Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 305 (2006) 562–576
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Finite linear groups, lattices, and products of elliptic curves

Vladimir L. Popov [a,1], Yuri G. Zarhin [b,c,*,2]

[a] *Steklov Mathematical Institute, Russian Academy of Sciences, Gubkina 8, 119991 Moscow, Russia*
[b] *Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA*
[c] *Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, Russia*

Received 21 September 2005
Available online 11 May 2006
Communicated by Michel Broué

Abstract

Let V be a finite-dimensional complex linear space and G an irreducible finite subgroup of $\mathrm{GL}(V)$. For a G-invariant lattice Λ in V of maximal rank, we describe the structure of complex torus V/Λ.

1. Introduction

Studying complex tori (in particular, abelian varieties) with finite group actions (and, more generally, with certain endomorphisms) is a subject matter of several recent papers: see, e.g., [DL, LR, Vo]. In particular, it is a starting point for examples of compact Kähler manifolds that do not have the homotopy type of projective complex manifolds [Vo]. Among such tori, abelian varieties are of a special interest. For instance, they arise as the Jacobians of smooth projective curves with group actions. These actions induce decompositions of Jacobians up to isogeny. For hyperelliptic curves, such decompositions go back to classical interest in hyperelliptic integrals expressible in

* Corresponding author.
E-mail addresses: popovvl@orc.ru (V.L. Popov), zarhin@math.psu.edu (Yu.G. Zarhin).
[1] Supported in part by ETH, Zürich (Switzerland), Russian grants РФФИ 05-01-00455, НШ-9969.2006.1, and a (granting) program of the Mathematics Branch of the Russian Academy of Sciences.
[2] Partially supported by the MSRI.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.04.007

terms of elliptic integrals, because the problem boils down to decomposing Jacobians, up to isogeny, as products of elliptic curves.

Complex tori with group actions arise in the following way. Let V be a complex linear space of nonzero dimension $n < \infty$ and let G be a finite subgroup of $\mathrm{GL}(V)$. If there is a G-invariant lattice Λ in V of rank $2n$ (hereinafter a *lattice* is a discrete additive subgroup of a complex or real linear space), then V/Λ is a complex torus with G-action. This naturally leads to the following questions: (1) when is there a G-invariant lattice Λ of rank $2n$? (2) if Λ exists, when is V/Λ an abelian variety? (3) if Λ exists and V/Λ is an abelian variety, what can one say about decomposition of V/Λ, up to isogeny? Note that the Riemann condition reduces (2) to the linear algebra problem: when is there a *polarization* of V/Λ, i.e., a positive definite Hermitian bilinear form $V \times V \to \mathbf{C}$, whose imaginary part takes integral values on $\Lambda \times \Lambda$?

In this paper we answer these questions for irreducible G. In Theorem 2.6, we give a criterion (in terms of the character and the Schur $\mathbf{Q}$-index of the G-module V) of the existence of a nonzero G-invariant lattice Λ in V. The structure of complex torus V/Λ is described in Theorems 3.1 and 4.1. In particular, we prove that in the majority of cases (but not in all) V/Λ is an abelian variety. Moreover, we show that if the latter holds, then in many cases V/Λ is isogenous to a self-product of an elliptic curve or even isomorphic to a product of mutually isogenous elliptic curves with complex multiplication, while in the other cases, V/Λ is isogenous to a self-product of an abelian surface. We prove (Theorem 4.1 and Example 4.3) that G and Λ such that the complex torus V/Λ is not an abelian variety do exist, but one can always replace Λ by another G-invariant lattice Δ such that V/Δ is a product of mutually isogenous elliptic curves with complex multiplication (Theorem 4.6).

1.1. Notation and terminology

$\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{F}_q$, and $\mathbf{H}$ are respectively the ring of integers, the field of rational numbers, the field of real numbers, the field of complex numbers, the finite field that consists of q elements, and the Hamiltonian quaternion $\mathbf{R}$-algebra $(\frac{-1,-1}{\mathbf{R}})$.

The identity map of a set S is denoted by id_S.

$\mathbf{Z}[S]$ is the subring of $\mathbf{C}$ generated by a subset S of $\mathbf{C}$. For a subring A of $\mathbf{C}$ and a subset P of a complex linear space W, the A-submodule of W generated by P is denoted by AP. If $K/\mathbf{Q}$ is a field extension and A is a $\mathbf{Q}$-algebra, we denote by A_K the K-algebra $A \otimes_{\mathbf{Q}} K$ and naturally identify A with $A \otimes 1$.

If P is a subset of $\mathrm{End}_{\mathbf{C}}(V)$, then we put $\mathrm{Tr}(P) := \{\mathrm{tr}(g) \mid g \in P\}$.

$\mathrm{M}_r(R)$ is the algebra of $r \times r$-matrices over a ring R (associative and with identity element), I_r is the identity matrix of $\mathrm{M}_r(R)$, and R^d is the space of column vectors over R of height d.

If G is a finite subgroup of $\mathrm{GL}(V)$, then $\chi_{G,V}$ (respectively, $\mathrm{Schur}_{G,V}$) is the character (respectively, the Schur index with respect to $\mathbf{Q}$) of G-module V and $\mathbf{Q}(\chi_{G,V})$ is the field generated over $\mathbf{Q}$ by $\mathrm{Tr}(G)$. We have $G \subset \mathbf{Z}G \subset \mathbf{R}G \subset \mathbf{C}G \subset \mathrm{End}_{\mathbf{C}}(V)$.

Z_G is the center of $\mathbf{Q}$-algebra $\mathbf{Q}G$. If $\mathbf{Q}(\chi_{G,V})$ is $\mathbf{Q}$ (respectively, an imaginary quadratic number field), then the character $\chi_{G,V}$ is called *rational* (respectively, *imaginary quadratic*). The G-module V is called *orthogonal* (respectively, *symplectic*) if there is a symmetric (respectively, skew-symmetric) nondegenerate G-invariant bilinear form $V \times V \to \mathbf{C}$.

If Π is a lattice (i.e., a discrete additive subgroup) of rank $2\dim_{\mathbf{C}}(W)$ in a nonzero finite-dimensional complex linear space W, then the endomorphism ring of complex torus W/Π is $\mathrm{End}(W/\Pi) := \{u \in \mathrm{End}_{\mathbf{C}}(W) \mid u(\Pi) \subseteq \Pi\}$, and the $\mathbf{Q}$-algebra $\mathrm{End}^0(W/\Pi) := \mathrm{End}(W/\Pi) \otimes \mathbf{Q}$ is the *endomorphism algebra of* W/Π, see [OZ].

2. Some generalities

Let G be an irreducible finite subgroup of $\mathrm{GL}(V)$, i.e.,

$$\mathbf{C}G = \mathrm{End}_{\mathbf{C}}(V). \tag{1}$$

It is well known that $Z_G \subset \mathbf{C}\,\mathrm{id}_V$ is a field and $\mathbf{Q}G$ is a finite-dimensional central simple Z_G-algebra [D, pp. 124–125]; in particular, there is a central division Z_G-algebra D and an integer $r > 0$ such that

$$\mathbf{Q}G \simeq \mathrm{M}_r(D) \quad \text{(isomorphism of } Z_G\text{-algebras)}. \tag{2}$$

Below we shall naturally identify $\mathbf{C}\,\mathrm{id}_V$ with $\mathbf{C}$, and Z_G with the corresponding subfield of $\mathbf{C}$.

Lemma 2.1.

(i) *The natural* $\mathbf{C}$*-algebra homomorphism*

$$\psi : \mathbf{Q}G \otimes_{Z_G} \mathbf{C} \to \mathbf{C}G = \mathrm{End}_{\mathbf{C}}(V) \tag{3}$$

is an isomorphism. In particular, $n^2 = \dim_{Z_G}(\mathbf{Q}G) = r^2 \dim_{Z_G}(D)$.

(ii) $Z_G = \mathbf{Q}(\chi_{G,V})$.

(iii) $\mathrm{Schur}_{G,V} = \sqrt{\dim_{\mathbf{Q}(\chi_{G,V})} D}$. *In particular, the* Z_G*-algebras* $\mathbf{Q}G$ *and* $\mathrm{M}_n(Z_G)$ *are isomorphic if and only if* $\mathrm{Schur}_{G,V} = 1$.

(iv) *If* $\chi_{G,V}$ *is real valued, then* $\mathrm{Schur}_{G,V} \leqslant 2$.

(v) *Suppose that the greatest common divisor of the integers* $\dim_{\mathbf{C}}(\ker(u))$*, where* u *runs through* $\mathbf{Q}G$*, is equal to* 1*. Then* $\mathrm{Schur}_{G,V} = 1$.

