ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE DIRECT®

Journal of Number Theory 101 (2003) 185–194

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

On the involutions fixing the class of a lattice

H.-G. Quebbemann[a] and E.M. Rains[b,*]

[a] *Fachbereich 6 Mathematik, Universität Oldenburg, 26111 Oldenburg, Germany*
[b] *Center for Communication Research, Institute for Defense Analyses, Princeton, NJ 08540, USA*

Received 23 October 2002; revised 15 November 2002

Communicated by M. Pohst

Abstract

With any integral lattice Λ in n-dimensional Euclidean space we associate an elementary abelian 2-group $I(\Lambda)$ whose elements represent parts of the dual lattice that are similar to Λ. There are corresponding involutions on modular forms for which the theta series of Λ is an eigenform; previous work has focused on this connection. In the present paper $I(\Lambda)$ is considered as a quotient of some finite 2-subgroup of $O_n(\mathbb{R})$. We establish upper bounds, depending only on n, for the order of $I(\Lambda)$, and we study the occurrence of similarities of specific types.
© 2003 Elsevier Science (USA). All rights reserved.

Keywords: Lattices; Modular; Iso-dual; Involutions; 2-Groups

Introduction

The arithmetic of lattices in euclidean spaces contains a counterpart to the action of Atkin–Lehner involutions on elliptic modular forms. An involution here takes the isometry class of a lattice to that of a rescaled partial dual. There are remarkable cases of (non-unimodular) lattices that are invariant under this action; such a lattice is called strongly modular. Some prominent examples have arisen as sections of the Leech lattice or in the study of finite rational matrix groups. See [3,5,8,10].

A basic question that has remained open is when in general strong modularity can occur. For instance, given $n = 4r$ and $\ell = p_1 \cdot \ldots \cdot p_s$ with distinct primes p_i $(s > 0)$,

*Corresponding author.
E-mail addresses: quebbemann@mathematik.uni-oldenburg.de (H.-G. Quebbemann), rains@idaccr.org (E.M. Rains).

0022-314X/03/$ - see front matter © 2003 Elsevier Science (USA). All rights reserved.
doi:10.1016/S0022-314X(03)00022-2

there exist even lattices of dimension n and level ℓ whose genera have the necessary property of being invariant under all 2^s involutions. But as we shall see, a class can have this property only if $s \leqslant 2v_2(n)$, where v_2 denotes the 2-adic exponent valuation. More generally, we find that at most $4^{[n/2]}$ involutions fix the class of a given n-dimensional integral lattice. In cases of squarefree level here $[n/2]$ can be replaced by $v_2(n)$. These bounds are attained for any n by certain lattices built up from the case $n = 2$ (which was studied in detail in [7]).

When one considers a single involution, again the question arises what additional conditions must an invariant genus satisfy in order to contain an invariant class. Some restrictions have been found by studying congruence properties mod 2 of the relevant Atkin–Lehner eigenforms [6,8, Appendix]. A more elementary discussion related to this question is given in the final section of this paper.

1. Involutions and groups

We shall study the involutory invariance of an integral lattice by applying representation theory to its "isomorphism group". This object, which is defined below, has occurred in [3] as a subset of $\mathrm{GL}_n(\mathbb{R})$, and as a group it had a short appearance in [8, Theorem 6].

We fix positive integers ℓ and n. Let $\mathscr{L}$ denote the set of lattices Λ in euclidean $\mathbb{R}^n$ such that $\Lambda \subseteq \Lambda^*$ and $\ell\Lambda^* \subseteq \Lambda$, where Λ^* is the dual lattice. Then the orthogonal group $O_n(\mathbb{R})$ acts on $\mathscr{L}$. Furthermore, we have the elementary abelian 2-group $W(\ell)$ of positive divisors $m||\ell$ (i.e., $m|\ell$ and $\gcd(m, \ell/m) = 1$), with multiplication $m * m' = mm'/\gcd(m,m')^2$. Defining (as in [5, Section 1])

$$\Lambda_m = \sqrt{m}(\Lambda^* \cap m^{-1}\Lambda)$$

we also have a group action of $W(\ell)$ on $\mathscr{L}$, which clearly commutes with the action of $O_n(\mathbb{R})$. In particular, either group acts on the orbits of the other one.

