Lattices, Abelian varieties and curves

Jacques Martinet

Université de Bordeaux, IMB

Talence, January 28, 2020

This talk completes a talk delivered in March 23, 2019 at Marseille-Luminy, under the title

Automorphisms of Lattices. Application to Curves,

at the meeting

Cohomology of Arithmetic Groups, Lattices and Number Theory: Geometric and Computational Viewpoint,
CIRM, 25 - 29 March 2019.

Complex Abelian Varieties from a Euclidean viewpoint

These are the complex tori $\mathbb{T} := \mathbb{C}^g/\Lambda$ on which there exists g algebraically independent meromorphic functions, a property equivalent to the existence of a projective embedding, and also to the fact that they carry the structure of an algebraic variety, and above all, to the existence of

Riemann form on $\mathbb{T}$ *,*

that is a positive, definite Hermitian form on $\mathbb{C}^g$, the *polarization*, whose imaginary part is integral on the lattice.
Such a form is well-defined by its real part, which gives $\mathbb{C}^g$ the structure of a Euclidean space E (and also by its imaginary part, which is alternating).

Complex Abelian Varieties from a Euclidean viewpoint

These are the complex tori $\mathbb{T} := \mathbb{C}^g/\Lambda$ on which there exists g algebraically independent meromorphic functions, a property equivalent to the existence of a projective embedding, and also to the fact that they carry the structure of an algebraic variety, and above all, to the existence of

Riemann form on $\mathbb{T}$ *,*

that is a positive, definite Hermitian form on $\mathbb{C}^g$, the *polarization*, whose imaginary part is integral on the lattice.
Such a form is well-defined by its real part, which gives $\mathbb{C}^g$ the structure of a Euclidean space E (and also by its imaginary part, which is alternating).

To $x \mapsto i\,x$ corresponds $\pm u = u^{\pm 1} \in \mathrm{End}(E)$ with $u^2 = -\,\mathrm{Id}$, and the integrality property above reads

$$\forall\, x, y \in \Lambda \mid x \cdot u(y) \in \mathbb{Z} \iff u(\Lambda) \subset \Lambda^* \,.$$

Given (E, Λ), a *polarization* is now a linear map $u \in \mathrm{End}(E)$ such that

$$u^2 = -\,\mathrm{Id} \ \text{ and } \ u(\Lambda) \subset \Lambda^* \,.$$

and this is called *principal* when $u(\Lambda) = \Lambda^*$. We shall only consider *Principally Polarized Abelian Varieties*, PPAV for short.

Jacobians

We shall only need a formal definition, particular case of the more general notion of an Albanese variety attached to a compact, connected complex manifold (or to a projective algebraic variety).

Jacobians

We shall only need a formal definition, particular case of the more general notion of an Albanese variety attached to a compact, connected complex manifold (or to a projective algebraic variety).

In the setting of Riemann surfaces, its construction as a torus $\mathbb{C}^g/\Lambda$ makes use of integrals defining the “periods”; in the setting of algebraic curves (Weil, over any field), it makes use of classes of degree-zero divisors on a curve.

Jacobians

We shall only need a formal definition, particular case of the more general notion of an Albanese variety attached to a compact, connected complex manifold (or to a projective algebraic variety).

In the setting of Riemann surfaces, its construction as a torus $\mathbb{C}^g/\Lambda$ makes use of integrals defining the “periods”; in the setting of algebraic curves (Weil, over any field), it makes use of classes of degree-zero divisors on a curve.

If the automorphism group of a lattice Λ is “large enough”, we may hope that Λ should be algebraic, i.e., that it gets a Gram matrix with entries in a number field when rescaled to a rational minimum.

Using this device we may obtain explicit examples of Jacobians *up to scale*. This will be achieved in this talk for a few curves of genus 2 and 3.

Torelli's Theorem

Analytic theory: Ruggiero Torelli (1913).

Algebraic geometry: André Weil (1957); special proofs for genera $2, 3, 4$.

$\Longrightarrow$ dichotomy for 2-dimensional PPAVs:
either products of elliptic curves or Jacobians.

Torelli's Theorem

Analytic theory: Ruggiero Torelli (1913).

Algebraic geometry: André Weil (1957); special proofs for genera $2, 3, 4$.

$\Longrightarrow$ dichotomy for 2-dimensional PPAVs:
either products of elliptic curves or Jacobians.

Serre's formulation (in an appendix to a paper by Kristin Lauter).

Notation. $(f : C \to C') \to (F_J : \mathrm{Jac}(C) \to \mathrm{Jac}(C'))$.

Theorem. Let $\mathcal{C}, \mathcal{C}'$ be curves of genus $g \geq 2$, with polarized Jacobians $(J, u), (J', u')$, and let $F : J \to J'$ be an isomorphism of polarized Abelian varieties. Then:

1. If $\mathcal{C}$ is hyperelliptic, there exists a unique isomorphism $f : \mathcal{C} \to \mathcal{C}'$ such that $f_J = F$.
2. If $\mathcal{C}$ is not hyperelliptic, there exists an isomorphism $f : \mathcal{C} \to \mathcal{C}'$ and an integer $e = \pm 1$ such that $F = e \cdot f_J$, and (F, e) is uniquely defined by f.

