Galois embeddings of elliptic curves and abelian surfaces

Hisao YOSHIHARA

Niigata University

March 12, 2009

The purpose of this talk is

(1) to introduce the notion and results of Galois embedding,

(2) and its application to elliptic curves and abelian surfaces.

The purpose of this talk is

(1) to introduce the notion and results of Galois embedding,

(2) and its application to elliptic curves and abelian surfaces.

The purpose of this talk is

(1) to introduce the notion and results of Galois embedding,
(2) and its application to elliptic curves and abelian surfaces.

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Notation

k : ground field, $\bar{k} = k$ and $\mathrm{ch}(k) = 0$
V : nonsingular proj. variety, $\dim V = n$
D : very ample divisor
$f = f_D : V \longrightarrow \mathbb{P}^N$: embedding by $|D|$
where $N + 1 = \dim H^0(V, \mathcal{O}(D))$
W : linear subvariety of $\mathbb{P}^N$, $\dim W = N - n - 1$, $W \cap f(V) = \emptyset$
$\pi_W : \mathbb{P}^N \dashrightarrow W_0$: projection with the center W
(where W_0 linear subvariety, $\dim W_0 = n$ and $W \cap W_0 = \emptyset$)
$\pi = \pi_W \cdot f : V \longrightarrow W_0 \cong \mathbb{P}^n$
$K = k(V)$: function field of V
$K_0 = k(W_0)$: function field of W_0

Galois embedding

$\pi^* : K_0 \hookrightarrow K$: finite extension, $\deg = d = \deg f(V) = D^n$

The structure of this extension does not depend on W_0, but on W.

K_W : Galois closure of K/K_0

$G_W := \mathrm{Gal}(K_W/K_0)$

Remark

G_W is isomorphic to the monodromy group of $\pi : V \longrightarrow W_0$.

Definition

We call G_W the Galois group at W. If K/K_0 is Galois, W is said to be Galois subspace.

Galois embedding

$\pi^* : K_0 \hookrightarrow K$: finite extension, $\deg = d = \deg f(V) = D^n$
The structure of this extension does not depend on W_0, but on W.

K_W : Galois closure of K/K_0
$G_W := \mathrm{Gal}(K_W/K_0)$

Remark

G_W is isomorphic to the monodromy group of $\pi : V \longrightarrow W_0$.

Definition

We call G_W the Galois group at W. If K/K_0 is Galois, W is said to be Galois subspace.

Galois embedding

$\pi^* : K_0 \hookrightarrow K$: finite extension, $\deg = d = \deg f(V) = D^n$
The structure of this extension does not depend on W_0, but on W.
K_W : Galois closure of K/K_0
$G_W := \mathrm{Gal}(K_W/K_0)$

Remark

G_W is isomorphic to the monodromy group of $\pi : V \longrightarrow W_0$.

Definition

We call G_W the Galois group at W. If K/K_0 is Galois, W is said to be Galois subspace.

Galois embedding

$\pi^* : K_0 \hookrightarrow K$: finite extension, $\deg = d = \deg f(V) = D^n$
The structure of this extension does not depend on W_0, but on W.
K_W : Galois closure of K/K_0
$G_W := \mathrm{Gal}(K_W/K_0)$

Remark

G_W is isomorphic to the monodromy group of $\pi : V \longrightarrow W_0$.

Definition

We call G_W the Galois group at W. If K/K_0 is Galois, W is said to be Galois subspace.

Galois embedding

$\pi^* : K_0 \hookrightarrow K$: finite extension, $\deg = d = \deg f(V) = D^n$
The structure of this extension does not depend on W_0, but on W.
K_W : Galois closure of K/K_0
$G_W := \mathrm{Gal}(K_W/K_0)$

Remark

G_W is isomorphic to the monodromy group of $\pi : V \longrightarrow W_0$.

Definition

We call G_W the Galois group at W. If K/K_0 is Galois, W is said to be Galois subspace.

Galois embedding

$\pi^* : K_0 \hookrightarrow K$: finite extension, $\deg = d = \deg f(V) = D^n$
The structure of this extension does not depend on W_0, but on W.
K_W : Galois closure of K/K_0
$G_W := \mathrm{Gal}(K_W/K_0)$

Remark

G_W is isomorphic to the monodromy group of $\pi : V \longrightarrow W_0$.

Definition

We call G_W the Galois group at W. If K/K_0 is Galois, W is said to be Galois subspace.

Galois embedding

$\pi^* : K_0 \hookrightarrow K$: finite extension, $\deg = d = \deg f(V) = D^n$
The structure of this extension does not depend on W_0, but on W.
K_W : Galois closure of K/K_0
$G_W := \mathrm{Gal}(K_W/K_0)$

Remark

G_W is isomorphic to the monodromy group of $\pi : V \longrightarrow W_0$.

Definition

We call G_W the Galois group at W. If K/K_0 is Galois, W is said to be Galois subspace.

Galois embedding

Definition

The V is said to have a Galois embedding if there exists a very ample divisor D s.t. the embedding by $|D|$ has a Galois subspace. In particular, if W is a point or line, we call it a Galois point or Galois line respectively.

In this case we say that (V, D) defines a Galois embedding.

Remark

Similarly we can define the Galois embedding in the case where $W \cap f(V) \neq \emptyset$.
We do not treat this case in this talk.

Galois embedding

Definition

The V is said to have a Galois embedding if there exists a very ample divisor D s.t. the embedding by $|D|$ has a Galois subspace. In particular, if W is a point or line, we call it a Galois point or Galois line respectively.

In this case we say that (V, D) defines a Galois embedding.

Remark

Similarly we can define the Galois embedding in the case where $W \cap f(V) \neq \emptyset$.
We do not treat this case in this talk.

Galois embedding

Definition

The V is said to have a Galois embedding if there exists a very ample divisor D s.t. the embedding by $|D|$ has a Galois subspace. In particular, if W is a point or line, we call it a Galois point or Galois line respectively.

In this case we say that (V, D) defines a Galois embedding.

Remark

Similarly we can define the Galois embedding in the case where $W \cap f(V) \neq \emptyset$.
We do not treat this case in this talk.

Galois embedding

Definition

The V is said to have a Galois embedding if there exists a very ample divisor D s.t. the embedding by $|D|$ has a Galois subspace. In particular, if W is a point or line, we call it a Galois point or Galois line respectively.

In this case we say that (V, D) defines a Galois embedding.

Remark

Similarly we can define the Galois embedding in the case where $W \cap f(V) \neq \emptyset$.
We do not treat this case in this talk.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \to \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z)$, $(X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \to \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z)$, $(X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \to \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z)$, $(X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \to \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z)$, $(X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \to \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z)$, $(X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \rightarrow \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z)$, $(X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \to \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z),\ (X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Plane cubic

Example

E : smooth cubic in $\mathbb{P}^2$.
If there exists a Galois point,
then E is projectively equivalent to the curve defined by
$Y^2Z = 4X^3 + Z^3$
and it has just three Galois points
$(X : Y : Z) = (1 : 0 : 0), (0 : -\sqrt{-3} : 1)$ and
$(0 : \sqrt{-3} : 1)$. Then we have three projections
$\pi : \mathbb{P}^2 \cdots \to \mathbb{P}^1$
given by $\pi(X : Y : Z) = (Y : Z),\ (X : Y + \sqrt{-3}Z)$ and
$(X : Y - \sqrt{-3}Z)$,
which yield Galois coverings $\pi|_E : E \longrightarrow \mathbb{P}^1$.

Space quartic

Example

For any elliptic curve E there exists a Galois embedding in $\mathbb{P}^3$ whose Galois group is isomorphic to V_4.

Later we will see this in detail.

Example

The elliptic curve E with $J(E) = 1728$ has an embedding $C \subset \mathbb{P}^3$

Space quartic

Example

For any elliptic curve E there exists a Galois embedding in $\mathbb{P}^3$ whose Galois group is isomorphic to V_4.

Later we will see this in detail.

Example

The elliptic curve E with $J(E) = 1728$ has an embedding $C \subset \mathbb{P}^3$

satisfying that C has four Z_4-lines and three V_4-lines.

Therefore C has seven Galois lines.

Example

For any elliptic curve E there exists a Galois embedding in $\mathbb{P}^3$ whose Galois group is isomorphic to V_4.

Later we will see this in detail.

Example

The elliptic curve E with $J(E) = 1728$ has an embedding $C \subset \mathbb{P}^3$
satisfying that C has four Z_4-lines and three V_4-lines.
Therefore C has seven Galois lines.

Space quartic

Example

For any elliptic curve E there exists a Galois embedding in $\mathbb{P}^3$ whose Galois group is isomorphic to V_4.

Later we will see this in detail.

Example

The elliptic curve E with $J(E) = 1728$ has an embedding $C \subset \mathbb{P}^3$
satisfying that C has four Z_4-lines and three V_4-lines.
Therefore C has seven Galois lines.

Space quartic

Example

For any elliptic curve E there exists a Galois embedding in $\mathbb{P}^3$ whose Galois group is isomorphic to V_4.

Later we will see this in detail.

Example

The elliptic curve E with $J(E) = 1728$ has an embedding
$C \subset \mathbb{P}^3$
satisfying that C has four Z_4-lines and three V_4-lines.
Therefore C has seven Galois lines.

Space quartic

Example

For any elliptic curve E there exists a Galois embedding in $\mathbb{P}^3$ whose Galois group is isomorphic to V_4.

Later we will see this in detail.

Example

The elliptic curve E with $J(E) = 1728$ has an embedding
$C \subset \mathbb{P}^3$
satisfying that C has four Z_4-lines and three V_4-lines.
Therefore C has seven Galois lines.

Space quartic

Example

In fact, let C be the sapce curve defined by $Z^2 = XY$ and $W^2 = 4YZ - XZ$.

Then C has four Z_4-lines and three V_4-lines, the defining equations are given as follows :

(I) Z_4-liens :

① $\ell_1 : X = Y = 0$
② $\ell_2 : Z = X + 4Y = 0$
③ $\ell_3 : W = X - 4Y + 4iZ = 0$, where $i = \sqrt{-1}$
④ $\ell_4 : W = X - 4Y - 4iZ = 0$

(II) V_4-lines :

⑤ $\ell_5 : X - 4Y = Z = 0$
⑥ $\ell_6 : X + 4Y = X + 2Z = 0$
⑦ $\ell_7 : X + 4Y = X - 2Z = 0$

The arrangement of the lines are as follows:

Space quartic

Example

In fact, let C be the sapce curve defined by $Z^2 = XY$ and $W^2 = 4YZ - XZ$.
Then C has four Z_4-lines and three V_4-lines, the defining equations are given as follows :

(I) Z_4-liens :

① $\ell_1 : X = Y = 0$
② $\ell_2 : Z = X + 4Y = 0$
③ $\ell_3 : W = X - 4Y + 4iZ = 0$, where $i = \sqrt{-1}$
④ $\ell_4 : W = X - 4Y - 4iZ = 0$

(II) V_4-lines :

⑤ $\ell_5 : X - 4Y = Z = 0$
⑥ $\ell_6 : X + 4Y = X + 2Z = 0$
⑦ $\ell_7 : X + 4Y = X - 2Z = 0$

The arrangement of the lines are as follows:

Space quartic

Example

In fact, let C be the sapce curve defined by $Z^2 = XY$ and $W^2 = 4YZ - XZ$.
Then C has four Z_4-lines and three V_4-lines, the defining equations are given as follows :

(I) Z_4-liens :

① $\ell_1 : X = Y = 0$
② $\ell_2 : Z = X + 4Y = 0$
③ $\ell_3 : W = X - 4Y + 4iZ = 0$, where $i = \sqrt{-1}$
④ $\ell_4 : W = X - 4Y - 4iZ = 0$

(II) V_4-lines :

⑤ $\ell_5 : X - 4Y = Z = 0$
⑥ $\ell_6 : X + 4Y = X + 2Z = 0$
⑦ $\ell_7 : X + 4Y = X - 2Z = 0$

The arrangement of the lines are as follows:

Example

In fact, let C be the sapce curve defined by $Z^2 = XY$ and $W^2 = 4YZ - XZ$.
Then C has four Z_4-lines and three V_4-lines, the defining equations are given as follows :