Now fix Λ, and let ℓ be its level in the sense that ℓ is minimal for $\ell\Lambda^* \subseteq \Lambda$ (so ℓ divides $\det \Lambda = \#\Lambda^*/\Lambda$). Then the following groups are canonically associated with Λ. First, $O_n(\mathbb{R})$ contains the usual stabilizer $\mathrm{Aut}(\Lambda)$ and the stabilizer of the $W(\ell)$-orbit

$$\mathrm{Iso}(\Lambda) = \{\sigma \in O_n(\mathbb{R}) \mid \Lambda = \sigma\Lambda_m \text{ for some } m \in W(\ell)\}.$$

Next, in $W(\ell)$ there are again the stabilizer of Λ and the stabilizer of its $O_n(\mathbb{R})$-orbit, denoted by $A(\Lambda)$ and $I(\Lambda)$, respectively. Note that if $m \in I(\Lambda)$, then $\det \Lambda = \det \Lambda_m$, which implies $m^{n/2}||\det \Lambda$. Actually $A(\Lambda)$ is trivial. In fact, if $\Lambda = \Lambda_m$, then m must be a square, say $m = k^2$, and $(1/\sqrt{k})\Lambda$ is an integral lattice of level ℓ/k and determinant prime to m; so $m = 1$. As an immediate consequence we obtain a group isomorphism

$$\mathrm{Iso}(\Lambda)/\mathrm{Aut}(\Lambda) \cong I(\Lambda)$$

induced by $\sigma \mapsto m : \Lambda = \sigma\Lambda_m$. Note also that the squares in $I(\Lambda)$ form a subgroup $B(\Lambda)$ which corresponds to the quotient of $\mathrm{Iso}(\Lambda) \cap \mathrm{GL}(\Lambda \otimes \mathbb{Q})$ by $\mathrm{Aut}(\Lambda)$. Of course, $B(\Lambda) = I(\Lambda)$ for odd n.

If $I(\Lambda) = W(\ell)$, then Λ is said to be strongly modular. Two "trivial" constructions of such lattices will be used. Namely, if Λ and Λ' are strongly modular with coprime levels ℓ, ℓ', then so are, with level $\ell\ell'$,

- the orthogonal sum $\sqrt{k'}\Lambda \oplus \sqrt{k}\Lambda'$ in the case of squares $\ell = k^2, \ell' = k'^2$
- the tensor product $\Lambda \otimes \Lambda'$.

2. A general bound

To measure $I(\Lambda)$ we first replace the linear group $\mathrm{Iso}(\Lambda)$ by a 2-Sylow subgroup G, so that $I(\Lambda) \cong G/P$ for $P = G \cap \mathrm{Aut}(\Lambda)$. If n is odd, an even larger elementary abelian quotient of G arises from $P \cap SL_n(\mathbb{R})$ because P contains $-\mathrm{id}$. Put

$$d(G) = d(G/Q)$$

for any finite p-group G, where Q denotes the minimal normal subgroup such that G/Q is elementary abelian, in which case d means dimension over $\mathbb{F}_p$. We would like to use that $d(G) \leqslant n$ if G is a linear group of degree n. Actually this inequality is true in general for odd p, while for 2-subgroups of $\mathrm{GL}_n(\mathbb{C})$ one has $[3n/2]$ as the best possible general upper bound [1,11].

Theorem 2.1. *If G is a finite 2-subgroup of $\mathrm{GL}_n(\mathbb{R})$, then $d(G) \leqslant n$.*

This result can be extracted from [11, Lemma 4], in the case where the natural representation of G on $\mathbb{R}^n$ is monomial, but the method equally applies when this representation is induced from a 2-dimensional dihedral representation of a subgroup. (The inductive proof in any case requires to make a stronger statement, implying that if H is a normal subgroup of G, then $d(H) \leqslant n$ and $d(G/H) \leqslant n$ where at least one inequality is strict. Of course, over $\mathbb{C}$ this already fails for $n = 1$.) The remaining cases of reducible or not absolutely irreducible groups are easily dealt with, using induction on n or an upper bound over $\mathbb{C}$ in dimension $v = n/2$ (the crude bound $2v - 1$ suffices).

Theorem 2.2. *For any integral lattice $\Lambda \subset \mathbb{R}^n$,*

$$d(I(\Lambda)) \leqslant 2[n/2].$$

In particular, if Λ is strongly modular, at most $2[n/2]$ distinct primes divide the level ℓ. Lattices that attain this bound exist in any dimension n.

