Riemann surfaces with extra automorphisms and endomorphism rings of their Jacobians

T. Shaska

Oakland University
Rochester, MI, 48309

April 14, 2018

Problem

Let $\mathcal{X}$ be an algebraic curve defined over a field K. Denote its Jacobian by

$$J := \text{Jac}_K(\mathcal{X})$$

Let $\text{Aut}(\mathcal{X})$ be the automorphism group over $\bar{K}$ and $\text{End}_K(\text{Jac } C)$ the endomorphism ring of the Jacobian $\text{Jac}_K(\mathcal{X})$.

Problem: Determine the relation between $\text{Aut}(\mathcal{X})$ and End (Jac C).

Curves and their Jacobians

Given a curve $\mathcal{C}/k$, $\Sigma_{\mathcal{C}}(k)$ denotes the set of points on $\mathcal{C}$ with k-coordinates. The group of k-rational divisors $\mathrm{Div}_{\mathcal{C}}(k)$ is defined as

$$\mathrm{Div}_{\mathcal{C}}(k) = \bigoplus_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} \mathbb{Z}\cdot\mathfrak{p},$$

i.e. $\mathrm{Div}_{\mathcal{C}}(k)$ is the free abelian group with base $\Sigma_{\mathcal{C}}(k)$. Hence a **divisor** D of $\mathcal{C}$ is a formal sum

$$D = \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}\, P$$

where $z_{\mathfrak{p}} \in \mathbb{Z}$ and $z_{\mathfrak{p}} = 0$ for all but finitely many prime divisors $\mathfrak{p}$. The degree of D is defined as

$$\deg(D) := \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}.$$

The map $D \mapsto \deg(D)$ is a homomorphism from $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathbb{Z}$. Its kernel is the subgroup $\mathrm{Div}_{\mathcal{C}}(k)^0$ of divisors of degree 0.

Example

Let $f \in k(\mathcal{C})^*$ be a meromorphic function on $\mathcal{C}$. For $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we have defined the normalized valuation $w_{\mathfrak{p}}$. The divisor of f is defined as

$$(f) = \sum_{\Sigma_{\mathcal{C}}(k)} w_{\mathfrak{p}} \cdot \mathfrak{p}.$$

It is not difficult to verify that (f) is a divisor, and that its degree is 0. Moreover $(f\cdot g) = (f) + (g)$ for functions f, g, and $(f^{-1}) = -(f)$. The completeness of $\mathcal{C}$ implies that $(f) = 0$ if and only if $f \in k^*$, and so (f) determines f up to scalars $\neq 0$.

Thus, the set of principal divisors $\mathrm{PDiv}_{\mathcal{C}}(k)$ consisting of all divisors (f) with $f \in k(\mathcal{C})$ is a subgroup of $\mathrm{Div}^0_{\mathcal{C}}(k)$.

Definition.
The group of divisor classes of $\mathcal{C}$ is defined by

$$\mathrm{Pic}_{\mathcal{C}}(k) := \mathrm{Div}_{\mathcal{C}}(k)/\mathrm{PDiv}_{\mathcal{C}}(k)$$

*and is called the **divisor class group** of $\mathcal{C}$. The group of divisor classes of degree 0 of $\mathcal{C}$ is defined by*

$$\mathrm{Pic}^0_{\mathcal{C}}(k) := \mathrm{Div}^0_{\mathcal{C}}(k)/\mathrm{PDiv}_{\mathcal{C}}(k)$$

*and is called the **Picard group** (of degree 0) of $\mathcal{C}$.*

The Picard Functor:

Let L be a finite algebraic extension of k and $\mathcal{C}_L$ the curve obtained from $\mathcal{C}$ by constant field extension. Then places of $k(\mathcal{C})$ can be extended to places of $L(\mathcal{C}_L)$. By the conorm map we get an injection of $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathrm{Div}_{\mathcal{C}_L}(L)$. The well known formulas for the extensions of places yield that

$$\mathrm{conorm}_{L/k}(\mathrm{Div}^0_{\mathcal{C}}(k)) \subset \mathrm{Div}^0_{\mathcal{C}_L}(L)$$

and that principal divisors are mapped to principal divisors. Hence we get a homomorphism

$$\mathrm{conorm}_{L/k} : \mathrm{Pic}^0_{\mathcal{C}}(k) \to \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

and therefore a functor

$$\mathrm{Pic}^0 : L \mapsto \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

from the category of algebraic extension fields of k to the category of abelian groups. Coming "from above" we have a Galois theoretical description of this functor. Clearly,

$$\mathrm{Div}_{\mathcal{C}_L}(L) = \mathrm{Div}_{\mathcal{C}_{\{\bar{k}}}(\bar{k})^{G_L}$$

and the same is true for functions. With a little bit of more work one sees that an analogue result is true for $\mathrm{PDiv}_{\mathcal{C}_L}(L)$ and for $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$; see (Frey and Shaska, 2018) for details.