In particular, in case 1 (resp. 2), $\mathrm{Aut}(\mathrm{Jac}(\mathcal{C})) \simeq \mathrm{Aut}(\mathcal{C})$ (resp. $\mathrm{Aut}(\mathrm{Jac}(\mathcal{C})) \simeq \mathrm{Aut}(\mathcal{C}) \times \{\pm \mathrm{Id}\}$.)

Hyperbolic geometry

By the Riemann uniformization theorem, the universal covering of a Riemann surface S of genus $g \geq 2$ is the upper half-plane H, of which S can viewed as a quotient by a group of automorphisms.

These data can be interpreted in the setting of hyperbolic geometry, groups of automorphisms of S being characterized as the finite quotients of some finitely presented group.

Such a group has a presentation of the form:
- Generators: $a_1, b_1, \dots, a_g, b_g, c_1, \dots, c_r$;
- Relations: $\prod [a_i, b_i] \cdot \prod c_j = 1$; $c_j^{m_j} = 1, i = 1, \dots, r$.

Hyperbolic geometry

By the Riemann uniformization theorem, the universal covering of a Riemann surface S of genus $g \geq 2$ is the upper half-plane H, of which S can viewed as a quotient by a group of automorphisms.

These data can be interpreted in the setting of hyperbolic geometry, groups of automorphisms of S being characterized as the finite quotients of some finitely presented group.

Such a group has a presentation of the form:
- Generators: $a_1, b_1, \dots, a_g, b_g, c_1, \dots, c_r$;
- Relations: $\prod [a_i, b_i] \cdot \prod c_j = 1$; $c_j^{m_j} = 1, i = 1, \dots, r$.

With these methods one can more or less decide whether a given finite group G is **A** group of automorphisms of some curve, but G need not be **THE** group of automorphisms of some curve.

Hyperbolic geometry

By the Riemann uniformization theorem, the universal covering of a Riemann surface S of genus $g \geq 2$ is the upper half-plane H, of which S can viewed as a quotient by a group of automorphisms.

These data can be interpreted in the setting of hyperbolic geometry, groups of automorphisms of S being characterized as the finite quotients of some finitely presented group.

Such a group has a presentation of the form:
• Generators: $a_1, b_1, \dots, a_g, b_g, c_1, \dots, c_r$;
• Relations: $\prod [a_i, b_i] \cdot \prod c_j = 1$; $c_j^{m_j} = 1, i = 1, \dots, r$.

With these methods one can more or less decide whether a given finite group G is **A** group of automorphisms of some curve, but G need not be **THE** group of automorphisms of some curve.

One can prove bounds for the order of automorphism groups.
Hurwitz: $|\mathrm{Aut}(C)| \leq 84(g-1)$.
If this bound is not sharp: $|\mathrm{Aut}(C)| \leq 48(g-1)$, ...

The Craig Lattices

Data. p: an odd prime; $n = p - 1$; $\zeta = e^{2\pi i/p}$; $K = \mathbb{Q}(\zeta) \subset \mathbb{C}$;

$\mathfrak{P} = (1 - \zeta) \subset \mathbb{Z}_K$; T: the bilinear form $\frac{1}{p}\,\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{y})$ on K.

$\mathbb{A}_n^{(i)}$ is $\mathfrak{P}^i$ viewed as a lattice in $E := \mathbb{R} \otimes K$. [$\mathbb{A}_{p-1}^{(1)}$ is the root lattice $\mathbb{A}_{p-1}$.]

The Craig Lattices

Data. p: an odd prime; $n = p - 1$; $\zeta = e^{2\pi i/p}$; $K = \mathbb{Q}(\zeta) \subset \mathbb{C}$;

$\mathfrak{P} = (1 - \zeta) \subset \mathbb{Z}_K$; T: the bilinear form $\frac{1}{p}\,\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{y})$ on K.

$\mathbb{A}_n^{(i)}$ is $\mathfrak{P}^i$ viewed as a lattice in $E := \mathbb{R} \otimes K$. [$\mathbb{A}_{p-1}^{(1)}$ is the root lattice $\mathbb{A}_{p-1}$.]

Remarks. *Up to scale*,
1. $i \mapsto i + \frac{p-1}{2}$ is a period.
2. $i \mapsto \frac{p+1}{2} - i$ is a duality,
2' and in particular, $\mathbb{A}_{p-1}^{(p+3)/4}$ is symplectic.
[Use multiplication by the Gauss sum $S = \sum_{i=1}^{p-1} \left(\frac{p}{i}\right)\zeta^i$; note that $S^2 = -p$.]

The Craig Lattices

Data. p: an odd prime; $n = p - 1$; $\zeta = e^{2\pi i/p}$; $K = \mathbb{Q}(\zeta) \subset \mathbb{C}$;

$\mathfrak{P} = (1 - \zeta) \subset \mathbb{Z}_K$; T: the bilinear form $\frac{1}{p}\,\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{y})$ on K.