Proof. The bound is an immediate consequence of the preceding theorem and the remarks made at the beginning of this section. It is attained by strongly modular

lattices that arise by the first construction mentioned at the end of Section 1. All we must know is that, for $n=2$ and primes $p\neq q$, there exists such a lattice with level p^2q^2; for this see [7, Corollary 10]. For general even n we then take scaled orthogonal sums of such lattices, and for odd n we add a 1-dimensional summand. □

It should be noted at this point that also many pairs of primes $p\neq q$ admit a strongly modular 2-dimensional lattice with level pq; the condition is that p and q must be quadratic residues of each other [5,7]. Taking now tensor products of such lattices, the bound above is still attained for $n=4$, but otherwise this construction suggests a different bound which will be obtained in the next section.

It may be expected, however, that orthogonally indecomposable lattices attaining the bound of Theorem 2.2 exist in any dimension. To obtain an example for $n=3$, consider a solution of $a^2+b^2=c^2$ where a,b,c are coprime positive integers with $a+c$ divisible by 4. Take the orthogonal sum $(a)\oplus\left(\begin{smallmatrix}c & b\\ b & c\end{smallmatrix}\right)$, and construct its Kneser 2-neighbour with respect to the sum of the first two base vectors. For this second lattice Λ, which like the first has level $\ell=a^2$, we find the Gram matrix

$$C=\begin{pmatrix}\frac{1}{4}(a+c) & \frac{b}{2} & \frac{1}{2}(c-a)\\ \frac{b}{2} & c & b\\ \frac{1}{2}(c-a) & b & a+c\end{pmatrix}=S(\ell C^{-1})S^t,\quad S=\begin{pmatrix}0 & 0 & 1\\ 0 & -1 & 0\\ 1 & 0 & 0\end{pmatrix}.$$

This shows that again $\{1,\ell\}\subseteq I(\Lambda)$. For $(a,b,c)=(15,8,17)$, computation of Λ_9 moreover shows that Λ is strongly modular; it is clearly indecomposable. (C is reduced in the sense of Seeber–Eisenstein [4] whenever $a=4t^2-1$ and $b=4t$, $t>1$. For $t>2$, however, $I(\Lambda)$ does not contain $m=(2t-1)^2\in W(\ell)$. In fact, Λ has minimal norm $2t^2$, while Λ_m contains the vector of norm 8 given by $(1/\sqrt{m})(2,-2,1)$ with respect to C.)

3. The squarefree case

If we only consider lattices Λ with squarefree level or, in the general case, factor out $B(\Lambda)=I(\Lambda)\cap\{k^2\mid k=1,2,\ldots\}$, then the result of Section 2 can be improved considerably. We now make use of the fact that any element of $\mathrm{Iso}(\Lambda)$ up to some scalar factor $1/\sqrt{m}$ is defined over $\mathbb{Z}$, and so $\mathrm{Iso}(\Lambda)$ is conjugate to a subgroup of

$$\mathrm{GL}_n(\mathbb{Q})^+=\langle\,\mathrm{GL}_n(\mathbb{Q}),\{\sqrt{p}\cdot\mathrm{id}\mid p\ \text{prime}\}\,\rangle.$$

Theorem 3.1. *Let G be a finite 2-subgroup of $\mathrm{GL}_n(\mathbb{Q})^+$, and define $N=G\cap\mathrm{GL}_n(\mathbb{Q})$. Then $d(G/N)\leqslant 2v_2(n)$.*

Proof. We can write $G = G_1 \cup G_2 \cup \ldots$, where $G_m = G \cap \sqrt{m}\mathrm{GL}_n(\mathbb{Q})$ is a coset of $N = G_1$ or is empty. We may assume that N contains $-\mathrm{id}$ (or adjoin it). Let ϱ denote the natural representation of G on $V = K^n$, where K is the field obtained from $\mathbb{Q}$ by adjoining the relevant square roots $\sqrt{m}$ (i.e., those for which G_m is non-empty) together with $\zeta = e^{2\pi i/r}$, where r is the exponent of G. Let χ be the character of ϱ. Then the values of χ lie in the 2-power cyclotomic field $\mathbb{Q}(\zeta)$, while on the other hand $\chi(\sigma) \in \mathbb{Q}\sqrt{m}$ for $\sigma \in G_m$. This shows that χ vanishes outside $N \cup G_2$. Set $M = N$ if χ also vanishes on G_2, and $M = N \cup G_2$ otherwise. Denoting the restriction of χ to the subgroup M by χ_M, we obtain