Theorem

For any curve $\mathcal{C}_k$ and any finite extension L/k the functor

$$L \mapsto Pic^0_{\mathcal{C}_L}(L)$$

is the same as the functor

$$L \mapsto Pic^0_{\mathcal{C}_{\bar{k}}}(\bar{k})^{G_L}.$$

In particular, we have

$$Pic^0_{\mathcal{C}_{\bar{k}}}(\bar{k}) = \bigcup_{k \subset L \subset \bar{k}} Pic^0_{\mathcal{C}_L}(L),$$

where inclusions are obtained via conorm maps.

Remark

For a finite extension L/k we also have the norm map of places of $\mathcal{C}_L$ to places of $\mathcal{C}_k$ induces a homomorphism from $Pic^0_{\mathcal{C}_L}(L)$ to $Pic^0_{\mathcal{C}}(k)$. In general, this map will be neither injective nor surjective.

It is one of the most important facts for the theory of curves that the functor Pic ^{0} can be represented: There is a variety $\mathcal{J}_\mathcal{C}$ defined over k such that for all extension fields L of k we have a functorial equality

$$\mathcal{J}_\mathcal{C}(L) = \text{Pic}^0_{\mathcal{C}_L}(L).$$

$J_\mathcal{C}$ is the **Jacobian variety** of $\mathcal{C}$. This variety will be discussed soon.

Abelian varieties

Group schemes: A projective (affine) group scheme G defined over k is a projective (affine) scheme over k endowed with
i) addition, i.e., a morphism

$$m: \ G \times G \to G$$

ii) inverse, i.e., a morphism

$$i: \ G \to G$$

iii) the identity, i. e., a k-rational point $0 \in G(k)$,

such that it satisfies group laws. The group law is uniquely determined by the choice of the identity element. A morphism of group schemes that is compatible with the addition law is a homomorphism.
Let L/k be a field extension. $G(L)$ denotes the set of L-rational points of G and it is also a group. A homomorphism between groups schemes induces a homomorphism between the group of rational points. If G is an absolutely irreducible projective variety, then the group law m is commutative.

Definition.
*An **Abelian variety** defined over k is an absolutely irreducible projective variety defined over k which is a group scheme.*

Fact: A morphism of Abelian varieties $\mathcal{A}$ to $\mathcal{B}$ is a homomorphism if and only if it maps the identity element of $\mathcal{A}$ to the identity element of $\mathcal{B}$.
An abelian variety $\mathcal{A}/k$ is called **simple** if it has no proper non-zero Abelian subvariety over k, it is called **absolutely simple** (or **geometrically simple**) if it is simple over the algebraic closure of k.

Complex tori and abelian varieties

Abelian varieties are connected, projective algebraic group schemes. Their analytic counterparts are the connected compact Lie groups.
Let d be a positive integer and $\mathbb{C}^d$ the complex Lie group (i.e., with vector addition as group composition). The group $\mathbb{C}^d$ is not compact, but we can find quotients which are compact. Choose a lattice $\Lambda \subset \mathbb{C}^d$ which is a $\mathbb{Z}$-submodule of rank $2d$. The quotient $\mathbb{C}^d/\Lambda$ is a complex, connected Lie group which is called a **complex d-dimensional torus**. Every connected, compact Lie group of dimension d is isomorphic to a torus $\mathbb{C}^d/\Lambda$.
A hermitian form H on $\mathbb{C}^d \times \mathbb{C}^d$ is a form that can be decomposed as

$$H(x, y) = E(ix, y) + i\,E(x, y),$$

where E is a skew symmetric real form on $\mathbb{C}^d$ satisfying $E(ix, iy) = E(x, y)$. E is called the imaginary part $\mathrm{Img}(H)$ of H.
The torus $\mathbb{C}^d/\Lambda$ can be embedded into a projective space if and only if there exists a positive Hermitian form H on $\mathbb{C}^d$ with $E = \mathrm{Img}(H)$ such that restricted to $\Lambda \times \Lambda$ has values in $\mathbb{Z}$. Let $\mathbb{H}_g$ be the Siegel upper half plane

$$\mathbb{H}_d = \{\tau \in \mathrm{Mat}_d(\mathbb{C}) \mid \tau^T = \tau,\ \mathrm{Img}(\tau) > 0\}.$$

Then, we have the following.

Lemma
Let $\mathbb{C}^d/\Lambda$ be a complex torus attached to an abelian variety $\mathcal{A}$. Then Λ is isomorphic to $\mathbb{Z}^d \oplus \Omega \cdot \mathbb{Z}^d$, where $\Omega \in \mathbb{H}_d$.

