Robert L. Griess Jr.[1]
Department of Mathematics, University of Michigan
Ann Arbor, MI 48109

Positive definite lattices of rank at most 8.

(Submitted to Journal of Number Theory; version 9 March, 2003, Ann Arbor)

Abstract

We give a short uniqueness proof for the E_8 root lattice, and in fact for all positive definite unimodular lattices of rank up to 8. Our proof is done with elementary arguments, mainly these: (1) invariant theory for integer matrices; (2) an upper bound for the minimum of nonzero norms (either of the elementary bounds of Hermite or Minkowski will do). We make no use of p-adic completions, mass formulas or modular forms.

Contents

1 Introduction

A basic result in the theory of lattices[2] is uniqueness of the rank 8 even integral positive definite unimodular lattice. Such a lattice is isometric to L_{E_8}, the root lattice[3] of E_8. It is spanned by the 240 roots of a type E_8 root system. The isometry group is the Weyl group of type E_8, a finite group of order $2^{14}3^5 5^2 7$. It has shape $2{\cdot}O^+(8,2)$ and the lattice modulo 2 may be

[1] The author has been supported by NSA grants USDOD-MDA904-00-1-0011 and USDOD-MDA904-01-1-0042.

[2] See 4.1 for definitions. Most lattices in this article are positive definite.

[3] See 4.2 and 4.3.

identified with the natural representation of $O^+(8,2)$ on $\mathbb{F}_2^8$ with a quadratic form.

The present article gives a short uniqueness proof for L_{E_8}, using only elementary techniques. In fact, we classify all positive definite lattices of determinant 1 and rank at most 8. Besides L_{E_8}, there are only square[4] lattices. Our use of inequalities is limited to an easy upper bound on the minimum nonzero norm of a positive definite lattice, for which the bound of either Hermite or Minkowski will do.

A few impressions on uniqueness proofs of L_{E_8} follow. The reader is warned that our knowledge of this topic is not great.

The first proof of uniqueness of L_{E_8} is probably due to Mordell [Mor1] (see his comments about history). Mordell classifies all positive definite rank 8 unimodular lattices. His proof depends on "two deep theorems" on quadratic forms. One is the exact value in ranks $n = 6, 7, 8$ for $min_J\{\frac{\mu(J)}{det(J)^{1/n}}\}$, where J ranges over all positive definite lattices of rank n and $\mu(J)$ denotes the minimum norm of a nonzero vector[5]. The second is the characterization of a particular integral rank 6 lattice[6] of determinant 3 by the property of having minimum norm 2.

In [K], Kneser proves that the positive definite square unimodular lattice of rank 8 and L_{E_8} have the property that an integral unimodular lattice of rank 8 which is a neighbor[7] of either of these is isometric to one of these. An arithmetic argument (using completions) then proves that any positive definite integral unimodular lattice of rank 8 is isometric to one of these.

There is a proof with a Siegel mass formula [Si], and an account of it is given in [Se]. The sum of reciprocals of the orders of automorphism groups of certain positive definite lattices equals a computable constant. In the case of rank 8 unimodular and even, the contribution of L_{E_8} exhausts the allowed value, whence no other isometry type exists.

A later inequality due to Mordell [Mor2], based on works of Gauss and Hermite, and some results on lattices of rank at most 7 can be used to

[4] A lattice is *rectangular* if it has an orthogonal basis and is *square* if it has an orthogonal basis with all basis elements having the same norm.

[5] For all n, there are upper bounds for this minimum. Exact values of this minimum seem to be known for just $n \leq 8$ [Mor2], [Mar]; in [Mor1], this is denoted λ_n but the notation γ_n seems to be more popular.

[6] This lattice is generally known as the E_6 root lattice, L_{E_6}.

[7] Call two lattices in the same rational vector space *neighbors* if their intersection has index 2 in each one.

prove uniqueness of L_{E_8}. See the discussion which accompanies 6.1 Théorème [Mar], Chapitre VI, or 6.6.1 in [Mar03].

The theory of modular forms easily determines the theta function of a positive definite rank 8 even unimodular lattice (see [Se], p.110, 6.6.(i), and p.93). The first nontrivial coefficient is 240, which means that the number of norm 2 vectors in such a lattice is 240. The well-known classification of root systems indicates that this root system must have type E_8 and furthermore that the sublattice they span is even and unimodular, whence the lattice is uniquely determined.