Proof. Since $\mathbf{Q}G \otimes_{Z_G} \mathbf{C}$ is a simple $\mathbf{C}$-algebra, ψ is injective; (1) implies that ψ is surjective. This proves (i). Claims (ii) and (iii) are well known ([D, Lemma 24.7], [CR, (70.13)]). Claim (iv) is the result of R. Brauer and A. Speiser [F, Corollary 2.4, p. 277]. Claim (v) follows from (ii), (iii), and [Vi, Lemma 3]. □

Clearly, $\mathbf{Z}G$ is an order in $\mathbf{Q}G$; in particular, $\mathbf{Z}G$ is a free $\mathbf{Z}$-module of rank $\dim_{\mathbf{Q}}(\mathbf{Q}G)$. It is clear as well that $Z_G \cap \mathbf{Z}G$ is an order in Z_G; in particular, it is a free $\mathbf{Z}$-module of rank $\dim_{\mathbf{Q}} Z_G$.

Lemma 2.2. [Po, Section 3.1] *If* Λ *is a nonzero* G*-invariant lattice in* V*, then* $\mathrm{rk}(\Lambda) = n$ *or* $2n$.

Proof. Since $\mathbf{C}\Lambda = \mathbf{R}\Lambda + i\mathbf{R}\Lambda$ and $\mathbf{R}\Lambda \cap i\mathbf{R}\Lambda$ are G-invariant, the irreducibility of G yields $\mathbf{C}\Lambda = V$, and $\mathbf{R}\Lambda \cap i\mathbf{R}\Lambda = \{0\}$ or V. Since $\dim_{\mathbf{R}} \mathbf{R}\Lambda = \dim_{\mathbf{R}} i\mathbf{R}\Lambda = \mathrm{rk}(\Lambda)$, in the first case, $2n = \dim_{\mathbf{R}} V = \dim_{\mathbf{R}} \mathbf{R}\Lambda + \dim_{\mathbf{R}} i\mathbf{R}\Lambda = 2\,\mathrm{rk}(\Lambda)$, and in the second, $2n = \dim_{\mathbf{R}} V = \dim_{\mathbf{R}} \mathbf{R}\Lambda = \mathrm{rk}(\Lambda)$. □

Lemma 2.3. *Suppose that there exists a nonzero* G*-invariant lattice* Λ *in* V*. Then*:

(i) $\chi_{G,V}$ *is either rational or imaginary quadratic*;

(ii) *if* $\chi_{G,V}$ *is not rational, then* Z_G *is an imaginary quadratic field,* $\mathrm{rk}(\Lambda) = 2n$*, and* $\mathrm{Schur}_{G,V} = 1$.

Proof. Pick a nonzero element $v \in \Lambda$. Since Λ is G-invariant, it is also $\mathbf{Z}G$-invariant, and in particular, $Z_G \cap \mathbf{Z}G$-invariant. Since Z_G consists of scalars, $(Z_G \cap \mathbf{Z}G)v \subseteq \Lambda \cap \mathbf{C}v$; whence $Z_G \cap \mathbf{Z}G$ is a nonzero lattice in $\mathbf{C}$. Therefore $\dim_{\mathbf{Q}} Z_G \leqslant 2$, i.e., Z_G is either $\mathbf{Q}$ or a quadratic number field. Since the orders of every real quadratic number field are not discrete in $\mathbf{C}$ [BS, Chapter II, Section 7], claim (i) follows from Lemma 2.1(ii).

Assume now that $\chi_{G,V}$ is not rational. Then the assertion about Z_G follows from (i) and Lemma 2.1(ii). The $\mathbf{Q}$-linear space $\mathbf{Q}\Lambda$ carries a natural structure of Z_G-linear space, and (i) implies that $\dim_{Z_G}(\mathbf{Q}\Lambda) = \dim_{\mathbf{Q}}(\mathbf{Q}\Lambda)/2 = \mathrm{rk}(\Lambda)/2$. Since $\mathbf{Q}\Lambda$ is $\mathbf{Q}G$-stable, we get a Z_G-algebra homomorphism $\varphi : \mathbf{Q}G \to \mathrm{End}_{Z_G}(\mathbf{Q}\Lambda)$. Since $\varphi(1) = \mathrm{id}_{\mathbf{Q}\Lambda}$ and $\mathbf{Q}G$ is simple, φ is injective. This and Lemma 2.1(i) then imply $n^2 = \dim_{Z_G}(\mathbf{Q}G) \leqslant (\dim_{Z_G}(\mathbf{Q}\Lambda))^2 = (\mathrm{rk}(\Lambda)/2)^2 \leqslant n^2$. Hence $\mathrm{rk}(\Lambda) = 2n$ and φ is an isomorphism. The latter and Lemma 2.1(iii) imply that $\mathrm{Schur}_{G,V} = 1$. □

Lemma 2.4. *Suppose that $\chi_{G,V}$ is rational and* $\mathrm{Schur}_{G,V} \neq 1$. *Then D is a quaternion* $\mathbf{Q}$-*algebra, $n = 2r$, and exactly one of the following two possibilities holds*:

(i) *the G-module V is orthogonal and D is indefinite, i.e., $D_{\mathbf{R}}$ is* $\mathbf{R}$-*isomorphic to* $\mathrm{M}_2(\mathbf{R})$;
(ii) *the G-module V is symplectic and D is definite, i.e., $D_{\mathbf{R}}$ is* $\mathbf{R}$-*isomorphic to* $\mathbf{H}$.

Proof. Since $\chi_{G,V}$ is rational and $\mathrm{Schur}_{G,V} \neq 1$, Lemma 2.1(ii), (iv) imply that $Z_G = \mathbf{Q}$ and $\mathrm{Schur}_{G,V} = 2$. By Lemma 2.1(iii), this yields $\dim_{\mathbf{Q}}(D) = 4$. Since D is a division $\mathbf{Q}$-algebra, the latter equality implies that D is a quaternion $\mathbf{Q}$-algebra [Pi, §13.1]. Lemma 2.1(i) now implies that $n^2 = 4r^2$, i.e., $n = 2r$.

Since the $\mathbf{R}$-algebra $\mathbf{Q}G_{\mathbf{R}}$ is simple, the natural surjection $\mathbf{Q}G_{\mathbf{R}} \to \mathbf{R}G$ is an isomorphism of $\mathbf{R}$-algebras. Clearly, the linear group G is defined over $\mathbf{R}$ if and only if $\mathbf{R}G$ is isomorphic to $\mathrm{M}_n(\mathbf{R})$. Taking into account the $\mathbf{R}$-algebra isomorphisms $\mathbf{Q}G_{\mathbf{R}} \simeq \mathrm{M}_{n/2}(D)_{\mathbf{R}} \simeq \mathrm{M}_{n/2}(D_{\mathbf{R}})$, from this we deduce that G is defined over $\mathbf{R}$ if and only if D indefinite. Since a self-dual simple G-module is defined over $\mathbf{R}$ if and only if it is orthogonal [Se, Section 13.2], this completes the proof. □

Theorem 2.5. *Suppose that n is even and there exists a quaternion* $\mathbf{Q}$-*algebra H such that the* $\mathbf{Q}$-*algebras* $\mathbf{Q}G$ *and* $\mathrm{M}_{n/2}(H)$ *are isomorphic. Then*

(i) *for each imaginary quadratic subfield F of H, there exists a G-invariant lattice $\Lambda^{(F)}$ in V of rank $2n$ such that the complex torus $V/\Lambda^{(F)}$ is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication by an order of F*;
(ii) *there exists a G-invariant lattice Λ in V of rank $2n$ such that the* $\mathbf{Q}$-*algebras* $\mathrm{End}^0(V/\Lambda)$ *and* $\mathrm{M}_{n/2}(H)$ *are isomorphic.*

Proof. Clearly, $Z_G = \mathbf{Q}$. Fix an isomorphism of $\mathbf{Q}$-algebras $\tau : \mathbf{Q}G \to \mathrm{M}_{n/2}(H)$. The $\mathbf{Q}$-linear space $H^{n/2}$ carries a natural structure of *left* $\mathrm{M}_{n/2}(H)$-module. Fix in $H^{n/2}$ a nonzero $\tau(\mathbf{Z}G)$-stable finitely generated additive subgroup Π (for instance, take $\Pi = \tau(\mathbf{Z}G) \cdot v$ for a nonzero vector $v \in H^{n/2}$). Since $H^{n/2}$ is a $\mathbf{Q}$-linear space, Π is a free abelian group of finite rank and every its basis consists of linearly independent elements of $H^{n/2}$. Since the linear subspace $\mathbf{Q}\Pi$

of $H^{n/2}$ is stable with respect to $\mathbf{Q}\tau(\mathbf{Z}G) = \tau(\mathbf{Q}G) = \mathrm{M}_{n/2}(H)$, we have $\mathbf{Q}\Pi = H^{n/2}$. Hence the natural map is an isomorphism of $\mathbf{Q}$-linear spaces

$$\Pi_{\mathbf{Q}} := \Pi \otimes \mathbf{Q} \xrightarrow{\simeq} H^{n/2}. \tag{4}$$

The $\mathbf{Q}$-linear space $H^{n/2}$ carries also a natural structure of *right* H-module. The structures of left $\mathrm{M}_{n/2}(H)$-module and right H-module on $H^{n/2}$ yield the $\mathbf{Q}$-linear embeddings of respectively $\mathrm{M}_{n/2}(H)$ and H into $\mathrm{End}_{\mathbf{Q}}(H^{n/2})$. By Wedderburn's theorem [La1, Chapter XVII, §3, Corollary 3], the images of these embeddings are the centralizers of each other in $\mathrm{End}_{\mathbf{Q}}(H^{n/2})$.