The matrix Ω is called the **period matrix** of $\mathcal{A}$. The lattice $\hat{\Lambda}$ given by

$$\hat{\Lambda} := \{x \in \mathbb{C}^d \mid E(x, y) \in \mathbb{Z}, \text{ for all } y \in \Lambda\}$$

is called the **dual lattice** of Λ. If $\hat{\Lambda} = \Lambda$ then E is called a *principal polarization* on $\mathcal{A}$ and the pair $(\mathcal{A}, E)$ is called a **principally polarized** abelian variety; we may also say that $\mathcal{A}$ admits a principal polarization.
For a principally polarized abelian variety $(\mathcal{A}, E)$ there exists a basis $\{\mu_1, \ldots, \mu_{2d}\}$ of Λ such that

$$J := \left[E(\mu_i, \mu_j)\right]_{1 \leq i,j \leq 2d} = \begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}.$$

The symplectic group

$$Sp(2d, \mathbb{Z}) = \{M \in GL(2d, \mathbb{Z}) \mid MJM^T = J\}$$

acts on $\mathbb{H}_d$, via

$$\begin{aligned} Sp(2d, \mathbb{Z}) \times \mathcal{H}_d &\to \mathcal{H}_d \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \tau &\to (a\tau + b)(c\tau + d)^{-}1 \end{aligned}$$

where a, b, c, d, τ are $d \times d$ matrices. The moduli space of d-dimensional abelian varieties is

$$\mathbf{A}_g := \mathbb{H}_d / Sp(2d, \mathbb{Z}).$$

The Jacobian of a projective irreducible nonsingular curve admits a canonical principal polarization.

Automorphisms of Jacobian varieties

By functoriality it follows that automorphism of $\mathcal{C}$ induce automorphisms of $\mathcal{J}_{\mathcal{C}}$, or, to be more precise, of $(\mathbb{C}_{\mathcal{C}}, \iota)$ where ι is the principal polarization of $\mathcal{J}_{\mathcal{C}}$ attached to $\mathcal{C}$.

Theorem
Let $\mathcal{C}$ be an algebraic curve and $\mathcal{A} := Jac(\mathcal{C})$ with canonical principal polarization ι. Then,

$$Aut\mathcal{C} \cong \begin{cases} Aut(\mathcal{A}, \iota), & \text{if } \mathcal{C} \text{ is hyperelliptic} \\ Aut(\mathcal{A}, \iota)/\{\pm 1\}, & \text{if } \mathcal{C} \text{ is non-hyperelliptic} \end{cases}$$

See (`?Milne`) for a proof.

Endomorphism of Abelian varieties

Let $\mathcal{A}$, $\mathcal{B}$ be abelian varieties over a field k. We denote the $\mathbb{Z}$-module of homomorphisms $\mathcal{A} \mapsto \mathcal{B}$ by $\mathrm{Hom}(\mathcal{A}, \mathcal{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\mathrm{End}\ \mathcal{A}$.
In the context of Linear Algebra it can be more convenient to work with the $\mathbb{Q}$-vector spaces $\mathrm{Hom}^0(\mathcal{A}, \mathcal{B}) := \mathrm{Hom}(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\mathrm{End}^{\,0}\mathcal{A} := \mathrm{End}\ \mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. Determining $\mathrm{End}\ \mathcal{A}$ or $\mathrm{End}^{\,0}\mathcal{A}$ is an interesting problem on its own; see (Oort, 1988).
For any abelian variety $\mathcal{A}$ defined over a a number field K, computing $\mathrm{End}_K(\mathcal{A})$ is a harder problem than computation of $\mathrm{End}_{\bar{K}}(\mathcal{A})$; see (Frey and Shaska, 2018) for details.

Lemma
If there exists an algorithm to compute $\mathrm{End}_K(\mathcal{A})$ for any abelian variety of dimension $g \geq 1$ defined over a number field K, then there is an algorithm to compute $\mathrm{End}_{\bar{K}}(\mathcal{A})$.

The ring of endomorphisms of generic Abelian varieties is ”as small as possible”. For instance, if $\mathrm{char}(k) = 0$ $\mathrm{End}\ (\mathcal{A}) = \mathbb{Z}$ in general. If k is a finite field, the Frobenius endomorphism will generate a larger ring, but again, this will be all in the generic case.

Theorem (Zarhin)
Let $\mathcal{C}$ be a hyperelliptic curves with affine equation $y^2 = f(x)$, $n = \deg f$, and $f \in \mathbb{Q}[x]$. If $Gal\ (f)$ is isomorphic to A_n or S_n then $\mathrm{End}_{\overline{\mathbb{Q}}}(Jac\ \mathcal{C}) \cong \mathbb{Z}$.