Our article [POE], which revised the basic theory of the Leech lattice, Mathieu groups and Conway groups, motivated the search for an elementary characterization of L_{E_8}. After the present article was essentially written, we learned about similarities to work of Kneser ([K], [K73], [KS]), especially our 3.2. We do not use completions, however. We can classify positive definite integral lattices of rank at most 7 and determinant 2 as an easy consequence of our rank 8 unimodular classification 3.4 (the list is L_{E_7} and rectangular lattices). We can also deduce classification of positive definite lattices having rank at most 6 and determinant 3, but this is a bit more technical (the list is just L_{E_6} and rectangular lattices). Incidentally, this result implies the rank 6 characterization which was used in the proof of [Mor1]. Such classifications and more are contained in [K] Satz 3, p.250.

We thank Tom Fiore, Julia Gordon, Christopher Kennedy, Ivan Middleton, Michael Roitman and Kevin Woods in my 2002 graduate course at the University of Michigan for hearing an early version of my results. We are grateful to Gerald Höhn, Jacques Martinet and Jean-Pierre Serre for useful consultations. We are pleased to acknowledge the referee for a detailed, sensitive and quick report.

2 Notations for lattices and bounds of Hermite and Minkowski

Some definitions and general results on lattices used in our proofs are collected in the Appendix.

Notation 2.1. An orthogonal direct sum of lattices S and T is written $S \perp T$.

Definition 2.2. Denote by $\mathcal{U}_n$ the isometry types of integral unimodular positive definite lattices of rank n. Denote by $\mathcal{EU}_n$ and $\mathcal{OU}_n$ those isometry types in $\mathcal{U}_n$ which are even and odd, respectively.

Notation 2.3. Let n be a positive integer and $d \in (0, \infty)$.

Define $\mathcal{M}(n,d) := \frac{4}{\pi}\Gamma(1+\frac{n}{2})^{\frac{2}{n}} d^{\frac{1}{n}}$, the *Minkowski bound.*

Define $\mathcal{H}(n,d) := (\frac{4}{3})^{\frac{n-1}{2}} d^{\frac{1}{n}}$, the *Hermite bound.*

Theorem 2.4. *Let $b(n,d)$ be $\mathcal{M}(n,d)$ or $\mathcal{H}(n,d)$. Let n be a positive integer and $d \in (0,\infty)$. If a positive definite rank n lattice has determinant d, it contains a nonzero vector of squared length at most $b(n,d)$.*

These are elementary results. For modern proofs, see [W], [MH] for the Minkowski function and [J], [K73] for the Hermite function (note the comments on p.60 of [J] about ranks 6, 7 and 8).

Below is a table containing approximate values of $\mathcal{M}(n,d)$ and $\mathcal{H}(n,d)$. Since table entries will be used for upper bounds, we followed the referee's suggestion and used the Maple program below to round decimal expansions upward.

```
Digits := 50;
M := (n,d) -> evalf(4/Pi*GAMMA(1+n/2)^(2/n)*d^(1/n));
H := (n,d) -> evalf((4/3)^((n-1)/2)*d^(1/n));
for k from 1 to 8 do ceil(10^9*M(k,1)),ceil(10^9*M(k,2)); od ;
for k from 1 to 8 do ceil(10^9*H(k,1)),ceil(10^9*H(k,2)); od ;
```

Column 1 for $\mathcal{M}(n,d)$ is consistent with the table on p.17 of [MH].

$\mathcal{M}(n,d)$:	$d=1$	$d=2$	$\mathcal{H}(n,d)$:	$d=1$	$d=2$
$n=1$	1.000000000	2.000000000	$n=1$	1.000000000	2.000000000
$n=2$	1.273239545	1.800632633	$n=2$	1.154700539	1.632993162
$n=3$	1.539338927	1.939445517	$n=3$	1.333333334	1.679894734
$n=4$	1.800632633	2.141325138	$n=4$	1.539600718	1.830904128
$n=5$	2.058451326	2.364539652	$n=5$	1.777777778	2.042130409
$n=6$	2.313629797	2.596961641	$n=6$	2.052800958	2.304191168
$n=7$	2.566728337	2.833897841	$n=7$	2.370370371	2.617101070
$n=8$	2.818142368	3.073206044	$n=8$	2.737067943	2.984793757

For n small, we can use either function for our needs, so from now on, let $b(n,d)$ denote either one.

