JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 3, Number 4, October 1990

GROUP REPRESENTATIONS AND LATTICES

BENEDICT H. GROSS

This paper began as an attempt to understand the Euclidean lattices that were recently constructed (using the theory of elliptic curves) by Elkies [E] and Shioda [Sh1, Sh2], from the point of view of group representations. The main idea appears in a note of Thompson [Th2]: if one makes strong irreducibility hypotheses on a rational representation V of a finite group G, then the G-stable Euclidean lattices in V are severely restricted. Unfortunately, these hypotheses are rarely satisfied when V is absolutely irreducible over $\mathbf{Q}$. But there are many examples where the ring $\mathrm{End}_G(V)$ is an imaginary quadratic field or a definite quaternion algebra. These representations allow us to construct some of the Mordell-Weil lattices considered by Elkies and Shioda, as well as some interesting even unimodular lattices that do not seem to come from the theory of elliptic curves.

In §1 we discuss lattices and Hermitian forms on V, and in §§2–4 the strong irreducibility hypotheses we wish to make. In §5 we show how our hypotheses imply the existence of a finite number (up to isomorphism) of Euclidean $\mathbf{Z}[G]$-lattices L in V with $\mathrm{End}_G(L)$ a maximal order in $\mathrm{End}_G(V)$. We give some examples with $\dim V \leq 8$ in §6, and in §§7–9 discuss the invariants of L, such as the dual lattice and theta function. The rest of the paper is devoted to examples: in most, G is a finite group of Lie type and V is obtained as an irreducible summand of the Weil representation of G.

Some of the representation theoretic problems left open by this paper are: to find *all* examples of pairs (G, V) satisfying the strong irreducibility hypotheses of §§2–4, and to determine the invariants (shortest nonzero vector, theta function, Thompson series, ...) of the G-lattices L so effortlessly constructed inside V.

1. Lattices and Hermitian forms

In this section, we establish the notation that will be used throughout the paper. Let G be a finite group of order g. Elements of G will be denoted $s, t, \ldots$. Let V be a finite-dimensional rational vector space that affords a linear representation of G over $\mathbf{Q}$. We view elements of G as linear operators acting on the right of V, and so have the formula: $v^{st} = (v^s)^t$ for $v \in V$ and $s, t \in G$. Let $\chi(s) = \mathrm{Trace}_V(s)$ be the character of V.

Received by the editors April 20, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20C15, 20C20, 11H31.

Let $K = \mathrm{End}_G(V)$ be the commuting algebra of G in $\mathrm{End}(V)$, which consists of all $\mathbf{Q}$-linear transformations $\alpha: V \to V$ which satisfy $\alpha(v^s) = \alpha(v)^s$ for all $v \in V$ and $s \in G$. We view V as a left K-module. Recall that an order R in the $\mathbf{Q}$-algebra K is a subring that is free of rank $= \dim_{\mathbf{Q}}(K)$ as a $\mathbf{Z}$-module and satisfies $R \otimes \mathbf{Q} = K$. By definition, a lattice L in V is a free $\mathbf{Z}$-submodule of rank $= \dim_{\mathbf{Q}}(V)$ which satisfies $L \otimes \mathbf{Q} = V$. We say that L is an RG-lattice in V if it is stable under left multiplication by R and the right action of G.

If L_0 is any lattice in V, then

$$L = \sum_{s \in G} RL_0 s = R \cdot L_0 \cdot \mathbf{Z}[G] \tag{1.1}$$

is an RG-lattice. By an ideal $\mathfrak{a}$ of R we will always mean a two-sided, nonzero ideal; we say $\mathfrak{a}$ is maximal if there are no two-sided ideals $\mathfrak{b}$ which satisfy $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$. If L is an RG-lattice, then so is $\mathfrak{a}L = \{\alpha v : \alpha \in \mathfrak{a}, v \in L\}$.

Let $\alpha \mapsto \overline{\alpha}$ be a fixed anti-involution of the $\mathbf{Q}$-algebra K (so $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$). A K-Hermitian form φ on V is a $\mathbf{Q}$-bilinear pairing $\varphi : V \times V \to K$ which satisfies (cf. [MH, Appendix 2])

$$\begin{cases} \varphi(\alpha v, \beta w) = \alpha \varphi(v, w)\overline{\beta}, \\ \varphi(w, v) = \overline{\varphi(v, w)}. \end{cases} \tag{1.2}$$

We say φ is nondegenerate if the map $V \to \mathrm{Hom}_K(V, K)$ given by $w \mapsto f_w(v) = \varphi(v, w)$ is an isomorphism of $\mathbf{Q}$-vector spaces. We say that φ is G-invariant if $\varphi(v^s, w^s) = \varphi(v, w)$ for all $v, w \in V$ and all $s \in G$. If φ_0 is a K-Hermitian form on V, the sum

$$\varphi(v, w) = \sum_{s \in G} \varphi_0(v^s, w^s) \tag{1.3}$$

is G-invariant.

Let R be an order in K with $R = \overline{R}$, and let L be an RG-lattice in V. If φ is a nondegenerate, G-invariant Hermitian form on V, the Hermitian dual

$$L'_\varphi = \{w \in V : \varphi(L, w) \in R\} = \{v \in V : \varphi(v, L) \in R\} \tag{1.4}$$

is also an RG-lattice in V.

2. Irreducibility over R

In this section, we consider the representation of G on the real vector space $V \otimes \mathbf{R}$. Recall that a symmetric bilinear form on $V \otimes \mathbf{R}$ is a bilinear pairing $\langle\ ,\ \rangle : (V \otimes \mathbf{R}) \times (V \otimes \mathbf{R}) \to \mathbf{R}$ that satisfies $\langle v, w \rangle = \langle w, v \rangle$. This form is G-invariant if $\langle v^s, w^s \rangle = \langle v, w \rangle$ for all $s \in G$, and positive definite if $\langle v, v \rangle \geq 0$, with equality holding only for $v = 0$.

The space of G-invariant symmetric bilinear forms on V is finite dimensional over $\mathbf{R}$, and the positive-definite forms give an $\mathbf{R}_+^*$-cone in this vector space. This cone is always nonempty: if $\langle\ ,\ \rangle_0$ is any positive-definite symmetric bilinear form on V, the sum $\langle v, w \rangle = \sum_{s \in G} \langle v^s, w^s \rangle_0$ is positive definite and G-invariant.

Proposition 2.1. *The following are all equivalent.*

(1) *The representation of* G *on* $V \otimes \mathbf{R}$ *is irreducible (over* $\mathbf{R}$*).*
(2) *The* $\mathbf{R}$*-algebra* $K \otimes \mathbf{R}$ *is a division ring.*
(3) *We have* $\frac{1}{g}\sum_{s\in G}\frac{1}{2}\{\chi(s)^2 + \chi(s^2)\} = 1$.
(4) *The space of* G*-invariant symmetric bilinear forms on* $V \otimes \mathbf{R}$ *has dimension* $= 1$.
(5) *The cone of positive-definite* G*-invariant symmetric bilinear forms on* $V \otimes \mathbf{R}$ *is a principal homogeneous space for* $\mathbf{R}_+^*$.

Proof. (1) $\Rightarrow$ (2) by Schur's lemma. If $K \otimes \mathbf{R}$ is a division ring, it is isomorphic to $\mathbf{R}$, $\mathbf{C}$, or $\mathbf{H}$ by Frobenius' theorem. In the first case $\chi = \psi$ is an irreducible complex character of G, in the second $\chi = \psi + \overline{\psi}$ where ψ is irreducible and is not equal to its conjugate, in the third $\chi = 2\psi$ where ψ is irreducible and real valued. By the orthogonality relations on irreducible characters over $\mathbf{C}$, we find $\frac{1}{g}\sum_{s\in G}\chi(s)^2 = \langle \chi, \chi\rangle = 1, 2$, or 4 in the three cases. But by the criterion of Frobenius-Schur (cf. [S3, 13.2]), $\frac{1}{g}\sum_{s\in G}\chi(s^2) = 1, 0$, or -2. Hence, adding these sums and dividing by 2, we see that (2) $\Rightarrow$ (3).

The sum in (3) is the dimension of the fixed space in the representation $\mathrm{Sym}^2 V$, with character $\frac{1}{2}\{\chi(s)^2 + \chi(s^2)\}$. This is the same as the dimension of the fixed space in the dual representation $\mathrm{Sym}^2 V^*$, or equivalently, the G-invariant symmetric bilinear forms on V (or $V \otimes \mathbf{R}$). Hence (3) $\Rightarrow$ (4). Clearly (4) $\Rightarrow$ (5), as the cone of G-invariant positive-definite forms is always nonempty. Finally, if $V \otimes \mathbf{R} = W \oplus U$ is not irreducible, we have at least a two-dimensional cone of positive-definite bilinear forms on V that are G-invariant: $a\langle\ ,\ \rangle_W + b\langle\ ,\ \rangle_U$, where $a, b > 0$ and $\langle\ ,\ \rangle_W$ and $\langle\ ,\ \rangle_U$ are positive-definite G-invariant forms on W and U respectively. Hence (5) $\Rightarrow$ (1).

Corollary 2.2. *Assume that the representation of* G *on* $V \otimes \mathbf{R}$ *is irreducible. Then the* $\mathbf{Q}$*-algebra* $K = \mathrm{End}_G(V)$ *is isomorphic either to* $\mathbf{Q}$*, an imaginary quadratic field, or a definite quaternion algebra.*

Proof. These are the only $\mathbf{Q}$-algebras K with $K \otimes \mathbf{R}$ a division ring.

We henceforth assume $V \otimes \mathbf{R}$ is irreducible, so K is described by Corollary 2.2. Let $\alpha \mapsto \overline{\alpha}$ be the canonical anti-involution of K: this is the identity for $K = \mathbf{Q}$, the generator of $\mathrm{Gal}(K/\mathbf{Q})$ when K is quadratic, and induces the Galois automorphism of any quadratic subfield when K is quaternionic. In all cases, the subfield of K fixed by the anti-involution is equal to $\mathbf{Q}$, and $\alpha\overline{\alpha} \geq 0$ with equality holding only for $\alpha = 0$. We say a K-Hermitian form φ on V is positive definite if $\varphi(v, v) \geq 0$, with equality holding only for $v = 0$.

Proposition 2.3. *If* $V \otimes \mathbf{R}$ *is irreducible, the cone of positive-definite* G*-invariant* K*-Hermitian forms* $\varphi: V \times V \to K$ *is a principal homogeneous space for* $\mathbf{Q}_+^*$.

Proof. A positive-definite G-invariant form φ exists on V, by the standard averaging argument. Hence we must show that if φ and φ' are two such

forms, there is an element $\alpha \in \mathbf{Q}_+^*$ such that $\varphi' = \alpha\varphi$. Both φ and φ' give G-isomorphisms from V to $\mathrm{Hom}_K(V, K)$, so by Schur's lemma we have $\varphi(v, w) = \varphi'(v, \alpha w)$ for some $\alpha \in K^* = \mathrm{Aut}_G(V)$. Using the fact that the forms are both Hermitian, we find $\varphi'(v, \alpha w) = \varphi'(\alpha v, w)$ which implies that $\alpha \in \mathbf{Q}^*$. Hence $\varphi' = \alpha\varphi$, and we must have $\alpha > 0$ if both forms are positive definite.

If φ is a Hermitian, G-invariant, positive-definite form on V, we define

$$\langle v, w\rangle = \mathrm{Tr}_{K/\mathbf{Q}}\,\varphi(v, w) = \begin{cases} \varphi(v, w) & K = \mathbf{Q}, \\ \varphi(v, w) + \varphi(w, v) & K \neq \mathbf{Q}. \end{cases} \tag{2.4}$$

This is a positive-definite G-invariant symmetric bilinear form on V, and the map $\varphi \mapsto \langle\ ,\ \rangle$ is a bijection between the two $\mathbf{Q}_+^*$ cones of dimension one. If $\delta \in K$ satisfies $\mathrm{Tr}_{K/\mathbf{Q}}(\delta) = 0$, the form $\mathrm{Tr}_{K/\mathbf{Q}}(v, \delta w)$ is G-invariant and alternating. We obtain, in this manner, the vector space of G-invariant alternating forms on V, which has dimension $= \dim_{\mathbf{Q}}(K) - 1 = 0, 1$, or 3.

3. Irreducibility (modulo $\mathfrak{p}$)

We continue with the assumptions of the previous section, so $V \otimes \mathbf{R}$ is irreducible, and K is either $\mathbf{Q}$, imaginary quadratic, or a definite quaternion algebra. Let R be a maximal order in K, which is unique except in the quaternionic case. If $\mathfrak{p}$ is a maximal (two-sided) ideal of R, then $\mathfrak{p}$ contains pR for a unique rational prime p. In fact, either $\mathfrak{p} = pR$ or $\mathfrak{p} \cdot \bar{\mathfrak{p}} = pR$. If $\mathfrak{p}^2 = pR$ we say that $\mathfrak{p}$ is a ramified prime; the set of ramified primes is finite, and nonempty when $K \neq \mathbf{Q}$. For any maximal $\mathfrak{p}$ the quotient ring $k_{\mathfrak{p}} = R/\mathfrak{p}R$ is a simple $\mathbf{Z}/p\mathbf{Z}$-algebra, isomorphic either to $\mathbf{F}_p$, $\mathbf{F}_{p^2}$ or the ring $M_2(\mathbf{F}_p)$ of 2×2 matrices over the prime field.

Let L be an RG-lattice in V, and $\mathfrak{p}$ a maximal ideal of R. We define the reduced representation:

$$V_{\mathfrak{p}} = L/\mathfrak{p}L \quad \text{of } G \text{ over } k_{\mathfrak{p}} = R/\mathfrak{p}R. \tag{3.1}$$

This depends on the choice of lattice L, although it does not appear in our notation. We say $V_{\mathfrak{p}}$ is irreducible over $k_{\mathfrak{p}}$ if there are no nontrivial $k_{\mathfrak{p}}$-submodules that are stable under the right action of G.

Proposition 3.2. *The following are equivalent.*

(1) *For all maximal ideals $\mathfrak{p}$ of R the representation $V_{\mathfrak{p}}$ of G is irreducible over $k_{\mathfrak{p}} = R/\mathfrak{p}R$.*

(2) *Every RG-lattice in V has the form $\mathfrak{a}L$, where $\mathfrak{a}$ is a fractional ideal of R.*

Proof. Let $W_{\mathfrak{p}}$ be a nontrivial $k_{\mathfrak{p}}G$-submodule of $V_{\mathfrak{p}}$. Then $M = \{v \in L : v(\mathrm{mod}\,\mathfrak{p}L)$ is in $W_{\mathfrak{p}}\}$ is an RG-lattice in V with $\mathfrak{p}L \subsetneq M \subsetneq L$. Hence M is not of the form $\mathfrak{a}L$, and (2) $\Rightarrow$ (1).