$$\langle \chi, \chi \rangle = \frac{1}{\#G} \sum_{\sigma \in G} |\chi(\sigma)|^2 = \frac{1}{\#G} \sum_{\sigma \in M} |\chi(\sigma)|^2 = \frac{1}{(G:M)} \langle \chi_M, \chi_M \rangle.$$

It follows that $(G:M) \leqslant n^2$, since $\langle \chi, \chi \rangle \geqslant 1$ and $\langle \chi_M, \chi_M \rangle \leqslant n^2$. However, the theorem moreover asserts that $(G:N)$ divides n^2. To prove this we first observe that the Galois group $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ acts on the G-invariant subspaces of V. If such a subspace $U \neq 0$ is defined over $\mathbb{Q}$ (i.e., invariant also under Γ), then the kernel of the restriction of ϱ to U clearly is contained in N, and in the case $U \neq V$ it suffices to apply the theorem on U and V/U (using induction on n). Therefore we now assume that no such proper subspace exists. This implies that the isotypical summands of ϱ_M are permuted transitively by the (semidirect) product $G \cdot \Gamma$. So we have

$$\chi_M = a(\psi_1 + \cdots + \psi_b),$$

where $\psi_1, \ldots, \psi_b$ are pairwise inequivalent irreducible characters of M and all are of the same degree c. Then $n = abc$ and

$$n^2 = bc^2 \langle \chi_M, \chi_M \rangle = bc^2 \langle \chi, \chi \rangle (G:M).$$

Finally suppose that $(M:N) = 2$. Then it suffices to show that bc^2 is even. Since M is a 2-group, c is a power of 2, and we only have to show that b is even if $c = 1$. Let ψ be one of the linear characters ψ_i. If $\psi^2 = 1$, set $\tilde{\psi} = \lambda\psi$ where λ is the linear character of M with kernel N, and if $\psi^2 \neq 1$ set $\tilde{\psi} = \psi^{-1}$. It follows that $\tilde{\psi} \neq \psi$ and $\tilde{\psi}$ also appears in χ_M (to see this in the first case, use a Galois automorphism mapping $\sqrt{2}$ to $-\sqrt{2}$). Therefore the linear characters ψ_i appear in pairs. □

Theorem 3.2. *For any integral lattice $\Lambda \subset \mathbb{R}^n$,*

$$d(I(\Lambda)/B(\Lambda)) \leqslant 2v_2(n).$$

In particular, if Λ is strongly modular with squarefree level ℓ, then ℓ is the product of at most $2v_2(n)$ primes. Lattices that attain this bound exist in any dimension n.

Proof. Recall that $I(\Lambda)/B(\Lambda) \cong \mathrm{Iso}(\Lambda)/(\mathrm{Iso}(\Lambda) \cap \mathrm{GL}(\Lambda \otimes \mathbb{Q}))$, where the last two groups again may be replaced by Sylow 2-subgroups. So the bound immediately

follows from the preceding theorem. For $n = 2^e f$, f odd, this bound is attained by the f-fold orthogonal sum of the tensor product of e strongly modular 2-dimensional lattices with coprime levels $p_i q_i$ ($p_i \neq q_i$ primes). As was noted already, enough such lattices exist. □

If more is known on the action of a Sylow 2-subgroup of $\mathrm{Aut}(\Lambda)$, then of course the proof of Theorem 3.1 gives more information on $I(\Lambda)$. Suppose, for example, that this action is multiplicity-free. Then in that proof the equation $n = abc$ holds with $a = 1$ and $b = \langle \chi_M, \chi_M \rangle = (G : M)\langle \chi, \chi \rangle$, so for $M = N$ (in particular, for odd ℓ) we obtain

$$d(I(\Lambda)/B(\Lambda)) \leqslant v_2(n).$$

Given $\ell = p_1 \cdot \ldots \cdot p_s$ with s distinct primes p_i, this bound is attained by the tensor product of 2-dimensional lattices having the Gram matrix $\begin{pmatrix} 1 & 0 \\ 0 & p_i \end{pmatrix}$ or $\begin{pmatrix} 2 & 1 \\ 1 & q_i \end{pmatrix}, q_i = (p_i + 1)/2$. The condition of multiplicity 1 is satisfied because each of these lattices admits a reflection and the corresponding automorphisms of Λ generate an elementary abelian 2-group acting by its regular representation.