3 The classification

The idea is to find enough low norm orthogonal vectors to see that our lattice in $\mathcal{U}_n$, for $n \leq 8$, is a neighbor to a square lattice, hence easy to identify.

Lemma 3.1. *Suppose that J is an integral lattice of rank at least 2. Assume that J contains an element of norm 4.*

Then J contains a unit vector or there exists an integral lattice K satisfying: $det(K) = det(J)$, $K \cap J$ has index 2 in both K and J, and K contains a unit vector.

Proof. Let v be any norm 4 vector. If the unit vector $u := \frac{1}{2}v$ is in J, we are done. So we assume that u is not in J. Define $S := \{x \in J | (x, v) \in 2\mathbb{Z}\}$, a sublattice of index 1 or 2 in J which contains v. If $|J : S| = 2$, define $T := S$. If $J = S$, let T be any index 2 sublattice of J containing v (this is where we use $rank(J) > 1$). Define $K := \mathbb{Z}u + T$. $\square$

Lemma 3.2. *Let P and Q be positive definite unimodular integral lattices of rank n in $V := \mathbb{Q}^n$ so that $det(P \cap Q) = 4$ and Q is square.*

(i) Then $n \geq 4$ and P is the orthogonal direct sum $P_1 \perp P_2$, where P_1 is spanned by a set of unit vectors in Q and P_2 is isometric to the half-spin lattice of rank $m \in 4\mathbb{Z}$ (see 4.3). Also, $m > 0$.

(ii) P is square if and only if $m = 4$.

(iii) If P does not contain a unit vector, then $n = m \geq 8$.

Proof. (i) Since $det(P \cap Q) = 4$, $P \cap Q$ has index 2 in each of P and Q and $P \neq Q$, by 4.4. Write elements of V in coordinates with respect to an orthonormal basis $e_1, \dots, e_n$ of Q. An element v of $P \setminus Q$ has the form $(c_1, \dots, c_n) \in \frac{1}{2}\mathbb{Z}^n$ since $P+Q/Q \cong P/P\cap Q \cong \mathbb{Z}/2\mathbb{Z}$. The set $A \subseteq \{1, \dots, n\}$ of indices where $c_i \in \frac{1}{2} + \mathbb{Z}$ is nonempty (since $v \notin Q$) and has cardinality divisible by 4 (since $(v, v) \in \mathbb{Z}$). Furthermore, only one such A occurs here since $P + Q/Q \cong \mathbb{Z}/2\mathbb{Z}$.

We observe that $P = (P\cap Q)+\mathbb{Z}v$ and $P\cap Q = P^* \cap Q = \{x \in Q | (x, v) \in \mathbb{Z}\}$.

Each element of Q of the form e_i, for $i \notin A$, or $\pm e_k \pm e_\ell$, for $\{k, \ell\} \subset A$, has integral inner product with v, whence is in $P^* \cap Q = P \cap Q$. So, we may replace v by v plus a linear combination of such elements to arrange that v equals either $v_+ = \frac{1}{2}\sum_{i\in A} e_i$ or $v_- = -\frac{1}{2}e_j + \frac{1}{2}\sum_{i\in A'} e_i$ where $j \in A$ and $A' := A \setminus \{j\}$.

Let s, t be the orthogonal projections of V to $\sum_{i\in A} \mathbb{Q}e_i$, $\sum_{i\in\{1,2,\dots,n\}\setminus A} \mathbb{Q}e_i$. So, $v = s(v)$.

Obviously, $Q = s(Q) \perp t(Q)$. Define $R := \{x \in s(Q) | (x, v) \in \mathbb{Z}\} = P^* \cap s(Q) = P \cap s(Q)$. Since $(v, t(Q)) = 0$, $t(Q) \leq P^* \cap Q = P \cap Q$ and so by the Dedekind law 4.7, we have $P \cap Q = t(Q) + (P \cap s(Q)) = t(Q) \perp R$. Since $P \cap Q$ has index 2 in Q, R has index 2 in $s(Q)$.

Set $P_1 := t(Q)$ and $P_2 := R + \mathbb{Z}v \leq s(V)$. These lattices are orthogonal and intersect trivially. Now, $P = (P \cap Q) + \mathbb{Z}v = t(Q) + R + \mathbb{Z}v = P_1 + P_2$. We conclude that $P = P_1 \perp P_2$.