Put $\Pi_{\mathbf{R}} := \Pi \otimes \mathbf{R}$ and naturally identify Π with $\Pi \otimes 1$. By (4), the following isomorphisms of $\mathbf{R}$-linear spaces hold: $\Pi_{\mathbf{R}} \simeq (H^{n/2})_{\mathbf{R}} \simeq (H_{\mathbf{R}})^{n/2}$. Hence $\Pi_{\mathbf{R}}$ is a $2n$-dimensional $\mathbf{R}$-linear space that carries the natural structures of left $\mathrm{M}_{n/2}(H_{\mathbf{R}})$-module and right $H_{\mathbf{R}}$-module, and Π is a *lattice* in $\Pi_{\mathbf{R}}$ of rank $2n$. These structures yield the $\mathbf{R}$-linear embeddings

$$\iota_l : \mathrm{M}_{n/2}(H_{\mathbf{R}}) \hookrightarrow \mathrm{End}_{\mathbf{R}}(\Pi_{\mathbf{R}}), \qquad \iota_r : H_{\mathbf{R}} \hookrightarrow \mathrm{End}_{\mathbf{R}}(\Pi_{\mathbf{R}})$$

whose images are the centralizers of each other in $\mathrm{End}_{\mathbf{R}}(\Pi_{\mathbf{R}})$.

Since elements of G are invertible in $\mathbf{Q}G$, composition of the following embeddings of $\mathbf{Q}$-algebras

$$\mathbf{Q}G \xrightarrow[\simeq]{\tau} \mathrm{M}_{n/2}(H) \overset{\mathrm{id}}{\hookrightarrow} \mathrm{M}_{n/2}(H_{\mathbf{R}}) \overset{\iota_l}{\hookrightarrow} \mathrm{End}_{\mathbf{R}}(\Pi_{\mathbf{R}}) \tag{5}$$

embeds G into the group of invertible elements of $\mathrm{End}_{\mathbf{R}}(\Pi_{\mathbf{R}})$. This defines an $\mathbf{R}$-linear action of G on $\Pi_{\mathbf{R}}$. By construction, the lattice Π in $\Pi_{\mathbf{R}}$ is G-invariant.

We want to define on the real linear space $\Pi_{\mathbf{R}}$ a structure of complex linear space in such a way that the algebra of its $\mathbf{C}$-linear transformations contains $\iota_l(\mathrm{M}_{n/2}(H_{\mathbf{R}}))$. In order to do this, choose an element $c \in H_{\mathbf{R}}$ with $c^2 = -1$: using that $\mathbf{R}$-algebra $H_{\mathbf{R}}$ is isomorphic to either $\mathbf{H}$ or $\mathrm{M}_2(\mathbf{R})$ (see, e.g., [Pi, §§1.7, 13.2]), it is easy to see that such c exists and, moreover, since $(aca^{-1})^2 = -1$ for every invertible element a of $H_{\mathbf{R}}$, the set of such c's is uncountable (the latter fact will be used below). Define now the complex structure on $\Pi_{\mathbf{R}}$ by letting $\iota_r(c)$ be the multiplication by i. Let V_c be the n-dimensional complex linear space defined by this complex structure on $\Pi_{\mathbf{R}}$. Since $\iota_r(c)$ commutes with the elements of $\iota_l(\mathrm{M}_{n/2}(H_{\mathbf{R}}))$, we have

$$\iota_l\bigl(\mathrm{M}_{n/2}(H_{\mathbf{R}})\bigr) \subset \mathrm{End}_{\mathbf{C}}(V_c). \tag{6}$$

From (5) and (6) we deduce that the action of G on $\Pi_{\mathbf{R}}$ defined above is $\mathbf{C}$-linear with respect to this complex structure. Also, (5) and (6) clearly yield a nonzero homomorphism of $\mathbf{C}$-algebras $\mathbf{Q}G_{\mathbf{C}} \to \mathrm{End}_{\mathbf{C}}(V_c)$ that endows V_c with a nonzero structure of $\mathbf{Q}G_{\mathbf{C}}$-module of $\mathbf{C}$-dimension n. On the other hand, V is a nontrivial $\mathbf{Q}G_{\mathbf{C}}$-module of $\mathbf{C}$-dimension n as well. Notice now that there is a unique (up to isomorphism) $\mathbf{Q}G_{\mathbf{C}}$-module of $\mathbf{C}$-dimension n since, by Lemma 2.1, the $\mathbf{C}$-algebra $\mathbf{Q}G_{\mathbf{C}}$ is isomorphic to $\mathrm{M}_n(\mathbf{C})$. This implies that there is an isomorphism of $\mathbf{Q}G_{\mathbf{C}}$-modules

$$\nu_c : V_c \to V. \tag{7}$$

It follows from $G \subset \mathbf{Q}G \subset \mathbf{Q}G_{\mathbf{C}}$ that ν_c is an isomorphism of G-modules.

Determine now the structure of endomorphism algebra $\mathrm{End}^0(V_c/\Pi)$ of complex torus V_c/Π. Recall from [OZ] that the *Hodge algebra* $\mathrm{HDG}(V_c/\Pi)$ of V_c/Π is the smallest $\mathbf{Q}$-subalgebra B of $\mathrm{End}_{\mathbf{Q}}(\Pi_{\mathbf{Q}}) \subset \mathrm{End}_{\mathbf{R}}(\Pi_{\mathbf{R}})$ such that $\iota_r(c) \in \mathbf{R}B$, and $\mathrm{End}^0(V_c/\Pi)$ coincides with the centralizer of B in $\mathrm{End}_{\mathbf{Q}}(\Pi_{\mathbf{Q}})$. Since $c \in H_{\mathbf{R}}$, we conclude that $\mathrm{HDG}(V_c/\Pi) \subset \iota_r(H)$. Since the centralizer of $\iota_r(H)$ in $\mathrm{End}_{\mathbf{Q}}(\Pi_{\mathbf{Q}})$ is $\iota_l(\mathrm{M}_{n/2}(H))$, this implies that $\mathrm{End}^0(V_c/\Pi) \supset \iota_l(\mathrm{M}_{n/2}(H))$. As $c \notin \mathbf{R} \cdot 1$, we have $\dim_{\mathbf{Q}} \mathrm{HDG}(V_c/\Pi) \geqslant 2$. Hence, since H is a quaternion $\mathbf{Q}$-algebra, $\mathrm{HDG}(V_c/\Pi)$ is either $\iota_r(H)$ or $\iota_r(F)$, where F is a quadratic subfield of H. If $\mathrm{HDG}(V_c/\Pi) = \iota_r(F)$, then by dimension reason,

$$F_{\mathbf{R}} = \mathbf{R} \cdot 1 + \mathbf{R} \cdot c \simeq \mathbf{C}, \tag{8}$$

and therefore F is an imaginary quadratic field. If $\mathrm{HDG}(V_c/\Pi) = \iota_r(H)$, then $\mathrm{End}^0(V_c/\Pi)$ is the centralizer of $\iota_r(H)$, i.e., $\mathrm{End}^0(V_c/\Pi) = \iota_l(\mathrm{M}_{n/2}(H))$.

Prove now that when c varies, all possibilities for $\mathrm{HDG}(V_c/\Pi)$ do occur, i.e.,

(a) if F is an imaginary quadratic subfield of H, then for some c,

$$\iota_r(F) = \mathrm{HDG}(V_c/\Pi); \tag{9}$$

(b) there exists c such that $\mathrm{End}^0(V_c/\Pi) = \iota_l(\mathrm{M}_{n/2}(H))$.

First, if F is as in (a), then $F_{\mathbf{R}} \simeq \mathbf{C}$ and therefore there is an element $c_F \in F_{\mathbf{R}} \subset H_{\mathbf{R}}$ such that $c_F^2 = -1$ (in fact, there are exactly two such elements). Clearly, then (9) holds for $c = c_F$. This proves (a).

Second, notice that clearly the set of imaginary quadratic subfields of H is at most countable. For every such field F, the intersection of $F_{\mathbf{R}}$ with the set $S := \{c \in H_{\mathbf{R}} \mid c^2 = -1\}$ consists of two elements. Since S is uncountable, this implies that there exists $c_0 \in H_{\mathbf{R}}$ such that $c_0^2 = -1$ and c_0 does not lie in $F_{\mathbf{R}}$ for every imaginary quadratic subfield F of H. Hence $\mathrm{HDG}(V_{c_0}/\Pi) = \iota_r(H)$. This proves (b).