Moreover, it is this last bound, $s \leqslant v_2(n)$ for a strongly modular lattice, which some of the "extremal" lattices discovered during the past few years attain.

4. Single involutions

In this section we fix a positive integer m which is not of the form k^2 or $2k^2$ for an integer k. If m belongs to $I(\Lambda)$ for an integral lattice Λ, then as before Λ is the image of $\Lambda^* \cap m^{-1}\Lambda$ under a similarity $\tau = \sqrt{m}\sigma$ where $\sigma \in O_n(\mathbb{R})$ is of 2-power order; that is, we have $f(\tau) = 0$ with $f = X^{2r} - m^r$ for some $r = 2^k$, $k \geqslant 0$. Let such a polynomial f be fixed, and define the algebra

$$E = \mathbb{Q}[X]/(f) = \mathbb{Q}[\alpha], \quad \alpha = X + (f).$$

In E we consider the root of unity $\zeta = \alpha^2/m$ and the order $R = \mathbb{Z}[\alpha, \zeta]$ (over which our lattices will be defined). Now f factors into the rationally irreducible polynomials

$$f_0 = X^2 - m, \quad f_j = X^{2^j} + m^{2^{j-1}} \quad (1 \leqslant j \leqslant k).$$

So we have $E \cong E_0 \times \cdots \times E_k$ where $E_j = \mathbb{Q}[X]/(f_j) = \mathbb{Q}(\alpha_j)$ is a quadratic extension of the 2^jth cyclotomic field $\mathbb{Q}(\zeta_j)$, with $\alpha_j^2 = m\zeta_j$. Defining $\bar{\alpha} = m\alpha^{-1}$ we obtain an involutory automorphism "bar" on E, and correspondingly on each E_j. For $j \geqslant 1$ this involution of E_j is not the identity, so then E_j also is a (totally complex) quadratic extension of the totally real field $\mathbb{Q}(\beta_j), \beta_j = \alpha_j + \overline{\alpha_j}$, with $\beta_j^2 = m(1 + \zeta_j)(1 + \zeta_j^{-1})$. Note that $R = \bar{R}$.

By an inner product space over E, we mean a finitely generated E-module V carrying an E-valued, totally positive definite hermitian form h for the involution defined above. Clearly such a hermitian module splits as an orthogonal sum of hermitian spaces over the fields E_j (for $j=0$ "hermitian" here means "symmetric bilinear"). By definition, h is totally positive definite if each of these summands is. In this case V also carries the rational inner product

$$u \cdot v = (2r)^{-1} \operatorname{Tr}_{E/\mathbb{Q}} h(u,v),$$

where $\operatorname{Tr}_{E/\mathbb{Q}}$ denotes the sum of the field traces. Given an R-lattice $\Lambda \subset V$, we denote its R-dual with respect to h by Λ^h and its $\mathbb{Z}$-dual with respect to the dot product by Λ^*.

Theorem 4.1. *If (V,h) is an inner product space over E and Λ is an R-lattice on V, then the duals are related by $\Lambda^h = \tau(\Lambda^*)$, where $\tau(v) = \alpha v$. In particular, Λ is contained in Λ^h with index prime to m precisely when*

$$\Lambda \subseteq \Lambda^*, \quad m \in I(\Lambda), \quad \Lambda = \tau(\Lambda^* \cap m^{-1}\Lambda).$$

Conversely, if these conditions are satisfied by a lattice $\Lambda \subset \mathbb{R}^n$ and a similarity τ with $f(\tau) = 0$, then Λ and τ arise from R in the way above.