If $v = v_+$, P_2 is just the half-spin lattice defined in 4.3, over the index set A. If $v = v_-$, P_2 is isometric to the half-spin lattice (see the alternate version described in 4.3). Finally, note that $m = |A| > 0$.

(ii) This statement follows from the fact that the half-spin lattice is square precisely when its rank is 4.

(iii) Trivial. □

Lemma 3.3. *If an integral lattice L contains a unit vector u, then L is the orthogonal direct sum $L = \mathbb{Z}u \perp (u^\perp \cap L)$.*

Proof. If $x \in L$, $x = (x, u)u + (x - x(x, u)u)$. □

Theorem 3.4. *Let $n \leq 8$. Then $\mathcal{OU}_n$ consists of just square lattices, $\mathcal{EU}_n$ is empty for $n \leq 7$ and $\mathcal{EU}_8$ has just one isometry type, that of L_{E_8}.*

Proof. Let L be unimodular of rank $n \leq 8$. The case $n = 1$ is trivial, so assume $n \geq 2$.

Since $b(n, 1) < 3$ and $b(n - 1, 2) < 3$ for $n \leq 8$, 4.6 shows that L contains a unit vector or an orthogonal pair of roots. If L contains a unit vector, we are done by 3.3 and induction, and if it contains an orthogonal pair of roots, we are done by 3.1, induction, and 3.2. □

4 Appendix: Background material for lattices

For completeness, we assemble a few general definitions, notations and background results on lattices used in our proofs. Probably all may be found in the literature or are well-known. In this appendix, a lattice has arbitrary signature, except for 4.2, 4.3 and 4.6 where it is positive definite.

Definition 4.1. A *lattice* is a free abelian group of finite rank with a rational valued symmetric bilinear form. We think of it as embedded in a rational vector space with the same basis. The *dual* of a lattice M is denoted M^*. The *determinant* of a lattice is $det(G)$, where G is any *Gram matrix*, meaning the square matrix $((x_i, x_j))$ of size $rank(M)$, where $\{x_i\}$ is any basis. Now assume that M is *integral*, i.e., (x, y) are integers for all $x, y \in M$. We call M *even* if (x, x) is an even integer, for all $x \in M$. If M is not even, it is *odd*. The *discriminant group* of M is $\mathcal{D}(M) := M^*/M$. When $det(M) \neq 0$, $|\mathcal{D}(M)| = |det(M)|$. We call M *unimodular* if $\mathcal{D}(M) = 0$, i.e., $det(M) = \pm 1$. We say that M is *positive definite* if $(x, x) > 0$ for all $x \in M, x \neq 0$.

Definition 4.2. In a lattice, a *root* is an element of norm 2. A *root lattice* is a lattice spanned by a root system whose indecomposable components have types ADE only and which are normalized so that their members have norm 2 (so our two meanings of roots are compatible). When X is a type of root system, we write L_X for a root lattice spanned by a set of roots which forms a system of type X. Thus, we write $L_{E_8}, L_{E_7}, L_{E_6}, L_{A_1A_1}, L_{A_1A_2E_6}$, etc.

Definition 4.3. For an integer $n > 0$, define the *half-spin lattice* to be $\{(x_1, \ldots, x_n) \mid x_i \in \frac{1}{2}\mathbb{Z}, x_i - x_j \in \mathbb{Z}, \sum_{i=1}^n x_i \in 2\mathbb{Z}\}$. It is unimodular for all n, integral for $n \in 4\mathbb{Z}$ and even for $n \in 8\mathbb{Z}$. When $n = 8$, this lattice is isometric to L_{E_8}.

There is another version of the half-spin lattice, which is $\{(x_1, \ldots, x_n) \mid x_i \in \frac{1}{2}\mathbb{Z}, x_i - x_j \in \mathbb{Z}, \sum_{i=1}^n x_i \in 2\mathbb{Z}$ when the $x_i \in \mathbb{Z}, \sum_{i=1}^n x_i \in 1+2\mathbb{Z}$ when the $x_i \in \frac{1}{2}+\mathbb{Z}\}$. It is obtained from the previous lattice by applying a reflection which changes sign at one of the coordinates (cf. [CS], p.120).