$\mathbb{A}_n^{(i)}$ is $\mathfrak{P}^i$ viewed as a lattice in $E := \mathbb{R} \otimes K$. [$\mathbb{A}_{p-1}^{(1)}$ is the root lattice $\mathbb{A}_{p-1}$.]

Remarks. *Up to scale*,
1. $i \mapsto i + \frac{p-1}{2}$ is a period.
2. $i \mapsto \frac{p+1}{2} - i$ is a duality,
2' and in particular, $\mathbb{A}_{p-1}^{(p+3)/4}$ is symplectic.
[Use multiplication by the Gauss sum $S = \sum_{i=1}^{p-1} \left(\frac{p}{i}\right)\zeta^i$; note that $S^2 = -p$.]

Theorem (Craig). $\min A_n^{(i)} \geq 2i$.

Theorem (Elkies). Equality holds if $i = \frac{p+3}{4}$.
Proof. Identify $i = \frac{p+1}{4}$ with a Mordell-Weil lattice over a global function fields !

$\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$ (1)

Gram matrices depend on two parameters:

$$A = \begin{pmatrix} 2 & t_1 & t_2 & t_3 & t_3 & t_2 \\ t_1 & 2 & t_1 & t_2 & t_3 & t_3 \\ t_2 & t_1 & 2 & t_1 & t_2 & t_3 \\ t_3 & t_2 & t_1 & 2 & t_1 & t_2 \\ t_3 & t_3 & t_2 & t_1 & 2 & t_1 \\ t_2 & t_3 & t_3 & t_2 & t_1 & 2 \end{pmatrix} \text{ where } t_1 + t_2 + t_3 = -1\,,$$

for parameters t_i such that $\min A = 2$.

These conditions define a hexagonal domain $\mathcal{D}$ with vertices $A_1\,, B_1\,, A_2, B_2, A_3, B_3$, representing alternatively the Craig lattices $\mathbb{A}_6^{(1)} \simeq \mathbb{A}_6$ and $\mathbb{A}_6^{(2)}$.

$\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$ (1)

Gram matrices depend on two parameters:

$$A = \begin{pmatrix} 2 & t_1 & t_2 & t_3 & t_3 & t_2 \\ t_1 & 2 & t_1 & t_2 & t_3 & t_3 \\ t_2 & t_1 & 2 & t_1 & t_2 & t_3 \\ t_3 & t_2 & t_1 & 2 & t_1 & t_2 \\ t_3 & t_3 & t_2 & t_1 & 2 & t_1 \\ t_2 & t_3 & t_3 & t_2 & t_1 & 2 \end{pmatrix} \text{ where } t_1 + t_2 + t_3 = -1\,,$$

for parameters t_i such that $\min A = 2$.

These conditions define a hexagonal domain $\mathcal{D}$ with vertices $A_1, B_1, A_2, B_2, A_3, B_3$, representing alternatively the Craig lattices $\mathbb{A}_6^{(1)} \simeq \mathbb{A}_6$ and $\mathbb{A}_6^{(2)}$.

Automorphisms. $\mathrm{Aut}(\mathbb{A}_6) = \mathrm{Aut}(\mathbb{A}_6^*) = \{\pm\mathrm{Id}\} \times S_7$;

$\mathrm{Aut}\left(\mathbb{A}_6^{(2)}\right) = \{\pm\mathrm{Id}\} \times \mathrm{PGL}_2(7)$, better understood as

$\{\pm\mathrm{Id}\} \times (\mathrm{PSL}_3(2) \cdot 2)$; $\mathrm{Aut}^+\left(\mathbb{A}_6^{(2)}\right) \simeq \{\pm\mathrm{Id}\} \times \mathrm{PSL}_3(2)$.

$\mathbb{A}_6^{(2)}$: unique symplectic structure, with centralizer $\{\pm\mathrm{Id}\} \times \mathrm{PSL}_3(2)$.
$\Longrightarrow$ defines a PPAV with automorphism group this centralizer.

$\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$ (2)

Orbits under $\pm\sigma$. Three at vertices, two on edges, one in $\mathrm{Int}(\mathcal{D})$.

$\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$ (2)

Orbits under $\pm\sigma$. Three at vertices, two on edges, one in $\mathrm{Int}(\mathcal{D})$.

Automorphisms. $\mathrm{Aut} = D_{14}$ and $\mathrm{Aut}^+ = C_{14}$, except for $\mathbb{A}_6$ and $\mathbb{A}_6^*$ ($2 \times S_7$) and $\mathbb{A}_6^{(2)}$ ($2 \times (\mathrm{PSL}_3(2) \cdot 2 \simeq 2 \times \mathrm{PSL}_2(7)$).

$\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$ (2)

Orbits under $\pm\sigma$. Three at vertices, two on edges, one in $\mathrm{Int}(\mathcal{D})$.

Automorphisms. $\mathrm{Aut} = D_{14}$ and $\mathrm{Aut}^+ = C_{14}$, except for $\mathbb{A}_6$ and $\mathbb{A}_6^*$ ($2 \times S_7$) and $\mathbb{A}_6^{(2)}$ ($2 \times (\mathrm{PSL}_3(2) \cdot 2 \simeq 2 \times \mathrm{PSL}_2(7)$)).