(I) Z_4-liens :

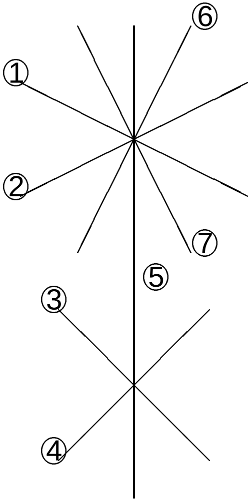
① $\ell_1 : X = Y = 0$
② $\ell_2 : Z = X + 4Y = 0$
③ $\ell_3 : W = X - 4Y + 4iZ = 0$, where $i = \sqrt{-1}$
④ $\ell_4 : W = X - 4Y - 4iZ = 0$

(II) V_4-lines :

⑤ $\ell_5 : X - 4Y = Z = 0$
⑥ $\ell_6 : X + 4Y = X + 2Z = 0$
⑦ $\ell_7 : X + 4Y = X - 2Z = 0$

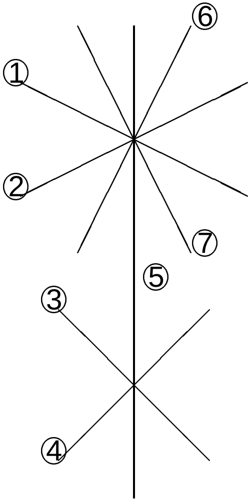
The arrangement of the lines are as follows:

Figure



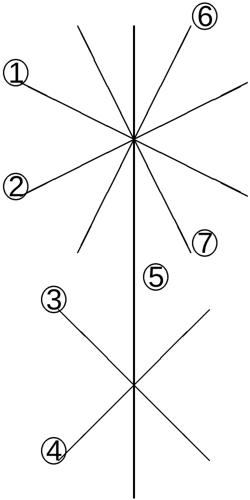
① to ④ : Z_4-lines, ⑤, ⑥ and ⑦ : V_4-lines

Figure



① to ④ : Z_4-lines, ⑤, ⑥ and ⑦ : V_4-lines

Figure



① to ④ : Z_4-lines, ⑤, ⑥ and ⑦ : V_4-lines

Remark

No divisor of degree five on elliptic curve has Galois embedding.

Problems

Problem

(1) *Find the structure of G_W.*

(2) *Find the subset $\mathcal{S}$ of $Pic(V)$ such that it consists of D which gives the Galois embedding.*

(3) *Find the arrangement of Galois subspaces for $f(V)$.*

(4) *For an embedding (V, D) find the structure of Galois group G_W for each $W \in \mathrm{Grass}(N-n-1, N)$.*

(5) *How is the set $\{ W \in \mathrm{Grass}(N-n-1, N) \mid G_W \cong S_d \}$? In particular, is it true that the codimension of the complement of the set is at least two ?*

(6) *Suppose that $\dim Lin(f(V)) = 0$, W and W' are close and $W \neq W'$. Then is it true that K_W is not isomorphic to K'_W ?*

Problems

Problem

(1) *Find the structure of* G_W.

(2) *Find the subset* $\mathcal{S}$ *of* $Pic(V)$ *such that it consists of* D *which gives the Galois embedding.*

(3) *Find the arrangement of Galois subspaces for* $f(V)$.

(4) *For an embedding* (V, D) *find the structure of Galois group* G_W *for each* $W \in \mathrm{Grass}(N-n-1, N)$.

(5) *How is the set* $\{\, W \in \mathrm{Grass}(N-n-1, N) \mid G_W \cong S_d \}$ *? In particular, is it true that the codimension of the complement of the set is at least two ?*

(6) *Suppose that* $\dim Lin(f(V)) = 0$, W *and* W' *are close and* $W \neq W'$. *Then is it true that* K_W *is not isomorphic to* K'_W *?*

Problems

Problem

(1) *Find the structure of* G_W.

(2) *Find the subset* $\mathcal{S}$ *of* $Pic(V)$ *such that it consists of* D *which gives the Galois embedding.*

(3) *Find the arrangement of Galois subspaces for* $f(V)$.

(4) *For an embedding* (V, D) *find the structure of Galois group* G_W *for each* $W \in \mathrm{Grass}(N-n-1, N)$.

(5) *How is the set* $\{ W \in \mathrm{Grass}(N-n-1, N) \mid G_W \cong S_d \}$ *? In particular, is it true that the codimension of the complement of the set is at least two ?*

(6) *Suppose that* $\dim Lin(f(V)) = 0$, W *and* W' *are close and* $W \neq W'$. *Then is it true that* K_W *is not isomorphic to* K'_W *?*

Problems

Problem

(1) *Find the structure of* G_W.

(2) *Find the subset* $\mathcal{S}$ *of* $Pic(V)$ *such that it consists of* D *which gives the Galois embedding.*

(3) *Find the arrangement of Galois subspaces for* $f(V)$.

(4) *For an embedding* (V, D) *find the structure of Galois group* G_W *for each* $W \in \mathrm{Grass}(N - n - 1, N)$.

(5) *How is the set* $\{ W \in \mathrm{Grass}(N - n - 1, N) \mid G_W \cong S_d \}$ *? In particular, is it true that the codimension of the complement of the set is at least two ?*

(6) *Suppose that* $\dim Lin(f(V)) = 0$, W *and* W' *are close and* $W \neq W'$. *Then is it true that* K_W *is not isomorphic to* K'_W *?*

Problems

Problem

(1) *Find the structure of* G_W.

(2) *Find the subset* $\mathcal{S}$ *of* $Pic(V)$ *such that it consists of* D *which gives the Galois embedding.*

(3) *Find the arrangement of Galois subspaces for* $f(V)$.

(4) *For an embedding* (V, D) *find the structure of Galois group* G_W *for each* $W \in \mathrm{Grass}(N-n-1, N)$.

(5) *How is the set* $\{ W \in \mathrm{Grass}(N-n-1, N) \mid G_W \cong S_d \}$ *? In particular, is it true that the codimension of the complement of the set is at least two ?*

(6) *Suppose that* $\dim Lin(f(V)) = 0$, W *and* W' *are close and* $W \neq W'$. *Then is it true that* K_W *is not isomorphic to* K'_W *?*

Problems

Problem

(1) *Find the structure of* G_W.

(2) *Find the subset* $\mathcal{S}$ *of* $Pic(V)$ *such that it consists of* D *which gives the Galois embedding.*

(3) *Find the arrangement of Galois subspaces for* $f(V)$.

(4) *For an embedding* (V, D) *find the structure of Galois group* G_W *for each* $W \in \mathrm{Grass}(N-n-1, N)$.

(5) *How is the set* $\{ W \in \mathrm{Grass}(N-n-1, N) \mid G_W \cong S_d \}$ *? In particular, is it true that the codimension of the complement of the set is at least two ?*

(6) *Suppose that* $\dim Lin(f(V)) = 0$, W *and* W' *are close and* $W \neq W'$. *Then is it true that* K_W *is not isomorphic to* K'_W *?*

Problems

Problem

(1) *Find the structure of* G_W.

(2) *Find the subset* $\mathcal{S}$ *of* $Pic(V)$ *such that it consists of* D *which gives the Galois embedding.*

(3) *Find the arrangement of Galois subspaces for* $f(V)$.

(4) *For an embedding* (V, D) *find the structure of Galois group* G_W *for each* $W \in \mathrm{Grass}(N-n-1, N)$.

(5) *How is the set* $\{\, W \in \mathrm{Grass}(N-n-1, N) \mid G_W \cong S_d \}$ *? In particular, is it true that the codimension of the complement of the set is at least two ?*

(6) *Suppose that* $\dim Lin(f(V)) = 0$, W *and* W' *are close and* $W \neq W'$. *Then is it true that* K_W *is not isomorphic to* K'_W *?*

Results

The results change greatly whether

(A) $ch(k) = 0$ or > 0,

(B) $W \cap f(V) = \emptyset$ or not.

We treat only the case where ch(k)=0 and $W \cap f(V) = \emptyset$.
First we show general results.

Results

The results change greatly whether

(A) $ch(k) = 0$ or > 0,

(B) $W \cap f(V) = \emptyset$ or not.

We treat only the case where ch(k)=0 and $W \cap f(V) = \emptyset$.

First we show general results.

Results

The results change greatly whether

(A) $ch(k) = 0$ or > 0,

(B) $W \cap f(V) = \emptyset$ or not.

We treat only the case where ch(k)=0 and $W \cap f(V) = \emptyset$.

First we show general results.

Results

The results change greatly whether

(A) $ch(k) = 0$ or > 0,

(B) $W \cap f(V) = \emptyset$ or not.

We treat only the case where ch(k)=0 and $W \cap f(V) = \emptyset$.

First we show general results.

Results

The results change greatly whether

(A) $ch(k) = 0$ or > 0,

(B) $W \cap f(V) = \emptyset$ or not.

We treat only the case where ch(k)=0 and $W \cap f(V) = \emptyset$.
First we show general results.

Basic results

Hereafter we assume W is a Galois subspace.

Proposition

There exists an injective representation $\alpha : G_W \hookrightarrow Aut(V)$.

Corollary

If $Aut(V)$ *is trivial, then* V *has no Galois embedding.*

Proposition

We have another injective representation $\beta : G_W \hookrightarrow PGL(N, k)$.

Basic results

Hereafter we assume W is a Galois subspace.

Proposition

There exists an injective representation $\alpha : G_W \hookrightarrow Aut(V)$.

Corollary

If $Aut(V)$ is trivial, then V has no Galois embedding.

Proposition

We have another injective representation $\beta : G_W \hookrightarrow PGL(N, k)$.

Basic results

Hereafter we assume W is a Galois subspace.

Proposition

There exists an injective representation $\alpha : G_W \hookrightarrow Aut(V)$.

Corollary

If $Aut(V)$ *is trivial, then* V *has no Galois embedding.*

Proposition

We have another injective representation $\beta : G_W \hookrightarrow PGL(N, k)$.

Basic results

Hereafter we assume W is a Galois subspace.

Proposition

There exists an injective representation $\alpha : G_W \hookrightarrow Aut(V)$.

Corollary

If $Aut(V)$ *is trivial, then* V *has no Galois embedding.*

Proposition

We have another injective representation $\beta : G_W \hookrightarrow PGL(N, k)$.

Criterion

Proposition

We have $W_0 \cong V/G_W$

The projection $\pi : V \longrightarrow W_0$ *turns out a finite morphism.*

In particular the fixed loci of G_W *consists of divisors.*

Theorem

(V, D) *defines a Galois embedding iff*

There exsits a subgroup G *of* $\mathrm{Aut}(V)$ *with* $|G| = D^n$

Criterion

Proposition

We have $W_0 \cong V/G_W$
The projection $\pi : V \longrightarrow W_0$ *turns out a finite morphism.*
In particular the fixed loci of G_W *consists of divisors.*

Theorem

(V, D) *defines a Galois embedding iff*

(1) *There exists a subgroup* G *of* $\mathrm{Aut}(V)$ *with* $|G| = D^2$

Criterion

Proposition

We have $W_0 \cong V/G_W$
The projection $\pi : V \longrightarrow W_0$ *turns out a finite morphism.*
In particular the fixed loci of G_W *consists of divisors.*

Theorem

(V, D) *defines a Galois embedding iff*

(1) *There exsits a subgroup* G *of* $Aut(V)$ *with* $|G| = D^n$.

Criterion

Proposition

We have $W_0 \cong V/G_W$
The projection $\pi : V \longrightarrow W_0$ *turns out a finite morphism.*
In particular the fixed loci of G_W *consists of divisors.*

Theorem

(V, D) *defines a Galois embedding iff*

(1) *There exsits a subgroup* G *of* $Aut(V)$ *with* $|G| = D^n$*.*

(2) *There exsits a G-invariant linear subspace* $\mathcal{L}$ *of* $H^0(V, \mathcal{O}(D))$ *of dimension* $n+1$ *such that, for any* $\sigma \in G$*, the restriction* $\sigma^*|_{\mathcal{L}}$ *is a multiple of the identity.*

(3) *The linear system* $\mathcal{L}$ *has no base points.*

Criterion

Proposition

We have $W_0 \cong V/G_W$
The projection $\pi : V \longrightarrow W_0$ *turns out a finite morphism.*
In particular the fixed loci of G_W *consists of divisors.*

Theorem

(V, D) *defines a Galois embedding iff*

(1) *There exsits a subgroup* G *of* $Aut(V)$ *with* $|G| = D^n$.

