of the group $O(\Lambda)$	128
11.3	The simplicity of M_{24}	130
11.4	Sublattices of Leech and subgroups of the isometry group	132
11.5	Involutions on the Leech lattice	134
	References	137
	Index	143
	Appendix A The Finite Simple Groups	149

Appendix B Reprints of Selected Articles	153
B.1 Pieces of Eight: Semiselfdual Lattices and a New Foundation for the Theory of Conway and Mathieu Groups.....	155
B.2 Pieces of 2^d : Existence and Uniqueness for Barnes-Wall and Ypsilanti Lattices.....	181
B.3 Involutions on the Barnes-Wall Lattices and Their Fixed Point Sublattices, I.....	223

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 group 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 $\text{rank}(M) \leq \text{rank}(L)$. 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.

Bilinear Forms, Quadratic Forms and Their Isometry Groups

In this section we cover a few basic definitions which shall apply throughout this book. We include the definition of rational lattice.

Definition 2.0.1. Let R be a commutative ring and let M and N be R -modules. An R -bilinear map $f : M \times M \rightarrow N$ is a function which satisfies

$$\begin{aligned} f(x + x', y) &= f(x, y) + f(x', y), & f(rx, y) &= rf(x, y); \\ f(x, y + y') &= f(x, y) + f(x, y'), & f(x, ry) &= rf(x, y) \end{aligned}$$

for all $x, x', y, y' \in M$ and all $r \in R$.

Such a map is called *symmetric* if $f(x, y) = f(y, x)$ for all $x, y \in M$. It is called *alternating* if $f(x, x) = 0$ for all $x \in M$.

The alternating property implies that $f(x, y) = -f(y, x)$, but the converse statement is not generally true. Consider the map $f(x, x) = x$, for $x \in \mathbb{F}_2$.

Definition 2.0.2. Let R be a commutative ring and let M, N be R -modules with respective bilinear forms $f : M \times M \rightarrow R$ and $g : N \times N \rightarrow R$. An *isometry* from M to N is an R -linear isomorphism of modules $T : M \rightarrow N$ which preserves the bilinear forms, i.e., for all $x, y \in M$, $g(Tx, Ty) = f(x, y)$. When such a T exists, we say that M and N are *isometric*. In case $M = N$, the set of such maps forms a group under composition, called the *isometry group* of f . We may write $O(M, f)$ or $O(f)$ for this group.

Definition 2.0.3. Let R be a commutative ring and A, B modules over R . A *quadratic map* is a function $Q : A \rightarrow B$ such that,

- (1) $f(x, y) := Q(x + y) - Q(x) - Q(y)$ is bilinear;
- (2) $Q(cx) = c^2Q(x)$ for all $c \in R$ and $x \in A$.

The function f is called the *bilinear function associated to Q* . A *quadratic form* is a quadratic map $Q : A \rightarrow R$. We say that Q is *nondegenerate* if f is nondegenerate.

Remark 2.0.4. (1) The definition implies that $Q(0) = 0$ and the bilinear form f associated to Q is symmetric.

(2) If $g : A \times A \rightarrow R$ is a bilinear form, then $Q(x) := g(x, x)$ is a quadratic form. The bilinear form f associated to Q is in this case equal to $g(x, y) + g(y, x)$.