Duality. 3 to 1 from A_i to A_0: $(-\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3})$, representing $\mathbb{A}_6^*$ indeed the barycenter of the A_i's (and of the B_i's), 1 to 1 on B_i, 2 to 1 on edges, 1 to 1 in $\mathrm{Int}(\mathcal{D})$ except 1 to 3 at A_0 and 1 to 2 on the images of pairs A — B — A of edges.

$\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$ (2)

Orbits under $\pm\sigma$. Three at vertices, two on edges, one in $\mathrm{Int}(\mathcal{D})$.

Automorphisms. $\mathrm{Aut} = D_{14}$ and $\mathrm{Aut}^+ = C_{14}$, except for $\mathbb{A}_6$ and $\mathbb{A}_6^*$ $(2 \times S_7)$ and $\mathbb{A}_6^{(2)}$ $(2 \times (\mathrm{PSL}_3(2) \cdot 2 \simeq 2 \times \mathrm{PSL}_2(7))$.

Duality. 3 to 1 from A_i to A_0: $(-\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3})$, representing $\mathbb{A}_6^*$ indeed the barycenter of the A_i's (and of the B_i's), 1 to 1 on B_i, 2 to 1 on edges, 1 to 1 in $\mathrm{Int}(\mathcal{D})$ except 1 to 3 at A_0 and 1 to 2 on the images of pairs A—B—A of edges.

These are arcs of hyperbola connecting the B_i's to A_0. Example:

$$t_1^2 - 4t_1 t_2 - 3t_2^2 - 3t_1 - 8t_2 - 3 = 0\,,$$

or

$$t_1 = \frac{-3t^2-50t+25}{-6t^2+40t+50},\quad t_2 = \frac{17t^2-20t-25}{-6t^2+40t+50}\ .$$

Note that $0 \mapsto (\frac{1}{2}, -\frac{1}{2})$ and $1 \mapsto (-\frac{1}{3}, -\frac{1}{3})$.

$\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$ (3)

Known matrices in $\mathcal{D}$ for symplectic lattices: B_i, representatives for $\mathbb{A}_6^{(2)}$.
Any other isodual lattice must lie in $\mathrm{Int}(\mathcal{D})$, off the arcs of hyperbolas. Choose a connected components $\mathcal{D}' \subset \mathcal{D}$ of this complementary set, and guess in $\mathcal{D}'$ on one matrix M the set of minimal vectors of M^{-1}. This then holds in the whole connected component
It turns out that we may choose

$$\pm\{e_3^*, -e_1^* + e_4^*, -e_2^* + e_5^*, -e_3^* + e_6^*, -e_4^*, e_1^* - e_5^*, e_2^* - e_6^*\}$$

(seven vectors adding to zero). Corresponding parameters (adding to -1):

$$u_1 = e_3^* \cdot (-e_1^* + e_4^*),\ u_2 = e_3^* \cdot (-e_2^* + e_5^*),\ u_3 = e_3^* \cdot (-e_3^* + e_6^*)\,.$$

We obtain

$$u_1 = \frac{-5t_1^2 - 8t_1t_2 + t_2^2 + t_1 - 2t_2 + 1}{t_1^2 + 3t_1t_2 + 4t_2^2 + 4t_1 + 6t_2 - 3} \quad \text{and} \quad u_2 = \frac{2t_1^2 + 6t_2t_1 + t_2^2 + t_1 + 5t_2 + 1}{t_1^2 + 3t_1t_2 + 4t_2^2 + 4t_1 + 6t_2 - 3}\ .$$

Solving the system $\{u_1 = t_1, u_2 = t_2\}$, we find

$$t_1 = -(1 + 6\theta + \theta^2)/2 = -0.176\ldots\ t_2 = \theta = -0.109\ldots\,,$$

where $\theta = -1 - 2\cos(4\pi/7)$, the only choice for which $(t_1, t_2) \in \mathcal{D}$.

PPAV for $\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$

With the data above we may associate a similarity class of lattices, with field of definition $\mathbb{Q}(2\cos\frac{2\pi}{7}) \subset \mathbb{C}$, having a unique class of symplectic isodualities. Let Λ_0 be such a lattice. We have proved that there exist

exactly two isomorphism classes of PPAVs having an automorphism of order 7.

PPAV for $\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$

With the data above we may associate a similarity class of lattices, with field of definition $\mathbb{Q}(2\cos\frac{2\pi}{7}) \subset \mathbb{C}$, having a unique class of symplectic isodualities. Let Λ_0 be such a lattice. We have proved that there exist

exactly two isomorphism classes of PPAV*s having an automorphism of order* 7.