Now assume $V_{\mathfrak{p}}$ is irreducible for all $\mathfrak{p}$, and let M be an RG-lattice in V. Define $L_p = L \otimes \mathbf{Z}_p$, $R_p = R \otimes \mathbf{Z}_p$, $K_p = K \otimes \mathbf{Q}_p$, and $V_p = V \otimes \mathbf{Q}_p$. We will show that any R_pG lattice $M_p = M \otimes \mathbf{Z}_p$ in V_p has the form $M_p = \alpha_p L_p$ with α_p an element of K_p^* which normalizes R_p. The global result follows from this, taking $\mathfrak{a}$ to be the fractional ideal $K \cap \prod_p \alpha_p R_p$, so $M = \mathfrak{a}L$.

First assume K_p is a division ring, so R_p is a local ring with maximal ideal $\mathfrak{p} = \pi R_p$. If M_p is an R_pG lattice we may assume, after scaling by a power of π, that M_p is contained in L_p but not in πL_p. Hence the image of M_p in $V_{\mathfrak{p}} = L_p/\pi L_p$ is nonzero. By the hypothesis that $V_{\mathfrak{p}}$ is irreducible, the image must be equal to $L_p/\pi L_p$, so $M_p + \pi L_p = L_p$. Nakayama's lemma (applied to L_p/M_p) shows that $M_p = L_p$. Hence any R_pG-lattice M_p has the form $\pi^n L_p$ for some $n \in \mathbf{Z}$.

Next assume that $K_p = \mathbf{Q}_p \times \mathbf{Q}_p$, so $pR = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p} \neq \bar{\mathfrak{p}}$. Then $V_p = W_{\mathfrak{p}} \oplus W_{\bar{\mathfrak{p}}}$ is the sum of nonisomorphic irreducible representations of G over $\mathbf{Q}_p$, with $W_{\bar{\mathfrak{p}}} \simeq \mathrm{Hom}(W_{\mathfrak{p}}, \mathbf{Q}_p)$. We have a decomposition $L_p = N_{\mathfrak{p}} \oplus N_{\bar{\mathfrak{p}}}$, where $N_{\mathfrak{p}}$ and $N_{\bar{\mathfrak{p}}}$ are $\mathbf{Z}_pG$-lattices in $W_{\mathfrak{p}}$ and $W_{\bar{\mathfrak{p}}}$. The irreducibility of $V_{\mathfrak{p}} \simeq N_{\mathfrak{p}}/pN_{\mathfrak{p}}$ and $V_{\bar{\mathfrak{p}}} \simeq N_{\bar{\mathfrak{p}}}/pN_{\bar{\mathfrak{p}}}$ implies, by the argument above, that any R_pG-lattice M_p in V_p has the form $p^a N_{\mathfrak{p}} \oplus p^b N_{\bar{\mathfrak{p}}} = \alpha_p L_p$ with $\alpha_p = (p^a, p^b)$ in K_p^*.

Finally, assume $K \otimes \mathbf{Q}_p$ is isomorphic to $M_2(\mathbf{Q}_p)$; we fix an isomorphism taking R_p to the standard maximal order $M_2(\mathbf{Z}_p)$ (this is possible, as all maximal orders are locally conjugate). The isomorphism $K_p \simeq M_2(\mathbf{Q}_p)$ gives a decomposition $V_p = W_p \oplus W_p$, where W_p is irreducible over $\mathbf{Q}_p$, and $L_p = N_p \oplus N_p$ with N_p a $\mathbf{Z}_pG$-lattice in W_p. The irreducibility of $V_{\mathfrak{p}} = N_p/pN_p \oplus N_p/pN_p$ over $k_{\mathfrak{p}} = M_2(\mathbf{F}_p)$ implies that N_p/pN_p is an irreducible G-module over $\mathbf{F}_p$. Hence, by the above, any $\mathbf{Z}_pG$ stable lattice in W_p has the form $p^a N_p$, and any R_pG stable lattice in V_p has the form $p^a N_p \oplus p^a N_p = p^a L_p$.

4. Global irreducibility and characters

We henceforth only consider rational representations V of G that satisfy the conditions in Propositions 2.1 and 3.2; such representations will be called "globally irreducible."

An interesting problem is to determine all globally irreducible rational representations V of a finite group G. Of course, any one-dimensional representation over $\mathbf{Q}$ is globally irreducible, but there may be others. In this section, we suppose that we are given the table of all irreducible complex characters ψ of G, as well as the table of its irreducible modular characters ρ over an algebraically closed field of characteristic p, for all rational primes p. We wish to find some simple conditions that imply the existence of a globally irreducible rational representation V for G.

Lemma 4.1. *Let ψ be an irreducible complex character of G, and let $\mathfrak{p}$ be a finite place of the number field $\mathbf{Q}(\psi)$. If the reduction of $\psi(\mathrm{mod}\,\mathfrak{p})$ is an absolutely irreducible Brauer character ρ of G, then a representation W of G with character ψ can be defined over the completion $\mathbf{Q}(\psi)_{\mathfrak{p}}$.*

Proof. The obstruction to defining W is the Schur index $e_{\mathfrak{p}}(\psi)$. Let ρ be any absolutely irreducible Brauer character of G and $\mathbf{F}_\rho$ the finite field generated by its values over $\mathbf{F}_p$. Then $e_{\mathfrak{p}}(\psi)$ divides the product $\deg(\mathbf{F}_\rho \cdot \mathbf{F}_{\mathfrak{p}} : \mathbf{F}_{\mathfrak{p}}) \cdot \mathrm{mult}_\rho(\psi)$ [F2, Theorem IV.9.3]. If $\psi \equiv \rho$ is irreducible, this product is $= 1$, so $e_{\mathfrak{p}}(\psi) = 1$.

Proposition 4.2. *Let ψ be an irreducible complex character of G. (1) Assume $\mathbf{Q}(\psi) = \mathbf{Q}$ and $\psi \equiv \rho \pmod{p}$ is an absolutely irreducible Brauer character of G for all rational primes p. Then $\chi = \psi$ is the character of a globally irreducible rational representation V of G.*

(2) Assume $\mathbf{Q}(\psi)$ is an imaginary quadratic field, and $\psi \equiv \rho \pmod{\mathfrak{p}}$ is an absolutely irreducible Brauer character of G for all primes $\mathfrak{p}$ of $\mathbf{Q}(\psi)$. Then $\chi = \psi + \overline{\psi}$ is the character of a globally irreducible rational representation V of G.

(3) Assume $\mathbf{Q}(\psi) = \mathbf{Q}$, that $\frac{1}{g}\sum_{s \in G} \psi(s^2) = -1$, and that, for all rational primes p, either $\psi \equiv \rho \pmod{p}$ is either absolutely irreducible, or $\psi \equiv \rho + \rho^p \pmod{p}$ where ρ is an absolutely irreducible Brauer character with $\mathbf{F}_\rho = \mathbf{F}_{p^2}$. Then $\chi = 2\psi$ is the character of a globally irreducible rational representation V of G.

Proof. (1) By Lemma 4.1 we have $e_p(\psi) = 1$ for all finite p. Hence $e(\psi) = 1$, as the obstruction would be a quaternion algebra split at all finite primes, and therefore globally split. Hence $\chi = \psi$ is the character of a rational representation V. It is clearly globally irreducible with $\mathrm{End}_G(V) = \mathbf{Q}$.

(2) The same argument shows that ψ is the character of a representation W of G over $\mathbf{Q}(\psi) = K$. Viewing W as a rational representation V of G with $\mathrm{End}_G(V) = K$, it is clear that V is globally irreducible.

(3) The condition $\frac{1}{g}\sum \psi(s^2) = -1$ implies that $e_\infty(\psi) = 2$ [Se, Proposition 39]. But when $\mathbf{Q}(\psi) = \mathbf{Q}$ we have $e(\psi) = 1$ or 2 by the Brauer-Speiser theorem (cf. [F1, §2]), so $e(\psi) = 2$ and $\chi = 2\psi$ is the character of a rational representation V of G with $\mathrm{End}_G(V) = K$ a definite quaternion algebra. V is clearly globally irreducible.

Note 4.3. In case (3), the primes $\mathfrak{p}$ which ramify in K (where $e_{\mathfrak{p}}(\psi) = 2$) are among those where the reduction $\psi \equiv \rho + \rho^p \pmod{p}$ is not absolutely irreducible. Indeed, if $\mathfrak{p}^2 = pR$, the character of $V_{\mathfrak{p}}$ over $k_{\mathfrak{p}}$ is equal to ρ (after choosing a suitable identification of $k_{\mathfrak{p}}$ with $\mathbf{F}_{p^2}$).

Note 4.4. The absolute irreducibility of $\psi \pmod{\mathfrak{p}}$ is automatic if the residue characteristic p does not divide the order of G. So there are only finitely many conditions to check in Proposition 4.2.

5. Hermitian lattices

Let V be a globally irreducible representation of G, and let R be a maximal order in $K = \mathrm{End}_G(V)$. Let L be an RG-lattice in V, and let φ be a positive

definite G-invariant Hermitian form on V. Since $\varphi(v, v) > 0$ for $v \neq 0$, the form φ is nondegenerate and we may define the dual

$$L'_\varphi = \{v \in V : \varphi(v, L) \in R\}. \tag{5.1}$$

Then L'_φ is an RG-lattice, so by Proposition 3.2 $L'_\varphi = \mathfrak{a}L$ for a fractional ideal $\mathfrak{a}$ of R which depends on φ. We now show that φ may be chosen so that $\mathfrak{a}$ is the product of certain ramified primes $\mathfrak{p}$ in R.

Proposition 5.2. *Let L be an RG-lattice in V. Then there is a G-invariant, positive definite Hermitian form φ on V such that*

$$L'_\varphi = \left(\prod_{\mathfrak{p} \in S} \mathfrak{p}\right) \cdot L,$$

where S is a subset of the ramified primes in R. The subset S is determined uniquely by the representation V, and the form φ is determined uniquely by the RG-lattice L.

Proof. Let φ_0 be any G-invariant positive-definite Hermitian form on V. Then $L'_{\varphi_0} = \mathfrak{a}L$ with $\mathfrak{a}$ a fractional ideal; since φ_0 is Hermitian: $\mathfrak{a} = \bar{\mathfrak{a}}$. Hence $\mathfrak{a} = \prod_{\mathfrak{p} \in S} \mathfrak{p} \cdot \alpha \cdot R$, with S a subset of the ramified primes and $\alpha \in \mathbf{Q}_+^*$. If $\varphi = \alpha\varphi_0$ we have $L'_\varphi = \prod_S \mathfrak{p} \cdot L$ as claimed. Clearly φ is uniquely determined by L, as the set S and the rational number $\alpha > 0$ are uniquely determined by $\mathfrak{a}$.

If $M = \mathfrak{b}L$ is another RG-lattice in V, and $\varphi_m = \mathbf{N}\mathfrak{b}^{-1} \cdot \varphi$ with $\mathbf{N}\mathfrak{b}$ the positive generator of $\mathfrak{b} \cdot \bar{\mathfrak{b}}$, we find $M'_{\varphi_M} = \prod_S \mathfrak{p} \cdot M$. Hence the set S depends only on V.

Note 5.3. In fact, the set S in Proposition 5.2 depends only on the local representations $V \otimes \mathbf{Q}_p$ at primes p which ramify in R : $pR = \mathfrak{p}^2$. In §7 we will show how the question of whether $\mathfrak{p}$ is in S can often be answered by a consideration of the reduced representation $V_\mathfrak{p}$ over $k_\mathfrak{p}$.

If L is any RG lattice in V, we give it a Hermitian structure using the form φ uniquely defined by Proposition 5.2 and a Euclidean structure using the bilinear form $\langle v, w \rangle = \mathrm{Tr}_{K/\mathbf{Q}} \varphi(v, w)$.

Let $Cl(R)$ be the two-sided class group of R: this is the quotient of the group of two-sided fractional ideals of R by the subgroup of two-sided principal ideals αR, with $\alpha \in K^*$ normalizing R. The group $Cl(R)$ is finite in all cases; when $K = \mathbf{Q}$ it is trivial and when K is quaternionic it is an elementary abelian two-group [V, Chapter III, §5].

Proposition 5.4. *The group $Cl(R)$ acts simply transitively on the set of isomorphism classes of Euclidean $\mathbf{Z}[G]$-lattices L in V with $\mathrm{End}_G(L) = R$.*

Proof. We define a simply transitive action of the group of fractional ideals on the set of RG-lattices, by $L \mapsto \mathfrak{a}L$. The lattices L and $\mathfrak{a}L$ are isomorphic

$\mathbf{Z}[G]$-modules if and only if $\mathfrak{a} = \alpha R$ with $\alpha \in K^*$, by Schur's lemma. Hence $Cl(R)$ acts simply transitively on the isomorphism classes of $\mathbf{Z}[G]$-modules with $\mathrm{End}_G(L) = R$. Since the map from L to αL taking v to αv preserves the normalized inner product, we have classified the Euclidean $\mathbf{Z}[G]$-lattices in V with $\mathrm{End}_G(L) = R$.

There may be some identification of the Euclidean lattices L so constructed in V if one chooses to ignore the action of G. For example,

Lemma 5.5. *Let $K = \mathrm{End}_G(V)$ be imaginary quadratic, and assume that there is an involution τ of V which acts K-antilinearly and normalizes G. Then there is an RG-lattice in V with $\tau(L) = L$. If $\mathfrak{a}$ is an ideal of K we have $\tau(\mathfrak{a}L) = \bar{\mathfrak{a}}L$ and the map $v \mapsto \tau(v)$ gives an isometry between the Euclidean lattices $\mathfrak{a}L$ and $\bar{\mathfrak{a}}L$.*

Proof. Let M be an RG-lattice. Then τM is also an RG-lattice, so $\tau M = \mathfrak{b}M$ for an ideal $\mathfrak{b}$ of K. Since $\tau^2 = 1$ and τ is antilinear, $\mathfrak{b}\cdot\bar{\mathfrak{b}} = R$. Hence $\mathfrak{b} = \mathfrak{c}/\bar{\mathfrak{c}}$ and the lattice $L = \mathfrak{c}M$ is fixed by τ. Clearly $\tau(\mathfrak{a}L) = \bar{\mathfrak{a}}L$, as τ is K-antilinear. Since the bilinear forms on $\mathfrak{a}L$ and $\bar{\mathfrak{a}}L$ are both equal to $\mathbf{N}\mathfrak{a}^{-1}\cdot\langle\ ,\ \rangle_L$, we must show that $\langle v, w\rangle = \langle \tau v, \tau w\rangle$.

The group $G' = G \rtimes \langle\tau\rangle$ acts on V with $\mathrm{End}_{G'}(V) = \mathbf{Q}$. Hence G' stabilizes a one-dimensional space of symmetric bilinear forms, which is exactly the space stabilized by the subgroup G. Hence τ is an isometry of $\langle\ ,\ \rangle_L$.

6. Examples in low dimension

We now give some simple examples of globally irreducible faithful representations V of finite groups G. In each case the class group of R is trivial (and all maximal orders are conjugate in K) so we obtain a unique $\mathbf{Z}[G]$ lattice L in V with $\mathrm{End}_G(L) = R$.