(2) *There exsits a* G*-invariant linear subspace* $\mathcal{L}$ *of* $H^0(V, \mathcal{O}(D))$ *of dimension* $n+1$ *such that, for any* $\sigma \in G$, *the restriction* $\sigma^*|_{\mathcal{L}}$ *is a multiple of the identity.*

(3) *The linear system* $\mathcal{L}$ *has no base points.*

Criterion

Proposition

We have $W_0 \cong V/G_W$
The projection $\pi : V \longrightarrow W_0$ *turns out a finite morphism.*
In particular the fixed loci of G_W *consists of divisors.*

Theorem

(V, D) *defines a Galois embedding iff*

(1) *There exsits a subgroup* G *of* $Aut(V)$ *with* $|G| = D^n$.

(2) *There exsits a* G*-invariant linear subspace* $\mathcal{L}$ *of* $H^0(V, \mathcal{O}(D))$ *of dimension* $n+1$ *such that, for any* $\sigma \in G$, *the restriction* $\sigma^*|_{\mathcal{L}}$ *is a multiple of the identity.*

(3) *The linear system* $\mathcal{L}$ *has no base points.*

Criterion

Proposition

We have $W_0 \cong V/G_W$
The projection $\pi : V \longrightarrow W_0$ *turns out a finite morphism.*
In particular the fixed loci of G_W *consists of divisors.*

Theorem

(V, D) *defines a Galois embedding iff*

(1) *There exsits a subgroup* G *of* $Aut(V)$ *with* $|G| = D^n$*.*
(2) *There exsits a* G*-invariant linear subspace* $\mathcal{L}$ *of* $H^0(V, \mathcal{O}(D))$ *of dimension* $n+1$ *such that, for any* $\sigma \in G$*, the restriction* $\sigma^*|_{\mathcal{L}}$ *is a multiple of the identity.*
(3) *The linear system* $\mathcal{L}$ *has no base points.*

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma) z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma)z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{\, \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{\, M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma) z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma) z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.

$k = \mathbb{C}$: field of complex numbers

A : abelian variety, $\dim A = n$

G : subgroup of Aut(A)

$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma) z + t(\sigma)$

where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$

$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,

$H = \{ M(\sigma) \mid \sigma \in G \}$

We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma)z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma) z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma) z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma) z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

abelian variety

Let us apply the above method to abelian varieties.
$k = \mathbb{C}$: field of complex numbers
A : abelian variety, $\dim A = n$
G : subgroup of Aut(A)
$\sigma \in G$ has the analytic representation $\widetilde{\sigma} z = M(\sigma)z + t(\sigma)$
where $M(\sigma) \in GL(n, \mathbb{C})$, $z \in \mathbb{C}^n$, $t(\sigma) \in \mathbb{C}^n$
$G_0 = \{ \sigma \in G \mid M(\sigma) = 1_n \}$,
$H = \{ M(\sigma) \mid \sigma \in G \}$
We have the following exact sequence of groups:

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow H \longrightarrow 1.$$

Basic property 1

Assume A has the Galois embedding and let G be the Galois group.
$B = A/G_0$ is abelian variety.
$H \cong G/G_0$ is a subgroup of $Aut(B)$.
We determin the structures of G and H in the cases where $d = 1$ and 2 respectively.

Basic property 1

Assume A has the Galois embedding and let G be the Galois group.
$B = A/G_0$ is abelian variety.
$H \cong G/G_0$ is a subgroup of $Aut(B)$.
We determin the structures of G and H in the cases where $d = 1$ and 2 respectively.

Basic property 1

Assume A has the Galois embedding and let G be the Galois group.
$B = A/G_0$ is abelian variety.
$H \cong G/G_0$ is a subgroup of $Aut(B)$.
We determin the structures of G and H in the cases where $d = 1$ and 2 respectively.

Basic property 2

Suppose (A, D) defines Galois embedding.

Let R be the ramification divisor for $\pi : A \longrightarrow W_0$.

Then, each component of R is a translation of an abelian survariety of dimension $n - 1$.

$R \sim (n+1)D$

R is very ample and $R^n = (n+1)^n|G|$.

Basic property 2

Suppose (A, D) defines Galois embedding.
Let R be the ramification divisor for $\pi : A \longrightarrow W_0$.
Then, each component of R is a translation of an abelian survariety of dimension $n - 1$.
$R \sim (n + 1)D$
R is very ample and $R^n = (n + 1)^n |G|$.

Basic property 2

Suppose (A, D) defines Galois embedding.
Let R be the ramification divisor for $\pi : A \longrightarrow W_0$.
Then, each component of R is a translation of an abelian survariety of dimension $n - 1$.
$R \sim (n+1)D$
R is very ample and $R^n = (n+1)^n |G|$.

Basic property 2

Suppose (A, D) defines Galois embedding.
Let R be the ramification divisor for $\pi : A \longrightarrow W_0$.
Then, each component of R is a translation of an abelian survariety of dimension $n - 1$.
$R \sim (n+1)D$
R is very ample and $R^n = (n+1)^n |G|$.

Basic property 2

Suppose (A, D) defines Galois embedding.
Let R be the ramification divisor for $\pi : A \longrightarrow W_0$.
Then, each component of R is a translation of an abelian survariety of dimension $n-1$.
$R \sim (n+1)D$
R is very ample and $R^n = (n+1)^n |G|$.

Corollary

Simple abelian variety A does not have Galois embedding if $\dim A \geq 2$.

Let us apply the above method to elliptic curves.

$A = E$: elliptic curve

Lemma

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff $|G| \geq 3$ and $|G_0| \neq 1$.

So the question is to find all finite subgroups of $Aut(E)$.
As a direct consequence the following assertion holds:

Corollary

For any smooth elliptic curve E there exists a Galois embedding whose Galois group is isomorphic to D_n.

elliptic curve

Let us apply the above method to elliptic curves.
$A = E$: elliptic curve

Lemma

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff $|G| \geq 3$ and $|G_0| \neq 1$.

So the question is to find all finite subgroups of $Aut(E)$.
As a direct consequence the following assertion holds:

Corollary

For any smooth elliptic curve E there exists a Galois embedding whose Galois group is isomorphic to D_n.

Let us apply the above method to elliptic curves.
$A = E$: elliptic curve

Lemma

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff $|G| \geq 3$ and $|G_0| \neq 1$.

So the question is to find all finite subgroups of $Aut(E)$.
As a direct consequence the following assertion holds:

Corollary

For any smooth elliptic curve E there exists a Galois embedding whose Galois group is isomorphic to D_n.

elliptic curve

Let us apply the above method to elliptic curves.
$A = E$: elliptic curve

Lemma

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff $|G| \geq 3$ and $|G_0| \neq 1$.

So the question is to find all finite subgroups of $Aut(E)$.
As a direct consequence the following assertion holds:

Corollary

For any smooth elliptic curve E there exists a Galois embedding whose Galois group is isomorphic to D_n.

Let us apply the above method to elliptic curves.
$A = E$: elliptic curve

Lemma

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff $|G| \geq 3$ and $|G_0| \neq 1$.

So the question is to find all finite subgroups of $Aut(E)$.
As a direct consequence the following assertion holds:

Corollary

For any smooth elliptic curve E there exists a Galois embedding whose Galois group is isomorphic to D_n.

Let us apply the above method to elliptic curves.
$A = E$: elliptic curve

Lemma

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff $|G| \geq 3$ and $|G_0| \neq 1$.

So the question is to find all finite subgroups of $Aut(E)$.
As a direct consequence the following assertion holds:

Corollary

For any smooth elliptic curve E there exists a Galois embedding whose Galois group is isomorphic to D_n.

Bidihedral group

Definition

A finite group G is called a bidihedral group if it is generated by the elements a, b and c s.t.
(1) $a^2 = b^m = c^n = id,\ aba = b^{-1},\ aca = c^{-1}, bc = cb$
(2) $n \geq m \geq 2$ and $n \geq 3$

We denote this group by BD_{mn} or BD

Bidihedral group

Definition

A finite group G is called a bidihedral group if it is generated by the elements a, b and c s.t.

(1) $a^2 = b^m = c^n = id,\ aba = b^{-1},\ aca = c^{-1}, bc = cb$

(2) $n \geq m \geq 2$ and $n \geq 3$

We denote this group by BD_{mn} or BD

Bidihedral group

Definition

A finite group G is called a bidihedral group if it is generated by the elements a, b and c s.t.
(1) $a^2 = b^m = c^n = id,\ aba = b^{-1},\ aca = c^{-1}, bc = cb$
(2) $n \geq m \geq 2$ and $n \geq 3$

We denote this group by BD_{mn} or BD

Bidihedral group

Definition

A finite group G is called a bidihedral group if it is generated by the elements a, b and c s.t.

(1) $a^2 = b^m = c^n = id, \ aba = b^{-1}, \ aca = c^{-1}, bc = cb$

(2) $n \geq m \geq 2$ and $n \geq 3$

We denote this group by BD_{mn} or BD

Bidihedral group

Definition

A finite group G is called a bidihedral group if it is generated by the elements a, b and c s.t.
(1) $a^2 = b^m = c^n = id,\ aba = b^{-1},\ aca = c^{-1}, bc = cb$
(2) $n \geq m \geq 2$ and $n \geq 3$

We denote this group by BD_{mn} or BD

Exceptional elliptic group

Definition

A finite non-abelian group G of order m^2kl is called an exceptional elliptic group
if it satisfies the following conditions (1), (2) and (3).

(1) $l = 3, 4$ or 6

(2) G is the semi-direct product $H \rtimes K$ with some action of K onto H,
where K is a cyclic group of order l and H is the normal abelian subgroup of G of order m^2k with one or two generators such that the orders of them are m and mk respectively.

(3) In case H has one generator we regard $m = 1$.

Exceptional elliptic group

Definition

A finite non-abelian group G of order m^2kl is called an exceptional elliptic group
if it satisfies the following conditions (1), (2) and (3).

(1) $l = 3, 4$ or 6

(2) G is the semi-direct product $H \rtimes K$ with some action of K onto H,
where K is a cyclic group of order l and H is the normal abelian subgroup of G of order m^2k with one or two generators such that the orders of them are m and mk respectively.

(3) In case H has one generator we regard $m = 1$.

Exceptional elliptic group

Definition

A finite non-abelian group G of order m^2kl is called an exceptional elliptic group
if it satisfies the following conditions (1), (2) and (3).

(1) $l = 3, 4$ or 6

(2) G is the semi-direct product $H \rtimes K$ with some action of K onto H ,
where K is a cyclic group of order l and H is the normal abelian subgroup of G of order m^2k with one or two generators such that the orders of them are m and mk respectively.

(3) In case H has one generator we regard $m = 1$.

Exceptional elliptic group

Definition

A finite non-abelian group G of order m^2kl is called an exceptional elliptic group
if it satisfies the following conditions (1), (2) and (3).

(1) $l = 3, 4$ or 6

(2) G is the semi-direct product $H \rtimes K$ with some action of K onto H ,
where K is a cyclic group of order l and H is the normal abelian subgroup of G of order m^2k with one or two generators such that the orders of them are m and mk respectively.

(3) In case H has one generator we regard $m = 1$.

Exceptional elliptic group

Definition

A finite non-abelian group G of order m^2kl is called an exceptional elliptic group if it satisfies the following conditions (1), (2) and (3).

(1) $l = 3, 4$ or 6

(2) G is the semi-direct product $H \rtimes K$ with some action of K onto H,
where K is a cyclic group of order l and H is the normal abelian subgroup of G of order m^2k with one or two generators such that the orders of them are m and mk respectively.

(3) In case H has one generator we regard $m = 1$.

Exceptional elliptic group

Definition

$k = 1$ or $k = q_1 \cdots q_s$, where q_i are distinct prime numbers satisfying the following condition (3.1) or (3.2).

(3.1) If $l = 3$ or 6, then $q_i = 3$ or $q_i \equiv 1 \pmod 3$, where $i = 1, \ldots, s$.