Consider the projective curves H (hyperelliptic) and K (Klein's quartic):

$$H : y^2 z^5 = x^7 + z^7\,, \quad K : x^3 y + y^3 z + z^3 x = 0\,,$$

and their respective automorphisms of order 7

$$\sigma_1 : (x, y, z) \mapsto (\zeta x, y, z) \text{ and } \sigma_2 : (x, y, z) \mapsto (\zeta x, \zeta^4 y, \zeta^2 z)\,.$$

PPAV for $\dim \Lambda = 6$, $|\mathrm{Aut}(\Lambda)| \supset C_7$

With the data above we may associate a similarity class of lattices, with field of definition $\mathbb{Q}(2\cos\frac{2\pi}{7}) \subset \mathbb{C}$, having a unique class of symplectic isodualities. Let Λ_0 be such a lattice. We have proved that there exist

exactly two isomorphism classes of PPAVs having an automorphism of order 7.

Consider the projective curves H (hyperelliptic) and K (Klein's quartic):

$$H : y^2z^5 = x^7 + z^7\,, \quad K : x^3y + y^3z + z^3x = 0\,,$$

and their respective automorphisms of order 7

$$\sigma_1 : (x,y,z) \mapsto (\zeta x, y, z) \text{ and } \sigma_2 : (x,y,z) \mapsto (\zeta x, \zeta^4 y, \zeta^2 z)\,.$$

Observe that K has an automorphism of order 3, whereas $|\mathrm{Aut}^+(\Lambda_0)| = 14$.

This shows that there are two curves having an automorphism of order 7: H, with lattice Λ_0 and $\mathrm{Aut}(H) = C_{14}$, and K, with lattice $\mathbb{A}_6^{(2)}$. In this latter case, the Hurwitz bound shows that $\mathrm{Aut}(K)$ has index 2 in $\mathrm{Aut}^+(\mathbb{A}_6^{(2)})$, hence is equal to $\mathrm{PSL}_3(2)$, since this group is simple.

Of course all that concerns K was known to Klein !

$|G| = 9$

We again find a hexagonal domain, but for which A_i, B_i represent alternatively the perfect lattices $\mathbb{E}_6$ and $\mathbb{E}_6^*$.

Lattices having a dual containing two orbits of minimal vectors lie on six arcs of conics connecting consecutive vertices. Their complementary set in $\mathrm{Int}(\mathcal{D})$ is the union of six, pairwise equivalent connected components which do not contain any isodual lattice, and of the connected component of the origin, which represents $\Lambda = \mathbb{A}_2 \perp \mathbb{A}_2 \perp \mathbb{A}_2$, its only isodual lattice.

Thus $\mathcal{E}_4 \times \mathcal{E}_4 \times \mathcal{E}_4$ is the only PPAV having an automorphism of order 9.

In particular there do not exist curves of genus 3 having an automorphism of order 9.

Dimension 4 : an overview

We intend to make a somewhat crude classification of the possible actions of a group $G \subset \mathbb{SO}(E)$.
Reducible lattices, some of which define product of elliptic curves, are considered apart.

Next there is not a lot to say about "small" groups: G 2-elementary $\implies |\mathrm{Aut}^+(\Lambda)| \leq 8, |\mathrm{Aut}_u(\Lambda)| \leq 4$.

Now let G contain an element σ of order $m \geq 3$. Then $\varphi(m) \leq 4$.
$\varphi(m) = 4$: $m = 5$ *or* $10, 8, 12$.
$\varphi(m) = 2$: $m = 3, 4$.

Dimension 4 : an overview

We intend to make a somewhat crude classification of the possible actions of a group $G \subset \mathbb{SO}(E)$.
Reducible lattices, some of which define product of elliptic curves, are considered apart.

Next there is not a lot to say about "small" groups: G 2-elementary $\implies |\mathrm{Aut}^+(\Lambda)| \le 8, |\mathrm{Aut}_u(\Lambda)| \le 4$.

Now let G contain an element σ of order $m \ge 3$. Then $\varphi(m) \le 4$.
$\varphi(m) = 4$: $m = 5$ *or* $10,\ 8,\ 12$.
$\varphi(m) = 2$: $m = 3,\ 4$.

One must consider more closely minimal polynomials of σ
(alias canonical decompositions of the representation over $\mathbb{Q}$).
Negating σ if need be we are left with
Cyclotomic: $\phi_5, \phi_8, \phi_{12}$; ϕ_3, ϕ_4 .
Non-cyclo.: $X^3 - 1,\ (X^2+1)(X-1)$ (and $(X^2+X+1)(X^2+1)$).

Dimension 4 : an overview

We intend to make a somewhat crude classification of the possible actions of a group $G \subset \mathbb{SO}(E)$.
Reducible lattices, some of which define product of elliptic curves, are considered apart.

Next there is not a lot to say about "small" groups: G 2-elementary $\implies |\mathrm{Aut}^+(\Lambda)| \le 8, |\mathrm{Aut}_u(\Lambda)| \le 4$.

Now let G contain an element σ of order $m \ge 3$. Then $\varphi(m) \le 4$.
$\varphi(m) = 4$: $m = 5$ *or* $10,\ 8,\ 12$.
$\varphi(m) = 2$: $m = 3,\ 4$.