Determine now the structure of V/Π_c in case $\mathrm{HDG}(V_c/\Pi) = \iota_r(F)$, where F is an imaginary quadratic subfield of H. The definition of Hodge algebra implies that $\iota_r(F) \subset \mathrm{End}^0(V_c/\Pi)$, i.e., $\mathbf{Q}\Pi$ is $\iota_r(F)$-stable. From (8) and the definition of V_c we deduce that $\iota_r(F_{\mathbf{R}}) = \mathbf{C} \cdot \mathrm{id}_{V_c}$. Since $\mathbf{Q}\Pi$ is $\iota_r(F)$-stable, there is an order $\mathcal{O}'$ in F such that Π is $\iota_r(\mathcal{O}')$-stable. This endows Π with a structure of $\mathcal{O}'$-module. By a theorem of Z.I. Borevich and D.K. Faddeev [BF] (see also [Sc, Satz 2.3]), this $\mathcal{O}'$-module splits into a direct sum of n submodules of rank 1,

$$\Pi = \Gamma_1 \oplus \cdots \oplus \Gamma_n. \tag{10}$$

Clearly, each $\Gamma_j \otimes \mathbf{R}$ is a one-dimensional $\mathbf{C}$-linear space and (10) implies that V_c/Π is isomorphic to $\prod_{j=1}^n (\Gamma_j \otimes \mathbf{R})/\Gamma_j$. Every $(\Gamma_j \otimes \mathbf{R})/\Gamma_j$ is an elliptic curve with complex multiplication by $\mathcal{O}'$. Therefore these curves are mutually isogenous.

To complete the proof, it only remains to remark that due to the existence of isomorphism (7), the complex tori V_c/Π and $V/\nu_c(\Pi)$ are isomorphic. So in the above cases (a) and (b), putting respectively $\nu_c(\Pi) := \Lambda^{(F)}$ and Λ, we obtain respectively the proofs of statements (i) and (ii) of the theorem. □

We now give a criterion of the existence of a nonzero G-invariant lattice.

Theorem 2.6.

(A) *The following properties are equivalent*:
  (i) *there is a nonzero G-invariant lattice in V*;
  (ii) *there is a G-invariant lattice in V of rank $2n$*;
  (iii) *one of the following conditions holds*:
    (a) $\mathrm{Schur}_{G,V} = 1$ *and* $\chi_{G,V}$ *is either rational or imaginary quadratic*;
    (b) $\mathrm{Schur}_{G,V} = 2$ *and* $\chi_{G,V}$ *is rational.*

(B) *A G-invariant lattice Λ in V of rank n exists if and only if G is defined over $\mathbf{Q}$, i.e.,* $\mathrm{Schur}_{G,V} = 1$ *and* $\chi_{G,V}$ *is rational. For such Λ and every nonreal $c \in \mathbf{C}$, the additive subgroup $\Lambda + c\Lambda$ of V is a G-invariant lattice in V of rank $2n$.*

Proof. (A) The equivalence of (i) and (ii) follows from (B) that is proved below.

Let (i) holds. If $\chi_{G,V}$ is not rational, then $\mathrm{Schur}_{G,V} = 1$ and $\chi_{G,V}$ is imaginary quadratic by Lemmas 2.1(ii), 2.3(ii). If $\chi_{G,V}$ is rational, then $\mathrm{Schur}_{G,V} \leqslant 2$ by Lemma 2.1(iv). Hence (i) $\Rightarrow$ (iii).

Conversely, let (iii) holds. If (b) is fulfilled, then (2), Lemma 2.4, and Theorem 2.5 imply that (i) holds. Consider now the case, where (a) is fulfilled. If $\chi_{G,V}$ is rational, then by definition of the Schur index, G is defined over $\mathbf{Q}$. It is known (see, e.g., [CR, (73.5)]) that then G is defined over $\mathbf{Z}$, i.e., there exists a basis $e_1, \ldots, e_n$ in V such that the lattice $\mathbf{Z}e_1 + \cdots + \mathbf{Z}e_n$ is G-invariant. Thus in this case, (i) holds as well. Finally, assume that $\chi_{G,V}$ is imaginary quadratic. Since $\mathrm{Schur}_{G,V} = 1$, there exists a G-invariant $\mathbf{Q}(\chi_{G,V})$-form L of V. Let $\mathcal{O}$ be the maximal order of $\mathbf{Q}(\chi_{G,V})$. Take a nonzero vector $v \in L$ and let Λ be the submodule of $\mathcal{O}$-module L generated by the G-orbit of v,

$$\Lambda := \sum_{g \in G} \mathcal{O} g(v). \tag{11}$$

Since $\mathcal{O}$ is a Dedekind ring ([BS], [CR, §18]) and Λ is a finitely generated torsion free $\mathcal{O}$-module, the latter is isomorphic to a direct sum of some fractional ideals $\mathcal{I}_1, \ldots, \mathcal{I}_d$ of $\mathbf{Q}(\chi_{G,V})$ (see, e.g., [CR, (22.5)]). Hence there are linearly independent over $\mathcal{O}$ vectors $v_1, \ldots, v_d \in L$ such that

$$\Lambda = \mathcal{I}_1 v_1 + \cdots + \mathcal{I}_d v_d. \tag{12}$$

Since the fraction field of $\mathcal{O}$ is $\mathbf{Q}(\chi_{G,V})$, vectors $v_1, \ldots, v_d$ are linearly independent over $\mathbf{Q}(\chi_{G,V})$ as well, and since L is a $\mathbf{Q}(\chi_{G,V})$-form of V, they are linearly independent over $\mathbf{C}$. Notice now that since $\mathbf{Q}(\chi_{G,V})$ is an imaginary quadratic number field, all its fractional ideals are lattices (of rank 2) in $\mathbf{C}$. This and (12) imply now that Λ is a nonzero lattice in V. On the other hand, (11) clearly implies that Λ is G-invariant. Hence (i) holds. This completes the proof that (iii) $\Rightarrow$ (i).

(B) We have already proven that if $\mathrm{Schur}_{G,V} = 1$ and $\chi_{G,V}$ is rational, then there exists a G-invariant lattice of rank n. Conversely, let Λ be a G-invariant lattice of rank n. Since $\mathbf{C}\Lambda = V$ because of the irreducibility of G, the equality $\mathrm{rk}(\Lambda) = \dim_{\mathbf{C}} V$ implies that every basis $e_1, \ldots, e_n$ of the $\mathbf{Z}$-module Λ is a basis of the $\mathbf{C}$-linear space V. Hence $\mathbf{Q}\Lambda$ is a G-invariant $\mathbf{Q}$-form of V, i.e., G is defined over $\mathbf{Q}$. Therefore

$$\Lambda + c\Lambda = (\mathbf{Z} + c\mathbf{Z})e_1 \oplus \cdots \oplus (\mathbf{Z} + c\mathbf{Z})e_n. \tag{13}$$

The condition $c \notin \mathbf{R}$ implies that $\mathbf{Z} + c\mathbf{Z}$ is a lattice of rank 2 in $\mathbf{C}$. Hence $\Lambda + c\Lambda$ is a lattice of rank $2n$, which is clearly G-invariant. This completes the proof. □

Corollary 2.7. *Suppose that the greatest common divisor of the integers* $\dim_{\mathbf{C}}(\ker(u))$, *where* u *runs through* $\mathbf{Q}G$, *is equal to* 1. *Then*

(i) *a nonzero* G*-invariant lattice in* V *exists* $\Leftrightarrow$ $\chi_{G,V}$ *is either rational or imaginary quadratic*;
(ii) *a* G*-invariant lattice in* V *of rank* n *exists if and only if* $\chi_{G,V}$ *is rational.*

Proof. This follows from Lemma 2.1(v) and Theorem 2.6. □

Lemma 2.8. *Let* Λ *and* Λ' *be lattices of rank* $2n$ *in* V *such that* $\Lambda' \subseteq \Lambda$.

(i) *The following properties are equivalent*:
  (a) V/Λ *is an abelian variety*;
  (b) V/Λ' *is an abelian variety.*
(ii) *If* (a) *and* (b) *hold, then the abelian varieties* V/Λ *and* V/Λ' *are isogenous.*

Proof. (i) If (a) holds, then V/Λ admits a polarization Ψ. Since $\Lambda' \subseteq \Lambda$, the same Ψ is a polarization for V/Λ'; whence (b). Conversely, let (b) holds and let Ψ' be a polarization for V/Λ'. Then, clearly, $[\Lambda : \Lambda'] < \infty$ and $[\Lambda : \Lambda']^2 \cdot \Psi'$ is a polarization for V/Λ; whence (a).