(3.2) If $l = 4$, then $q_i = 2$ or $q_i \equiv 1 \pmod 4$, where $i = 1, \ldots, s$.

We denote this group by $E(k, l)$ and $E(m, k, l)$ if $m = 1$ and $m \neq 1$ respectively.

Exceptional elliptic group

Definition

$k = 1$ or $k = q_1 \cdots q_s$, where q_i are distinct prime numbers satisfying the following condition (3.1) or (3.2).

(3.1) If $l = 3$ or 6, then $q_i = 3$ or $q_i \equiv 1 \pmod 3$, where $i = 1, \ldots, s$.

(3.2) If $l = 4$, then $q_i = 2$ or $q_i \equiv 1 \pmod 4$, where $i = 1, \ldots, s$.

We denote this group by $E(k, l)$ and $E(m, k, l)$ if $m = 1$ and $m \neq 1$ respectively.

Exceptional elliptic group

Definition

$k = 1$ or $k = q_1 \cdots q_s$, where q_i are distinct prime numbers satisfying the following condition (3.1) or (3.2).

(3.1) If $l = 3$ or 6, then $q_i = 3$ or $q_i \equiv 1 \pmod 3$, where $i = 1, \ldots, s$.

(3.2) If $l = 4$, then $q_i = 2$ or $q_i \equiv 1 \pmod 4$, where $i = 1, \ldots, s$.

We denote this group by $E(k, l)$ and $E(m, k, l)$ if $m = 1$ and $m \neq 1$ respectively.

Exceptional elliptic group

Definition

$k = 1$ or $k = q_1 \cdots q_s$, where q_i are distinct prime numbers satisfying the following condition (3.1) or (3.2).

(3.1) If $l = 3$ or 6, then $q_i = 3$ or $q_i \equiv 1 \pmod 3$, where $i = 1, \ldots, s$.

(3.2) If $l = 4$, then $q_i = 2$ or $q_i \equiv 1 \pmod 4$, where $i = 1, \ldots, s$.

We denote this group by $E(k, l)$ and $E(m, k, l)$ if $m = 1$ and $m \neq 1$ respectively.

Theorem

A finite group G can be a subgroup of $A(E)$ for some E if and only if G is isomorphic to one of the following:

(1) *abelian case:*

(1.1) Z_m $(m \geq 1)$ or $Z_m \oplus Z_{mk}$ $(m \geq 2,\ k \geq 1)$

(1.2) $Z_2,\ {Z_2}^{\oplus 2},\ {Z_2}^{\oplus 3},\ Z_3,\ {Z_3}^{\oplus 2},\ Z_4,\ Z_2 \oplus Z_4$ or Z_6

(2) *non-abelian case:*

(2.1) D_n or BD_{mn} $(n \geq 3)$

(2.2) $E(k, l)$ or $E(m, k, l)$

Moreover, the cases (1.1), (1.2), (2.1) *and* (2.1) *appear in the cases where* $|G_0| = 1,\ |G_0| > 1,\ |G_0| = 2$ *and* $|G_0| > 2$ *respectively.*

Theorem

A finite group G can be a subgroup of $A(E)$ for some E if and only if G is isomorphic to one of the following:
(1) *abelian case:*

(1.1) Z_m $(m \geq 1)$ *or* $Z_m \oplus Z_{mk}$ $(m \geq 2,\ k \geq 1)$

(1.2) $Z_2,\ Z_2^{\oplus 2},\ Z_2^{\oplus 3},\ Z_3,\ Z_3^{\oplus 2},\ Z_4,\ Z_2 \oplus Z_4$ *or* Z_6

(2) *non-abelian case:*

(2.1) D_n *or* BD_{mn} $(n \geq 3)$

(2.2) $E(k, l)$ *or* $E(m, k, l)$

Moreover, the cases (1.1), (1.2), (2.1) *and* (2.1) *appear in the cases*
where $|G_0| = 1,\ |G_0| > 1,\ |G_0| = 2$ *and* $|G_0| > 2$ *respectively.*

Theorem

A finite group G can be a subgroup of $A(E)$ for some E if and only if G is isomorphic to one of the following:
(1) *abelian case:*

(1.1) Z_m $(m \geq 1)$ or $Z_m \oplus Z_{mk}$ $(m \geq 2,\ k \geq 1)$

(1.2) Z_2, $Z_2{}^{\oplus 2}$, $Z_2{}^{\oplus 3}$, Z_3, $Z_3{}^{\oplus 2}$, Z_4, $Z_2 \oplus Z_4$ or Z_6

(2) *non-abelian case:*

(2.1) D_n or BD_{mn} $(n \geq 3)$

(2.2) $E(k,l)$ or $E(m,k,l)$

Moreover, the cases (1.1), (1.2), (2.1) *and* (2.1) *appear in the cases where* $|G_0| = 1$, $|G_0| > 1$, $|G_0| = 2$ *and* $|G_0| > 2$ *respectively.*

Theorem

A finite group G can be a subgroup of $A(E)$ for some E if and only if G is isomorphic to one of the following:
(1) *abelian case:*

(1.1) Z_m $(m \geq 1)$ or $Z_m \oplus Z_{mk}$ $(m \geq 2,\ k \geq 1)$

(1.2) Z_2, ${Z_2}^{\oplus 2}$, ${Z_2}^{\oplus 3}$, Z_3, ${Z_3}^{\oplus 2}$, Z_4, $Z_2 \oplus Z_4$ or Z_6

(2) *non-abelian case:*

(2.1) D_n or BD_{mn} $(n \geq 3)$

(2.2) $E(k,l)$ or $E(m,k,l)$

Moreover, the cases (1.1), (1.2), (2.1) *and* (2.1) *appear in the cases where* $|G_0| = 1$, $|G_0| > 1$, $|G_0| = 2$ *and* $|G_0| > 2$ *respectively.*

Theorem

A finite group G can be a subgroup of $A(E)$ for some E if and only if G is isomorphic to one of the following:
(1) *abelian case:*

(1.1) Z_m $(m \geq 1)$ or $Z_m \oplus Z_{mk}$ $(m \geq 2,\ k \geq 1)$

(1.2) $Z_2,\ {Z_2}^{\oplus 2},\ {Z_2}^{\oplus 3},\ Z_3,\ {Z_3}^{\oplus 2},\ Z_4,\ Z_2 \oplus Z_4$ or Z_6

(2) *non-abelian case:*

(2.1) D_n or BD_{mn} $(n \geq 3)$

(2.2) $E(k,l)$ or $E(m,k,l)$

Moreover, the cases (1.1), (1.2), (2.1) *and* (2.1) *appear in the cases*
where $|G_0| = 1,\ |G_0| > 1,\ |G_0| = 2$ *and* $|G_0| > 2$ *respectively.*

Theorem

A finite group G can be a subgroup of $A(E)$ *for some* E *if and only if G is isomorphic to one of the following*:

(1) *abelian case:*

(1.1) Z_m $(m \geq 1)$ or $Z_m \oplus Z_{mk}$ $(m \geq 2,\ k \geq 1)$

(1.2) $Z_2,\ {Z_2}^{\oplus 2},\ {Z_2}^{\oplus 3},\ Z_3,\ {Z_3}^{\oplus 2},\ Z_4,\ Z_2 \oplus Z_4$ or Z_6

(2) *non-abelian case:*

(2.1) D_n or BD_{mn} $(n \geq 3)$

(2.2) $E(k,l)$ or $E(m,k,l)$

Moreover, the cases (1.1), (1.2), (2.1) *and* (2.1) *appear in the cases*

where $|G_0| = 1,\ |G_0| > 1,\ |G_0| = 2$ *and* $|G_0| > 2$ *respectively.*

Theorem

A finite group G can be a subgroup of $A(E)$ for some E if and only if G is isomorphic to one of the following:
(1) *abelian case:*

(1.1) Z_m $(m \geq 1)$ or $Z_m \oplus Z_{mk}$ $(m \geq 2,\ k \geq 1)$

(1.2) Z_2, ${Z_2}^{\oplus 2}$, ${Z_2}^{\oplus 3}$, Z_3, ${Z_3}^{\oplus 2}$, Z_4, $Z_2 \oplus Z_4$ or Z_6

(2) *non-abelian case:*

(2.1) D_n or BD_{mn} $(n \geq 3)$

(2.2) $E(k,l)$ or $E(m,k,l)$

Moreover, the cases (1.1), (1.2), (2.1) *and* (2.1) *appear in the cases where* $|G_0| = 1$, $|G_0| > 1$, $|G_0| = 2$ *and* $|G_0| > 2$ *respectively.*

Theorem

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff G is one of the following:

(1) *abelian case:*
$Z_2{}^{\oplus 2}$, $Z_2{}^{\oplus 3}$, Z_3, $Z_3{}^{\oplus 2}$, Z_4, $Z_2 \oplus Z_4$ *or* Z_6

(2) *non-abelian case:*
D_m, BD_{mn}, $E(k,l)$ *or* $E(m,k,l)$

Theorem

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff G is one of the following:

(1) *abelian case:*
$Z_2{}^{\oplus 2}$, $Z_2{}^{\oplus 3}$, Z_3, $Z_3{}^{\oplus 2}$, Z_4, $Z_2 \oplus Z_4$ *or* Z_6

(2) *non-abelian case:*
D_m, BD_{mn}, $E(k,l)$ *or* $E(m,k,l)$

Theorem

A finite subgroup G of $Aut(E)$ can be a Galois group of some Galois embedding of E iff G is one of the following:

(1) *abelian case:*
$Z_2{}^{\oplus 2}$, $Z_2{}^{\oplus 3}$, Z_3, $Z_3{}^{\oplus 2}$, Z_4, $Z_2 \oplus Z_4$ *or* Z_6

(2) *non-abelian case:*
D_m, BD_{mn}, $E(k,l)$ *or* $E(m,k,l)$

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point.

Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x, y)^G = \mathbb{C}(s)$.

Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.

Let D be the polar divisor of s on E.

Next, find an element $t \in \mathbb{C}(x, y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x, y) = \mathbb{C}(s, t)$.

Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*

Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem
and suppose $\mathbb{C}(x,y)^G = \mathbb{C}(s)$.
Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.
Let D be the polar divisor of s on E.
Next, find an element $t \in \mathbb{C}(x,y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.
Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*
Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x, y)^G = \mathbb{C}(s)$.

Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.

Let D be the polar divisor of s on E.

Next, find an element $t \in \mathbb{C}(x, y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x, y) = \mathbb{C}(s, t)$.

Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*

Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x,y)^G = \mathbb{C}(s)$.
Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.
Let D be the polar divisor of s on E.
Next, find an element $t \in \mathbb{C}(x,y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.
Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*
Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x, y)^G = \mathbb{C}(s)$.
Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.
Let D be the polar divisor of s on E.
Next, find an element $t \in \mathbb{C}(x, y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x, y) = \mathbb{C}(s, t)$.
Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*
Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x, y)^G = \mathbb{C}(s)$.
Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.
Let D be the polar divisor of s on E.
Next, find an element $t \in \mathbb{C}(x, y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x, y) = \mathbb{C}(s, t)$.
Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*
Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x, y)^G = \mathbb{C}(s)$.
Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.
Let D be the polar divisor of s on E.
Next, find an element $t \in \mathbb{C}(x, y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x, y) = \mathbb{C}(s, t)$.
Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*
Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x, y)^G = \mathbb{C}(s)$.
Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.
Let D be the polar divisor of s on E.
Next, find an element $t \in \mathbb{C}(x, y)$ satisfying that $\mathrm{div}(t) + D \geq 0$ and $\mathbb{C}(x, y) = \mathbb{C}(s, t)$.
Then, the curve C defined by s and t has the Galois point at ∞ with the Galois group G.
Of course C is birational to E.

Make examples

Remark

By projecting an embedded elliptic curve with Galois subspace into the plane, we get a singular elliptic curve with Galois point. Let us make examples of plane elliptic curve with a Galois point. Let G be the group in the above theorem and suppose $\mathbb{C}(x,y)^G = \mathbb{C}(s)$.
Then, taking an affine coordinate s, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$.
Let D be the polar divisor of s on E.
Next, find an element $t \in \mathbb{C}(x,y)$ *satisfying that* $\mathrm{div}(t) + D \geq 0$ *and* $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.
Then, the curve C defined by s and t has the Galois point at ∞ *with the Galois group G.*
Of course C is birational to E.