One must consider more closely minimal polynomials of σ (alias canonical decompositions of the representation over $\mathbb{Q}$).
Negating σ if need be we are left with
Cyclotomic: $\phi_5, \phi_8, \phi_{12}$; ϕ_3, ϕ_4 .
Non-cyclo.: $X^3 - 1,\ (X^2 + 1)(X - 1)$ (and $(X^2 + X + 1)(X^2 + 1)$).

In this latter case, only scaled copies of $\mathbb{A}_2 \otimes \mathbb{A}_2$ and $\mathbb{D}_4$, and orthogonal sums of 2-dimensional lattices (some with two non-equivalent polarizations) are isodual.

Dimension 4, G of order 5

Consider the matrices

$$A(t) = \begin{pmatrix} 2 & t & -t-1 & -t-1 \\ t & 2 & t & -t-1 \\ -t-1 & t & 2 & t \\ -t-1 & -t-1 & t & 2 \end{pmatrix}, \quad \text{and} \quad P = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

and the Moebius transformation $\alpha : t \mapsto \frac{2t+1}{t-2}$. Then the map

$$[-\tfrac{1}{2}, 0] \to \mathrm{Sym}_4(\mathbb{R}) : t \mapsto A(t)$$

parametrizes the set of 4-dimensional lattices of minimum 2 having an automorphism σ of order 5. On $(-\frac{1}{2}, 0)$ the group $\mathrm{Aut}(\Lambda)$ is dihedral of order 20. We have

$$ {}^tPA(\alpha(t))\, P = 5\, \frac{1-t-t^2}{2+t}\, A(t)^{-1} \text{ and } {}^tP = -P,$$

so that duality exchanges t and $\alpha(t)$. The unique isodual lattice corresponds to the value $\theta := 2 - \sqrt{5}$ of t. This defines a unique PPAV,

Dimension 4, G of order 5

Consider the matrices

$$A(t) = \begin{pmatrix} 2 & t & -t-1 & -t-1 \\ t & 2 & t & -t-1 \\ -t-1 & t & 2 & t \\ -t-1 & -t-1 & t & 2 \end{pmatrix}, \quad \text{and} \quad P = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

and the Moebius transformation $\alpha : t \mapsto \frac{2t+1}{t-2}$. Then the map

$$[-\tfrac{1}{2}, 0] \to \mathrm{Sym}_4(\mathbb{R}) : t \mapsto A(t)$$

parametrizes the set of 4-dimensional lattices of minimum 2 having an automorphism σ of order 5. On $(-\frac{1}{2}, 0)$ the group $\mathrm{Aut}(\Lambda)$ is dihedral of order 20. We have

$${}^tPA(\alpha(t))\,P = 5\,\frac{1-t-t^2}{2+t}\,A(t)^{-1} \text{ and } {}^tP = -P\,,$$

so that duality exchanges t and $\alpha(t)$. The unique isodual lattice corresponds to the value $\theta := 2-\sqrt{5}$ of t. This defines a unique PPAV,

which is the Jacobian of the curve $\mathcal{C}_5$ of equation $y^2 = x^5 + 1$.

Dimension 4, G of order 5

Consider the matrices

$$A(t) = \begin{pmatrix} 2 & t & -t-1 & -t-1 \\ t & 2 & t & -t-1 \\ -t-1 & t & 2 & t \\ -t-1 & -t-1 & t & 2 \end{pmatrix}, \quad \text{and} \quad P = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

and the Moebius transformation $\alpha : t \mapsto \frac{2t+1}{t-2}$. Then the map

$$[-\tfrac{1}{2}, 0] \to \mathrm{Sym}_4(\mathbb{R}) : t \mapsto A(t)$$

parametrizes the set of 4-dimensional lattices of minimum 2 having an automorphism σ of order 5. On $(-\frac{1}{2}, 0)$ the group $\mathrm{Aut}(\Lambda)$ is dihedral of order 20. We have

$${}^tPA(\alpha(t))\,P = 5\,\frac{1-t-t^2}{2+t}\,A(t)^{-1} \text{ and } {}^tP = -P\,,$$

so that duality exchanges t and $\alpha(t)$. The unique isodual lattice corresponds to the value $\theta := 2 - \sqrt{5}$ of t. This defines a unique PPAV,

which is the Jacobian of the curve $\mathcal{C}_5$ of equation $y^2 = x^5 + 1$.

This also shows that $|\mathrm{Aut}(\mathcal{C}_5)|$ is not larger than $|\mathrm{Aut}^+(\Lambda)| = 10$.

$\mathbb{Z}^n$

$E = \mathbb{R}^n$, equipped with its Canonical basis $\mathcal{B} = (\varepsilon_1, \dots, \varepsilon_n)$.
Lattice $\mathbb{Z}^n \subset E$. $\mathrm{Aut}(\mathbb{Z}^n) \simeq 2^n \cdot S_n$.

Now $n = 2m$ is even. Let $\mathcal{E}_4$ of equation $y^2 = x^3 + x$.
u_i, $i = 1, 3, \dots, n-1$: $\varepsilon_i \mapsto \varepsilon_{i+1}$, $\varepsilon_{i+1} \mapsto -\varepsilon_i$, otherwise ε_j invariant.
$u = \prod_i u_i$ is a symplectic automorphism, unique up to conjugacy.