The simplest examples are obtained by taking $V = K$ and G a subgroup of R^* which does not lie in a proper $\mathbf{Q}$-subspace of K. Unfortunately, this puts a severe restriction on the field K; the only possibilities are $K = \mathbf{Q}, \mathbf{Q}(\mu_4), \mathbf{Q}(\mu_6)$ and the definite quaternion algebras ramified at $\{2, \infty\}$ and $\{3, \infty\}$. When $K = \mathbf{Q}$ the group G has order 1 or 2 and L is the A_1-root lattice. When $K = \mathbf{Q}(\mu_4)$ the group G is cyclic of order 4 and L is the $A_1 \times A_1$-root lattice. When $K = \mathbf{Q}(\mu_6)$ the group G is cyclic of order 3 or 6 and L is the A_2-root lattice. When K is the quaternion algebra ramified at $\{2, \infty\}$ we have $R^* \simeq \mathrm{SL}_2(3)$ of order 24, which contains the quaternion group of order 8 as a normal subgroup. Both act globally irreducibly on K, and the stable lattice is the D_4-root lattice of Hurwitz quaternions. When K is the quaternion algebra ramified at $\{3, \infty\}$ we have $G = R^* = \tilde{S}_3$ of order 12. The stable lattice L is the $A_2 \times A_2$-root lattice.

Examples where $\dim_K V > 1$ are harder to find. For example, when $K = \mathbf{Q}$ we will see that any such V has $\dim V \equiv 0 \pmod 8$ (Proposition 7.4). The simplest example in this case is to take $G =$ the Weyl group of E_8, of order

$696729600 = 2^{14}3^5 5^2 7$ and V its eight-dimensional reflection representation! The stable lattice L is the E_8-root lattice.

When $K = \mathbf{Q}(\sqrt{-2})$ there is an example with $\dim_K V = 2$. Let $G = \mathrm{GL}_2(3) = \tilde{S}_4$, which has order $48 = 2^4 \cdot 3$. Let ψ be the character of a discrete series representation of $\mathrm{GL}_2(3)$, corresponding to a character of order 8 of the nonsplit torus, that satisfies $\mathbf{Q}(\psi) = K$. This has degree 2; its reduction $(\mathrm{mod}\sqrt{-2})$ is the irreducible representation ρ of degree 2 of S_4, and its reduction modulo the two primes dividing 3 is the standard two-dimensional representation of $\mathrm{GL}_2(3)$ and its dual. Hence $\chi = \psi + \overline{\psi}$ is the character of a globally irreducible V of dimension four by Proposition 4.2. The Hermitian form φ has matrix

$$\varphi = \begin{pmatrix} 2 & \alpha \\ \overline{\alpha} & 2 \end{pmatrix} \quad \text{with } \alpha = 1 + \sqrt{-2} \tag{6.1}$$

with respect to a suitable R-basis of $L = L'$. The corresponding Euclidean lattice is (a scaling of) the D_4-lattice. This Hermitian lattice arises from the theta polarization of the Jacobian of the complex curve X of genus 2 with equation $y^2 = x^5 - x$; we have $\mathrm{Aut}_{\mathbf{C}}(X) = G$.

When $K = \mathbf{Q}(\sqrt{-7})$ there is an example with $\dim_K V = 3$. Let $G = \mathrm{PSL}_2(7) = \mathrm{SL}_3(2)$, which has order $168 = 2^3 \cdot 3 \cdot 7$. Let ψ be the character of a $\frac{1}{2}$-discrete series representation of $\mathrm{PSL}_2(7)$, corresponding to the quadratic character of the nonsplit torus, which satisfies $\mathbf{Q}(\psi) = K$. This has degree 3 and its reduction is absolutely irreducible at all primes. Indeed, if $\rho \neq 1$ is an irreducible Brauer character of G then $\dim \rho \geq 3$. At the two primes dividing 2 one obtains the standard three-dimensional representation of $\mathrm{SL}_3(2)$ and its dual; $(\mathrm{mod}\sqrt{-7})$ one obtains the adjoint representation of $\mathrm{PSL}_2(7)$. Hence $\chi = \psi + \overline{\psi}$ is the character of a globally irreducible representation V of dimension six by Proposition 4.2. The Hermitian form φ has the matrix

$$\varphi = \begin{pmatrix} 2 & \alpha & \overline{\alpha} \\ \overline{\alpha} & 2 & -1 \\ \alpha & -1 & 2 \end{pmatrix} \quad \text{with } \alpha = \frac{1 + \sqrt{-7}}{2} \tag{6.2}$$

with respect to a suitable R-basis of $L = L'$. This Hermitian lattice has 42 short vectors with $\varphi(v, v) = 2$, and arises from the theta polarization of the Jacobian of the complex curve X of genus 3 with equation $xy^3 + yz^3 + zx^3 = 0$. We have $\mathrm{Aut}_{\mathbf{C}}(X) = G$; for a more detailed description of L due to Serre, see [Ma, pp. 235–236].

7. Ramified primes

To make Proposition 5.2 more precise, we wish to determine the subset S of ramified primes which occurs. Let $\mathfrak{p}$ be a ramified prime in R. The residue field $R/\mathfrak{p} = k_{\mathfrak{p}}$ is isomorphic to $\mathbf{F}_p$ or $\mathbf{F}_{p^2}$, and the canonical anti-involution of R gives an involution of $k_{\mathfrak{p}}$ (which is trivial when $k_{\mathfrak{p}} = \mathbf{F}_p$ and $x \mapsto x^p$ when $k = \mathbf{F}_{p^2}$).

Proposition 7.1. (1) *If* $\mathfrak{p}$ *is not in* S, *there is a nondegenerate* G*-invariant* $k_{\mathfrak{p}}$*-Hermitian form* $\varphi_{\mathfrak{p}}: V_{\mathfrak{p}} \times V_{\mathfrak{p}} \to k_{\mathfrak{p}}$.

(2) *If* $\mathfrak{p}$ *is in* S, *there is a nondegenerate* G*-invariant, strictly alternating,* $k_{\mathfrak{p}}$*-bilinear form* $\varphi_{\mathfrak{p}}: V_{\mathfrak{p}} \times V_{\mathfrak{p}} \to k_{\mathfrak{p}}$.

Proof. (1) In this case, the Hermitian for φ on V gives a nondegenerate pairing of $R_p = R \otimes \mathbf{Z}_p$-modules $L_p \times L_p \to R_p$, with $L_p = L \otimes \mathbf{Z}_p$. Its reduction (modulo $\mathfrak{p}R_p$) is the $k_{\mathfrak{p}}$-Hermitian form $\varphi_{\mathfrak{p}}$.

(2) In this case, let π be a uniformizing parameter in R_p, so $\pi R_p = \mathfrak{p}R_p$. Then the form $\varphi': L_p \times L_p \to R_p$ defined by $\varphi'(v, w) = \varphi(v, w) \cdot \pi$ is $\mathbf{Z}_p$-bilinear and nondegenerate; its reduction is the form $\varphi_{\mathfrak{p}}$. Clearly $\varphi_{\mathfrak{p}}$ is $k_{\mathfrak{p}}$-linear in the first argument, so it suffices to show that $\varphi_{\mathfrak{p}}(v, v) = 0$, or equivalently, that $\varphi(v, v)\pi$ lies in $\mathfrak{p}R_p$. But $\varphi(v, v)\pi$ lies in the intersection of $\mathbf{Q}_p\pi$ with R_p, which is equal to $\mathbf{Z}_p\pi \subset \mathfrak{p}R_p$.

We can make a simple hypothesis on $V_{\mathfrak{p}}$ which assures that the situations (1) and (2) of Proposition 7.1 cannot occur simultaneously.

Corollary 7.2. *Assume that* $\mathrm{End}_{\mathbf{F}_p[G]}(V_{\mathfrak{p}}) = k_{\mathfrak{p}}$ *and that the residue field* $k_{\mathfrak{p}}$ *has more than two elements. Then* $\mathfrak{p}$ *is in* S *if and only if* $V_{\mathfrak{p}}$ *is a symplectic representation of* G *over* $k_{\mathfrak{p}}$.

Proof. If $k_{\mathfrak{p}} = \mathbf{F}_{p^2}$ our hypothesis implies that $V_{\mathfrak{p}}$ is not isomorphic to its conjugate representation $V_{\mathfrak{p}}^{p}$. Hence $V_{\mathfrak{p}}$ either has a nondegenerate Hermitian form or a nondegenerate symplectic form, but not both. For one identifies the dual $\mathrm{Hom}_G(V_{\mathfrak{p}}, k_{\mathfrak{p}})$ with $V_{\mathfrak{p}}^{p}$, and the other identifies the dual with $V_{\mathfrak{p}}$.

If $k_{\mathfrak{p}} = \mathbf{F}_p$, our hypothesis implies that the space of bilinear forms on V has dimension $= 1 = \dim \mathrm{Hom}_G(V_{\mathfrak{p}}, V_{\mathfrak{p}})$. If $p > 2$, we cannot have both nondegenerate symmetric *and* alternating forms on $V_{\mathfrak{p}}$.

Note 7.3. When $k_{\mathfrak{p}} = \mathbf{F}_2$, the symmetric form $\varphi_{\mathfrak{p}}$ on $V_{\mathfrak{p}}$ constructed in (1) is strictly alternating once $\dim V_{\mathfrak{p}} > 1$. For $l(v) = \varphi_{\mathfrak{p}}(v, v)$ gives a G-invariant *linear* form on $V_{\mathfrak{p}}$.

We end this section with some elementary remarks on the dimension of V over $\mathbf{Q}$. If V has dimension one then $K = \mathbf{Q}$ and L is isomorphic to $\mathbf{Z}$.

Proposition 7.4 [Th2; S3, Example 15.4]. (1) *If* $K = \mathbf{Q}$ *and* $\dim V > 1$ *then any* $\mathbf{Z}[G]$*-lattice* L *in* V *is even and unimodular. Hence* $\dim V \equiv 0 \pmod 8$.

(2) *If* K *is quadratic, then* $\dim V \equiv 0 \pmod 2$. *If* $\dim V \equiv 2 \pmod 4$, *then* S *is empty and* $L'_{\varphi} = L$. *If* 2 *is ramified in* K *and* $\dim V > 2$, *then* $\dim V \equiv 0 \pmod 4$.

(3) *If* K *is quaternionic, then* $\dim V \equiv 0 \pmod 4$. *If* $\dim V \equiv 4 \pmod 8$, *then* S *is empty and* $L'_{\varphi} = L$.

Proof. (1) Since $R = \mathbf{Z}$ is unramified, $L' = L$ is unimodular. The map $v \mapsto \varphi(v, v) \pmod 2$ gives a G-invariant linear form on $L/2L$. By our irreducibility hypothesis, this must be zero when $\dim V > 1$, so L is even.

The fact that $\operatorname{rank} L \equiv 0 \pmod 8$ for even unimodular L is well known [S2, Chapter V, §2; MH, Theorem 5.1].

(2) Clearly $\dim V$ is divisible by $\dim K = 2$. If $\dim_K V$ is odd, then $\dim V_{\mathfrak{p}}$ is odd for all ramified $\mathfrak{p}$. Hence $V_{\mathfrak{p}}$ is not symplectic, and $\mathfrak{p} \notin S$ by Proposition 7.2 (2). (The same argument proves (3).) If 2 is ramified in K and $\dim V > 2$, the form $\varphi_{\mathfrak{p}}$ is strictly alternating in all cases, so $\dim V \equiv 0 \pmod 4$.

Corollary 7.5. *If* $\dim V \equiv 1 \pmod 2$ *then* $K = \mathbf{Q}$ *and* $\dim V = 1$. *If* $\dim V \equiv 2 \pmod 4$ *then* $K = \mathbf{Q}(i)$ *and* $\dim V = 2$, *or* $K = \mathbf{Q}(\sqrt{-N})$ *is imaginary quadratic with odd discriminant* $N \equiv 3 \pmod 4$.

8. The dual lattice

We henceforth assume $\dim V > 1$, to exclude trivial cases. Let $\langle\ ,\ \rangle = \operatorname{Tr}\varphi$ be the canonical positive-definite bilinear form on an RG-lattice L in V. We define the (Euclidean) dual lattice by

$$L^* = \{v \in V : \langle v, L\rangle \in \mathbf{Z}\}. \tag{8.1}$$

This is equal to L' when $R = \mathbf{Z}$, but is a larger RG-lattice in V when R has ramified primes.

Recall that the inverse different $\mathscr{D}^{-1}$ of R is the largest fractional ideal on which the trace takes integral values:

$$\mathscr{D}^{-1} = \{\alpha \in K : \operatorname{Tr}(\alpha R) \in \mathbf{Z}\}. \tag{8.2}$$

The integral ideal $\mathscr{D}$ is divisible precisely by the ramified primes $\mathfrak{p}$ of R; we have $\operatorname{ord}_{\mathfrak{p}}(\mathscr{D}) = 1$ except when K is imaginary quadratic and $\mathfrak{p}^2 = 2R$, when $\operatorname{ord}_{\mathfrak{p}}(\mathscr{D}) = 2$ or 3. We say R is tamely ramified when $\mathscr{D}$ is squarefree.

Proposition 8.3. *We have* $L^* = \mathscr{D}^{-1}L'$. *The form* $\langle\ ,\ \rangle$ *is integral and even on* L.

Proof. Since L is an R-module, we have $\operatorname{Tr}\varphi(v, L) \in \mathbf{Z}$ if and only if $\varphi(v, L) \in \mathscr{D}^{-1}$. Hence $L^* = \mathscr{D}^{-1}L'$.

By Proposition 5.2 we have $L' = (\prod_S \mathfrak{p})L$, hence $L^* = (\mathscr{D}/\prod_S \mathfrak{p})^{-1}L$. Since the ideal $\mathscr{D}/\prod_S \mathfrak{p}$ is integral, L^* contains L and $\langle\ ,\ \rangle$ is integral on L.

To show $\langle\ ,\ \rangle$ is even, we must show that $\langle v, v\rangle \in 2\mathbf{Z}$ for all $v \in L$. If $K = \mathbf{Q}$ this was proved in Proposition 7.4 (1) (under the assumption that $\dim V > 1$). If $K \neq \mathbf{Q}$ we have $\langle v, v\rangle = 2\varphi(v, v)$, so we must show $\varphi(v, v) \in \mathbf{Z}$. Since $\mathbf{Z} = \mathbf{Q} \cap \prod \mathbf{Z}_p$, it suffices to show that $\varphi(v, v) \in \mathbf{Z}_p$ for all primes p. This is clear when p does not ramify in R, as φ on L_p takes values in R_p. If p is ramified, let π be a uniformizing parameter in R_p. Then $\pi\varphi$ on L_p takes values in R_p. Hence $\varphi(v, v)$ lies in $\pi^{-1}R_p \cap \mathbf{Q}_p = \mathbf{Z}_p$.

If $L = \bigoplus_{i=1}^n \mathbf{Z}e_i$, we define the positive integer

$$\det L = \det(\langle e_i, e_j\rangle). \tag{8.4}$$

This is independent of the basis chosen, and we have $\det L = (L^* : L)$. If $\det L = 1$, or equivalently, $L^* = L$, we say L is unimodular.

Note 8.5. Let A be a finite abelian group L^*/L. Then $\langle\ ,\ \rangle$ takes rational values on L^*, and induces a pairing $A \times A \to \mathbf{Q}/\mathbf{Z}$ which identifies A with its Pontryagin dual. The unimodular M with $L \subseteq M \subseteq L^*$ correspond bijectively to subgroups B of A which are their own annihilators ($B = B^{\perp}$) under this pairing.