Example

Let $E : y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$.
Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$, where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.
The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2} \right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

$Z_2^{\oplus 2}$

Example

Let $E : y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$.
Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$, where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.
The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2} \right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

Example

Let $E : y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$.
Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that
the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$,
where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.
The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2}\right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

$Z_2^{\oplus 2}$

Example

Let $E : y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$. Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$, where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.

The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2} \right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

Example

Let $E: y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$.
Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$, where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.
The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2} \right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

Example

Let $E : y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$.
Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$, where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.
The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2} \right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

Example

Let $E : y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$.
Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$, where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.
The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2} \right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

Example

Let $E : y^2 = x(x-1)(x-b)$ be an elliptic curve, where $b \neq 0, 1$.
Take the automorphisms σ and τ of $\mathbb{C}(x, y)$ such that the complex representations are $\widetilde{\sigma}(z) = -z$ and $\widetilde{\tau}(z) = z + \beta$, where $2\beta \in \mathcal{L}$ and $\beta \notin \mathcal{L}$.
The point $(b, 0) \in E$ is of order 2 and we have

$$(x, y) * (b, 0) = \left(\frac{b(x-1)}{x-b}, \frac{b(b-1)y}{(x-b)^2} \right).$$

Then the translation τ of order two can be expressed as

$$\tau(x) = \frac{b(x-1)}{x-b} \text{ and } \tau(y) = \frac{b(b-1)y}{(x-b)^2}.$$

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2 - b}{x - b}$ is invariant by τ.

so put $s = \dfrac{x^2 - b}{x - b}$.

Let Q_1 and Q_2 be the points $(b : 0 : 1)$ and $(0 : 1 : 0)$ on E respectively,

where $(X : Y : Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.

Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2 - b}{x - b}$ is D.

Putting $t = \dfrac{y + a}{x - b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2 - b}{x - b}$ is invariant by τ.

so put $s = \dfrac{x^2 - b}{x - b}$.

Let Q_1 and Q_2 be the points $(b : 0 : 1)$ and $(0 : 1 : 0)$ on E respectively,

where $(X : Y : Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.

Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2 - b}{x - b}$ is D.

Putting $t = \dfrac{y + a}{x - b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2-b}{x-b}$ is invariant by τ.

so put $s = \dfrac{x^2-b}{x-b}$.

Let Q_1 and Q_2 be the points $(b:0:1)$ and $(0:1:0)$ on E respectively,
where $(X:Y:Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.
Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2-b}{x-b}$ is D.

Putting $t = \dfrac{y+a}{x-b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2-b}{x-b}$ is invariant by τ.

so put $s = \dfrac{x^2-b}{x-b}$.

Let Q_1 and Q_2 be the points $(b:0:1)$ and $(0:1:0)$ on E respectively,

where $(X:Y:Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.

Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2-b}{x-b}$ is D.

Putting $t = \dfrac{y+a}{x-b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2-b}{x-b}$ is invariant by τ.

so put $s = \dfrac{x^2-b}{x-b}$.

Let Q_1 and Q_2 be the points $(b:0:1)$ and $(0:1:0)$ on E respectively,

where $(X:Y:Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.

Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2-b}{x-b}$ is D.

Putting $t = \dfrac{y+a}{x-b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2-b}{x-b}$ is invariant by τ.

so put $s = \dfrac{x^2-b}{x-b}$.

Let Q_1 and Q_2 be the points $(b:0:1)$ and $(0:1:0)$ on E respectively,

where $(X:Y:Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.

Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2-b}{x-b}$ is D.

Putting $t = \dfrac{y+a}{x-b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2-b}{x-b}$ is invariant by τ.

so put $s = \dfrac{x^2-b}{x-b}$.

Let Q_1 and Q_2 be the points $(b:0:1)$ and $(0:1:0)$ on E respectively,

where $(X:Y:Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.

Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2-b}{x-b}$ is D.

Putting $t = \dfrac{y+a}{x-b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Since ∞ is the zero element and is fixed by σ, we see $\sigma(x) = x$, $\sigma(y) = -y$.

Let $G = \langle \sigma, \tau \rangle$. Crealy $x + \dfrac{b(x-1)}{x-b} = \dfrac{x^2-b}{x-b}$ is invariant by τ.

so put $s = \dfrac{x^2-b}{x-b}$.

Let Q_1 and Q_2 be the points $(b:0:1)$ and $(0:1:0)$ on E respectively,

where $(X:Y:Z)$ are homogeneous coordinates satisfying $x = X/Z$ and $y = Y/Z$.

Then put $D = 2Q_1 + 2Q_2$ as a divisor.

It is easy to see that the pole divisor of $\dfrac{x^2-b}{x-b}$ is D.

Putting $t = \dfrac{y+a}{x-b}$, where $a \neq 0, \pm 1$, we have $\mathrm{div}(t) + D \geq 0$.

$Z_2^{\oplus 2}$ (Continuation)

Example

Using the equations $s = \dfrac{x^2 - b}{x - b}$, $t = \dfrac{y + a}{x - b}$ and $y^2 = x(x-1)(x-b)$,

we infer by some computations that $\mathbb{C}(s,t) \ni x$ if $a \neq 0, \pm 1$.

Therefore we have $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.

Thus we have the defining equation

$$a^4 + a^3(4b - 2s)t + abt(-4b + 4b^2 + 2s + 2bs - 4b^2s - 2s^2 + 2bs^2 - 4bt^2 + 4b^2t^2 + 2st^2 - 2bst^2) + a^2(2b + 2b^2 - 6bs - 2b^2s + s^2 + 4bs^2 - s^3 - 2bt^2 + 6b^2t^2 - 4bst^2 + s^2t^2) = b^2(-1 + 2b - b^2 + 2s - 4bs + 2b^2s - s^2 + 2bs^2 - b^2s^2 - 2t^2 + 4bt^2 - 2b^2t^2 + 2st^2 - 4bst^2 + 2b^2st^2 - t^4 + 2bt^4 - b^2t^4)$$

${Z_2}^{\oplus 2}$ (Continuation)

Example

Using the equations $s = \dfrac{x^2 - b}{x - b}$, $t = \dfrac{y + a}{x - b}$ and
$y^2 = x(x-1)(x-b)$,
we infer by some computations that $\mathbb{C}(s,t) \ni x$ if $a \neq 0, \pm 1$.
Therefore we have $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.
Thus we have the defining equation

$$a^4 + a^3(4b - 2s)t + abt(-4b + 4b^2 + 2s + 2bs - 4b^2s - 2s^2 + 2bs^2 - 4bt^2 + 4b^2t^2 + 2st^2 - 2bst^2) + a^2(2b + 2b^2 - 6bs - 2b^2s + s^2 + 4bs^2 - s^3 - 2bt^2 + 6b^2t^2 - 4bst^2 + s^2t^2) = b^2(-1 + 2b - b^2 + 2s - 4bs + 2b^2s - s^2 + 2bs^2 - b^2s^2 - 2t^2 + 4bt^2 - 2b^2t^2 + 2st^2 - 4bst^2 + 2b^2st^2 - t^4 + 2bt^4 - b^2t^4)$$

$Z_2^{\oplus 2}$ (Continuation)

Example

Using the equations $s = \dfrac{x^2 - b}{x - b}$, $t = \dfrac{y + a}{x - b}$ and

$y^2 = x(x-1)(x-b)$,

we infer by some computations that $\mathbb{C}(s,t) \ni x$ if $a \neq 0, \pm 1$.

Therefore we have $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.

Thus we have the defining equation

$$a^4 + a^3(4b - 2s)t + abt(-4b + 4b^2 + 2s + 2bs - 4b^2s - 2s^2 + 2bs^2 - 4bt^2 + 4b^2t^2 + 2st^2 - 2bst^2) + a^2(2b + 2b^2 - 6bs - 2b^2s + s^2 + 4bs^2 - s^3 - 2bt^2 + 6b^2t^2 - 4bst^2 + s^2t^2) = b^2(-1 + 2b - b^2 + 2s - 4bs + 2b^2s - s^2 + 2bs^2 - b^2s^2 - 2t^2 + 4bt^2 - 2b^2t^2 + 2st^2 - 4bst^2 + 2b^2st^2 - t^4 + 2bt^4 - b^2t^4)$$

$Z_2^{\oplus 2}$ (Continuation)

Example

Using the equations $s = \dfrac{x^2 - b}{x - b}$, $t = \dfrac{y + a}{x - b}$ and
$y^2 = x(x-1)(x-b)$,
we infer by some computations that $\mathbb{C}(s,t) \ni x$ if $a \neq 0, \pm 1$.
Therefore we have $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.
Thus we have the defining equation

$$a^4 + a^3(4b - 2s)t + abt(-4b + 4b^2 + 2s + 2bs - 4b^2s - 2s^2 + 2bs^2 - 4bt^2 + 4b^2t^2 + 2st^2 - 2bst^2) + a^2(2b + 2b^2 - 6bs - 2b^2s + s^2 + 4bs^2 - s^3 - 2bt^2 + 6b^2t^2 - 4bst^2 + s^2t^2) = b^2(-1 + 2b - b^2 + 2s - 4bs + 2b^2s - s^2 + 2bs^2 - b^2s^2 - 2t^2 + 4bt^2 - 2b^2t^2 + 2st^2 - 4bst^2 + 2b^2st^2 - t^4 + 2bt^4 - b^2t^4)$$

Very ampleness

Lemma

Now, return to the case of abelian surface.
we apply the above method to abelian surfaces.
Let A be an abelian surface. Assume that G is a finite automorphism group of A
satisfying that A/G is isomorphic to $\mathbb{P}^2$
and let $\pi : A \longrightarrow \mathbb{P}^2$ be the quotient morphism.
If $\deg \pi \geq 10$, then $\pi^*(\ell) = D$ is very ample for each line ℓ in $\mathbb{P}^2$.

Corollary

Under the same assumption and notation of the above lemma, the pair (A, D) defines a Galois embedding.

Very ampleness

Lemma

Now, return to the case of abelian surface.
we apply the above method to abelian surfaces.
Let A be an abelian surface. Assume that G is a finite automorphism group of A satisfying that A/G is isomorphic to $\mathbb{P}^2$ and let $\pi : A \longrightarrow \mathbb{P}^2$ be the quotient morphism. If $\deg \pi \geq 10$, then $\pi^*(\ell) = D$ is very ample for each line ℓ in $\mathbb{P}^2$.

Corollary

Under the same assumption and notation of the above lemma, the pair (A, D) defines a Galois embedding.

Very ampleness

Lemma

Now, return to the case of abelian surface.
we apply the above method to abelian surfaces.
Let A be an abelian surface. Assume that G is a finite automorphism group of A
satisfying that A/G is isomorphic to $\mathbb{P}^2$
and let $\pi : A \longrightarrow \mathbb{P}^2$ be the quotient morphism.
If $\deg \pi \geq 10$, then $\pi^*(\ell) = D$ is very ample for each line ℓ in $\mathbb{P}^2$.

Corollary

Under the same assumption and notation of the above lemma, the pair (A, D) defines a Galois embedding.

Very ampleness

Lemma

Now, return to the case of abelian surface.
we apply the above method to abelian surfaces.
Let A be an abelian surface. Assume that G is a finite automorphism group of A
satisfying that A/G is isomorphic to $\mathbb{P}^2$
and let $\pi : A \longrightarrow \mathbb{P}^2$ be the quotient morphism.
If $\deg \pi \geq 10$, then $\pi^*(\ell) = D$ is very ample for each line ℓ in $\mathbb{P}^2$.

Corollary

Under the same assumption and notation of the above lemma, the pair (A, D) defines a Galois embedding.

Very ampleness

Lemma

Now, return to the case of abelian surface.
we apply the above method to abelian surfaces.
Let A be an abelian surface. Assume that G is a finite automorphism group of A
satisfying that A/G is isomorphic to $\mathbb{P}^2$
and let $\pi : A \longrightarrow \mathbb{P}^2$ be the quotient morphism.
If $\deg \pi \geq 10$, then $\pi^*(\ell) = D$ is very ample for each line ℓ in $\mathbb{P}^2$.