(ii) This is clear. □

Lemma 2.9. *If an abelian variety is isogenous to a self-product of an elliptic curve with complex multiplication, then, in fact, it is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication.*

Proof. This is proved in [K] (see also [SM,Sc]). □

3. The case of $\mathrm{Schur}_{G,V} = 1$

Theorem 3.1. *Suppose that* $\mathrm{Schur}_{G,V} = 1$ *and* Λ *is a* G*-invariant lattice of rank* $2n$ *in* V. *Let* $\mathcal{O}$ *be the maximal order in* Z_G. *Fix a* Z_G*-algebra isomorphism* $\tau : \mathrm{M}_n(Z_G) \xrightarrow{\simeq} \mathbf{Q}G$. *Then*:

(i) *there is a lattice* Λ' *in* V *that enjoys the following properties*:
  (i_1) $\Lambda' \supseteq \Lambda$ *and* Λ' *is* $\tau(\mathrm{M}_n(\mathcal{O}))$*-invariant*;
  (i_2) *there exists a lattice* Γ *of rank* 2 *in* $\mathbf{C}$ *and a* $\mathbf{C}$*-linear isomorphism* $\varphi : \mathbf{C}^n \xrightarrow{\simeq} V$ *such that* $\mathcal{O}\Gamma = \Gamma$, $\varphi(\Gamma^n) = \Lambda'$, *and* $\varphi(y(v)) = \tau(y)(\varphi(v))$ *for all* $v \in \mathbf{C}^n$, $y \in \mathrm{M}_n(Z_G)$;
(ii) V/Λ *is an abelian variety isogenous to the self-product of elliptic curve* $\mathbf{C}/\Gamma$;
(iii) *if* Z_G *is an imaginary quadratic number field, then* V/Λ *is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication.*

Proof. Clearly, the map $\mathcal{O} \otimes \mathbf{Q} \to Z_G$, $a \otimes r \mapsto ar$, is a ring isomorphism that yields the ring isomorphism $\mathrm{M}_n(\mathcal{O}) \otimes \mathbf{Q} \xrightarrow{\simeq} \mathrm{M}_n(Z_G)$, $z \otimes r \mapsto zr$. Thus $\mathrm{M}_n(\mathcal{O})$ is an order in the $\mathbf{Q}$-algebra $\mathrm{M}_n(Z_G)$; whence $\tau(\mathrm{M}_n(\mathcal{O}))$ is an order in the $\mathbf{Q}$-algebra $\mathbf{Q}G$. Since $\mathbf{Z}G$ is an order in $\mathbf{Q}G$ as well, $\mathbf{Z}G \cap \tau(\mathrm{M}_n(\mathcal{O}))$ is a subgroup of finite index in $\tau(\mathrm{M}_n(\mathcal{O}))$. Since Λ is $\mathbf{Z}G$-invariant, this entails that there are only finitely many sets of the form $z(\Lambda)$, where $z \in \tau(\mathrm{M}_n(\mathcal{O}))$. Every such set $z(\Lambda)$ is a finitely generated additive subgroup in V, and $[z(\Lambda) : (\Lambda \cap z(\Lambda))] < \infty$. This implies that the sum of these subgroups,

$$\Lambda' := \sum_{z \in \tau(\mathrm{M}_n(\mathcal{O}))} z(\Lambda), \tag{14}$$

is a $\tau(\mathrm{M}_n(\mathcal{O}))$-invariant lattice in V containing Λ as a subgroup of finite index.

The $\tau(\mathrm{M}_n(\mathcal{O}))$-module Λ' is faithful. Indeed, notice that since Λ' is $\tau(\mathrm{M}_n(\mathcal{O}))$-invariant and $\tau(\mathrm{M}_n(\mathcal{O}))$ is an order in $\mathbf{Q}G$, the $\mathbf{Q}$-linear subspace $\mathbf{Q}\Lambda'$ in V is $\mathbf{Q}G$-invariant. Therefore if $z\Lambda' = 0$ for $z \in \tau(\mathrm{M}_n(\mathcal{O}))$, then z lies in the kernel of natural $\mathbf{Q}$-algebra homomorphism $\mathbf{Q}G \to \mathrm{End}_{\mathbf{Q}}(\mathbf{Q}\Lambda')$. Since $\mathbf{Q}G$ is a simple $\mathbf{Q}$-algebra, this kernel is trivial. Thus $z = 0$; whence the faithfulness.

By construction, (i_1) holds. We are going to prove that (i_2), (ii), and (iii) hold as well. Tensoring τ by $\mathbf{C}$ over Z_G, we obtain a $\mathbf{C}$-algebra isomorphism

$$\mathrm{M}_n(\mathbf{C}) = \mathrm{M}_n(Z_G) \otimes_{Z_G} \mathbf{C} \xrightarrow{\simeq} \mathbf{Q}G \otimes_{Z_G} \mathbf{C}. \tag{15}$$

On the other hand, by Lemma 2.1(i), we have the $\mathbf{C}$-algebra isomorphism (3). Composing isomorphisms (15) and (3), we get a $\mathbf{C}$-algebra isomorphism

$$\tau_{\mathbf{C}} : \mathrm{M}_n(\mathbf{C}) \xrightarrow{\simeq} \mathrm{End}_{\mathbf{C}}(V).$$

Consider the coordinate $\mathbf{C}$-linear space $\mathbf{C}^n$ endowed with the natural structure of left $\mathrm{M}_n(\mathbf{C})$-module. Since $\mathbf{C}^n$ is the unique (up to isomorphism) left $\mathrm{M}_n(\mathbf{C})$-module of $\mathbf{C}$-dimension n, there is a $\mathbf{C}$-linear isomorphism $\varphi : \mathbf{C}^n \xrightarrow{\simeq} V$ such that $\varphi(y(v)) = \tau_{\mathbf{C}}(y)(\varphi(v))$ for all $v \in \mathbf{C}^n$, $y \in \mathrm{M}_n(\mathbf{C})$. Clearly, $\Lambda'' := \varphi^{-1}(\Lambda')$ is an $\mathrm{M}_n(\mathcal{O})$-invariant lattice of rank $2n$ in $\mathbf{C}^n$. Let $e_1, \dots, e_n$ be the standard basis in $\mathbf{C}^n$. Since Λ'' is $\mathrm{M}_n(\mathcal{O})$-invariant, it is easily seen that there exists a lattice Γ in $\mathbf{C}$ such that

$$\mathcal{O}\Gamma = \Gamma \quad \text{and} \quad \Lambda'' = \Gamma e_1 + \cdots + \Gamma e_n. \tag{16}$$

Since $\mathrm{rk}(\Lambda'') = 2n$, we deduce from the second equality in (16) that $\mathrm{rk}(\Gamma) = 2$, and the complex torus V/Λ' is isomorphic to the self-product of elliptic curve $\mathbf{C}/\Gamma$, hence is an abelian variety. Since Λ is a subgroup of finite index in Λ', Lemma 2.8 implies that V/Λ is an abelian variety as well and V/Λ and V/Λ' are isogenous. This proves (i_2) and (ii). Assume now that Z_G is an imaginary quadratic field. Then $\mathcal{O} \neq \mathbf{Z}$, and the first equality in (16) yields that the elliptic curve $\mathbf{C}/\Gamma$ has complex multiplication. Hence V/Λ is isogenous to a self-product of an elliptic curve with complex multiplication. Now (iii) follows from Lemma 2.9. □

Example 3.2. Let p be a prime that is congruent to 3 modulo 4, r a positive integer, $q = p^{2r-1}$, and $G = \mathrm{SL}_2(\mathbf{F}_q)$. Then there exists a faithful simple complex G-module V such that $\dim_{\mathbf{C}}(V) = (q-1)/2$, $Z_G = \mathbf{Q}(\chi_{G,V}) = \mathbf{Q}(\sqrt{-q}) = \mathbf{Q}(\sqrt{-p})$ and $\mathrm{Schur}_{G,V} = 1$, see [J, p. 4], [F, p. 284–285]. By Theorem 2.6, there are G-invariant lattices of rank $q-1$ in V. It follows from Theorem 3.1 that if Λ is a G-invariant lattice of rank $q-1$ in V, then V/Λ is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication by $\mathbf{Q}(\sqrt{-p})$.

Combining Theorem 3.1 with the results of Section 2, we obtain the following applications.

Theorem 3.3. *Suppose that $\chi_{G,V}$ is not rational. If there exists a nonzero G-invariant lattice Λ in V, then Z_G is an imaginary quadratic number field,* $\mathrm{rk}(\Lambda) = 2n$ *and V/Λ is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication by Z_G.*

Proof. This follows from the combination of Lemma 2.3(b) and Theorem 3.1. □

Theorem 3.4. *Assume that the greatest common divisor of the integers* $\dim_{\mathbf{C}}(\ker(u))$*, where u runs through* $\mathbf{Q}G$*, is equal to* 1*. If there exists a G-invariant lattice Λ of rank* $2n$ *in V, then the conclusions of Theorem* 3.1 *hold true.*

Proof. This follows from the combination of Lemma 2.1(v) and Theorem 3.1. □

Example 3.5. Since $\dim_{\mathbf{C}}(\ker(0)) = n$ and $\dim_{\mathbf{C}}(\ker(\mathrm{id}_V - r)) = n - 1$ for every (complex) reflection $r \in \mathrm{GL}(V)$, the assumption of Theorem 3.4 always holds for every complex reflection group G. Hence the conclusion of Theorem 3.1 holds true for every irreducible complex reflection group G that admits a G-invariant lattice Λ of rank $2n$. A posteriori, the latter statement follows also from the classification of all lattices invariant with respect to finite complex reflection groups obtained in [Po]; in fact, the present paper arose from our attempt to find an a priori proof of this statement. Below is such a proof providing a more precise information than Theorems 3.1 and 3.4.