Lemma 4.4. *Let L be a lattice and M a finite index sublattice. Then $det(M) = det(L)|L{:}M|^2$.*

Proof. This follows from the theory of modules for a PID. There exists a basis $x_1, \ldots, x_n$ of L and nonzero integers $d_1, \ldots, d_n$ so that $d_1x_1, \ldots, d_nx_n$ is a basis of M. □

Lemma 4.5. *Let L be an integral lattice and M any sublattice. Assume $det(L) \neq 0$ and $det(M) \neq 0$.*

(i) If π is the natural map of L to $\mathcal{D}(M)$, then $det(M^\perp \cap L)det(M) = det(L)|\pi(L)|^2$.

(ii) Also, $det(M^\perp \cap L)$ divides $det(M)det(L)$. In fact, $\frac{det(M)det(L)}{det(M^\perp \cap L)}$ is the square of an integer.

Proof. We have $Ker(\pi) = (M^\perp \cap L) \perp M$ and so $det(M^\perp \cap L)det(M) = det(L)|\pi(L)|^2$, whence (i). This equation implies that $det(M^\perp \cap L)(\frac{det(M)}{|\pi(L)|}) = |\pi(L)|det(L)$. By Lagrange's theorem, $|\pi(L)|$ divides $|\mathcal{D}(M)| = |det(M)|$, so we get the first part of (ii). By multiplying both sides of (i) by $det(L)$, we see that the ratio $\frac{det(M)det(L)}{det(M^\perp \cap L)}$ is the square of a rational number. Therefore the second part of (ii) follows from the first. □

Lemma 4.6. *Let L be a positive definite integral lattice and $x_1, x_2, \dots, x_m \in L$ be an orthogonal set of nonzero vectors with respective norms $n_1, n_2, \dots, n_m$. Their common annihilator in L contains a nonzero vector whose norm is at most $b(n-m, det(L)n_1 \dots n_m)$.*

Proof. Let T be the span of $x_1, x_2, \dots, x_m$. The possible values for $q := det(T^\perp \cap L)$ satisfy (among other conditions) $q|det(L)det(T)$ (see 4.5(ii)), i.e., $q|det(L)n_1 \dots n_m$. We finish by quoting 2.4 and using the property that $b(n-m, d)$ is increasing for $d \in (0, \infty)$. □

Lemma 4.7. *(Dedekind law.) If A, B, C are subgroups of some additive group and $A \leq B \leq A + C$, then $B = A + (B \cap C)$.*

Proof. Write $b \in B$ as $b = a + c$, for $a \in A$, $c \in C$ and note that $c = b - a \in B$. □

References

[CS] John Conway and Neil Sloane, Sphere Packings, Lattices and Groups, Grundlehren der mathematischen Wissenschaften 290, Springer Verlag, 1988.

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

[J] Burton W. Jones, The arithmetic theory of quadratic forms, The Carus Mathematical Monographs, Number 10, Mathematical Association of America, John Wiley and Sons, Inc., 1950.

[K] Martin Kneser, Klassenzahlen definiter quadratischer Formen. (German) Arch. Math. 8 (1957), 241–250.

[K73] Martin Kneser, Quadatische Formen Vorlesung, Mathematisches Institut der Universität Göttingen, 1973.

[KS] Martin Kneser and Rudolph Scharlau, Quadratische Formen, Springer Verlag, 2001.

[Mar] Jacques Martinet, Les Réseaux parfaits des espaces Euclidiens, Masson, Paris, 1996.

[Mar03] Jacques Martinet, Perfect lattices in Euclidean spaces, Grundlehren der mathematischen Wissenschaften 327, Springer Verlag, 2003.

[MH] John Milnor and Dale Husemoller, Symmetric Bilinear Forms, Ergebnisse der Mathematik und Ihrer Grenzgebiete, Band 73, Springer Verlag, New York, 1973.

[Mor1] L. J. Mordell, The definite quadratic forms in eight variables with determinant unity, J. Math. Pures Appl. 17 (1938), 41–46.

[Mor2] L. J. Mordell, Observation on the minimum of a positive quadratic form in eight variables, Journal of the London Mathematical Society, 19 (1944), 3–6.

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

[Si] Carl Ludwig Siegel, Gesammelte Abhandlungen, I, No. 20 and III, No. 79. Springer-Verlag, 1966.

[W] Edwin Weiss, Algebraic Number Theory, McGraw-Hill, New York, 1963.