Proposition 8.6. *If R is tamely ramified, we have an isomorphism of finite $R[G]$-modules:*

$$L^*/L \simeq \bigoplus_{\mathfrak{p} \notin S} V_{\mathfrak{p}}.$$

The pairing $\langle\ ,\ \rangle$ on L^*/L is the sum of the symmetric bilinear forms $\langle\ ,\ \rangle_{\mathfrak{p}} = \operatorname{Tr} \varphi_{\mathfrak{p}}$ on $V_{\mathfrak{p}}$ defined in Proposition 7.1 (1).

Proof. The hypothesis of tame ramification implies that $L^* = (\mathscr{D}/\prod_{\mathfrak{p} \in S} \mathfrak{p})^{-1} L = (\prod_{\mathfrak{p} \in S} \mathfrak{p})^{-1} L$, so $L^*/L \simeq \bigoplus_{\mathfrak{p} \notin S} \mathfrak{p}^{-1} L/L \simeq \bigoplus_{\mathfrak{p} \notin S} V_{\mathfrak{p}}$. The identification of the bilinear forms follows from the fact that $\varphi_{\mathfrak{p}}$ is the reduction of φ.

9. Theta series

In this section, we assume R is tamely ramified, for simplicity. Let $\mathfrak{n}$ be the integral ideal $\prod_{\mathfrak{p} \notin S} \mathfrak{p}$ of R, and let N be the positive integral generator of the ideal $\mathfrak{n} \cdot \bar{\mathfrak{n}}$.

We have seen in §7 that the assumption $\dim V > 1$ implies $\dim V \equiv 0 \pmod 2$. Write $\dim V = 2k$. If k is even, let ε be the trivial character of the group $(\mathbf{Z}/N\mathbf{Z})^*$. If k is odd, then by Proposition 7.1 (2),we have K imaginary quadratic of discriminant $= -N$. Let ε be the quadratic character of $(\mathbf{Z}/N\mathbf{Z})^*$ associated to the extension K: $\varepsilon(l) = +1$ iff the prime l splits in K.

If L is an RG-lattice in V, we define its theta series by

$$\theta_L = \sum_{v \in L} e^{\pi i \langle v, v \rangle \tau} = \sum_{n \geq 0} \operatorname{Card}(L_{2n}) q^n, \tag{9.1}$$

where τ is in the upper half-plane, $q = e^{2\pi i \tau}$, and $L_{2n} = \{v \in L : \langle v, v \rangle = 2n\}$. This series is easily shown to be convergent, and defines a holomorphic function in τ.

Proposition 9.2. *The function $\theta_L(\tau)$ is a holomorphic modular form of weight k and character ε for the group $\Gamma_0(N)$.*

If w_N is the Fricke involution which normalizes $\Gamma_0(N)$, we have the formula: $\theta_L | w_N = (-i)^k \theta_{\mathfrak{n}L}$.

Proof. This follows from the results in §8 and the formulae in [Sch]. We omit the details.

We note that the level, weight, and character of θ_L depend only on the representation V of G, and not on the RG-lattice L chosen. Hence the sum

$$\theta = \sum_L \frac{1}{w_L} \cdot \theta_L \tag{9.3}$$

over the $\mathbf{Z}[G]$-lattices L (up to isomorphism) in V, with $\mathrm{End}_G L$ a maximal order in K and $w_L = \mathrm{Card}(\mathrm{Aut}_G L)$, is a modular form of the same type.

More generally, for $n \geq 0$ let $\gamma_{2n}(L)$ denote the permutation representation of G on the finite set L_{2n}. Then the Thompson series

$$\begin{cases} \Gamma_L = \sum_{n \geq 0} \gamma_{2n}(L) \cdot q^n, \\ \Gamma = \sum_L \frac{1}{w_L} \cdot \Gamma_L = \sum_{n \geq 0} \gamma_{2n} \cdot q^n, \end{cases} \tag{9.4}$$

with coefficients in the rational representation ring of G, are interesting invariants of L and V respectively. We note that $w_L = \mathrm{Card}(R^*) = w_R$, where $\mathrm{End}_G L = R$. Hence

$$\gamma_0 = \sum_R h_R / w_R, \tag{9.5}$$

where the sum is taken over the conjugacy classes of maximal orders R in K and $h_R = \mathrm{Card}(Cl(R))$. In particular, γ_0 is a multiple of the trivial representation that depends only on the field $K = \mathrm{End}_G(V)$. The higher coefficients γ_{2n} are much more difficult to determine. An interesting invariant of V is the minimal value of $n > 0$ such that $\gamma_{2n} \neq 0$.

10. Examples when $K = \mathbf{Q}$ (cf. [Th1, Th2])

Unfortunately, this section is rather short. We have seen that if V is a globally irreducible representation of G with $\dim V > 1$ and $K = \mathrm{End}_G(V) = \mathbf{Q}$, then $\dim V \equiv 0 \pmod 8$ as L is even and unimodular. There are only three examples known where L is indecomposable! They are listed in the following table, using the notation of the ATLAS [C]; in each case the representation V of G is uniquely determined by its dimension.

(10.1)

G	$\dim V$
$W(E_8) = 2.O_8^+(2).2$	8
$.0 = 2.Co_1$	24
$2.Th$	248

The stable lattices are the E_8-root lattice, the Leech lattice, and the Thompson-Smith lattice, respectively.

11. Examples when $K = \mathbf{Q}(\sqrt{-p})$ and $G = \mathrm{PSL}_2(p)$

In this section, p is a prime with $p \equiv 3 \pmod 4$ and K is the imaginary quadratic field $\mathbf{Q}(\pi)$ with $\pi^2 = -p$. The unique maximal order R is the ring $\mathbf{Z} \oplus \mathbf{Z}((1+\pi)/2)$ and the unique ramified ideal is $\mathfrak{p} = \pi R$. The class group $CL(R)$ has *odd* order h; in the quadratic case $Cl(R)/2Cl(R)$ has order 2^{t-1} where t is the number of ramified primes in K. For each globally irreducible V with $\mathrm{End}_G(V) = K$ we obtain exactly h $\mathbf{Z}[G]$-Euclidean lattices (or $R[G]$-Hermitian lattices) L up to isomorphism in V.

In general, the lattices L constructed form a principal homogeneous space for the class group $Cl(R)$, but when a larger group acts on V we can often fix a basepoint and index the lattices naturally by ideal classes. For example, if $G' = G \rtimes \langle \tau \rangle$ acts on V as in Lemma 5.5, there is a *unique* isomorphism class L stable under τ, as if $\mathfrak{a}$ is an ideal with nontrivial class, then $\mathfrak{a}$ is not equivalent to $\bar{\mathfrak{a}}$ in the class group (there are no nontrivial classes of order 2).

If L is an RG-lattice in V, there are only two possibilities for the dual lattice, by Proposition 8.6:

$$L^* = \begin{cases} L, & \det L = 1,\ V_{\mathfrak{p}} \text{ symplectic}, \\ \pi^{-1}L, & \det L = p^k,\ V_{\mathfrak{p}} \text{ orthogonal}. \end{cases} \tag{11.1}$$

Here $k = \frac{1}{2}\dim V = \dim_K V = \dim V_{\mathfrak{p}}$. In the first case, θ_L is a modular form of weight k on $\mathrm{SL}_2(\mathbf{Z})$; in the second θ_L is modular of weight k on $\Gamma_0(p)$, with quadratic character $\varepsilon(d) = (\frac{d}{p})^k$, and by Proposition 9.2 we have $\theta_L | w_p = (-i)^k \theta_L$.

A sequence of examples with $k = (p-1)/2 \equiv 1 \pmod 2$ was constructed by Hecke [H, A].

Proposition 11.2. *Let $G = \mathrm{PSL}_2(p) = \mathrm{SL}_2(p)/\langle \pm 1 \rangle$ of order $\frac{1}{2}p(p^2-1)$. There is a unique irreducible representation V of G of dimension $(p-1)$ over $\mathbf{Q}$ with $\mathrm{End}_G(V) = K$. The representation V is globally irreducible, and the reduction $V_{\mathfrak{p}}$ is orthogonal.*

Proof. Let ψ be the complex character of a $\frac{1}{2}$-discrete series representation of G, which has dimension $(p-1)/2$ and $\mathbf{Q}(\psi) = K$ [Hu]. At an unramified prime of R, the reduction of ψ is an irreducible Brauer character: in fact, its restriction to a Borel subgroup $B = \{\left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right)\}$ of $\mathrm{SL}_2(p)$ remains absolutely irreducible! This follows from the fact that the restriction of ψ to the unipotent subgroup $N = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\}$ contains $(p-1)/2$ distinct characters, which are permuted transitively by B. Since these characters remain distinct in all characteristics $\neq p$, $\psi \equiv \rho$ is absolutely irreducible.

The reduced representation at $\mathfrak{p}$ is isomorphic to $\mathrm{Sym}^{(p-3)/2} U_2$, where U_2 is the standard two-dimensional representation of $\mathrm{SL}_2(p)$ in characteristic p. This follows from [A, §4]; we will give another argument using hyperelliptic curves at the end of this section. This is an absolutely irreducible, orthogonal

representation of G over $\mathbf{F}_p$. Hence, by Proposition 4.2 (2), $\chi = \psi + \overline{\psi}$ is the character of a globally irreducible representation V of G.

To show V is unique, we observe $V \otimes \mathbf{Q} = W \oplus \overline{W}$ where W has character ψ. If V' were another such representation, $V' \otimes \mathbf{C} = W' \oplus \overline{W'}$ and it suffices to show $W' = W$ or $\overline{W}$ (two rational representations that are isomorphic over $\mathbf{C}$ are isomorphic over $\mathbf{Q}$). But W and $\overline{W}$ are the only irreducible representations of dimension $(p-1)/2$ for G (at least when $p \neq 3$; when $p = 3$ they are the only one-dimensional representations with $W \neq \overline{W}$).

Lemma 11.3. *The group* $G' = \mathrm{PGL}_2(p) = G \rtimes \langle \tau \rangle$ *with* $\tau = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *acts* $\mathbf{Q}$*-linearly on* V*, and the involution* τ *acts* K*-antilinearly.*

Proof. Indeed, V is the representation space for the discrete series representation of $\mathrm{GL}_2(p)$, corresponding to a quartic character of the nonsplit torus. Since this is absolutely irreducible, $\mathrm{End}_{G'}(V) = \mathbf{Q}$ and τ acts antilinearly on $\mathrm{End}_G(V) = K$.

From Proposition 11.2 and Lemma 11.3 we see that there are exactly h $\mathbf{Z}[G]$-lattices L up to isomorphism in V, indexed canonically by elements of $Cl(R)$. We let L_1 be the class fixed by τ, and $L_{\mathfrak{a}} = \mathfrak{a}L_1$. Each lattice L has invariants:

$$\text{(11.4)} \qquad \begin{cases} \operatorname{rank} L = p-1, \\ L^* = \pi^{-1}L, \\ \det L = (p)^{(p-1)/2}. \end{cases}$$

When $p = 3$, L is the A_2-root lattice; the representation V of G factors through the quotient μ_3. When $p = 7$, L is the lattice described in §6; the form φ is given by (6.2).

A cyclotomic model for the lattices $L_{\mathfrak{a}}$ in V is due to Adler [A, §5]. Let ζ_p be a pth root of unity in $\mathbf{C}$, and recall that $K = \mathbf{Q}(\sqrt{-p})$ is a subfield of the cyclotomic field $\mathbf{Q}(\zeta_p)$. We may realize the representation V of G on $\mathbf{Q}(\zeta_p)$ in a way that the unipotent element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ acts by multiplication by ζ_p, and $\left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right)$ acts via the element in the Galois group taking ζ_p to $\zeta_p^{a^2}$. If $\mathfrak{a}$ is an ideal of R, we let $i(\mathfrak{a})$ be the extended ideal $\mathfrak{a}\mathbf{Z}[\zeta_p]$. Then

$$\text{(11.5)} \qquad L_{\mathfrak{a}} = \mathfrak{i}(\mathfrak{a}) \cdot (1 - \zeta_p)^{-((p-3)/4)}$$

with G-invariant Hermitian form:

$$\text{(11.6)} \qquad \varphi(v, w) = \frac{1}{\mathbf{N}\mathfrak{a}} \operatorname{Trace}_{\mathbf{Q}(\zeta_p)/K}(v\overline{w}).$$

In particular, taking $\mathfrak{a} = (\pi)$, so $\mathfrak{i}(\mathfrak{a}) = (1 - \zeta_p)^{(p-1)/2}\mathbf{Z}[\zeta_p]$, we see that L_1 is isomorphic to the Craig lattice $A_{p-1}^{(m)}$ with $m = (p+1)/4$ [CS, p. 223].

Another model for the lattices $L_{\mathfrak{a}}$ was shown to me by Elkies; for the rest of this section, all varieties and morphisms between varieties are understood to be defined over the prime field $\mathbf{F}_p$. Let X be the hyperelliptic curve, of genus

$g = (p-1)/2$, defined by the equation $y^2 = x^p - x$, and let J_X be the Jacobian of X. The group $G = \mathrm{PSL}_2(p)$ acts on X by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(x, y) = \left(\frac{ax+b}{cx+d}, \frac{y}{(cx+d)^{(p+1)/2}} \right). \tag{11.7}$$

The group $\mathrm{Aut}(X)$ is isomorphic to the direct product of G with the hyperelliptic involution $(x, y) \mapsto (x, -y)$, which acts as -1 on J_X. Let E be the elliptic curve with equation $v^2 = u^3 - u$.

Lemma 11.8. *The Frobenius endomorphism F_E of E satisfies $F_E^2 = -p$ in $\mathrm{End}(E)$. We have $\mathrm{End}(E) \simeq R$, and for each ideal (class) $\mathfrak{a}$ of R there is a unique elliptic curve $E_\mathfrak{a}$ with $\mathrm{End}(E_\mathfrak{a}) = R$ and $\mathrm{Hom}(E, E_\mathfrak{a}) \simeq \mathfrak{a}$ as an R-module.*

Proof. E is the reduction of the curve $V^2 = U^3 - U$ over $\mathbf{Q}$, which has multiplication by $\mathbf{Z}[i]$ over $\mathbf{C}$. Hence the reduction is supersingular $(\mathrm{mod}\, p)$, as $p \equiv 3$ (4) is inert in $\mathbf{Z}[i]$ [S1, §2]. For $p > 3$ this implies E has exactly $p+1$ points over $\mathbf{F}_p$ and hence that $F_E^2 = -p$; for $p = 3$ we can check this directly. Consequently, $\mathbf{Z}[\pi] \subset \mathrm{End}(E)$ with $\pi^2 = -p$. To show $\mathrm{End}(E) = R$ we must show that $1 + \pi$ is divisible by 2 in $\mathrm{End}(E)$, or equivalently, that all 2-torsion points on E are rational over $\mathbf{F}_p$. This is clear, as the polynomial $u^3 - u = u(u-1)(u+1)$ factors completely. The existence and uniqueness of the curve $E_\mathfrak{a}$ follows from Serre's theory of complex multiplication (cf. [S1, §2] where $E_\mathfrak{a}$ is written as $\mathfrak{a} * E$).