Given a (complex) reflection $r \in \mathrm{GL}(V)$, the linear subspace $l_r := (\mathrm{id}_V - r)(V)$ is one-dimensional, r-invariant, and r acts on it as scalar multiplication by a root of unity $\theta_r \neq 1$. This implies that the assumptions and conclusions of Lemma 2.1(v) and Corollary 2.7 hold if G is a reflection group.

It is well known [ST,Po] that every finite irreducible reflection group in V is generated by n or $n + 1$ reflections and, in the last case, it contains an irreducible reflection subgroup generated by n reflections. Therefore describing invariant lattices of finite irreducible reflection groups in V, we may consider only the groups generated by n reflections. Let G be such a group, and let $r_1, \dots, r_n$ be a system of reflections generating G. We put $l_{r_j} = l_j$, $\theta_{r_j} = \theta_j$.

Fix a G-invariant positive definite Hermitian inner product $\langle\,,\rangle$ on V, and, for every reflection $r \in G$, fix a vector $e_r \in l_r$ of length 1. Then $r(v) = v - (1 - \theta_r)\langle v, e_r\rangle e_r$, $v \in V$. We put $e_j := e_{l_j}$.

Let $\mathcal{L}$ be the set of all the lines l_r where r runs through all the reflections in G. Since G is irreducible, $V = l_1 \oplus \cdots \oplus l_n$.

Let Λ be a G-invariant lattice in V. We put $\Lambda^0 := \sum_{l \in \mathcal{L}} \Lambda_l$, where $\Lambda_l := \Lambda \cap l$, and $\Lambda_j := \Lambda_{l_j}$. Then Λ^0 is a subgroup of Λ, hence Λ^0 is a lattice in V.

Lemma 3.6. [Po, Section 4.1] *The following properties hold*:

(i) Λ^0 *is G-invariant*;
(ii) $[\Lambda : \Lambda^0] < \infty$;
(iii) $\Lambda^0 = \Lambda_1 + \cdots + \Lambda_n$;
(iv) *if* $\mathrm{rk}(\Lambda) = 2n$*, then* $\mathrm{rk}(\Lambda^0) = 2n$ *and* $\mathrm{rk}(\Lambda_j) = 2$ *for every j.*

Proof. Clearly, $\mathcal{L}$ is G-invariant; whence (i). Let $s := (\mathrm{id}_V - r_1) + \cdots + (\mathrm{id}_V - r_n)$. If $v \in \ker(s)$, then $\langle v, e_j\rangle = 0$ for all j. Hence s is nondegenerate. Therefore $\mathrm{rk}(\Lambda) = \mathrm{rk}(s(\Lambda))$. We now deduce (ii) from $s(\Lambda) \subseteq \Lambda_1 + \cdots + \Lambda_n \subseteq \Lambda^0 \subseteq \Lambda$.

By [Po, Section 3.2], every reflection in G is conjugate to a power of some r_j. Hence for every $l \in \mathcal{L}$, there are $g \in G$ and $j \in [1, n]$ such that $g(l) = l_j$. Therefore $g(\Lambda_l) \subseteq \Lambda_j$. On the other hand, $\Lambda_1 + \cdots + \Lambda_n$ is invariant with respect to every $\mathrm{id}_V - r_j$, hence G-invariant. This entails (iii).

By (ii), if $\mathrm{rk}(\Lambda) = 2n$, then $\mathrm{rk}(\Lambda^0) = 2n$, hence, by (iii), $\mathrm{rk}(\Lambda_j) = 2$ for every j; whence (iv). □

Theorem 3.7. *Let* $\mathrm{rk}(\Lambda) = 2n$. *Then*:

(i) V/Λ^0 *is an abelian variety isomorphic to a product of mutually isogenous elliptic curves*;
(ii) V/Λ *is an abelian variety isogenous to* V/Λ^0;
(iii) *if G is not complexification of the Weyl group of an irreducible root system, then V/Λ is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication.*

Proof. Since $\Lambda^0 \subseteq \Lambda$, Lemma 3.6(iii), (iv) implies that V/Λ, V/Λ^0 are complex tori, every l_j/Λ_j is an elliptic curve, V/Λ^0 is isomorphic to $l_1/\Lambda_1 \times \cdots \times l_n/\Lambda_n$, and, in particular, V/Λ^0 is an abelian variety. Whence (ii) by Lemma 2.8.

Since $(\mathrm{id}_V - r_k)(l_j) \subseteq l_k$ for every j and k, the $\mathbf{C}$-linear map $\varphi_{jk} := (\mathrm{id}_V - r_k)|_{l_j} : l_j \to l_k$ is either 0 or an isomorphism. In the latter case, φ_{jk} induces an isomorphism of elliptic curves $l_j/\Lambda_j \xrightarrow{\simeq} l_k/((\mathrm{id}_V - r_k)(\Lambda_j))$. On the other hand, since Λ is G-invariant, $(\mathrm{id}_V - r_k)(\Lambda_j) \subseteq \Lambda_k$. Hence if φ_{jk} is an isomorphism, then $l_k/((\mathrm{id}_V - r_k)(\Lambda_j))$ and l_k/Λ_k are isogenous elliptic curves. So in this case, l_j/Λ_j and l_k/Λ_k are isogenous as well. But φ_{jk} is an isomorphism if and only if $\langle e_j, e_k\rangle \neq 0$, and, since G is irreducible, every pair of vectors from the sequence $e_1, \ldots, e_n$ can be included in a subsequence in which every two neighboring elements are not orthogonal. Hence l_j/Λ_j and l_k/Λ_k are isogenous elliptic curves for every j, k. This implies (i).

To prove (iii), notice that $(\mathrm{id}_V - r_{j_1})(\mathrm{id}_V - r_{j_m})(\mathrm{id}_V - r_{j_{m-1}}) \cdots (\mathrm{id}_V - r_{j_2})(e_{j_1}) = c_{j_1 \ldots j_m} e_{j_1}$, where $c_{j_1 \ldots j_m} := \langle e_{j_1}, e_{j_2}\rangle \langle e_{j_2}, e_{j_3}\rangle \cdots \langle e_{j_{m-1}}, e_{j_m}\rangle \langle e_{j_m}, e_{j_1}\rangle \prod_{t=1}^{m}(1 - \theta_{j_t})$. From this we deduce that $\mathrm{tr}(\mathrm{id}_V - r_{j_1})(\mathrm{id}_V - r_{j_m})(\mathrm{id}_V - r_{j_{m-1}}) \cdots (\mathrm{id}_V - r_{j_2}) = c_{j_1 \ldots j_m}$.

Additivity of tr implies that $\mathbf{Z}[\mathrm{Tr}(G)] = \mathbf{Z}[\mathrm{Tr}(\mathbf{Z}G)]$. Since $\mathrm{id}_V - r_1, \ldots, \mathrm{id}_V - r_n$ generate the ring $\mathbf{Z}G$, the monomials $(\mathrm{id}_V - r_{j_1}) \cdots (\mathrm{id}_V - r_{j_m})$ generate $\mathbf{Z}G$ as a $\mathbf{Z}$-module. This entails that $\mathbf{Z}[\mathrm{Tr}(G)] = \mathbf{Z}[\ldots, c_{j_1 \ldots j_m}, \ldots]$, whence $\mathbf{Q}(\chi_{G,V}) = \mathbf{Q}(\ldots, c_{j_1 \ldots j_m}, \ldots)$.

Suppose that G is not complexification of the Weyl group of an irreducible root system. Then $\chi_{G,V}$ is not rational. Indeed, otherwise Theorem 2.6 would imply that G is complexification of a finite real n-dimensional irreducible reflection group that has an invariant lattice of rank n, and it is well known that such a real group is the Weyl group of an irreducible root system [Bo].

Since $\chi_{G,V}$ is not rational, $c_{j_1 \ldots j_m} \notin \mathbf{Q}$ for some $j_1, \ldots, j_m$. We have $c_{j_1 \ldots j_m} \cdot \Lambda_{j_1} \subseteq \Lambda_{j_1}$ since Λ is G-invariant. Hence l_{j_1}/Λ_{j_1} is an elliptic curve with complex multiplication. But V/Λ is isogenous to $(l_{j_1}/\Lambda_{j_1})^n$ by (i) and (ii). Now (iii) follows from Lemma 2.9. □

Remark 3.8. The classification of invariant lattices of reflection groups obtained in [Po] implies that elliptic curves arising from V/Λ for nonreal reflection groups admit complex multiplication only by $\mathbf{Q}(\sqrt{-d})$ with $d = 1, 2, 3$, and 7; it would be interesting to find an a priori proof of this fact.