Corollary

Under the same assumption and notation of the above lemma, the pair (A, D) defines a Galois embedding.

Very ampleness

Lemma

Now, return to the case of abelian surface.
we apply the above method to abelian surfaces.
Let A be an abelian surface. Assume that G is a finite automorphism group of A
satisfying that A/G is isomorphic to $\mathbb{P}^2$
and let $\pi : A \longrightarrow \mathbb{P}^2$ be the quotient morphism.
If $\deg \pi \geq 10$, then $\pi^*(\ell) = D$ is very ample for each line ℓ in $\mathbb{P}^2$.

Corollary

Under the same assumption and notation of the above lemma, the pair (A, D) defines a Galois embedding.

Very ampleness

Lemma

Now, return to the case of abelian surface.
we apply the above method to abelian surfaces.
Let A be an abelian surface. Assume that G is a finite automorphism group of A
satisfying that A/G is isomorphic to $\mathbb{P}^2$
and let $\pi : A \longrightarrow \mathbb{P}^2$ be the quotient morphism.
If $\deg \pi \geq 10$, then $\pi^*(\ell) = D$ is very ample for each line ℓ in $\mathbb{P}^2$.

Corollary

Under the same assumption and notation of the above lemma, the pair (A, D) defines a Galois embedding.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups:* $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$
To state case (3) more precisely, we put $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*
In the former case $H' \cong D_4$, *we have*
$aba = bc^2$, $aca = c$, $c^4 = 1$, $b^2 = 1$ *and* $bcb = c^{-1}$.
In the latter case $H' \cong Z_m \times Z_m$, *we have*
$aba = b^{-1}$, $aca = c^{-1}$, $b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups*: $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$
To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*
In the former case $H' \cong D_4$, *we have*
$aba = bc^2,\ aca = c,\ c^4 = 1,\ b^2 = 1$ *and* $bcb = c^{-1}$.
In the latter case $H' \cong Z_m \times Z_m$, *we have*
$aba = b^{-1},\ aca = c^{-1},\ b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups:* $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$
To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*
In the former case $H' \cong D_4$, *we have* $aba = bc^2,\ aca = c,\ c^4 = 1,\ b^2 = 1$ *and* $bcb = c^{-1}$.
In the latter case $H' \cong Z_m \times Z_m$, *we have* $aba = b^{-1},\ aca = c^{-1},\ b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups*: $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$

To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*

In the former case $H' \cong D_4$, *we have*
$aba = bc^2, \ aca = c, \ c^4 = 1, \ b^2 = 1$ *and* $bcb = c^{-1}$.

In the latter case $H' \cong Z_m \times Z_m$, *we have*
$aba = b^{-1}, \ aca = c^{-1}, \ b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups:* $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$

To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*

In the former case $H' \cong D_4$, *we have* $aba = bc^2$, $aca = c$, $c^4 = 1$, $b^2 = 1$ *and* $bcb = c^{-1}$.

In the latter case $H' \cong Z_m \times Z_m$, *we have* $aba = b^{-1}$, $aca = c^{-1}$, $b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups:* $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$
To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$*. Then the actions of* Z_2 *on* H' *are as follows:*
In the former case $H' \cong D_4$*, we have*
$aba = bc^2,\ aca = c,\ c^4 = 1,\ b^2 = 1$ *and* $bcb = c^{-1}$.
In the latter case $H' \cong Z_m \times Z_m$*, we have*
$aba = b^{-1},\ aca = c^{-1},\ b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ *is isomorphic to one of the following:*

(1) D_3

(2) D_4

(3) *the semi-direct product of groups:* $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$
To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*
In the former case $H' \cong D_4$, *we have*
$aba = bc^2, \ aca = c, \ c^4 = 1, \ b^2 = 1$ *and* $bcb = c^{-1}$.
In the latter case $H' \cong Z_m \times Z_m$, *we have*
$aba = b^{-1}, \ aca = c^{-1}, \ b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups:* $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$
To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*
In the former case $H' \cong D_4$, *we have*
$aba = bc^2, \; aca = c, \; c^4 = 1, \; b^2 = 1$ *and* $bcb = c^{-1}$.
In the latter case $H' \cong Z_m \times Z_m$, *we have*
$aba = b^{-1}, \; aca = c^{-1}, \; b^m = c^m = 1$ *and* $bc = cb$.

Theorem

Theorem

If an abelian surface A has the Galois embedding, then $H = G/G_0$ is isomorphic to one of the following:

(1) D_3

(2) D_4

(3) *the semi-direct product of groups:* $Z_2 \ltimes H'$, *where* $H' \cong D_4$ *or* $Z_m \times Z_m$ $(m = 3, 4, 6)$
To state case (3) *more precisely, we put* $Z_2 = \langle a \rangle$ *and* $H' = \langle b, c \rangle$. *Then the actions of* Z_2 *on* H' *are as follows:*
In the former case $H' \cong D_4$, *we have*
$aba = bc^2,\ aca = c,\ c^4 = 1,\ b^2 = 1$ *and* $bcb = c^{-1}$.
In the latter case $H' \cong Z_m \times Z_m$, *we have*
$aba = b^{-1},\ aca = c^{-1},\ b^m = c^m = 1$ *and* $bc = cb$.

Corollary

If A has a Galois embedding, then the abelian surface $B = A/G_0$ is isomorphic to $E \times E$ for some elliptic curve E.

Example 1

Example

Let A be the abelian surface with the period matrix

$$\Omega = \begin{pmatrix} -1 & \rho^2 & -\tau & \tau\rho^2 \\ 1 & \rho & \tau & \tau\rho \end{pmatrix} = \begin{pmatrix} -1 & \rho^2 \\ 1 & \rho \end{pmatrix} \begin{pmatrix} 1 & 0 & \tau & 0 \\ 0 & 1 & 0 & \tau \end{pmatrix},$$

where $\Im\tau > 0$ and $\rho = \exp(2\pi\sqrt{-1}/6)$. Clearly we have $A \cong E \times E$ where $E = \mathbb{C}/(1, \tau)$.

Letting $z \in \mathbb{C}^2$ and $\boldsymbol{v}_i$ be the i-th column vector of Ω $(1 \leq i \leq 4)$, we define t_i to be the translation on A such that $t_i z = z + \boldsymbol{v}_i/m$, where m is an integer ≥ 2.

Let a and b be the automorphism of A such that the complex representations are

Example 1

Example

Let A be the abelian surface with the period matrix

$$\Omega = \begin{pmatrix} -1 & \rho^2 & -\tau & \tau\rho^2 \\ 1 & \rho & \tau & \tau\rho \end{pmatrix} = \begin{pmatrix} -1 & \rho^2 \\ 1 & \rho \end{pmatrix} \begin{pmatrix} 1 & 0 & \tau & 0 \\ 0 & 1 & 0 & \tau \end{pmatrix},$$

where $\Im\tau > 0$ and $\rho = \exp(2\pi\sqrt{-1}/6)$. Clearly we have $A \cong E \times E$ where $E = \mathbb{C}/(1, \tau)$.
Letting $z \in \mathbb{C}^2$ and $\boldsymbol{v}_i$ be the i-th column vector of Ω $(1 \leq i \leq 4)$, we define t_i to be the translation on A such that $t_i z = z + \boldsymbol{v}_i/m$, where m is an integer ≥ 2.
Let a and b be the automorphism of A such that the complex representations are

Example 1

Example

Let A be the abelian surface with the period matrix

$$\Omega = \begin{pmatrix} -1 & \rho^2 & -\tau & \tau\rho^2 \\ 1 & \rho & \tau & \tau\rho \end{pmatrix} = \begin{pmatrix} -1 & \rho^2 \\ 1 & \rho \end{pmatrix} \begin{pmatrix} 1 & 0 & \tau & 0 \\ 0 & 1 & 0 & \tau \end{pmatrix},$$

where $\Im\tau > 0$ and $\rho = \exp(2\pi\sqrt{-1}/6)$. Clearly we have $A \cong E \times E$ where $E = \mathbb{C}/(1, \tau)$.

Letting $z \in \mathbb{C}^2$ and $\boldsymbol{v}_i$ be the i-th column vector of Ω $(1 \leq i \leq 4)$, we define t_i to be the translation on A such that $t_i z = z + \boldsymbol{v}_i/m$, where m is an integer ≥ 2.

Let a and b be the automorphism of A such that the complex representations are

Example 1

Example

Let A be the abelian surface with the period matrix

$$\Omega = \begin{pmatrix} -1 & \rho^2 & -\tau & \tau\rho^2 \\ 1 & \rho & \tau & \tau\rho \end{pmatrix} = \begin{pmatrix} -1 & \rho^2 \\ 1 & \rho \end{pmatrix} \begin{pmatrix} 1 & 0 & \tau & 0 \\ 0 & 1 & 0 & \tau \end{pmatrix},$$

where $\Im\tau > 0$ and $\rho = \exp(2\pi\sqrt{-1}/6)$. Clearly we have $A \cong E \times E$ where $E = \mathbb{C}/(1, \tau)$.
Letting $z \in \mathbb{C}^2$ and $\boldsymbol{v}_i$ be the i-th column vector of Ω $(1 \leq i \leq 4)$, we define t_i to be the translation on A such that $t_i z = z + \boldsymbol{v}_i/m$, where m is an integer ≥ 2.
Let a and b be the automorphism of A such that the complex representations are

Example 1

Example

Let A be the abelian surface with the period matrix

$$\Omega = \begin{pmatrix} -1 & \rho^2 & -\tau & \tau\rho^2 \\ 1 & \rho & \tau & \tau\rho \end{pmatrix} = \begin{pmatrix} -1 & \rho^2 \\ 1 & \rho \end{pmatrix} \begin{pmatrix} 1 & 0 & \tau & 0 \\ 0 & 1 & 0 & \tau \end{pmatrix},$$

where $\Im\tau > 0$ and $\rho = \exp(2\pi\sqrt{-1}/6)$. Clearly we have $A \cong E \times E$ where $E = \mathbb{C}/(1, \tau)$.
Letting $z \in \mathbb{C}^2$ and $\boldsymbol{v}_i$ be the i-th column vector of Ω $(1 \leq i \leq 4)$, we define t_i to be the translation on A such that $t_i z = z + \boldsymbol{v}_i/m$, where m is an integer ≥ 2.
Let a and b be the automorphism of A such that the complex representations are

Example 1

Example

Let A be the abelian surface with the period matrix

$$\Omega = \begin{pmatrix} -1 & \rho^2 & -\tau & \tau\rho^2 \\ 1 & \rho & \tau & \tau\rho \end{pmatrix} = \begin{pmatrix} -1 & \rho^2 \\ 1 & \rho \end{pmatrix} \begin{pmatrix} 1 & 0 & \tau & 0 \\ 0 & 1 & 0 & \tau \end{pmatrix},$$

where $\Im\tau > 0$ and $\rho = \exp(2\pi\sqrt{-1}/6)$. Clearly we have $A \cong E \times E$ where $E = \mathbb{C}/(1, \tau)$.
Letting $z \in \mathbb{C}^2$ and $\boldsymbol{v}_i$ be the i-th column vector of Ω $(1 \leq i \leq 4)$, we define t_i to be the translation on A such that $t_i z = z + \boldsymbol{v}_i/m$, where m is an integer ≥ 2.
Let a and b be the automorphism of A such that the complex representations are

Example 1

Example

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} -\rho & 0 \\ 0 & \rho^2 \end{pmatrix}$$

respectively. Put $G_0 = \langle t_1, \ldots, t_4 \rangle$ and $G = \langle G_0, a, b \rangle$.
Then G_0 is a normal subgroup of G and $G/G_0 \cong D_3$.
Clearly we have $|G| = 6m^4$. Looking at the fixed loci of H, we infer that A/G is smooth.

Example 1

Example

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} -\rho & 0 \\ 0 & \rho^2 \end{pmatrix}$$

respectively. Put $G_0 = \langle t_1, \dots, t_4 \rangle$ and $G = \langle G_0, a, b \rangle$.
Then G_0 is a normal subgroup of G and $G/G_0 \cong D_3$.
Clearly we have $|G| = 6m^4$. Looking at the fixed loci of H, we infer that A/G is smooth.