We now define the Mordell-Weil lattice:

$$\begin{aligned} M_\mathfrak{a} &= \mathrm{Mor}(X, E_\mathfrak{a})/\text{ translations} \\ &= \mathrm{Hom}(J_X, E_\mathfrak{a}), \end{aligned} \tag{11.9}$$

where Hom means homomorphisms of abelian varieties over $\mathbf{F}_p$. This is the group of points, modulo torsion, on the elliptic curve $E_\mathfrak{a}$ over the global function field of X. It is clearly an $R = \mathrm{End}(E_\mathfrak{a})$ and $G \subseteq \mathrm{Aut}(X)$ module, and has the invariant Hermitian form

$$\varphi(v, w) = v \circ {}^t w \in R = \mathrm{End}(E_\mathfrak{a}), \tag{11.10}$$

where ${}^t w \colon E_\mathfrak{a} \to J_X$ is the dual homomorphism, and $E_\mathfrak{a}$ and J_X are identified with their dual varieties via the standard principal polarizations.

Proposition 11.11. *The RG-Hermitian lattice $M_\mathfrak{a}$ is isomorphic to $L_\mathfrak{a} \subseteq V$.*

Proof. We first consider the representation of G on the rational vector space $V' = M_\mathfrak{a} \otimes \mathbf{Q}$, and claim that $V' \simeq V$. Indeed, $(V')^G = 0$ and $\mathrm{End}_G(V')$ contains K, so it suffices to show $\dim V' = p - 1$ (by the unicity of V). This follows from Tate's theorem [Ta1] on isogenies of abelian varieties over fields, as one has $F_{J_X}^2 = -p$ in $\mathrm{End}(J_X)$ and $F_E^2 = -p$ in $\mathrm{End}(E)$ by Lemma 11.8.

(Actually, one does not need the full power of Tate's theorem in this case, as the calculation of Frobenius elements easily shows that $\dim V' \leq p-1 = 2g$. To show equality, it suffices to prove that $V' \neq 0$. But X is isogenous to the curve X^* with equation $y^2 = x^{p+1} - 1$ and E is isogenous to the curve E^* with equation $v^2 = u^4 - 1$, and there is an obvious map $\pi(x, y) = (x^{(p+1)/4}, y)$ from X^* to E^*. Hence there is a less obvious map (of degree $(p+1)/4$) from X to E.)

Since $M_{\mathfrak{a}}$ is an RG-lattice in $V' \simeq V$, it is isomorphic to one of the lattices $L_{\mathfrak{b}}$. To show $M_{\mathfrak{a}} \simeq L_{\mathfrak{a}}$ it suffices to show $M_1 \simeq L_1$; indeed, from the definition of the curve $E_{\mathfrak{a}}$ we find $M_{\mathfrak{a}} \simeq \mathfrak{a}M_1$. Since L_1 is the unique isomorphism class of RG-lattices in V fixed by the involution τ, it suffices to give an action of τ on M_1. Let i be a 4th root of unity in $\mathbf{F}_{p^2}$ and define the automorphisms $i_X(x, y) = (-x, iy)$, $i_E(u, v) = (-u, iv)$ of order 4 of X and E over $\mathbf{F}_{p^2}$. Then $\tau(m) = i_E \circ m \circ i_X$ gives the desired R-antilinear involution of M_1.

Corollary 11.12 (Elkies). *For all $v \neq 0$ in $L_{\mathfrak{a}}$, we have $\varphi(v, v) \geq (p+1)/4$.*

Proof. We use the model $M_{\mathfrak{a}} = \mathrm{Mor}(X, E_{\mathfrak{a}})/$ translations, where $v \neq 0$ corresponds to a covering $\pi_v : X \to E_{\mathfrak{a}}$ and $\varphi(v, v) = \deg \pi_v$. Since X has $(p+1)$ points over $\mathbf{F}_p$, all of which are Weierstrass points, their image (suitably translated to contain the origin) lies in the two-torsion subgroup of $E_{\mathfrak{a}}$, which has order 4. Hence $\deg \pi_v \geq (p+1)/4$.

Note 11.13. The lattice L_1 has at least $p(p-1)$ vectors v with $\langle v, v\rangle = 2\varphi(v, v) = (p+1)/2$, so the abstract estimate in Corollary 11.12 is best possible. These maps come from the obvious covering of E^* by X^*, discussed in the proof of Proposition 11.11, and form two orbits under the action of G (each with stabilizer the normalizer of a nonsplit torus).

Note 11.14. The fact that the reduction $V_{\mathfrak{p}}$ of V at the ramified prime $\mathfrak{p}$ of K is isomorphic to the representation $\mathrm{Sym}^{(p-3)/2} U_2$ can be deduced easily from Proposition 11.11. Indeed, $V_{\mathfrak{p}}$ is just the representation of G on the holomorphic differentials on X; since these have as basis the differentials $\langle dy, xdy, x^2dy, \ldots, x^{(p-3)/2}dy\rangle$, we obtain the representation $\mathrm{Sym}^{(p-3)/2} U_2$ of G as claimed.

12. Examples when K = Hamilton's quaternions: the Barnes-Wall lattices

In this section K is the division ring of Hamilton's quaternions, with the usual relations $i^2 = j^2 = -1$ and $ij = -ji = k$. The maximal orders in K are all conjugate to the Hurwitz order $R = \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k + \mathbf{Z}(\frac{1}{2}(1 + i + j + k))$.

The ring R has class number 1; its unique ramified ideal $\mathfrak{p}$ is principal, generated by $\pi = (1 + i)$. The unit group

$$R^* = \langle \pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2)\rangle$$

has order 24, with normal subgroup $H_8 = \langle \pm 1, \pm i, \pm j, \pm k \rangle$ the quaternion group of order 8.

For each globally irreducible representation V of a finite group G with $\mathrm{End}_G(V) = K$, we obtain, by the theory in §§1–5, a unique RG-Hermitian lattice L up to isomorphism. There are only two possibilities for the dual lattice, by Proposition 8.6:

$$L^* = \begin{cases} L, & \det L = 1,\ V_{\mathfrak{p}} \text{ symplectic}, \\ \pi^{-1}L, & \det L = 2^k,\ V_{\mathfrak{p}} \text{ Hermitian}. \end{cases} \tag{12.1}$$

Here $k = \frac{1}{2}\dim V = 2\dim_K V$ is even. In the first case, θ_L has weight k on $\mathrm{SL}_2(\mathbf{Z})$; in the second, θ_L has weight k on $\Gamma_0(2)$ and $\theta_L|w_2 = (-1)^{k/2}\theta_L$ by Proposition 9.2. A sequence of examples of globally irreducible V, with $k = 2^n$, $n \geq 1$, is constructed as follows.

Let $\tilde{A}$ be the extra-special 2-group (denoted 2_-^{1+2n} in the ATLAS [C]) which is a central extension of an elementary abelian 2-group $A \simeq (\mathbf{Z}/2)^{2n}$ by $\mathbf{Z}/2$, corresponding to a nondegenerate quadratic form Q on A of Arf invariant 1. This makes sense, as $H^2(A, \mathbf{Z}/2) = \mathrm{Sym}^2(A^*)$ is the space of quadratic forms on A; for an enlightening discussion of extraspecial 2-groups and their representation theory, see [Q, §§2–4; Gr]. We have an exact sequence

$$0 \to \mathbf{Z}/2 \to \tilde{A} \underset{\pi}{\longrightarrow} A \to 0; \tag{12.2}$$

for any $a \in A$ we let $\tilde{a}$ be an element of $\tilde{A}$ with $\pi(\tilde{a}) = a$. Then $Q(a) = \tilde{a}^2$ and the associated bilinear form $\langle a, b \rangle = Q(a+b) - Q(a) - Q(b)$ on A is given by the commutator: $\langle a, b \rangle = \tilde{a}\tilde{b}\tilde{a}^{-1}\tilde{b}^{-1}$. Let B be a maximal isotropic subspace of A, which has dimension $n-1$ by our hypothesis on $\mathrm{Arf}(Q)$, and write $B^{\perp} = B \oplus E$ where $\dim E = 2$ and $Q|_E = x^2 + xy + y^2$. Then $\tilde{E}$ is a quaternion group of order 8 in $\tilde{A}$. We identify $\tilde{E}$ with $\langle \pm 1, \pm i, \pm j, \pm k \rangle$ in R^* and write $\tilde{A}$ in Heisenberg form

$$\tilde{A} = \tilde{E} \times B \times B^*, \text{ with } B^* = \mathrm{Hom}(B, \mathbf{Z}/2) \text{ and multiplication,}$$
$$(\varepsilon, b, \lambda)(\varepsilon', b', \lambda') = ((-1)^{\langle b', \lambda \rangle}\varepsilon\varepsilon', b + b', \lambda + \lambda').$$

Let V be the Schrödinger representation of $\tilde{A}$, given by its right action on the left K-vector space of functions f on B^* with values in K:

$$f^{(\varepsilon, b, \lambda)}(\mu) = f(\mu - \lambda) \cdot (-1)^{\langle b, \mu - \lambda \rangle} \cdot \varepsilon. \tag{12.3}$$

Then $\dim_K(V) = 2^{n-1}$.

If we view V as a representation of $\tilde{A}$ over $\mathbf{Q}$, then $\dim V = 2^{n+1}$ and $\mathrm{End}_{\tilde{A}}(V) = K$. The character χ of V is equal to 2ψ, where ψ is the unique irreducible complex character of $\tilde{A}$ on which the center acts nontrivially. The reduction of $V \pmod{l}$ is irreducible over $R/lR = M_2(\mathbf{Z}/l\mathbf{Z})$ for all unramified primes $l \neq 2$ in R, as $\tilde{A}$ is a 2-group. The reduction at $\mathfrak{p} = (1+i)R$

dividing 2 is *not* irreducible for the same reason: the only irreducible representation of a 2-group in characteristic 2 is the trivial representation.

Note 12.4. A stable lattice $L(B^*)$ for $\tilde{A}$ on V is the R-module of functions on B^* with values in R. By (12.3) we see that the action of $\tilde{A}$ on $L(B^*)/\mathfrak{p}L(B^*)$ factors through the regular representation of the quotient B^*.

The unicity of V shows that it gives rise to a projective complex representation of dimension 2^n of the group $\mathrm{Aut}(\tilde{A})$. We have an exact sequence

$$0 \to A \to \mathrm{Aut}(\tilde{A}) \to O^-_{2n}(2) \to 0, \tag{12.5}$$

where $A = \tilde{A}/\text{center} = \mathrm{Inn}\,\mathrm{Aut}(\tilde{A})$, and $O^-_{2n}(2)$ is the orthogonal group of the quadratic space (A, Q) [Gr]. Let Ω^-_{2n} be the subgroup of index 2 in $O^-_{2n}(2)$ of elements with trivial Dickson determinant, and let $\mathrm{Aut}_+(\tilde{A})$ be the corresponding subgroup of $\mathrm{Aut}(\tilde{A})$.

When $n = 1$, $\tilde{A}$ is the quaternion group and $\mathrm{Aut}(\tilde{A})$ is isomorphic to S_4. The group $\mathrm{Aut}_+(\tilde{A})$ is isomorphic to A_4, and has a double cover $G = \mathrm{SL}_2(3)$ which contains $\tilde{A}$ as a normal subgroup with quotient $\Omega^-_2(2) = \mu_3$. The projective representation of $\mathrm{Aut}(\tilde{A})$ lifts to a linear action of G on $V = K$ with $\mathrm{End}_G(V) = K$. When $n > 2$ we have $H^2(\Omega^-_{2n}(2), \mathbf{C}^*) = H^1(\Omega^-_{2n}(2), \mathbf{C}^*) = 1$ [K, §8.4]; hence the projective representation of $\mathrm{Aut}(\tilde{A})$ lifts uniquely to a linear representation of dimension 2^n over $\mathbf{C}$ of the double cover $G = 2^{1+2n}_- \cdot \Omega^-_{2n}(2)$ of $\mathrm{Aut}_+(\tilde{A})$. The character of this representation of G takes rational values, and is given by the formula:

$$\psi(g) = \begin{cases} \pm 2^{\dim \ker(\overline{g}-1)/2}, \\ 0. \end{cases} \tag{12.6}$$

Here $\overline{g}$ is the image of g in $\Omega^-_{2n}(2)$, and the value $\psi(g) \neq 0$ if and only if $g \equiv 1$ in $\mathrm{Aut}(\tilde{C})$ where $C = \ker(g-1)$. The hypothesis that $\overline{g} \in \Omega^-_{2n}(2)$ insures that $\dim \ker(\overline{g}-1)$ is even, so $\mathbf{Q}(\psi) = \mathbf{Q}$. (The character of the linear representation on the full double cover of $\mathrm{Aut}(\tilde{A})$ takes values in a quadratic extension of $\mathbf{Q}$: for $n = 1$ this is the two-dimensional representation of $\tilde{S}_4$ with character in $\mathbf{Q}(\sqrt{-2})$, which was discussed in §6.) Hence G acts on V, extending the action of $\tilde{A}$, and $\mathrm{End}_G(V) = K$.

Proposition 12.7. *The representation V of dimension 2^{n+1} of $G = 2^{1+2n}_- \cdot \Omega^-_{2n}(2)$ is globally irreducible. Let L be an RG-lattice in V and $\mathfrak{p} = (1+i)R$ the ramified prime dividing 2. The representation $V_\mathfrak{p} = L/\mathfrak{p}L$ of G has dimension 2^{n-1} over $k_\mathfrak{p} = \mathbf{F}_4$, and the subgroup $\tilde{A}$ acts trivially on $V_\mathfrak{p}$. The quotient $\Omega^-_{2n}(2)$ acts irreducibly on $V_\mathfrak{p}$ via the restriction of a semi-spinorial representation of the algebraic group $\mathrm{Spin}_{2n}(\overline{\mathbf{F}}_2)$. The representation $V_\mathfrak{p}$ is Hermitian if $n \equiv 1 \pmod 2$, and alternating if $n \equiv 0 \pmod 2$.*

Proof. Everything has been proved except the irreducibility of $V_{\mathfrak{p}}$. Consider the semisimplification of the reduction of the character $\psi \pmod 2$. This has dimension 2^n over $\mathbf{F}_2$; since $\tilde{A}$ is a 2-group it acts trivially, and we obtain a semisimple representation of the quotient $\Omega_{2n}^-(2)$ with character

$$\psi(\overline{g}) \equiv \begin{cases} 1 & \text{if } \overline{g} - 1 \text{ acts invertibly,} \\ 0 & \text{otherwise.} \end{cases}$$

The irreducible modules of $\Omega_{2n}^-(2)$ come via restriction of the irreducible representations of $\Omega_{2n}^-(\mathbf{F}_2) = \mathrm{Spin}_{2n}(\overline{\mathbf{F}}_2)$ with highest weights λ satisfying: $\lambda = \sum_{i=1}^n a_i \omega_i$ with $0 \le a_i \le 1$ and ω_i the fundamental weights [St1, Chapter 13]. Let T be a maximal torus in Ω_{2n}, and let $\varepsilon_1, \ldots, \varepsilon_n$ be the standard characters of T. From the formula for the character ψ on $\Omega_{2n}^-(2)$, one concludes that the 2^n characters of T which occur in the corresponding semisimple representation of Ω_{2n} are precisely those of the form: $\frac{1}{2}\sum_{i=1}^n \pm\varepsilon_i$.