4. The case of $\mathrm{Schur}_{G,V} \neq 1$

Theorem 4.1. *Suppose that* $\mathrm{Schur}_{G,V} \neq 1$ *and* Λ *is a nonzero* G*-invariant lattice in* V. *Then*:

(i) *n is even, $\chi_{G,V}$ is rational, the G-module V is either orthogonal or symplectic, and there exists a quaternion $\mathbf{Q}$-algebra H such that $M_{n/2}(H) \simeq \mathbf{Q}G$.*
(ii) *Fix an order $\mathcal{O}$ in H. Then there exists a two-dimensional complex torus T that enjoys the following properties*:
   - (ii_1) *V/Λ is isogenous to a self-product of T*;
   - (ii_2) *there exists a ring embedding* $\mathcal{O} \hookrightarrow \mathrm{End}(T)$;
   - (ii_3) *if the G-module V is orthogonal, then H is indefinite, and T and V/Λ are abelian varieties*;
   - (ii_4) *if the G-module V is symplectic, then H is definite, and T and V/Λ either are not abelian varieties or are isomorphic to the products of mutually isogenous elliptic curves with complex multiplication.*

Proof. Theorem 2.6 and Lemmas 2.4 and 2.2 imply (i). Fix a $\mathbf{Q}$-algebra isomorphism $\tau : \mathrm{M}_{n/2}(H) \xrightarrow{\simeq} \mathbf{Q}G$. Both $\mathbf{Z}G$ and $\tau(\mathrm{M}_{n/2}(\mathcal{O}))$ are orders in $\mathbf{Q}G$. The same argument as in the part of proof of Theorem 3.1 related to formula (14) shows that there are only finitely many sets of the form $z(\Lambda)$, where $z \in \tau(\mathrm{M}_{n/2}(\mathcal{O}))$, and the sum

$$\Lambda' := \sum_{z \in \tau(\mathrm{M}_{n/2}(\mathcal{O}))} z(\Lambda) \subset V$$

is a $\tau(\mathrm{M}_{n/2}(\mathcal{O}))$-invariant lattice in V containing Λ as a subgroup of finite index and faithful as $\tau(\mathrm{M}_{n/2}(\mathcal{O}))$-module. Tensoring τ by $\mathbf{C}$ over $\mathbf{Q}$ and composing with (3), we get a $\mathbf{C}$-algebra isomorphism $\tau_{\mathbf{C}} : \mathrm{M}_{n/2}(H)_{\mathbf{C}} \xrightarrow{\simeq} \mathrm{End}_{\mathbf{C}}(V)$. Since the $\mathbf{C}$-algebras $H_{\mathbf{C}}$ and $\mathrm{M}_2(\mathbf{C})$ are isomorphic, we may (and shall) fix a $\mathbf{C}$-algebra isomorphism $\kappa : H_{\mathbf{C}} \xrightarrow{\simeq} \mathrm{M}_2(\mathbf{C})$. It induces the $\mathbf{C}$-algebra isomorphism $\kappa_{n/2} : \mathrm{M}_{n/2}(H)_{\mathbf{C}} = \mathrm{M}_{n/2}(H_{\mathbf{C}}) \xrightarrow{\simeq} \mathrm{M}_{n/2}(\mathrm{M}_2(\mathbf{C}))$. Hence we obtain a $\mathbf{C}$-algebra isomorphism $\tau_{\mathbf{C}} \circ \kappa_{n/2}^{-1} : \mathrm{M}_{n/2}(\mathrm{M}_2(\mathbf{C})) \xrightarrow{\simeq} \mathrm{End}_{\mathbf{C}}(V)$. Consider the coordinate $\mathbf{C}$-linear space $\mathbf{C}^n$ presented as the direct sum $\mathbf{C}^n = (\mathbf{C}^2)^{n/2} = \mathbf{C}^2 \oplus \cdots \oplus \mathbf{C}^2$ of $n/2$ copies of $\mathbf{C}^2$ and endowed with the natural structure of left $\mathrm{M}_{n/2}(\mathrm{M}_2(\mathbf{C}))$-module. Since $(\mathbf{C}^2)^{n/2}$ is the unique (up to isomorphism) left $\mathrm{M}_{n/2}(\mathrm{M}_2(\mathbf{C}))$ ($\simeq \mathrm{M}_n(\mathbf{C})$)-module of $\mathbf{C}$-dimension n, there is a $\mathbf{C}$-linear isomorphism $\varphi : (\mathbf{C}^2)^{n/2} \xrightarrow{\simeq} V$ such that $\varphi(y(v)) = (\tau_{\mathbf{C}} \circ \kappa_{n/2}^{-1})(y)(\varphi(v))$ for all $v \in (\mathbf{C}^2)^{n/2}$, $y \in \mathrm{M}_{n/2}(\mathrm{M}_2(\mathbf{C}))$. Clearly, $\Lambda'' := \varphi^{-1}(\Lambda')$ is a $\mathrm{M}_{n/2}(\kappa(\mathcal{O}))$-invariant lattice of rank $2n$ in $(\mathbf{C}^2)^{n/2}$. Using the $\mathrm{M}_{n/2}(\kappa(\mathcal{O}))$-invariance of Λ'', it is easy to see that there exists a lattice Γ in $\mathbf{C}^2$ such that

$$\kappa(\mathcal{O})\Gamma = \Gamma \quad \text{and} \quad \Lambda'' = \Gamma^{n/2} = \Gamma \oplus \cdots \oplus \Gamma. \tag{17}$$

Since $\mathrm{rk}(\Lambda'') = \mathrm{rk}(\Lambda') = \mathrm{rk}(\Lambda) = 2n$, we deduce from (17) that $\mathrm{rk}(\Gamma) = 4$. Hence $T := \mathbf{C}^2/\Gamma$ is a 2-dimensional complex torus and we have the ring embedding

$$\mathcal{O} \xrightarrow[\kappa]{\simeq} \kappa(\mathcal{O}) \hookrightarrow \mathrm{End}(T). \tag{18}$$

Clearly, the complex torus $(\mathbf{C}^2)^{n/2}/\Lambda'' \simeq (\mathbf{C}^2/\Gamma)^{n/2} = T^{n/2}$ is isomorphic to V/Λ'. Since Λ is a subgroup of finite index in Λ', the complex torus V/Λ is isogenous to $T^{n/2}$. This proves (ii$_1$) and (ii$_2$).

Let the G-module V be orthogonal. Then H is indefinite by Lemma 2.4 and T is an abelian surface by [La2, Theorem 4.3, p. 152]; whence V/Λ is an abelian variety by Lemma 2.8. This proves (ii$_3$).

Let now the G-module V be symplectic. Then H is definite by Lemma 2.4. By (18), the $\mathbf{Q}$-algebra $\operatorname{End}^0(T)$ contains a subalgebra isomorphic to $\mathcal{O} \otimes \mathbf{Q} \simeq H$ and therefore is noncommutative.

Suppose that T is an abelian surface. Using tables in [O], one may easily verify that T is not simple. On the other hand, if T is isogenous to a product of two nonisogenous elliptic curves, then $\operatorname{End}^0(T)$ is commutative and cannot contain a subalgebra isomorphic to H. If T is isogenous to a square of an elliptic curve without complex multiplication, then $\operatorname{End}^0(T)$ is isomorphic to $\mathrm{M}_2(\mathbf{Q})$ and hence cannot contain such a subalgebra as well. It follows that T is isogenous to a square of an elliptic curve with complex multiplication. This implies that V/Λ is isogenous to a self-product of an elliptic curve with complex multiplication, and hence, by Lemma 2.9, that V/Λ is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication.

Now assume that T is not an abelian surface. Then $T^{n/2}$ is not an abelian variety, because every polarization on $T^{n/2}$ obviously induces a polarization on (say, the first factor) T. It then follows from Lemma 2.8 that V/Λ is not an abelian variety as well. This proves (ii$_4$). □

The following examples show that both possibilities in conclusion (ii$_4$) of Theorem 4.1 may indeed occur. In particular, there are finite irreducible groups G and G-invariant lattices Λ in V such that $\operatorname{rk}(\Lambda) = 2n$ and the complex torus V/Λ is *not* an abelian variety.

Example 4.2. Let G be the image of a (unique up to isomorphism) irreducible 2-dimensional complex representation of the quaternion group. Fixing a basis in the representation space V, we may (and shall) identify V with $\mathbf{C}^2$ and G with the matrix group

$$\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}\right\}. \tag{19}$$

It is known [CR, §70] that $\operatorname{Schur}_{G,V} = 2$. The G-module $\mathbf{C}^2$ is symplectic and (19) clearly yields that the lattice $\Lambda := \{\binom{a}{b} \in \mathbf{C}^2 \mid a, b \in \mathbf{Z} + i\mathbf{Z}\}$ is G-stable and $\mathbf{C}^2/\Lambda$ is isomorphic to the square of the elliptic curve $\mathbf{C}/(\mathbf{Z} + i\mathbf{Z})$ with complex multiplication by $\mathbf{Z}[i]$.