Example 1

Example

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} -\rho & 0 \\ 0 & \rho^2 \end{pmatrix}$$

respectively. Put $G_0 = \langle t_1, \ldots, t_4 \rangle$ and $G = \langle G_0, a, b \rangle$. Then G_0 is a normal subgroup of G and $G/G_0 \cong D_3$.
Clearly we have $|G| = 6m^4$. Looking at the fixed loci of H, we infer that A/G is smooth.

Example 1

Example

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} -\rho & 0 \\ 0 & \rho^2 \end{pmatrix}$$

respectively. Put $G_0 = \langle t_1, \ldots, t_4 \rangle$ and $G = \langle G_0, a, b \rangle$.
Then G_0 is a normal subgroup of G and $G/G_0 \cong D_3$.
Clearly we have $|G| = 6m^4$. Looking at the fixed loci of H, we infer that A/G is smooth.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then $G = \langle a,\ b \rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then $G = \langle a,\ b\rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then $G = \langle a,\ b \rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then $G = \langle a,\ b\rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then $G = \langle a,\ b\rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then $G = \langle a,\ b\rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then
$G = \langle a,\ b\rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Example 2

Example

Let E be the elliptic curve $\mathbb{C}/\Omega$,
where $\Omega = (1, \tau)$ is a period matrix such that $\Im\tau > 0$.
Let a and b be the automorphisms of E defined by $a(z) = -z$ and $b(z) = z + 1/m$ respectively,
where $z \in \mathbb{C}$ and m is a positive integer ≥ 2.
Let G be the subgroup of $Aut(E)$ generated by a, b. Then $G = \langle a,\ b\rangle \cong D_m$; the dihedral group of order $2m$.
Let $y^2 = 4x^3 + px + q$ be the Weierstrass normal form of E and $K = \mathbb{C}(x, y)$.
Then the fixed field of K by G is rational $\mathbb{C}(t)$, where $t \in \mathbb{C}(x)$.
Putting $D = (t)_\infty$; the divisor of poles of t, we infer readily that $\deg D = 2m$ and (E, D) defines a Galois embedding for each m.

Continuation

Example

Let E be the elliptic curve E in the example above such that $\tau = e_m,\ m = 3,\ 4$ or 6.
Let A be the abelian surface $E \times E$. We define automorphisms on A as follows:
let a, b and c be the homomorphisms whose complex representations are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \tau \end{pmatrix}$$

respectively. Let $G = \langle a, b, c \rangle$.

Continuation

Example

Let E be the elliptic curve E in the example above such that $\tau = e_m,\ m = 3,\ 4$ or 6.
Let A be the abelian surface $E \times E$. We define automorphisms on A as follows:
let a, b and c be the homomorphisms whose complex representations are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \tau \end{pmatrix}$$

respectively. Let $G = \langle a, b, c \rangle$.

Continuation

Example

Let E be the elliptic curve E in the example above such that $\tau = e_m, \ m = 3, \ 4 \text{ or } 6$.
Let A be the abelian surface $E \times E$. We define automorphisms on A as follows:
let a, b and c be the homomorphisms whose complex representations are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \tau \end{pmatrix}$$

respectively. Let $G = \langle a, b, c \rangle$.

Continuation

Example

Let E be the elliptic curve E in the example above such that $\tau = e_m,\ m = 3,\ 4 \text{ or } 6$.
Let A be the abelian surface $E \times E$. We define automorphisms on A as follows:
let a, b and c be the homomorphisms whose complex representations are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \tau \end{pmatrix}$$

respectively. Let $G = \langle a, b, c \rangle$.

Continuation

Example

Let E be the elliptic curve E in the example above such that $\tau = e_m, \ m = 3, \ 4 \text{ or } 6$.
Let A be the abelian surface $E \times E$. We define automorphisms on A as follows:
let a, b and c be the homomorphisms whose complex representations are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \tau \end{pmatrix}$$

respectively. Let $G = \langle a, b, c \rangle$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.

Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.

Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,

then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.

It is well known that D is very ample if $n \geq 3$.

We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.

Let us examine the case $m = 3$ in a different point of view.

Since E is defined by the Weierstrass normal form

$y^2 = 4x^3 + 1$,

we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where ${y'}^2 = 4{x'}^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.
Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.
Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,
then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.
It is well known that D is very ample if $n \geq 3$.
We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.
Let us examine the case $m = 3$ in a different point of view.
Since E is defined by the Weierstrass normal form
$y^2 = 4x^3 + 1$,
we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where ${y'}^2 = 4{x'}^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.

Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.

Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,

then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.

It is well known that D is very ample if $n \geq 3$.

We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.

Let us examine the case $m = 3$ in a different point of view.

Since E is defined by the Weierstrass normal form

$y^2 = 4x^3 + 1$,

we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where ${y'}^2 = 4{x'}^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.
Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.
Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,
then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.
It is well known that D is very ample if $n \geq 3$.
We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.
Let us examine the case $m = 3$ in a different point of view.
Since E is defined by the Weierstrass normal form
$y^2 = 4x^3 + 1$,
we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where $y'^2 = 4x'^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.
Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.
Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,
then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.
It is well known that D is very ample if $n \geq 3$.
We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.
Let us examine the case $m = 3$ in a different point of view.
Since E is defined by the Weierstrass normal form
$y^2 = 4x^3 + 1$,
we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where ${y'}^2 = 4{x'}^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.
Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.
Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,
then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.
It is well known that D is very ample if $n \geq 3$.
We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.
Let us examine the case $m = 3$ in a different point of view.
Since E is defined by the Weierstrass normal form
$y^2 = 4x^3 + 1$,
we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where $y'^2 = 4x'^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.
Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.
Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,
then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.
It is well known that D is very ample if $n \geq 3$.
We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.
Let us examine the case $m = 3$ in a different point of view.
Since E is defined by the Weierstrass normal form
$y^2 = 4x^3 + 1$,
we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where $y'^2 = 4x'^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.
Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.
Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,
then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.
It is well known that D is very ample if $n \geq 3$.
We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.
Let us examine the case $m = 3$ in a different point of view.
Since E is defined by the Weierstrass normal form
$y^2 = 4x^3 + 1$,
we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where ${y'}^2 = 4{x'}^3 + 1$.

Continuation

Example

Clearly we have $a^2 = b^m = c^m = 1,\ bc = cb,\ ca = ab$ and $ba = ac$, and $|G| = 2m^2$.
Moreover we have $G \cong Z_2 \ltimes (Z_m \times Z_m)$.
Put $E_1 = E \times \{0\}$ and $E_2 = \{0\} \times E$, where 0 is the zero element of E,
then put $D = n(E_1 + E_2)$, clearly we have $D^2 = 2n^2$.
It is well known that D is very ample if $n \geq 3$.
We see from the criterion that (A, D) defines a Galois embedding whose Galois group is isomorphic to G.
Let us examine the case $m = 3$ in a different point of view.
Since E is defined by the Weierstrass normal form
$y^2 = 4x^3 + 1$,
we have that $\mathbb{C}(A) = \mathbb{C}(x, y, x', y')$, where ${y'}^2 = 4{x'}^3 + 1$.

Continuation

Example

The automorphisms a, b and c induce the ones of $\mathbb{C}(A)$ as follows:

(1) a^* interchanges x and x', y and y'.

(2) $b^*(x) = \rho^2 x$ and b^* fixes y, x' and y'.

(3) $c^*(x') = \rho^2 x'$ and c^* fixes x, y and y'.

Therefore, the fixed field $\mathbb{C}(A)^G$ is $\mathbb{C}(y + y', yy')$, and we have $(y + y') + D \geq 0$ and $(yy') + D \geq 0$. Embedding by $3(E_1 + E_2)$ is the composition of the embedding $E \times E \hookrightarrow \mathbb{P}^2 \times \mathbb{P}^2$

Continuation

Example

The automorphisms a, b and c induce the ones of $\mathbb{C}(A)$ as follows:

(1) a^* interchanges x and x', y and y'.

(2) $b^*(x) = \rho^2 x$ and b^* fixes y, x' and y'.

(3) $c^*(x') = \rho^2 x'$ and c^* fixes x, y and y'.

Therefore, the fixed field $\mathbb{C}(A)^G$ is $\mathbb{C}(y + y', yy')$,
and we have $(y + y') + D \geq 0$ and $(yy') + D \geq 0$.
Embedding by $3(E_1 + E_2)$ is the composition of the embedding $E \times E \hookrightarrow \mathbb{P}^2 \times \mathbb{P}^2$

Continuation

Example

The automorphisms a, b and c induce the ones of $\mathbb{C}(A)$ as follows:

(1) a^* interchanges x and x', y and y'.

(2) $b^*(x) = \rho^2 x$ and b^* fixes y, x' and y'.

(3) $c^*(x') = \rho^2 x'$ and c^* fixes x, y and y'.

Therefore, the fixed field $\mathbb{C}(A)^G$ is $\mathbb{C}(y+y', yy')$,
and we have $(y+y') + D \geq 0$ and $(yy') + D \geq 0$.
Embedding by $3(E_1+E_2)$ is the composition of the embedding $E \times E \hookrightarrow \mathbb{P}^2 \times \mathbb{P}^2$

Continuation

Example

The automorphisms a, b and c induce the ones of $\mathbb{C}(A)$ as follows:

(1) a^* interchanges x and x', y and y'.

(2) $b^*(x) = \rho^2 x$ and b^* fixes y, x' and y'.

(3) $c^*(x') = \rho^2 x'$ and c^* fixes x, y and y'.

Therefore, the fixed field $\mathbb{C}(A)^G$ is $\mathbb{C}(y + y', yy')$,
and we have $(y + y') + D \geq 0$ and $(yy') + D \geq 0$.
Embedding by $3(E_1 + E_2)$ is the composition of the embedding
$E \times E \hookrightarrow \mathbb{P}^2 \times \mathbb{P}^2$

Continuation

Example

The automorphisms a, b and c induce the ones of $\mathbb{C}(A)$ as follows:

(1) a^* interchanges x and x', y and y'.

(2) $b^*(x) = \rho^2 x$ and b^* fixes y, x' and y'.

(3) $c^*(x') = \rho^2 x'$ and c^* fixes x, y and y'.

Therefore, the fixed field $\mathbb{C}(A)^G$ is $\mathbb{C}(y + y', yy')$,

and we have $(y + y') + D \geq 0$ and $(yy') + D \geq 0$.

Embedding by $3(E_1 + E_2)$ is the composition of the embedding $E \times E \hookrightarrow \mathbb{P}^2 \times \mathbb{P}^2$

Continuation

Example

The automorphisms a, b and c induce the ones of $\mathbb{C}(A)$ as follows:

(1) a^* interchanges x and x', y and y'.

(2) $b^*(x) = \rho^2 x$ and b^* fixes y, x' and y'.

(3) $c^*(x') = \rho^2 x'$ and c^* fixes x, y and y'.

Therefore, the fixed field $\mathbb{C}(A)^G$ is $\mathbb{C}(y + y', yy')$,
and we have $(y + y') + D \geq 0$ and $(yy') + D \geq 0$.
Embedding by $3(E_1 + E_2)$ is the composition of the embedding $E \times E \hookrightarrow \mathbb{P}^2 \times \mathbb{P}^2$

Continuation

Example

The automorphisms a, b and c induce the ones of $\mathbb{C}(A)$ as follows:

(1) a^* interchanges x and x', y and y'.

(2) $b^*(x) = \rho^2 x$ and b^* fixes y, x' and y'.

(3) $c^*(x') = \rho^2 x'$ and c^* fixes x, y and y'.

Therefore, the fixed field $\mathbb{C}(A)^G$ is $\mathbb{C}(y + y', yy')$,
and we have $(y + y') + D \geq 0$ and $(yy') + D \geq 0$.
Embedding by $3(E_1 + E_2)$ is the composition of the embedding $E \times E \hookrightarrow \mathbb{P}^2 \times \mathbb{P}^2$

Continuation

Example

followed by the Segre embedding $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$.
Using homogeneous coordinates (X, Y, Z) [resp. (X', Y', Z')] satisfying that $x = X/Z$, $y = Y/Z$ [resp. $x' = X'/Z', y' = Y'/Z'$],
we can express this embedding as

$$f(X, Y, Z, X', Y', Z') = (XX', YX', ZX', XY', \dots, ZZ').$$

Letting $(T_0, \cdots, T_8)$ be a set of homogeneous coordinates of $\mathbb{P}^8$,
we can express the Galois subspace by $T_5 + T_7 = T_4 = T_8 = 0$.