But these characters break up into exactly two orbits for the Weyl group $W = N(T)/T$, each of size 2^{n+1} corresponding to the semi-spinorial representations of Ω_{2n} with highest weights ω_{n-1} and ω_n [B, §13.4]. When restricted to $\Omega_{2n}^-(2)$ these give irreducible conjugate representations of dimension 2^{n-1} over $\mathbf{F}_4$, so we have the congruence $\psi \equiv \rho + \rho^2 \pmod 2$ with ρ absolutely irreducible and $\mathbf{F}_2(\rho) = \mathbf{F}_4$. Hence $V_{\mathfrak{p}}$ is irreducible, and $\tilde{A}$ acts trivially on it (the subspace $F_{\mathfrak{p}}^{\tilde{A}}$, which is nontrivial, is G-stable).

When n is odd the dual of one semi-spinorial representation is the other ($\omega_{n-1}^* = \omega_n$) and when n is even the semispin representations are self-dual ($\omega_{n-1}^* = \omega_{n-1}$, $\omega_n^* = \omega_n$) [B, §13.4]. Since, when restricted to $\mathbf{F}_4$, the representations are conjugate, this gives the asserted duality of $V_{\mathfrak{p}}$.

Combining (12.5) with (12.1), we have constructed a unique Hermitian RG-lattice L in V, with

$$(12.8) \qquad \begin{cases} \operatorname{rank} L = 2^{n+1}, \\ \det L = \begin{cases} 1 & n \equiv 0 \pmod 2, \\ 2^{2^n} & n \equiv 1 \pmod 2. \end{cases} \end{cases}$$

When $n = 1$, L is the D_4-lattice, and when $n = 2$, L is the E_8-lattice.

Proposition 12.9. *For all $n \ge 1$ the Euclidean lattice L is isomorphic to the Barnes-Wall lattice $BW_{2^{n+1}}$.*

Proof. The Barnes-Wall lattices BW_m for $m = 2^k \ge 4$ are defined in [CS, Chapter 5, §6.5, Chapter 8, §8.2f]; one has $BW_4 = D_4$ and $BW_8 = E_8$ so we may assume $n \ge 3$ in Proposition 12.9. Then $BW_{2^{n+1}}$ has automorphism group $2_+^{1+(2n+2)}\Omega_{2n+2}^+(2)$ [BE, Chapter II, §§4–7], which contains the subgroup

$$2_-^{1+2}\Omega_2^-(2) \times_{\langle \pm 1 \rangle} 2_-^{1+2n}\Omega_{2n}^-(2)$$

(central product). Since $2_-^{1+2}\Omega_2^-(2) \simeq R^*$ and $2_-^{1+2n}\Omega_{2n}^-(2) = G$, $BW_{2^{n+1}}$ has an RG structure. Since the representation of G on $BW \otimes \mathbf{Q}$ is isomorphic to V (as the center of $\tilde{A}$ acts nontrivially), $BW \simeq L$ by unicity.

Corollary 12.10. *For all $v \neq 0$ in L, we have $\langle v, v\rangle \geq 2^{[(n+1)/2]}$. The number of vectors v with $\langle v, v\rangle = 2^{[(n+1)/2]}$ is equal to $2^{n+2}(2^n+1)(2^{n-1}+1)\cdots(2+1)$.*

Proof. These results are known for the lattice $BW_{2^{n+1}}$, by a consideration of the Reed-Muller codes [CS, p. 151]. For more discussion of the Barnes-Wall lattices and the Reed-Muller codes from a group-theoretic point of view, see [BE, VV].

Note 12.11. Elkies has realized L as a sublattice, of finite index, in the Mordell-Weil lattice:

$$\begin{aligned} M &= \mathrm{Mor}_{\mathbf{F}_{q^2}}(X, E)/\text{translations} \\ &= \mathrm{Hom}_{\mathbf{F}_{q^2}}(J_X, E), \end{aligned}$$

where X is the hyperelliptic curve $y^2 + y = x^{q+1}$ with $q = 2^n$ and E is the supersingular elliptic curve $u^2 + u = v^3$. L is generated by the coverings of E obtained by dividing X by a maximal elementary abelian 2-group in $\tilde{A} \subset \mathrm{Aut}_{\mathbf{F}_{q^2}}(X)$ which does not contain the center of $\tilde{A}$ [VV, 9.3]. These Galois coverings have degree 2^{n-1}.

Note 12.12. The lattice $L(B^*)$ discussed in 12.4 is *not* stable under the entire group G, but the lattice $\sum_B L(B^*)$ is G-stable.

13. Examples: the Weil representation of $\mathrm{Sp}_{2n}(q)$

In this section, p is an *odd* prime and $q = p^f$. Let A be a nondegenerate symplectic space of dimension $2n$ over the finite field $\mathbf{F}_q$, and let $G = \mathrm{Sp}(A) = \mathrm{Sp}_{2n}(q)$ be the symplectic group of A. Then the center of G has order 2, and is generated by the scalar transformation -1_A. The group G is a normal subgroup of the symplectic similitudes $C\mathrm{Sp}(A)$, and conjugation by this larger group gives an outer automorphism τ (of order 2) of G.

Fix a splitting $A = B \oplus B^*$, where B and B^* are maximal isotropic subspaces of dimension n. We identify B^* with the dual of B and, for $b \in B$ and $\lambda \in B^*$, write this pairing as $\langle b, \lambda\rangle$ in $\mathbf{F}_q$. The Heisenberg group

$$\begin{aligned} &\tilde{A} = \mathbf{F}_q \times B \times B^* \text{ with multiplication,} \\ &(\varepsilon, b, \lambda)\cdot(\varepsilon', b', \lambda') = (\varepsilon + \varepsilon' + \langle b', \lambda\rangle, b + b', \lambda + \lambda) \end{aligned}$$

defines a central extension of A by $\mathbf{F}_q = \{(\varepsilon, 0, 0)\}$:

$$0 \to \mathbf{F}_q \to \tilde{A} \underset{\pi}{\longrightarrow} A \to 0. \tag{13.1}$$

The commutator $[\tilde{a}, \tilde{a}']$ gives the symplectic form on A.

Fix a nontrivial character $\psi: \mathbf{F}_q^+ \to \mathbf{C}^*$. The Schrödinger representation $W = W(\psi)$ of $\tilde{A}$ (associated to ψ) is given by the following right action of $\tilde{A}$ on the $\mathbf{Q}(\zeta_p)$ vector space of functions on B^* with values in $\mathbf{Q}(\zeta_p) = \mathbf{Q}(\psi)$:

$$f^{(\varepsilon, b, \lambda)}(\mu) = \psi(\varepsilon + \langle b, \mu - \lambda \rangle) \cdot f(\mu - \lambda). \tag{13.2}$$

It is the unique irreducible representation of $\tilde{A}$ over $\mathbf{Q}(\zeta_p)$ (or even over $\mathbf{C}$) where the center acts by the character ψ, and we have $\dim W = q^n$.

The unicity of W shows that it gives rise to a projective representation of the group of automorphisms of $\tilde{A}$ which act trivially on the center. This group contains $G = \mathrm{Sp}(A)$, which is the subgroup centralizing the involution $-1_A(\varepsilon, \lambda, b) = (\varepsilon, -\lambda, -b)$. Hence G acts projectively on W over $\mathbf{Q}(\zeta_p)$. Since $H^2(G, \mathbf{C}^*) = 0$ (except in the case when $n = 1$ and $q = 3$ or 3^2) [K, §8.4] this projective representation lifts to a linear representation; since $H^1(G, \mathbf{C}^*) = 0$ (except in the one case when $n = 1$ and $q = 3$) the lifting to a linear representation is unique. (A unique lifting for $\mathrm{SL}_2(3^2)$ exists (cf. [Ge, Lemma 1.5]), and a lifting for $G = \mathrm{SL}_2(3)$ exists and is specified in [Ge, Theorem 2.4 a''].) We denote the lifted representation of G again by $W(\psi)$; is the Weil representation of G, of dimension q^n, associated to the character ψ.

The Siegel parabolic P of G, which fixes the isotropic subspace B, acts on $W(\psi)$ as follows [Ge, (2.7)–(2.9)]:

$$\begin{cases} f^{\left(\begin{smallmatrix} {}^t\alpha^{-1} & 0 \\ 0 & \alpha \end{smallmatrix}\right)}(\lambda) = \left(\frac{\det \alpha}{q}\right) \cdot f(\alpha\lambda), \\ f^{\left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)}(\lambda) = \psi(\tfrac{1}{2}\langle \beta(\lambda), \lambda \rangle) \cdot f(\lambda). \end{cases} \tag{13.3}$$

Here $\alpha \in \mathrm{GL}(B^*)$ and $\beta = {}^t\beta: B^* \to B$ is symmetric; the symbol $\left(\frac{x}{q}\right)$ denotes the Legendre symbol—the unique quadratic character of $\mathbf{F}_q^*$. We have the commutation law:

$$\begin{pmatrix} {}^t\alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix}^{-1} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} {}^t\alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & {}^t\alpha\beta\alpha \\ 0 & 1 \end{pmatrix}.$$

The action of the matrix $\left(\begin{smallmatrix} 0 & \beta \\ -\beta^{-1} & 0 \end{smallmatrix}\right)$, where $\beta: B^* \xrightarrow[\sim]{} B$ is invertible is given by a Fourier transform, but we will not need this fact here.

The distinct nontrivial characters of $\mathbf{F}_q^+$ all have the form $\psi_x(y) = \psi(xy)$ for $x \in \mathbf{F}_q^*$.

Lemma 13.4. (1) *We have an isomorphism of G-modules $W(\psi) \simeq W(\psi_x)$ if and only if x is a square in $\mathbf{F}_q^*$. If $x \in \mathbf{F}_q^* - \mathbf{F}_q^{*2}$, the distinct G-modules $W(\psi)$ and $W(\psi_x)$ are conjugate via the outer automorphism τ of G.*

(2) *If $a \in \mathbf{F}_p^*$ we have an isomorphism of G-modules $W(\psi_a) = W(\psi)^{\sigma_a}$, where σ_a is the automorphism of $\mathbf{Q}(\zeta_p)$ which maps ζ_p to ζ_p^a. In particular, the dual representation $W(\psi)^* \simeq \overline{W(\psi)}$ is isomorphic to $W(\psi_{-1})$.*

Proof. (1) is proved in [Ge, Theorem 2.4], and (2) follows from the fact that $\psi^{\sigma_a} = \psi_a$.

In particular, we see that the Weil representation W is self-dual if and only if $q \equiv 1 \pmod 4$, when $(\frac{-1}{q}) = +1$. In general, the tensor product representation $W \otimes W^*$ is independent of ψ, and is isomorphic to the natural representation of G (of dimension q^{2n}) on the $\mathbf{Q}(\zeta_p)$-valued functions on A [Ge, Theorem 4.4].

Lemma 13.5. (1) *The Weil representation $W = W(\psi)$ of G is the direct sum of 2 absolutely irreducible representations W^+ and W^- over $\mathbf{Q}(\zeta_p)$. We have* $\dim W^{\pm} = (q^n \pm 1)/2$ *and the center -1_A of G acts on $W^{\pm}$ via the scalar* $\pm(\frac{-1}{q})^n$.

(2) *Let $\chi = \chi^+ + \chi^-$ be the decomposition of the character of W. If q is a square, then $\mathbf{Q}(\chi) = \mathbf{Q}(\chi^+) = \mathbf{Q}(\chi^-) = \mathbf{Q}$. If $q = p^f$ with f odd, then*

$$\mathbf{Q}(\chi) = \mathbf{Q}(\chi^+) = \mathbf{Q}(\chi^-) = \begin{cases} \mathbf{Q}(\sqrt{-p}) & p \equiv 3 \pmod 4, \\ \mathbf{Q}(\sqrt{p}) & p \equiv 1 \pmod 4. \end{cases}$$

Proof. (1) We have $\langle \chi, \chi \rangle = \langle 1, \chi \cdot \overline{\chi} \rangle = 2$, as G has 2 orbits on A. Hence the eigenspaces for -1_A in W are absolutely irreducible: the even functions on B^* give W^+ of dimension $(q^n - 1)/2$. The action of -1_A is given by (13.3), taking $\alpha = -1_B$.

(2) If q is a square, then any a in $\mathbf{F}_p^*$ is a square in $\mathbf{F}_q^*$. Hence, by Lemma 13.4 (2), χ is fixed by the automorphisms of $\mathbf{Q}(\zeta_p)$. Since χ^+ and χ^- are not conjugate, they must also lie in $\mathbf{Q}$. If q is not a square, the same argument shows that $\mathbf{Q}(\chi)$ is the unique quadratic field contained in $\mathbf{Q}(\zeta_p)$.

We now determine the local behavior of the characters $\chi^{\pm}$ at all places of the field $\mathbf{Q}(\chi)$.

Proposition 13.6. *Let $\mathfrak{p}$ be a finite place of $\mathbf{Q}(\chi)$.* (1) *If $\mathfrak{p}$ does not divide $2p$, then the characters $\chi^{\pm}$ both have absolutely irreducible reduction* $(\mathrm{mod}\,\mathfrak{p})$.

(2) *If $\mathfrak{p}$ divides 2, then χ^- has absolutely irreducible reduction* $(\mathrm{mod}\,\mathfrak{p})$ *and* $\chi^+ \equiv 1 + \chi^- \pmod{\mathfrak{p}}$.

(3) *If $\mathfrak{p}$ is the unique prime dividing p, then the characters $\chi^{\pm}$ have absolutely irreducible reduction* $(\mathrm{mod}\,\mathfrak{p})$ *if and only if $f = 1$ (that is, if $q = p$). In this case, the reduction is symplectic when $\chi^{\pm}(-1_A) = -\chi^{\pm}(1_A)$, and orthogonal when $\chi^{\pm}(-1_A) = \chi^{\pm}(1_A)$.*

(4) *The character χ^+ is unobstructed at all real places of $\mathbf{Q}(\chi)$, and the character χ^- is obstructed at all real places of $\mathbf{Q}(\chi)$.*

Proof. From (13.3), one sees that the restriction of χ^- to the Siegel parabolic P is irreducible in all characteristics $\neq p$. Similarly, the restriction of χ^+ to P is the direct sum of the line of functions supported on 0 in B^*, on which P acts via the character $((\det\alpha)/q)$, with an irreducible representation. This decomposition is preserved by G only when $l = 2$: W^+ has the smallest

dimension of an irreducible representation with central character not equal to that of W^- [LS]. This proves (1) and (2).

