February 18, 2008

Groups and Lattices

Graduate Course Winter 2008,
Zheijiang University,
Hangzhou, China

Groups and Lattices: main goals

This course will be an introduction to lattices and their isometry groups. The level will be for graduate students who have had basic theory of groups, rings and fields.

A lattice is a finitely generated free abelian group with a rational-valued symmetric bilinear form. An isometry of a lattice is a homomorphism of the lattice onto itself which preserves the bilinear form. The set of isometries forms a group under composition of maps.

Example: in the plane $\mathbb{R}^2$, take the square lattice $\mathbb{Z}^2$. Its isometry group is dihedral of order 8.

The lattices in this course will almost always be positive definite. Isometry groups of positive definite lattices are finite groups, so we have an interaction of arithmetic with finite group theory and combinatorics.

The course will begin with general theory of lattices and integral representations of groups.

We shall examine certain lattices and their isometry groups in detail, especially the Weyl groups, the combinatorics of the Leech lattice and the twelve sporadic groups found within the isometry group (the Mathieu groups, the groups of Higman-Sims, McLaughlin, Hall-Janko, Suzuki and Conway), the Barnes-Wall lattices in dimensions 2^d and their groups of shape $2_+^{1+2d}\Omega^+(2d,2)$.

Groups and Lattices: a course outline

General properties of lattices. Integral lattices and their duals and discriminant groups. Comparisons of lattices with sublattices, neighbors. Codes.

Existence and uniqueness theorems for lattices. The theta function. Some arithmetic. The modular group $SL(2,\mathbb{Z})$.

Isometry groups. Isometries of order 2. Extraspecial groups. Rational representations of finite groups and invariant lattices.

Lattices of special importance and their isometry groups. Certain lattices of ranks up to 8. Root lattices. The Leech lattice of dimension 24 and its isometry group of order $2^{22}3^9 5^6 7^2 11 \cdot 13 \cdot 23$. Covering groups. Twelve sporadic simple groups.

The series of Barnes-Wall lattices, of dimensions 2^d. Sublattices and overlattices of these. Associated finite groups. The Reed-Muller codes and affine geometry over the field of 2 elements.

Sphere packing, covering. Relations to hyperbolic lattices. Modular forms and arithmetic. Extremal lattices.

A broader look at finite groups and arithmetic.

Prerequisites

Graduate-level basic courses in group theory, field theory and rings, plus some representation theory of finite groups. Students should know most of the material below, and fill in what is missing as soon as possible.

Sylow theorems, actions of a group on a set, orbits, multiple transitivity, systems of imprimitivity. Abelian, nilpotent and solvable groups. Simple groups. The symmetric groups, Alt_n, the general linear group, $PSL(n, F)$.

Principal ideal domains (PID) and their finitely generated modules. The equivalence of matrices over such rings (by row operations which add a multiple of one row to another, permute rows and multiply rows by a unit from the ring; similarly for columns). The theory of fundamental invariants (Smith invariants). For us, this means mostly the ring of integers, but sometimes polynomial rings, certain rings of integers like $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, etc.

Tensors and Hom. The symmetric algebra and exterior algebra of a module over a commutative ring. Multilinear forms, especially bilinear forms and the cases of symmetric and alternating forms. Canonical forms for bilinear forms (e.g., Sylvester's theorem over the real numbers; direct sums of hyperbolic planes and null spaces for alternating forms). The group of isometries of a bilinear form. Witt's theorem (sufficient conditions for an isometry between subspaces to extend to an isometry on the space).

Wedderburn theory for simple rings with ascending chain condition.

Some familiarity with basic representation theory of finite groups (irreducible modules, character theory, orthogonality relations, etc.).

Very Helpful

We will use some material which is a bit advanced. I can sketch what we need and leave it to the students to fill in the rest by themselves.

Root systems and Weyl groups (these come up in the theory of Lie algebras).

A little algebraic number theory, mainly rings of integers of quadratic and cyclotomic fields.

Elementary homological algebra (Ext-functors, long exact sequences, group cohomology, etc.).

Familiarity with computer algebra, e.g. Maple, Gap, Magma, etc.

References

[1] E. S. Barnes and G. E. Wall, Some extreme forms defined in terms of abelian groups, JAMS 1 (1959), 47-63.