Proof. For the $\mathbb{Z}$-basis $1, \zeta, \ldots, \zeta^{r-1}, \alpha, \alpha\zeta, \ldots, \alpha\zeta^{r-1}$ of R it is easily seen that all elements have trace 0, except for $\operatorname{Tr}_{E/\mathbb{Q}}(1) = 2r$. Therefore, given $\varepsilon \in E$, the condition $(2r)^{-1}\operatorname{Tr}_{E/\mathbb{Q}}(\varepsilon R) \subseteq \mathbb{Z}$ is equivalent to $\varepsilon \in \alpha^{-1}R$. This proves the first part. As to the converse, the action of τ makes $V = \Lambda \otimes \mathbb{Q}$ into an E-module, and since Λ is stable under both τ and $(1/m)\tau^2$, it is an R-lattice. We have to show that the inner product arises from one over E in the way described. For fixed u and v in V consider the linear map t from E to $\mathbb{Q}$ defined by $t(\varepsilon) = (\varepsilon u) \cdot v$. There is a unique ε' in E such that

$$\operatorname{Tr}_{E/\mathbb{Q}}(\varepsilon\varepsilon') = 2rt(\varepsilon)$$

for all $\varepsilon \in E$, and we define $h(u,v)$ to be this element ε'. The verification of further details will be omitted. (Compare [2]; the discussion restricted there to isometries carries over to similarities.) □

In the following m is supposed to be odd. The theorem may be applied to find restrictions for the rational quadratic space $V = \Lambda \otimes \mathbb{Q}$ when $I(\Lambda)$ contains m. Recall that in this case $\det \Lambda = m^{n/2}d'$ where m and d' are relatively prime. The necessary condition that V admits the similarity factor m just means that (i) m is a square modulo each prime $p > 2$ dividing d' with odd multiplicity and (ii) d' is a square modulo each prime p dividing m with odd multiplicity. This can be seen, for instance, by Scharlau [9, Chapter 5, Corollary 3.6].

Let Λ be an even lattice. We use the rational invariants defined at an arbitrary prime number p by the Gauss sum

$$\gamma_p(\Lambda) = (\det_p \Lambda)^{-1/2} \sum \exp(\pi i v \cdot v),$$

where the summation extends over the elements $v + \Lambda$ in the p-primary component of Λ^*/Λ; $\det_p \Lambda$ denotes the order of this group. The product $\prod \gamma_p(\Lambda)$ taken over all primes p is $i^{n/2}$. (See [9, Chapter 5, Section 8].)

Recall that if $m \in I(\Lambda)$, then V is defined over the direct product of the fields $E_0 = \mathbb{Q}(\sqrt{m}), E_1 = \mathbb{Q}(\sqrt{-m}), E_2, \ldots, E_k$, where E_j for $j > 1$ has degree 2^{j-1} over $\mathbb{Q}(i)$. Assume for the moment that the contributions from E_0 and E_1 are zero. Then the dimension n is a multiple of 4, and the rational quadratic form on V arises from a hermitian form over $\mathbb{Q}(i)$, so it is an orthogonal sum $\phi \perp \phi$ and has square determinant. We compute that for $p^s || m$,

$$\gamma_p(\Lambda) = \begin{cases} 1 & \text{if } p^s \equiv 1 \pmod 4, \\ (-1)^{n/4} & \text{if } p^s \equiv 3 \pmod 4, \end{cases}$$

which gives

$$\prod_{p|m} \gamma_p(\Lambda) = (-1)^{\frac{n}{4}\frac{m-1}{2}}.$$

When $m \equiv 7 \pmod 8$, the assumption used here is eliminated by the following theorem (first proved in [6] by less elementary arguments, a special case can be found in [8]).

Theorem 4.2. *Let m be congruent to* 7 mod 8, *and let m' be a positive integer relatively prime to m such that $-m$ is a square* mod m'. *Then for any even lattice Λ of level dividing mm' with $m \in I(\Lambda)$,*

$$\prod_{p|m'} \gamma_p(\Lambda) = \prod_{p|m'} \left(\frac{\sqrt{-m}}{\det_p \Lambda} \right),$$

where in the factor corresponding to p, $\sqrt{-m}$ represents either square root of $-m$ *in the p-adic integers.*

Proof. First, note that for odd $p|m'$ such that m is not a square modulo p, $\det_p \Lambda$ must be a square (since otherwise V does not admit the similarity factor m). In particular, since $-m$ is assumed to be a square modulo p, we find that either $\det_p \Lambda$ is a square or -1 is a square modulo p, and thus the given Legendre symbols are all well-defined.