(3) The irreducible representations of $G = \mathrm{Sp}_{2n}(q)$ in characteristic p all have the form

$$U = U_1 \otimes U_2^p \otimes \cdots \otimes U_f^{p^{f-1}},$$

where U_i are irreducible algebraic representations of $\mathrm{Sp}_{2n}(\overline{\mathbf{F}}_p)$ restricted to G [St2]. If $\omega_1, \ldots, \omega_n$ are the fundamental dominant weights for Sp_{2n}, then the highest weights λ_i of the irreducible representations U_i have the form $\lambda_i = \sum_{j=1}^n a_{ij}\omega_j$ with $0 \le a_{ij} \le p-1$ [St1]. The highest weight of U is then $\lambda_1 + p\lambda_2 + p^2\lambda_3 + \cdots + p^{f-1}\lambda_f = \sum_{j=1}^n b_j\omega_j$ with $0 \le b_j \le q-1$.

From (13.3) we see that the weights occurring in the reduction of W are the characters

$$\lambda = \sum a_i e_i \quad \text{with} \quad -\left(\frac{q-1}{2}\right) \le a_i \le \left(\frac{q-1}{2}\right),$$

$$e_i \begin{pmatrix} t_1 & & & & 0 \\ & \ddots & & & \\ & & t_n & & \\ & 0 & & t_1^{-1} & \\ & & & & \ddots \\ & & & & & t_n^{-1} \end{pmatrix} = t_i.$$

Each weight occurs with multiplicity one in W, and occurs in W^+ iff $\sum a_i \equiv n((q-1)/2) \pmod 2$. In particular,

$$\lambda^+ = \sum((q-1)/2)e_i = ((q-1)/2)\omega_n$$

is the highest dominant weight of W^+, and

$$\lambda^- = \sum((q-1)/2)e_i - e_n = \omega_{n-1} + ((q-3)/2)\omega_n$$

is the highest dominant weight in W^- [B, §13.3].

Let U_+ be the irreducible algebraic representation of $\mathrm{Sp}_{2n}(\overline{\mathbf{F}}_p)$ with highest weight $((p-1)/2)\omega_n$, and let U_- be the irreducible algebraic representation with highest weight $\omega_{n-1} + ((p-3)/2)\omega_n$. By the above remarks, the semisimplification of $W^+ \pmod p$ contains the irreducible representation $U_+ \otimes U_+^p \otimes U_+^{p^2} \otimes \cdots \otimes U_+^{p^{f-1}}$ and the semi-simplification of $W^- \pmod p$ contains $U_- \otimes U_+^p \otimes U_+^{p^2} \otimes \cdots \otimes U_+^{p^{f-1}}$.

But it is known that for $q = p$, $W^+ \equiv U_+$, and $W^- \equiv U_-$ are irreducible [ZS]. Hence $\dim U_\pm = ((p^n \pm 1)/2)$. By a dimension count, $W^\pm$ is not irreducible once $f > 1$. The autoduality of $U_\pm$ is determined by the action of the center -1_A of G: the representation is symplectic if -1_A acts nontrivially and orthogonal if -1_A acts trivially [St1, Lemmas 78, 79].

(4) The field $\mathbf{Q}(\chi)$ has real places iff $q \equiv 1 \pmod 4$, so we assume this is the case. Then -1_A acts as ± 1 on $W^{\pm}$. The space $\mathrm{Hom}_G(W, W^*)$ has dimension 2, and transpose is *not* a scalar on it: hence one of $W^{\pm}$ is obstructed and one is unobstructed over $\mathbf{R}$, by the Frobenius-Schur criterion [S3, Proposition 39]. But W^+ is a representation of $P\mathrm{Sp}_{2n}(q)$, which is unobstructed by [Go1, Go2]. An alternate argument is to reduce to the case of $\mathrm{SL}_2(q)$ using [Ge, Corollary 4.4].

Corollary 13.7. (1) *If $q \equiv 3 \pmod 4$, a representation $V^{\pm}$ with character $\chi^{\pm}$ can be defined over the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-p})$.*

(2) *If $q \equiv 1 \pmod 4$ but f is odd, a representation V^+ with character χ^+ can be defined over the real quadratic field $K = \mathbf{Q}(\sqrt{p})$. A representation V^- with character $2\chi^-$ can be defined over K, and $\mathrm{End}_{K[G]} V^-$ is the quaternion division algebra over K ramified at $\{\infty, \infty\}$.*

(3) *If q is a square, a representation V^+ with character χ^+ can be defined over $\mathbf{Q}$. A representation V^- with character $2\chi^-$ can be defined over $\mathbf{Q}$, and $\mathrm{End}_G V^-$ is the quaternion division algebra over $\mathbf{Q}$ ramified at $\{\infty, p\}$.*

Proof. We use the criterion in Lemma 4.1 to see that the character $\chi^{\pm}$ is unobstructed at all places of $\mathbf{Q}(\chi^{\pm}) = \mathbf{Q}(\chi)$ not dividing p and ∞ (χ^+ is unobstructed at 2 as the irreducible pieces in its decomposition have multiplicity one and the same field of definition as χ^+).

When $q \equiv 3 \pmod 4$ there is only one possible place $\mathfrak{p} = (\sqrt{-p})$ of K where $\chi^{\pm}$ can be obstructed. But any division algebra over K which splits outside $\mathfrak{p}$ is globally split, by the Hasse reciprocity law. Hence the characters $\chi^{\pm}$ are unobstructed.

When $q \equiv 1 \pmod 4$ the representation χ^+ can only be obstructed at $\mathfrak{p}$, so by the above argument is unobstructed. The representation χ^- is obstructed by a quaternion algebra, as $e_{\mathbf{R}}(\chi^-) = 2$, and the ramification of this algebra can be determined from the number of real places or $\mathbf{Q}(\chi^-)$ (it must ramify at an even number of places).

Proposition 13.8. (1) *If $p \equiv 3 \pmod 4$ there is a unique globally irreducible representation V of $G = \mathrm{Sp}_{2n}(p)$ of dimension $p^n - 1$ over $\mathbf{Q}$ with $\mathrm{End}_G(V) = \mathbf{Q}(\sqrt{-p})$. The reduction $V_{\mathfrak{p}}$ at the ramified prime $\mathfrak{p} = (\sqrt{-p})$ is $(-1)^{n-1}$-symmetric.*

(2) *If p is odd, there are two globally irreducible representations V of $G = \mathrm{Sp}_{2n}(p^2)$ of dimension $p^{2n} - 1$ over $\mathbf{Q}$, with $\mathrm{End}_G(V) = K$, the definite quaternion algebra ramified at $\{p, \infty\}$. These two representations are conjugate by the outer automorphism τ of G. The reduction $V_{\mathfrak{p}}$ at the ramified prime dividing p is symplectic.*

Proof. (1) V is the rational representation of G on the $\mathbf{Q}(\sqrt{-p})$ vector space V^- of Corollary 13.7. It is globally irreducible by Proposition 13.6. Its reduction is $(-1)^{n-1}$-symmetric, as -1_A acts as $-(\frac{-1}{p})^n = (-1)^{n-1}$ on V and $V_{\mathfrak{p}}$.

(2) V is the rational representation of G on V^- of Corollary 13.7. We muse check that the reduction $V_{\mathfrak{p}}$ is irreducible; in fact the argument in the proof of Proposition 13.6 (3) shows that we have an isomorphism of $k_{\mathfrak{p}}$ with $\mathbf{F}_{p^2}$ such that $V_{\mathfrak{p}} \simeq U_- \otimes U_+^p$. This representation is symplectic, as U_- and U_+ are both self-dual, with opposite parity.

Combining Proposition 13.8 with our basic construction of Hermitian RG-lattices, we obtain the following:

Corollary 13.9. *If $p \equiv 3 \pmod 4$ there are, up to isomorphism, $h = h(-p)$ Hermitian $R = \mathbf{Z} + \mathbf{Z}((1+\sqrt{-p})/2)$ lattices L in V which are stable under $G = \mathrm{Sp}_{2n}(p)$. These lattices have invariants*

$$\begin{cases} \operatorname{rank} L = p^n - 1, \\ \det L = \begin{cases} p^{(p^n-1)/2} & n \text{ odd}, \\ 1 & n \text{ even}. \end{cases} \end{cases}$$

When $n = 1$ these are Hecke's lattices, constructed in §11. In general, they are indexed canonically by elements of the class group of R, as the larger group $G' = G \rtimes \langle \tau \rangle$, where τ is the similitude with matrix $\left(\begin{smallmatrix} -1_n & 0_n \\ 0_n & 1_n \end{smallmatrix}\right)$, acts $\mathbf{Q}$-linearly on V.

Corollary 13.10. *Let p be odd, let R be a maximal order in the quaternion algebra K ramified at p and ∞ and let $G = \mathrm{Sp}_{2n}(p^2)$. Then there are $h_R (= 1$ or $2)$ Euclidean $\mathbf{Z}[G]$-lattices L up to isomorphism in V with $\mathrm{End}_G(L) = R$. These lattices have invariants:*

$$\begin{cases} \operatorname{rank} L = p^{2n} - 1, \\ \det L = 1. \end{cases}$$

We note that the sum over the conjugacy classes of maximal orders R in K of the weighted class numbers:

$$\sum_R h_R / w_R = \frac{p-1}{24} \tag{13.11}$$

by Eichler's mass formula [Ei] (cf. [V, Chapter V, §2]). Since $w_R = \mathrm{Card}(R^*) = 2$ for all but possibly 2 maximal orders, we have constructed about $(p-1)/12$ $\mathbf{Z}[G]$-lattices in V with $\mathrm{End}_G(L)$ a maximal order in K.

The unimodular lattices constructed in 13.9 are among the unimodular lattices constructed in 13.10. Indeed, the restriction of the Weil representation of $\mathrm{Sp}_{4n}(p)$ to the subgroup $\mathrm{Sp}_{2n}(p^2)$ stabilizing an $\mathbf{F}_{p^2}$-linear structure on A, is the Weil representation of $\mathrm{Sp}_{2n}(p^2)$. We obtain the unimodular lattices L of rank $p^{2n} - 1$ which are associated to those maximal orders R in the quaternion division algebra which contain the maximal order $\mathbf{Z} + \mathbf{Z}((1+\sqrt{-p})/2)$ of $\mathbf{Q}(\sqrt{-p})$. These special lattices have automorphisms by $\mathrm{Sp}_{4n}(p)$ commuting with $\sqrt{-p}$; I do not know their automorphism groups over $\mathbf{Z}$.

For example, take $n = 1$ and $p = 3$. The unique lattice constructed is the E_8-lattice, with automorphisms by $\mathrm{Sp}_4(3)$ commuting with $\sqrt{-3}$. When $p = 7$ the unique lattice constructed has rank 48, automorphisms by $\mathrm{Sp}_4(7)$ commuting with $\sqrt{-7}$, and shortest vector v satisfying $\langle v, v\rangle = 4$. A model for the lattices when $G = \mathrm{SL}_2(p^2)$ is due to Elkies. Let X be the hyperelliptic curve with equation $y^2 = x^{p^2} - x$ over $\mathbf{F}_{p^2}$, and let E be a supersingular ellip tic curve with Frobenius $= -p$ and $\mathrm{End}(E) = R$. Then $L = \mathrm{Mor}_{\mathbf{F}_{p^2}}(X, E)/$ translations $= \mathrm{Hom}_{\mathbf{F}_{p^2}}(J_X, E)$ with Hermitian form $\varphi(v, w) = \frac{1}{p} v \circ {}^t w$. Arguing as in 11.11, we obtain the estimate $\langle v, v\rangle \geq (p+1)/2$ for $v \neq 0$ in L, with equality holding for some $v \in L$ in the case when $p \equiv 3 \pmod 4$ and $j(E) = 1728$. The group $\mathrm{Sp}_4(p)$ acts on L when E can be defined over $\mathbf{F}_p$.

I know of no good model for the unimodular lattices with automorphisms by $\mathrm{Sp}_{2n}(p^2)$ (or $\mathrm{Sp}_{4n}(p)$) once $n > 1$. In particular, I have no estimate for their shortest vectors.

14. Examples: the unipotent cuspidal representation of $\mathrm{PU}_3(q)$

In this section, p is an arbitrary prime number and $q = p^f$. We let G be the finite group $\mathrm{PU}_3(q)$, the projective unitary group of a nondegenerate Hermitian form in 3-variables over $\mathbf{F}_{q^2}$. The group G has order $= (q^3+1)(q^3)(q^2-1)$ acts 2-transitively on the set of q^3+1 isotropic lines. It acts by algebraic automorphisms of the Fermat curve X with equation $x^{q+1} + y^{q+1} + z^{q+1} = 0$ in characteristic p; indeed this equation may be rewritten as $x\bar{x} + y\bar{y} + z\bar{z} = 0$ over $\mathbf{F}_{q^2}$, where $\bar{\alpha} = \alpha^q$ is the nontrivial involution of $\mathbf{F}_{q^2}$ over $\mathbf{F}_q$.

We let ψ denote the character of the irreducible cuspidal unipotent representation, of dimension $q(q-1)$, of G over $\mathbf{C}$ [Ca, §13.7]. Then $\mathbf{Q}(\psi) = \mathbf{Q}$, and for all $l \neq p$ a model for the representation with character ψ over $\mathbf{Q}_l$ is given by the action of G on the étale cohomology $H^1(X, \mathbf{Q}_l)$ of the Fermat curve over an algebraically closed field of characteristic p [HM]. It is known that $e_{\mathbf{R}}(\psi) = 2$; this follows from the Frobenius-Schur criterion, as G fixes the alternating form on $H^1(X)$ (cf. [L, Proposition 7.6]). Hence $e(\psi) = 2$ and ψ must be obstructed at p. We let V be the irreducible representation of dimension $2q(q-1)$ for G over $\mathbf{Q}$ with character 2ψ. Then $\mathrm{End}_G(V) = K$, the quaternion division algebra over $\mathbf{Q}$ ramified at p and ∞.

Proposition 14.1. *The representation V of $G = \mathrm{PU}_3(q)$ is irreducible over $\mathbf{R}$, and for all primes $l \neq p$ its reduction is irreducible over $k_l = M_2(\mathbf{Z}/l\mathbf{Z})$. If $\mathfrak{p}$ is the unique ramified prime in K, the reduction $V_{\mathfrak{p}}$ is irreducible over $k_{\mathfrak{p}} = \mathbf{F}_{p^2}$ if and only if $q = p$ or $q = p^2$. When $q = p$ the representation $V_{\mathfrak{p}}$ is an absolutely irreducible Hermitian representation: when $q = p^2$ the representation $V_{\mathfrak{p}}$ is symplectic and $\mathrm{End}_{k_{\mathfrak{p}}}(V_{\mathfrak{p}}) = \mathbf{F}_{p^4}$.*

Proof. We have already seen that V is irreducible over $\mathbf{R}$. It is irreducible $(\mathrm{mod}\, l)$ by the results of §4, as $\psi \equiv \rho$ is an absolutely irreducible Brauer character for all primes $l \neq p$. This follows from the fact that $q(q-1)$ is the smallest dimension of an absolutely irreducible, nontrivial representation of G in any characteristic $\neq p$ [LS]. One can prove it directly by restricting to a Borel subgroup fixing an isotropic line, as in Proposition 11.2.