$\Longrightarrow \mathbb{Z}^n$ defines a unique PPAV, namely $\mathcal{E}_4^m$,

$\mathrm{Aut}_u(\mathbb{Z}^n) \simeq 4^m \cdot S_m$; order: 4, 32, 384, …

$\mathbb{D}_4$

$\mathbb{D}_n,\ n \geq 4$: the even sublattice of $\mathbb{Z}^n$.

H: Usual quaternions over $\mathbb{Q}$.
$\mathfrak{O}$: order $\mathbb{Z}[1, i, j, k]$.
$\mathfrak{M}$: Hurwitz's order $\langle \mathfrak{O}, \omega := \frac{-1+i+j+k}{2} \rangle$.
$\mathbb{D}_4$, embedded into $\mathfrak{O}$, is the subset of $\mathfrak{O}$ or of $\mathfrak{M}$ of quaternions having an *even* reduced norm. This identifies $\mathbb{D}_4^*$ with $\mathfrak{M}$.

$\mathfrak{M}^* \mapsto \mathfrak{M}^*/\{\pm 1\} \simeq A_4$ defines the non-trivial double cover $\tilde{A}_4$ (or $\hat{A}_4$) of A_4.

The left multiplication φ by $(j + k)$ (of square -2) maps $\mathbb{D}_4^*$ onto $\mathbb{D}_4$.

$\Longrightarrow \frac{1}{\sqrt{2}} \mathbb{D}_4$ is symplectic.
Again, this structure is unique up to conjugacy.

Right multiplications by $\mathfrak{M}^*$ and conjugacy by $\frac{j+k}{\sqrt{2}}$ commute with φ

$\Longrightarrow \mathrm{Aut}_\varphi(\mathbb{D}_4)$ contains a group $\mathcal{G}$ of order 48, actually the whole automorphism group. This groups extends $\tilde{A}_4$, hence is one of $\tilde{S}_4$ or $\hat{S}_4$, indeed $\tilde{S}_4 \simeq \mathrm{GL}_2(3)$. [Note that $\mathrm{PGL}_2(3) \simeq S_4$.]

Dimension 4, G of order 8

Consider the matrices

$$A(t) = \begin{pmatrix} 2 & t & 0 & -t \\ t & 2 & t & 0 \\ 0 & t & 2 & t \\ -t & 0 & t & 2 \end{pmatrix}, \; 0 \le t \le 1, \quad \text{and} \quad P = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Then the map

$$[0,1] \to \mathrm{Sym}_4(\mathbb{R}) : t \mapsto A(t)$$

parametrizes the set of 4-dimensional lattices of minimum 2 having an automorphism σ of order 8. On $(0,1)$ the group $\mathrm{Aut}(\Lambda)$ is dihedral of order 16. We have

$$^tPA(t)P = A(-t)\,, \; A(t)\,A(-t) = 2(2-t^2)\,I_4\,, \; \text{and} \; ^tP = -P\,,$$

so that all lattices Λ_t are symplectic. Up to conjugacy, there are two symplectic isodualities, namely u, defined by P, and $v = u\tau\sigma^2$, with centralizers $\langle \tau\sigma^2, -\mathrm{Id}\,\rangle \simeq C_2 \times C_2$ and $\langle \tau, \sigma^2 \rangle \simeq D_4$, respectively. The 2-dimensional PPAVs with lattice Λ_t, $0 < t < 1$, do not have automorphisms of order 8.

The Bolza curve

By the previous three slides there exist exactly two PPAVs having an automorphism of order 8. One is $\mathcal{E}_4 \times \mathcal{E}_4$. The Bolza curve *Bo*, defined by the equation

$$y^2 = x(x^4 + 1)\,,$$

has the automorphism $(x, y) \mapsto (\zeta_8^2\, x, \zeta_8\, y)$. Hence,

its Jacobian is the PPAV *attached to the uniquely polarized lattice* $\frac{1}{\sqrt{2}}\,\mathbb{D}_4$.

We have thus proved that $\mathrm{Aut}(Bo) \simeq \mathrm{GL}_2(3)$,
though automorphisms of order 3 (known to Bolza) are not visible on the equation above.

Cyclotomic groups of order 3 and 4

To complete the description of all possible automorphisms of curves and of their associated lattices, there only remains to consider
(1) the orthogonal sums of isometric 2-dimensional lattices equipped with a *twisted* polarization (i.e., exchanging the two components) ,
and
(2) the cyclotomic actions of order 3 and 4.

Case (1) gives rise to curves with automorphism group $\mathbb{C}_2 \times C_2$ except D_4 if the 2-dimensional lattice has a unique symmetry,
and a group of order 24 in the hexagonal case. This group is attained on the curve $y^2 = x^6 + 1$ (map (x, y) onto $(\zeta_6\, x, y)$, $(x, -y)$, and $(1/x, y/x^3)$.)

Case (2) is displayed in the next four slides.