Example 4.3. Consider the order $\Lambda := \mathbf{Z}\mathbf{1} + \mathbf{Z}\boldsymbol{i} + \mathbf{Z}\boldsymbol{j} + \mathbf{Z}\boldsymbol{k}$ in $H := (\frac{-1,-1}{\mathbf{Q}}) = \mathbf{Q}\mathbf{1} + \mathbf{Q}\boldsymbol{i} + \mathbf{Q}\boldsymbol{j} + \mathbf{Q}\boldsymbol{k}$. It is a lattice of rank 4 in the underlying 4-dimensional real linear space V of the quaternion $\mathbf{R}$-algebra $H_{\mathbf{R}} = \mathbf{H} := \mathbf{R}\mathbf{1} + \mathbf{R}\boldsymbol{i} + \mathbf{R}\boldsymbol{j} + \mathbf{R}\boldsymbol{k}$. The quaternion group $G := \{\pm\mathbf{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$ acts $\mathbf{R}$-linearly and faithfully on V by *left* multiplication in $\mathbf{H}$. This action is irreducible and Λ is G-invariant. Pick any element $c \in \mathbf{H}$ such that $c^2 = -\mathbf{1}$, and endow V with a structure of 2-dimensional complex linear space V_c defining multiplication by i as *right* multiplication by c in $\mathbf{H}$. Since left and right multiplications commute, the action of G on V_c is $\mathbf{C}$-linear (and irreducible). Thus we may (and shall) view G as an irreducible group of complex linear transformations of V_c.

Assume now that $c \notin \mathbf{R}F$ for any imaginary quadratic subfield F of H (such c's do exist, see the proof of Theorem 2.5). Consider the endomorphism ring $\operatorname{End}(V_c/\Lambda)$ of the 2-dimensional complex torus V_c/Λ. Our assumption on c implies that every $\mathbf{Q}$-linear endomorphism of H that becomes an element of $\mathrm{End}_{\mathbf{C}}(V_c)$ after the extension of scalars from $\mathbf{Q}$ to $\mathbf{R}$ must commute with right multiplication by every element of H, and therefore is left multiplication by an element of H. Hence $\mathrm{End}(V_c/\Lambda)$ consists of all $u \in H$ such that $u \cdot \Lambda \subseteq \Lambda$. It follows that $\mathrm{End}(V_c/\Lambda)$ coincides with the set of left multiplications by elements of Λ and therefore $\mathrm{End}(V_c/\Lambda) \simeq \Lambda$. Thus $\mathrm{End}(V_c/\Lambda)$ is an order in H and therefore $\mathrm{End}^0(V_c/\Lambda) = H$. But there are no complex abelian surfaces whose endomorphism algebra is a definite quaternion $\mathbf{Q}$-algebra [O]. Since H is a definite quaternion $\mathbf{Q}$-algebra, V_c/Λ is *not* an abelian variety.

Note that if $c \in \mathbf{R}F$ for an imaginary quadratic subfield F of H, then the endomorphism algebra of V_c/Λ is isomorphic to $H_F \simeq \mathrm{M}_2(F)$ and therefore V_c/Λ is isogenous to a square of an elliptic curve with complex multiplication by an order of F.

Example 4.4. Here is another example of the outcome (ii_4) of Theorem 4.1. Let p be an odd prime, r a positive integer, $q = p^{2r}$, and $G = \mathrm{SL}_2(\mathbf{F}_q)$. Then there exists a faithful simple complex G-module V such that $\dim_{\mathbf{C}}(V) = (q-1)/2$, $\chi_{G,V}$ is rational, $\mathrm{Schur}_{G,V} = 2$, and the quaternion $\mathbf{Q}$-algebra H from Theorem 4.1(iii) is ramified exactly at p and ∞, see [J, p. 4], [F, pp. 284–285]. In particular, H is definite. By Theorem 2.6, there are G-invariant lattices Λ of rank $q-1$ in V.

Example 4.5. Here is an example of the outcome (ii_3) of Theorem 4.1. Let G be the simple group HJ. Then there exists a simple complex G-module V such that $\dim_{\mathbf{C}}(V) = 336$, $\chi_{G,V}$ is rational, $\mathrm{Schur}_{G,V} = 2$, and the quaternion $\mathbf{Q}$-algebra H from Theorem 4.1(iii) is indefinite, see [F, p. 283]. By Theorem 2.6, there is a G-invariant lattice Λ of rank 672 in V.

According to Example 4.3, there exist G-invariant lattices Λ such that the complex torus V/Λ *is not* an abelian variety. However, the following statement tells us that one can always replace Λ by another G-invariant lattice Δ such that V/Δ *is* an abelian variety.

Theorem 4.6. *The following properties are equivalent.*

(i) *there exists a nonzero G-invariant lattice in V;*
(ii) *there exists a G-invariant lattice Δ in V such that V/Δ is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication.*

Proof. Let (i) holds. Theorems 2.6 and 3.1 reduce proving (ii) to the cases, where $\chi_{G,V}$ is rational and $\mathrm{Schur}_{G,V} = 1$ or 2.

Assume that $\chi_{G,V}$ is rational and $\mathrm{Schur}_{G,V} = 1$. Let $\mathcal{O}$ be an order in an imaginary quadratic field. We have $\mathcal{O} = \mathbf{Z} + c\mathbf{Z}$ for some nonreal $c \in \mathbf{C}$. Then Theorem 2.6 implies that (13) is a G-invariant lattice of rank $2n$; denote it by Δ. By construction, $\mathbf{C}/\mathcal{O}$ is an elliptic curve with complex multiplication by $\mathcal{O}$, and (13) implies that V/Δ is isomorphic to $(\mathbf{C}/\mathcal{O})^n$. Thus in this case, (ii) holds.

Now assume that $\chi_{G,V}$ is rational and $\mathrm{Schur}_{G,V} = 2$. Then Lemma 2.4 and Theorem 2.5 reduce proving (ii) to showing that every quaternion $\mathbf{Q}$-algebra $H = (\frac{a,b}{\mathbf{Q}})$ contains an imaginary quadratic subfield. But the latter property indeed holds, since the maximal subfields of H are precisely (up to isomorphism) the fields $\mathbf{Q}(\sqrt{ar_1^2 + br_2^2 - abr_3^2})$, where $r_1, r_2, r_3 \in \mathbf{Q}$ and $r_1^2 + r_2^2 + r_3^2 \neq 0$ (see, e.g., [Pi, §13.1, Exercise 4]). □

Acknowledgment

We thank E.B. Vinberg for stimulating remarks.

References

[BF] Z.I. Borevich, D.K. Faddeev, Integral representations of quadratic rings, Vestnik Leningrad. Univ. 15 (19) (1960) 52–64 (in Russian, MR0153707(27#3668)).
[BS] Z.I. Borevich, I.R. Shafarevich, Number Theory, Academic Press, New York, 1966.
[Bo] N. Bourbaki, Groupes et algèbres de Lie, Chapitres IV, V, VI, Hermann, Paris, 1968.
[CR] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience, New York, 1962.
[DL] R. Donagi, R. Livné, Abelian varieties with quaternion multiplication, arXiv: math.AG/0507493.
[D] L. Dornhoff, Group Representation Theory, Part A, Marcel Dekker, New York, 1971.
[F] W. Feit, The computations of some Schur indices, Israel J. Math. 46 (1983) (1971) 274–300.
[J] G. Janusz, Simple components of $\mathbf{Q}[\mathrm{SL}(2, q)]$, Comm. Algebra 1 (1974) (1971) 1–22.
[K] T. Katsura, On the structure of singular abelian varieties, Proc. Japan Acad. 51 (4) (1975) 224–228.
[La1] S. Lang, Algebra, Addison–Wesley, Reading, MA, 1965.
[La2] S. Lang, Introduction to Algebraic and Abelian Functions, second ed., Springer-Verlag, New York, 1982.
[LR] H. Lange, S. Recillas, Abelian varieties with group action, J. Reine Angew. Math. 575 (2004) 135–155.
[O] F. Oort, Endomorphism algebras of abelian varieties, in: H. Hijikata, et al. (Eds.), Algebraic Geometry and Commutative Algebra in Honor of M. Nagata, vol. II, Kinokuniya, Tokyo, 1988, pp. 469–502.
[OZ] F. Oort, Yu.G. Zarhin, Endomorphism algebras of complex tori, Math. Ann. 303 (1995) 11–29.
[Pi] R. Pierce, Associative Algebras, Springer-Verlag, New York, 1982.
[Po] V.L. Popov, Discrete Complex Reflection Groups, Communications of the Mathematical Institute, vol. 15, Rijksuniversiteit Utrecht, 1982 (89 pp., MR 83g:20049).
[Sc] C. Schoen, Produkte Abelscher Varietäten und Moduln über Ordnungen, J. Reine Angew. Math. 429 (1992) 115–123.
[Se] J.-P. Serre, Représentations linéaires des groupes finis, Hermann, Paris, 1978.
[ST] G.C. Shephard, J.A. Todd, Finite unitary reflection groups, Canad. J. Math. 6 (1954) 274–304.
[SM] T. Shioda, N. Mitani, Singular abelian surfaces and binary quadratic forms, in: Classification of Algebraic and Compact Complex Manifolds, in: Lecture Notes in Math., vol. 412, Springer-Verlag, 1974, pp. 259–287.
[Vi] E.B. Vinberg, Rings of definition of dense subgroups of semisimple linear groups, Math. USSR Izv. 5 (1972) 45–55.
[Vo] C. Voisin, On the homotopy types of Kähler compact and complex projective manifolds, Invent. Math. 157 (2004) 329–343.