When $l = p$, the representation with character ψ over the Witt vectors W_{q^2} of $\mathbf{F}_{q^2}$ is given by the action of G on the crystalline cohomology group $H^1(X, W_{q^2})$. The representation of G with character ψ $(\mathrm{mod}\, p)$ is therefore given by the action of automorphisms on the de Rham cohomology, $H^1_{dR}(X, \mathbf{F}_{q^2}) = H^1(X, W_{q^2})/pH^1(X, W_{q^2})$. We have then an isomorphism of G-modules over $\mathbf{F}_{q^2}$:

$$V_{\mathfrak{p}} \otimes_{\mathbf{F}_{p^2}} \mathbf{F}_{q^2} \simeq H^0(X, \Omega^1/\mathbf{F}_{q^2}). \tag{14.2}$$

On the other hand, it is easy to see that the representation of G on holomorphic differentials on X is isomorphic to $\mathrm{Sym}^{q-2}(U) \otimes \det U$, where U is the standard three-dimensional representation of $U_3(q)$ over $\mathbf{F}_{q^2}$. The differentials

$$\omega_{m,n} = x^m y^n d(x/y^q) \quad \text{with } 0 \leq m, n \text{ and } m+n \leq q-2 \tag{14.3}$$

give a basis, and are eigenvectors for the torus T of $\mathrm{PU}_3(q)$ consisting of transformations $(x, y, z) \mapsto (\alpha x, \beta y, \gamma z)$ with $\alpha^{q+1} = \beta^{q+1} = \gamma^{q+1} = 1$. The eigenvalue of this transformation on $\omega_{m,n}$ is equal to $\alpha^{m+1}\beta^{n+1}\gamma^{s+1}$ with $m+n+s = q-2$, and these are the weights in the representation $\mathrm{Sym}^{q-2}(U) \otimes \det U$.

The highest weight in the representation Sym^{q-2} is equal to $(q-2)\omega_1 = (p-2)\omega_1 + (p-1)p\omega_1 + \cdots + (p-1)p^{f-1}\omega_1$. By the theory of irreducible representations of $U_3(q)$ in characteristic p, $V_{\mathfrak{p}} \otimes \mathbf{F}_{q^2}$ contains an irreducible factor

$$\mathrm{Sym}^{p-2}(U) \otimes \mathrm{Sym}^{p-1}(U^p) \otimes \mathrm{Sym}^{p-1}(U^{p^2}) \otimes \cdots \otimes \mathrm{Sym}^{p-1}(U^{p^{f-1}}) \otimes \det U \tag{14.4}$$

with this highest weight [St2]. The representation $V_{\mathfrak{p}}$ is irreducible over F_{p^2} if and only if all its irreducible factors over $\mathbf{F}_{q^2}$ are conjugate to (14.4). This occurs iff $q = p, p^2$ by a dimension count. When $q = p$, $V_{\mathfrak{p}} \simeq \mathrm{Sym}^{p-2}(U) \otimes \det U$ is an absolutely irreducible Hermitian representation. When $q = p^2$, $V_{\mathfrak{p}}$ is the restriction to $\mathbf{F}_{p^2}$ of the representation $\mathrm{Sym}^{p-2}(U) \otimes \mathrm{Sym}^{p-1}(U^p) \otimes \det U$ over $\mathbf{F}_{p^4}$; this is self-dual over $\mathbf{F}_{p^2}$.

Corollary 14.5. *Let $q = p$ or p^2 and let V be the globally irreducible representation of $G = \mathrm{PU}_3(q)$ over $\mathbf{Q}$ of dimension $2q(q-1)$. Let R be a maximal order in the quaternion division algebra ramified at p and ∞. There are h_R $(= 1$ or $2)$ Euclidean $\mathbf{Z}[G]$ lattices L in V up to isomorphism with $\mathrm{End}_G(L) = R$.*

These lattices have invariants

$$\operatorname{rank}(L) = 2q(q-1),$$

$$L^* = \begin{cases} \mathfrak{p}^{-1}L, & \det L = p^{p(p-1)} \quad \text{if } q = p, \\ L, & \det L = 1 \quad \text{if } q = p^2. \end{cases}$$

A model for the lattices L constructed in Corollary 14.5 has been obtained by Elkies. Let E be a supersingular elliptic curve over $\mathbf{F}_{q^2}$ with Frobenius endomorphism equal to $-q$ and $\operatorname{End}(E) \simeq R$, and recall that X is the Fermat curve of exponent $(q+1)$. Then

$$\begin{aligned} L &= \operatorname{Mor}_{\mathbf{F}_{q^2}}(X, E)/\text{ translations} \\ &= \operatorname{Hom}_{\mathbf{F}_{q^2}}(J_X, E). \end{aligned} \tag{14.6}$$

When $q = p$, the Hermitian form $\varphi(v, w) = v \circ {}^t w$ is nondegenerate on $\operatorname{Hom}(J_X, E)$. We have $\varphi(v, v) = \deg v$ where $v: X \to E$ is the associated covering. Since X has $p^3 + 1$ points over $\mathbf{F}_{p^2}$, and E has $(p+1)^2$ points over $\mathbf{F}_{p^2}$, we have the estimate

$$\langle v, v \rangle \geq 2(p-1) \tag{14.7}$$

for all $v \neq 0$ in L. When $p = 2$, L is therefore isomorphic to the D_4-lattice, and when $p = 3$, L is isomorphic to the Coxeter-Todd lattice of rank 12.

When $q = p^2$, the natural Hermitian form $\varphi(v, w) = v \circ {}^t w$ on $\operatorname{Hom}(J_X, E)$ gives a bilinear form with determinant $p^{2q(q-1)} = p^{\operatorname{rank}(L)}$. Hence the form giving a unimodular L is equal to φ/p, which takes values in $\mathfrak{p}^{-1}R$. In particular, $\varphi(v, v)/p$ is integral, so the degree of any covering $v: X \to E$ is divisible by p! Counting points as above, we find

$$\langle v, v \rangle \geq 2p \tag{14.8}$$

for all $v \neq 0$ in L, where $\langle\ ,\ \rangle$ is the pairing under which $L^* = L$ is unimodular. When $p = 2$, L is the Leech lattice of rank 24.

For $q = p^f$ arbitrary, one can consider the Mordell-Weil lattice of (14.6); this has an action of $G = \mathrm{PU}_3(q)$ through its unipotent cuspidal representation, but the reduction is *not* irreducible at $\mathfrak{p}$ once $f \geq 3$. The conjecture of Birch and Swinnerton-Dyer for the elliptic curve E over the function field $k = \mathbf{F}_{q^2}(X)$, which in this case is a theorem due to Tate [Ta2] and Milne [M], gives the identity:

$$\det L \cdot \#Ш(E/k) = q^{p(p-1)}, \tag{14.9}$$

where $\det L$ is calculated for the Euclidean structure $\langle v, w \rangle = \operatorname{Tr} \varphi(v, w) = v \circ {}^t w + w \circ {}^t v$ and $Ш(E/k)$ is the Tate-Shafarevitch group.

Proposition 14.10. *The group $Ш(E/k)$ is trivial if and only if $f \leq 2$ (that is, $q = p$ or $q = p^2$). The subgroup $Ш(E/k)_\pi$ which is annihilated by the isogeny $\pi: E \to E^{(p)}$ of degree p has order q^{2d}/p^{2g}, where $d = \frac{1}{4}q(p-1)(q/p+1)$ is the*

dimension of the space of exact holomorphic differentials on X *and* $g = \frac{1}{2}q(q-1)$ *is the genus of* X.

Proof. By formula (14.9) we see that $Ш(E/k)$ is a p-group, so it is trivial if and only if $Ш(E/k)_\pi = 0$. We calculate $Ш(E/k)_\pi$ from a first π-descent; it is the cokernel of the injection:

$$E^{(p)}(k)/\pi E(k) \hookrightarrow \mathrm{Sel}_\pi(E/k) = H^1(X, \alpha_p).$$

The first group has order p^{2g}, as it is an $\mathbf{F}_{p^2}$ vector space of dimension $g = \frac{1}{4}\operatorname{rank} L$. The Selmer group is an $\mathbf{F}_{q^2}$ vector space of dimension $d \leq g$. A calculation of the Cartier operator C on X shows that $\omega_{m,n} = x^m y^n d(x/y^q)$ is exact (that is, $C\omega_{m,n} = 0$) if an only if $m \equiv m_0$, $n \equiv n_0 \pmod{p-1}$ with $0 \leq m_0, n_0 \leq p-1$ and $m_0 + n_0 \leq p-2$. This gives the above formula for d.

Note 14.11. One can show that $C^f = 0$ on $H^0(X, \Omega^1)$, where $q = p^f$. The irreducible summand with highest weight $(q-2)\omega_1$ described in (14.4) is exactly the image of C^{f-1}.

15. A SUMMARY OF THE EVEN UNIMODULAR LATTICES CONSTRUCTED

We tabulate the relevant invariants of the even unimodular lattices L we have constructed from globally irreducible representations V in §§12–14. In each case, $\mathrm{End}_G(V) = K$ is a quaternion algebra ramified in a set S of two rational places. In the following table p is a prime and $n \geq 1$ is an integer.

§	G	rank L	short vectors $v \neq 0$ in L	$S =$ ramified places
14	$\mathrm{PU}_3(p^2)$	$2p^2(p^2-1)$	$\langle v, v\rangle \geq 2p$	$\{p, \infty\}$
13	$\mathrm{Sp}_{2n}(p^2)$ $p \neq 2$	$p^{2n}-1$	$\langle v, v\rangle \geq \frac{p+1}{2}$ $n=1$ $\geq ??$ $n \geq 2$	$\{p, \infty\}$
12	$2^{1+4n} \cdot O_{4n}^-(2)$	2^{2n+1}	$\langle v, v\rangle \geq 2^n$	$\{2, \infty\}$

ACKNOWLEDGMENTS

It is a great pleasure to thank Noam Elkies for introducing me to the subject of lattices and sphere packings, and for his many helpful suggestions on this paper. I have also profited from conversation and correspondence with E. Bayer, J. Bernstein, W. Feit, J. Humphreys, J. McKay, J.-P. Serre, T. Shioda, J. Thompson, and G. van der Geer.

BIBLIOGRAPHY

[A] A. Adler, *Some integral representations of* $\mathrm{PSL}_2(\mathbf{F}_p)$ *and their applications*, J. Algebra **72** (1981), 115–145.

[B] N. Bourbaki, *Groupes et algèbres de Lie*, Chapitres VII–VIII, Hermann, Paris 1975.

[BE] M. Broué and M. Enguehard, *Une famille infinie de formes quadratiques entières; leurs groupes d'automorphismes*, Ann. Sci. École Norm. Sup. **6** (1973), 17–52.

[Ca] R. Carter, *Finite groups of Lie type*, John Wiley, New York, 1985.

[C] J. H. Conway, et al., ATLAS *of finite groups*, Clarendon Press, Oxford, 1985.

[CS] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren Math. Wiss., vol. 290, Springer-Verlag, Berlin and New York, 1988.

[Ei] M. Eichler, *Über die Klassenzahl total definiter quaternionenalgebren*, Math. Z. **43** (1937), 102–109.

[E] N. Elkies, Letters to N. J. Sloane, 15 August 1989, 15 September 1989.

[F1] W. Feit, *The computations of some Schur indices*, Israel J. Math. **46** (1983), 274–300.

[F2] ____, *The representation theory of finite groups*, North-Holland, Amsterdam, 1982.

[Ge] P. Gérardin, *Weil representations associated to finite fields*, J. Algebra **46** (1977), 54–101.

[Go1] R. Gow, *Schur indices of some groups of Lie type*, J. Algebra **42** (1976), 102–120.

[Go2] ____, *On the Schur indices of characters of finite classical groups*, J. London Math. Soc. **24** (1981), 135–147.

[Gr] R. Greiss, *Automorphisms of extra-special groups and non-vanishing degree* 2 *cohomology*, Pacific J. Math. **48** (1973), 403–422.

[H] E. Hecke, *Über ein fundamentalproblem aus der theorie der Elliptischen modulfunktionen*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 235–257 (= Werke 28).

[HM] R. Hotta and K. Matsui, *On a lemma of Tate-Thompson*, Hiroshima Math. J. **8** (1978), 255–268.

[Hu] J. E. Humphreys, *Representations of* SL(2, p), Amer. Math. Monthly **82** (1975), 21–39.

[K] G. Karpilovsky, *The Schur multiplier*, London Math. Soc. Monographs vol. 2, Clarendon Press, Oxford, 1987.

[LS] V. Landazurri and J. Seitz, *On the minimal degrees of projective representations of finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

[L] G. Lusztig, *Coxeter orbits and eigenspaces of Frobenius*, Invent. Math. **38** (1976), 101–159.

[Ma] B. Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. **14** (1986), 207–259.

[M] J. Milne, *The Tate-Šafarevič group of a constant abelian variety*, Invent. Math. **6** (1968), 91–105.

[MH] J. Milnor and D. Husemoller, *Symmetric bilinear forms*, Ergeb. Math. Grenzgeb., vol. 73, Springer-Verlag, Berlin and New York, 1973.

[Q] D. Quillen, *The* mod 2 *cohomology rings of extra-special* 2*-groups and the spinor groups*, Math. Ann. **194** (1977), 197–212.

[Sch] B. Schoeneberg, *Elliptic modular functions*, Grundlehren Math. Wiss., vol. 203, Springer-Verlag, Berlin, 1974.

[S1] J.-P. Serre, *Complex multiplication*, Algebraic Number Theory (J.W.S. Cassels and A. Frohlich, eds.), Academic Press, New York, 1967, pp. 292–296.

[S2] ____, *A course in arithmetic*, Graduate Texts in Math., vol. 7, Springer-Verlag, Berlin and New York, 1973.

[S3] ____, *Linear representations of finite groups*, Graduate Texts in Math., vol. 42, Springer-Verlag, Berlin and New York, 1977.

[Sh1] T. Shioda, *Mordell-Weil lattices and Galois representations*. I, II, III, Proc. Japan Acad. **65** (1989), 268–271; 296-299; 300–303.

[Sh2] ____, *Mordell-Weil lattices and sphere packings*, preprint, 1989.

[St1] R. Steinberg, *Lectures on Chevalley groups*, Yale Univ. Press, 1967.

[St2] ____, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33–56.

[Ta1] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Ta2] ——, *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog*, Sém. Bourbaki **306** 1965–1966.

[Th1] J. G. Thompson, *A simple subgroup of* $E_8(3)$, Finite Groups (N. Iwahori, ed.), Tokyo, 1976, pp. 113–116.

[Th2] ——, *Finite groups and even lattices*, J. Algebra **38** (1976), 523–524.

[V] M.-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., vol. 800, Springer-Verlag, Berlin and New York, 1980.

[VV] G. van der Geer and M. van der Vlugt, *Reed-Muller codes and supersingular curves*, Ann. École. Norm. Sup. (to appear).

[ZS] A. E. Zalesskii and I. D. Suprunenko, *Representations of dimension* $((p^n \pm 1)/2)$ *of a symplectic group of degree* $2n$ *over a field of characteristic* p, Vestsī Akad. Navuk BSSR Ser. Fiz.-Math. Navuk **6** (1987), 9–15.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138