Cyclotomic lattices, σ of order 3 (1)

(t_1, t_2)	Aut	$\pm$	$\|orb\|$	Groups
$(1, 0)$	$(2^4 \cdot S_4) \cdot C_3$	$-$	1	$\mathrm{PSL}_2(3)$
$(1, -1/2)$	$C_2 \times ((D_3 \times D_3) \cdot C_2)$	$-$	1	D_6
$(1, -1/3)$	$D_6 \times D_3$	$-$	1	D_6
$(0, 0)$	$(D_6 \times D_6) \cdot C_2$	$-$	2	$(C_6 \times C_6) \cdot C_2,\ C_3 \cdot D_4$
$(1/2, 0)$	D_{12}	$+$	3	D_4, D_6 (twice)
$(1/2, -1/4)$	$D_6 \times C_2$	$+$	2	$C_2 \times C_2, D_6$
$(1/2, -1/3)$	D_6	$+$	2	$C_2 \times C_2, D_6$

Table: Order 3, W-R

Some lattices:

$$(1,0) : \mathbb{D}_4\,; \quad (1,-1/2) : \mathbb{A}_2 \otimes \mathbb{A}_2\,; \quad (0,0) : \mathbb{A}_2 \perp \mathbb{A}_2\,.$$

Large groups:

$$(1,0) : 48\,; (0,0) : 72, 24.$$

Cyclotomic lattices, σ of order 3 (2)

(t_1, t_2)	Aut	$\pm$	$\lvert orb \rvert$	Groups
$(1, 0)$	$D_6 \times D_3$	$-$	1	D_6
$(1, -1/2)$	$D_6 \times C_2$	$+$	2	$C_2 \times C_2, D_6$
$(1, -1/3)$	D_6	$+$	2	$C_2 \times C_2, D_6$
$(0, 0)$	$D_6 \times D_6$	$-$	1	D_6
$(1/2, 0)$	D_6	$+$	2	$C_2 \times C_2, D_6$
$(1/2, -1/4)$	D_6	$+$	1	C_2
$(1/2, -1/3)$	C_6	$+$	1	C_2

Table: Order 3, non-W-R

Cyclotomic lattices, σ of order 4 (1)

(t_1, t_2)	Aut	$\pm$	$\lvert orb \rvert$	Groups
(1,-1)	$(2^4 \cdot S_4) \cdot C_3$	$-$	1	$\mathrm{PSL}_2(3)$
$(1,0)$	$(D_6 \times D_6) \cdot C_2)$	$-$	2	$(C_6 \times C_6) \cdot C_2,\ C_3 \cdot D_4$
$(1,-1/2)$	D_{12}	$+$	3	D_4, D_6 (twice)
$(0,0)$	${C_2}^4 \cdot S_4$	$-$	1	$(C_4 \times C_4) \cdot C_2$
$(1/2,0)$	ord. 32, exp. 4	$-$	2	D_4 (twice)
$(1/2,-1/2)$	D_8	$+$	2	$C_2 \times C_2, D_4$
$(1/2,-1/3)$	D_4	$+$	3	$C_2 \times C_2$ (twice), D_4

Table: Order 4, W-R

Some lattices:

$$(1,-1) : \mathbb{D}_4 \,; \qquad (0,0) : \mathbb{Z}^4 \,.$$

Large groups:

$$(1,-1) : 48 \,; (0,0) : 32 \,.$$

Cyclotomic lattices, σ of order 4 (2)

(t_1, t_2)	Aut	$\pm$	$\lvert orb \rvert$	Groups
(1,-1)	$D_4 \cdot D_4$	$-$	1	D_4
$(1, 0)$	$D_4 \cdot (C_2 \times C_2)$	$-$	2	D_4 (twice)
$(1, -1/2)$	D_4	$+$	3	$C_2 \times C_2$ (twice), D_4
$(0, 0)$	$D_4 \times D_4$	$-$	1	D_4
$(1/2, 0)$	D_4	$+$	3	$C_2 \times C_2$ (twice), D_4
$(1/2, -1/2)$	D_4	$+$	1	C_2
$(1/2, -1/3)$	C_4	$+$	2	C_2 (twice)

Table: Order 4, non-W-R

Automorphisms of curves

Theorem. *Let G be one of the groups*

$$C_2, C_2^2, D_4, C_{10}, D_6, H_{12} \rtimes C_2, \text{ and } \mathrm{GL}_2(3)\,,$$

of orders $2, 4, 8, 10, 12, 24$, and 48, respectively.
Then a group is the automorphism group of some curve $\mathcal{C}$ of genus 2 if and only if it belongs to the list above.
Moreover, for each of the orders 10, 24 and 48, the curve $\mathcal{C}$ is unique up to isomorphism, and may be defined by the equations $y^2 = x^5 + 1$, $y^2 = x^6 + 1$ and $y^2 = x^5 + x$, respectively.

Proof. Only the last assertion needs a proof.
We observe that, disregarding products of elliptic curves, there are *two* groups of order divisible by 3 and larger than 12. One of them corresponds to the Bolza curve. There just remains the lattice $\frac{1}{\sqrt{3}}(\mathbb{A}_2 \perp \mathbb{A}_2)$ with a twisted polarization which accounts for the curve $y^2 = x^6 + 1$.