Now consider the R-lattice structure for the order R as before. Let R_j be the image of R in E_j for $j = 0, \ldots, k$, and define the order

$$R' = R_0 \times \cdots \times R_k.$$

Since the index of R in R' is a power of 2, there exists a positive integer t such that $R'(2^t\Lambda)$ is an even lattice satisfying the hypotheses (possibly m' has to be multiplied by a power of 2), with the same Gauss sums and p-determinants modulo squares as Λ. Since R' is a product of orders preserved by the involution, $R'(2^t\Lambda)$ splits as a product of lattices, one over each order. Since the desired identity is preserved under taking products, we may reduce to the case that Λ is a lattice over one of the factors R_j of R'.

Case $j>1$: As noted already, here Λ has square determinant and dimension divisible by 4. The computations preceding the theorem and the product formula give

$$\prod_{p|m'} \gamma_p(\Lambda) = (-1)^{n/4} \prod_{p|m} \gamma_p(\Lambda) = 1$$

as required.

Case $j=1, \mathbb{Q}(\sqrt{-m})$: The rational quadratic form on V now splits as $\phi \perp m\phi$; since $-m$ is a square in $\mathbb{Z}_p$, $V\otimes\mathbb{Q}_p$ is hyperbolic for all $p|m'$. In particular, $\det_p \Lambda$ is a square and $\gamma_p(\Lambda)=1$ for all $p|m'$.

Case $j=0, \mathbb{Q}(\sqrt{m})$: Then Λ contains a sublattice of index prime to m that splits as an orthogonal sum of 2-dimensional lattices preserved by $\mathbb{Z}[\sqrt{m}]$. (Indeed, if $v\in\Lambda$ has norm prime to m, then the sum of $\Lambda\cap\mathbb{Q}(\sqrt{m})v$ and $\Lambda\cap(\mathbb{Q}(\sqrt{m})v)^{\perp}$ has index prime to m; proceed by induction.) It thus suffices to consider the case of a primitive 2-dimensional even lattice of level exactly mm', in which case the claim follows from Theorem 11 of [7]. □

For example, let $4|n$ and *let* $\ell>1$ be squarefree. Given signs $\gamma_p=\pm1$ for the primes $p|\ell$ such that $\prod\gamma_p=(-1)^{n/4}$, there exist even lattices Λ of dimension n, level ℓ, determinant $\ell^{n/2}$ and rational invariant γ_p at each p. In this situation all divisors of ℓ are similarity factors of $\Lambda\otimes\mathbb{Q}$. However, when $\ell=mm'$ where $m\equiv 7 \pmod 8$ and $-m$ is a square modulo m', we obtain

$$\prod_{p|m'} \gamma_p = 1$$

as a necessary condition for having $m\in I(\Lambda)$. For m incongruent to 7 mod 8 there is no similar restriction in general.

References

[1] I.M. Isaacs, The number of generators of a linear p-group, Canad. J. Math. 24 (1972) 851–858.
[2] J. Milnor, On isometries of inner product spaces, Invent. Math. 8 (1969) 83–97.
[3] G. Nebe, The normalizer action and strongly modular lattices, L'Enseignement Math. 43 (1997) 67–76.
[4] O.T. O'Meara, On indecomposable quadratic forms, J. Reine Angew. Math. 317 (1980) 120–156.

[5] H.-G. Quebbemann, Atkin–Lehner eigenforms and strongly modular lattices, L'Enseignement Math. 43 (1997) 55–65.
[6] E.M. Rains, Non-existence results for modular lattices, preprint 1999.
[7] E.M. Rains, Class groups and modular lattices, J. Number Theory 88 (2001) 211–224.
[8] E.M. Rains, N.J.A. Sloane, The shadow theory of modular and unimodular lattices, J. Number Theory 73 (1998) 359–389.
[9] W. Scharlau, Quadratic and Hermitian Forms, Springer, Berlin, 1985.
[10] R. Scharlau, R. Schulze-Pillot, Extremal lattices, in: B.H. Matzat, G.-M. Greuel, G. Hiss (Eds.), Algorithmic Algebra and Number Theory, Springer, Berlin, 1998, pp. 139–170.
[11] B.A.F. Wehrfritz, The rank of a linear p-group, an apology, J. London Math. Soc. 21 (2) (1980) 237–243.