[2] Beverly Bolt, T. G. Room and G. E. Wall, On the Clifford Collineations, Transform and Similarity Groups, I. Journal of the Australian Mathematical Society, 2, 1961, 60-79.

[3] Beverly Bolt, T. G. Room and G. E. Wall, On the Clifford Collineations, Transform and Similarity Groups, II. Journal of the Australian Mathematical Society, 1961, 80-96.

[4] Beverly Bolt, T. G. Room and G. E. Wall, On the Clifford Collineations, Transform and Similarity Groups, III; Generators and Relations, Journal of the Australian Mathematical Society, 1961

[5] N. Bourbaki, Élements de Mathématique, Groupes et algèbres de Lie, Chapitres 2 et 3, Diffusion C.C. L. S., Paris, 1972.

[6] Michel Broué and Michel Enguehard, Une famille infinie de formes quadratiques entière; leurs groupes d'automorphismes, Ann. scient. Éc. Norm. Sup., 4^{eme} série, t. 6, 1973, 17-52.

[7] Roger Carter, Simple Groups of Lie Type, Wiley-Interscience, London (1972).

[8] John Conway and Neil Sloane, Self-dual codes over the integers modulo 4, Journal of Combinatorial Theory, Series A 62, 30-45 (1993).

[9] Charles Curtis and Irving Reiner, Representation Theory of Groups and Associative Algebras, Interscience, 1962.

[10] C. Dong, R. Griess. Jr. and G. Hoehn, Framed vertex operator algebras, codes and the moonshine module, *Comm. Math. Phys.* **193** (1998), 407-448.

[11] Daniel Gorenstein, Finite Groups, Harper and Row, New York, 1968.

[12] Robert L. Griess, Jr., On a subgroup of order $2^{15}|GL(5,2)|$ in $E_8(C)$, the Dempwolff group and $Aut(D_8 \circ D_8 \circ D_8)$, J. Algebra, 40, 1976, 271-279.

[13] Robert L. Griess, Jr., Elementary abelian subgroups of algebraic groups, Geometria Dedicata, **39**, 253-305, 1991.

[14] Robert L. Griess, Jr., Positive definite lattices of rank at most 8, Journal of Number Theory, 103 (2003), 77-84.

[15] Robert L. Griess, Jr., Automorphisms of extra special groups and nonvanishing degree 2 cohomology, Pacific J. Math., 48, 403-422, 1973.

[16] Robert L. Griess, Jr., Sporadic groups, code loops and nonvanishing cohomology, J. Pure Appl. Algebra, 44, 1987, 191-214.

[17] Robert L. Griess, Jr., The monster and its nonassociative algebra, in Proceedings of the Montreal Conference on Finite Groups, Contemporary Mathematics, 45, 121-157, 1985, American Mathematical Society, Providence, RI.

[18] Robert L. Griess, Jr., Twelve Sporadic Groups, Springer Verlag, 1998.

[19] Robert L. Griess, Jr, Pieces of Eight, Advances in Mathematics, 148, 75-104 (1999).

[20] R. W. Hamming, Error detecting and error correcting codes, Bell Syst. Tech. J. 29 (1950), 147-160. MR 12:35.

[21] Bertram Huppert, Endliche Gruppen I, Springer Verlag, Berlin, 1968.

[22] Oliver King, A mass formula for unimodular lattices with no roots. (English. English summary) Math. Comp. 72 (2003), no. 242, 839–863 (electronic). 11H55 (11E41) MR1954971 (Review)

[23] M. Kneser, Theorie der Kristalgitter, Math. Ann. 127, 105-106 (1954).

[24] Jesse MacWilliams and Neal Sloane, The Theory of Error Correcting Codes, North-Holland, 1977.

[25] Milnor and Husemoller, Symmetric Bilinear Forms, Ergebnisse der Mathematick und Ihrer Grenzgebiete, Band 73, Springer Verlag, New York, 1973.

[26] H. Minkowski, Zur Theorie der positiven quadratischen Formen, Jour. für die reine und angew. Math. 101 (1887), 196-202.

[27] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, An Introduction to the Theory of Numbers, Fifth Edition, Wiley, New York, 1991.

[28] B. L. Rothschild and J. H. van Lint, Characterizing finite subspaces, J. comb Theory, 16A, (1974) 97-110.

[29] Jean-Pierre Serre, A Course in Arithmetic, Springer Verlag, Graduate Texts in Mathematics 7, 1973.