Continuation

Example

followed by the Segre embedding $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$.
Using homogeneous coordinates (X, Y, Z) [resp. (X', Y', Z')]
satisfying that $x = X/Z,\ y = Y/Z$ [resp.
$x' = X'/Z', y' = Y'/Z'$],
we can express this embedding as

$$f(X, Y, Z, X', Y', Z') = (XX', YX', ZX', XY', \ldots, ZZ').$$

Letting $(T_0, \cdots, T_8)$ be a set of homogeneous coordinates of $\mathbb{P}^8$,
we can express the Galois subspace by $T_5 + T_7 = T_4 = T_8 = 0$.

Continuation

Example

followed by the Segre embedding $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$.
Using homogeneous coordinates (X, Y, Z) [resp. (X', Y', Z')] satisfying that $x = X/Z,\ y = Y/Z$ [resp. $x' = X'/Z', y' = Y'/Z'$],
we can express this embedding as

$$f(X, Y, Z, X', Y', Z') = (XX', YX', ZX', XY', \dots, ZZ').$$

Letting $(T_0, \cdots, T_8)$ be a set of homogeneous coordinates of $\mathbb{P}^8$,
we can express the Galois subspace by $T_5 + T_7 = T_4 = T_8 = 0$.

Continuation

Example

followed by the Segre embedding $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$.
Using homogeneous coordinates (X, Y, Z) [resp. (X', Y', Z')] satisfying that $x = X/Z,\ y = Y/Z$ [resp. $x' = X'/Z', y' = Y'/Z'$],
we can express this embedding as

$$f(X, Y, Z, X', Y', Z') = (XX', YX', ZX', XY', \ldots, ZZ').$$

Letting $(T_0, \cdots, T_8)$ be a set of homogeneous coordinates of $\mathbb{P}^8$,
we can express the Galois subspace by $T_5 + T_7 = T_4 = T_8 = 0$.

Continuation

Example

followed by the Segre embedding $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$.
Using homogeneous coordinates (X, Y, Z) [resp. (X', Y', Z')]
satisfying that $x = X/Z,\ y = Y/Z$ [resp.
$x' = X'/Z', y' = Y'/Z'$],
we can express this embedding as

$$f(X, Y, Z, X', Y', Z') = (XX', YX', ZX', XY', \ldots, ZZ').$$

Letting $(T_0, \cdots, T_8)$ be a set of homogeneous coordinates of $\mathbb{P}^8$,
we can express the Galois subspace by $T_5 + T_7 = T_4 = T_8 = 0$.

Continuation

Example

followed by the Segre embedding $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$.
Using homogeneous coordinates (X, Y, Z) [resp. (X', Y', Z')]
satisfying that $x = X/Z,\ y = Y/Z$ [resp.
$x' = X'/Z', y' = Y'/Z'$],
we can express this embedding as

$$f(X, Y, Z, X', Y', Z') = (XX', YX', ZX', XY', \ldots, ZZ').$$

Letting $(T_0, \cdots, T_8)$ be a set of homogeneous coordinates of $\mathbb{P}^8$,
we can express the Galois subspace by $T_5 + T_7 = T_4 = T_8 = 0$.

Remark

In case $f(V) \cap W \neq \emptyset$, H can be abelian, in fact, in the situation above

let W be the linear subspace defined by $T_5 = T_7 = T_8 = 0$.

Consider the projection π_W with the center W.

Then $f(A) \cap W$ consists of nine points.

The projection induces the Galois extension whose Galois group is isomorphic to

$\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Remark

In case $f(V) \cap W \neq \emptyset$, H can be abelian, in fact, in the situation above
let W be the linear subspace defined by $T_5 = T_7 = T_8 = 0$.
Consider the projection π_W with the center W.
Then $f(A) \cap W$ consists of nine points.
The projection induces the Galois extension whose Galois group is isomorphic to
$\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Remark

In case $f(V) \cap W \neq \emptyset$, H can be abelian, in fact, in the situation above
let W be the linear subspace defined by $T_5 = T_7 = T_8 = 0$.
Consider the projection π_W with the center W.
Then $f(A) \cap W$ consists of nine points.
The projection induces the Galois extension whose Galois group is isomorphic to

$\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Remark

In case $f(V) \cap W \neq \emptyset$, H can be abelian, in fact, in the situation above
let W be the linear subspace defined by $T_5 = T_7 = T_8 = 0$.
Consider the projection π_W with the center W.
Then $f(A) \cap W$ consists of nine points.
The projection induces the Galois extension whose Galois group is isomorphic to
$\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Remark

In case $f(V) \cap W \neq \emptyset$, H can be abelian, in fact, in the situation above
let W be the linear subspace defined by $T_5 = T_7 = T_8 = 0$.
Consider the projection π_W with the center W.
Then $f(A) \cap W$ consists of nine points.
The projection induces the Galois extension whose Galois group is isomorphic to

$\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Remark

In case $f(V) \cap W \neq \emptyset$, H can be abelian, in fact, in the situation above
let W be the linear subspace defined by $T_5 = T_7 = T_8 = 0$.
Consider the projection π_W with the center W.
Then $f(A) \cap W$ consists of nine points.
The projection induces the Galois extension whose Galois group is isomorphic to
$\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.

Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.
In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.
Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.
In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.
Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.
In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.
Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.
In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.
Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding
if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.
In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.
Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.
In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.
Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.

In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embedding

If an abelian surface is embedded into $\mathbb{P}^N$, then $N \geq 4$, and in case $N = 4$ the abelian surface has a special structure.
Reider's Theorem

Theorem

Suppose L is an ample line bundle of type $(1, d)$ with $d \geq 5$ and does not split.
Then the morphism $f_L : A \longrightarrow \mathbb{P}^{d-1}$ is an embedding if and only if there is no elliptic curve E on A with $(E, L) = 2$.

Similarly let us find the least number N that the abelian surface A has the Galois embedding into $\mathbb{P}^N$.
In the case of elliptic curve such a curve is unique and defined by $Y^2Z = 4X^3 + Z^3$.

Minimal embeddig

Theorem

Suppose (A, D) defines the Galois embedding. Then the least number N is seven, i.e., A is embedded into $\mathbb{P}^7$. Moreover H is isomorphic to D_4 or $Z_2 \ltimes D_4$.

Minimal embeddig

Theorem

Suppose (A, D) defines the Galois embedding. Then the least number N is seven, i.e., A is embedded into $\mathbb{P}^7$. Moreover H is isomorphic to D_4 or $Z_2 \ltimes D_4$.

Example 3

Example

$A = \mathbb{C}^2/\Omega$, Ω is the period matrix

$$\begin{pmatrix} 1 & 0 & \tau & 0 \\ 0 & 1 & 0 & \tau \end{pmatrix}, \text{ where } \Im\tau > 0.$$

$$\begin{aligned}
\widetilde{g_1}\vec{z} &= \vec{z} + \frac{1}{2}\begin{pmatrix} n_1 + n_3\tau \\ n_2 + n_4\tau \end{pmatrix}, \\
\widetilde{g_2}\vec{z} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\vec{z} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \\
\widetilde{g_3}\vec{z} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\vec{z} \\
&\text{where } (n_1, n_2, n_3, n_4) = (0,0,1,1), (1,1,0,0), (1,1,1,1), \\
&\begin{pmatrix} \alpha_1 + \alpha_2 \\ \alpha_1 + \alpha_2 \end{pmatrix} \in \mathcal{L}_A \text{ and } \begin{pmatrix} 2\alpha_1 \\ 0 \end{pmatrix} \in \mathcal{L}_A,
\end{aligned}$$

Example(continuation)

Example

Then we have ${g_1}^2 = {g_2}^2 = {g_3}^4 = id$, $g_2 g_3 g_2 = {g_3}^{-1}$ and $g_i g_1 = g_1 g_i$ $(i = 2, 3)$ on A.
Putting $G = \langle g_1, g_2, g_3 \rangle$, we have $G_1 = \langle g_1 \rangle$ and $G = G_1 \times G_2$ where $G_2 = \langle g_2, g_3 \rangle$.
Clearly $G_2 \cong D_4$.

Example(continuation)

Example

Then we have ${g_1}^2 = {g_2}^2 = {g_3}^4 = id$, $g_2 g_3 g_2 = {g_3}^{-1}$
and $g_i g_1 = g_1 g_i$ $(i = 2, 3)$ on A.
Putting $G = \langle g_1, g_2, g_3 \rangle$, we have $G_1 = \langle g_1 \rangle$ and $G = G_1 \times G_2$
where $G_2 = \langle g_2, g_3 \rangle$.
Clearly $G_2 \cong D_4$.

Example(continuation)

Example

Then we have ${g_1}^2 = {g_2}^2 = {g_3}^4 = id$, $g_2 g_3 g_2 = {g_3}^{-1}$
and $g_i g_1 = g_1 g_i$ $(i = 2, 3)$ on A.
Putting $G = \langle g_1, g_2, g_3 \rangle$, we have $G_1 = \langle g_1 \rangle$ and $G = G_1 \times G_2$
where $G_2 = \langle g_2, g_3 \rangle$.
Clearly $G_2 \cong D_4$.

Example 4

Example

$A = \mathbb{C}^2/\Omega$, Ω is the period matrix

$$\begin{pmatrix} 1 & 0 & i & (1+i)/2 \\ 0 & 1 & 0 & (1+i)/2 \end{pmatrix}, \text{ where } i = \sqrt{-1}.$$

Let g_1, g_2 and g_3 be the automorphisms defined by

$$\begin{aligned} \widetilde{g_1}\vec{z} &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \vec{z} + \begin{pmatrix} \varepsilon_{11} \\ \varepsilon_{12} \end{pmatrix}, \\ \widetilde{g_2}\vec{z} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \vec{z} + \begin{pmatrix} \varepsilon_{21} \\ \varepsilon_{22} \end{pmatrix}, \\ \widetilde{g_3}\vec{z} &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \vec{z}. \end{aligned}$$

Example(continuation)

Example

Then we have
$g_1{}^2 = g_2{}^2 = g_3{}^4 = 1,\ g_1g_2g_1 = g_2g_3{}^2,\ g_1g_3g_1 = g_3$ and
$g_2g_3g_2 = g_3{}^{-1}$.
Putting $G = \langle g_1, g_2, g_3 \rangle$, we see that G is isomorphic to
the semidirect product $Z_2 \ltimes D_4$
and G becomes a subgroup of $Aut(A)$ and $A/G \cong \mathbb{P}^2$.

Example(continuation)

Example

Then we have
$g_1{}^2 = g_2{}^2 = g_3{}^4 = 1,\ g_1g_2g_1 = g_2g_3{}^2,\ g_1g_3g_1 = g_3$ and
$g_2g_3g_2 = g_3{}^{-1}$.
Putting $G = \langle g_1, g_2, g_3\rangle$, we see that G is isomorphic to
the semidirect product $Z_2 \ltimes D_4$
and G becomes a subgroup of $Aut(A)$ and $A/G \cong \mathbb{P}^2$.

Example(continuation)

Example

Then we have
$g_1{}^2 = g_2{}^2 = g_3{}^4 = 1,\ g_1g_2g_1 = g_2g_3{}^2,\ g_1g_3g_1 = g_3$ and $g_2g_3g_2 = g_3{}^{-1}$.
Putting $G = \langle g_1, g_2, g_3\rangle$, we see that G is isomorphic to the semidirect product $Z_2 \ltimes D_4$
and G becomes a subgroup of $Aut(A)$ and $A/G \cong \mathbb{P}^2$.

Example(continuation)

Example

Then we have
$g_1{}^2 = g_2{}^2 = g_3{}^4 = 1,\ g_1g_2g_1 = g_2g_3{}^2,\ g_1g_3g_1 = g_3$ and
$g_2g_3g_2 = g_3{}^{-1}$.
Putting $G = \langle g_1, g_2, g_3 \rangle$, we see that G is isomorphic to
the semidirect product $Z_2 \ltimes D_4$
and G becomes a subgroup of $Aut(A)$ and $A/G \cong \mathbb{P}^2$.