From this point of view it will be interesting to find Abelian varieties with larger endomorphism rings. This leads to the theory of real and complex multiplication.
For instance, the endomorphism ring of the Jacobian of the Klein quartic contains an order in a totally real field of degree 3 over $\mathbb{Q}$.

Theorem ((Zarhin, 2017))

Let K be a field, char $K \neq 2$ and $f(x) \in K[x]$ an irreducible polynomial with $\deg f \geq 5$. *If one of the following conditions is satisfied:*

- *char $K \neq 3$ and Gal $_K(f) \cong A_n$ or S_n*
- *Gal $_K(f) \cong M_n$ (Mathiew group) for $n = 11, 12, 22, 23, 24$*

then the curve $C : y^2 = f(x)$ has End $J = \mathbb{Z}$. In particular, Jac C is absolutely simple.

Theorem ((Zarhin, 2017))

If $f(x)$ is as above, char $K = 0$, and p an odd prime then the superelliptic curve

$$\mathcal{X} : y^p = f(x)$$

has Jac $(\mathcal{X})$ absolutely simple and End (Jac C) $\cong \mathbb{Z}[\varepsilon_p]$.

Can we construct families of curves with these properties?

Galois groups of polynomials

Theorem (Bialostocki-Sh)

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree $p > 5$. Let r be the number of complex roots of $f(x)$. If $r > 0$ then $Gal(f)$ is A_p, S_p or one of the groups as in the following Table 2.

Proof.

The proof is computational and follows from the tables of transitive subgroups of S_p. It is easy to decide which ones of these groups are non-solvable and compute their cycle types. □

Remark

We used in Table 2 notations which we considered standard as D_n, M_{11}, and $L(p)$, otherwise we used the GAP notation (p, i) which is the i-th group in the list of transitive groups of degree p. These groups can be generated in GAP simple by typing "TransitiveGroup(n,i);". The group M_{23} is not realized as a Galois groups over $\mathbb{Q}$.

Notice that no two groups of Table 2 have the same cycle structure. Hence the Galois group can be determined uniquely by reduction mod p for all polynomials of prime degree ≤ 29 with non-real roots.

p	Solv.	Sign.	Nonsol.	Sign.
7	D_7	$(2)^3, (7)$	$L(7)$	$(2)^2, (4)(2), (3)^2, (7)$
	$(7, 4)$	$(2)^3, (3)^2, (7)$		
11	D_{11}	$(2)^5, (11)$	$L(11)$	$(2)^4, (3)^3, (5)^2, (2)(6)(3), (11)$
	$(11, 4)$	$(2)^5, (5)^2, (10), (11)$	M_{11}	$(2)^4, (2)(6)(3), (2)(8), (3)^3,$ $(4)^2, (5)^2, (11)$
13	D_{13}	$(2)^6, (13)$	$L(13)$	$(2)^4, (3)^3, (3)^4, (4)^2(2)^2,$ $(6)(3)(2), (8)(4), (13)$
	$(13, 4)$	$(2)^6, (4)^3, (13)$		
	$(13, 5)$	$(2)^6, (3)^4, (6)^2, (13)$		
	$(13, 6)$	$(2)^6, (3)^4, (4)^3,$ $(6)^2, (12), (13)$		
17	D_{17}	$(2)^8, (17)$	$PSL_2(16)$	$(2)^8, (3)^5, (5)^3, (15), (17)$
	$(17, 3)$	$(2)^8, (4)^4, (17)$	$(17, 7)$	$(2)^6, (2)^8, (3)^5, (4)^4,$ $(5)^3, (6)^2(3), (5)(10)(2),$ $(15), (17)$
	$(17, 4)$	$(2)^8, (4)^4, (8)^2, (17)$	$(17, 8)$	$(2)(5)(10), (2)(4), (2)(4)^3,$ $(2)^6, (2)^8, (3)(6)^2, (3)^5,$ $(3)^2(12), (4)^3, (5)^3, (8)^2,$ $(15), (17)$
	$(17, 5)$	$(2)^8, (4)^4, (8)^2, (16), (17)$		
19	D_{19}	$(2)^9, (19)$		
	$(19, 4)$	$(2)^9, (3)^6, (6)^3, (19)$		
	$(19, 6)$	$(2)^9, (3)^6, (6)^3, (9)^2,$ $(18), (19)$		
23	D_{23}	$(2)^{11}, (23)$	M_{23}	$(2)^8, (2)^2(4)^4, (2)(7)(14),$ $(2)(4)(8)^2, (2)^2(3)^2(6)^2,$ $(3)(5)(15), (5)^3, (5)^4,$ $(7)^3, (11)^2, (23)$
	$(23, 4)$	$(2)^{11}, (11)^2, (22), (23)$		
29	D_{29}	$(2)^{14}, (29)$		
	$(29, 3)$	$(2)^{14}, (4)^7, (29)$		
	$(29, 5)$	$(2)^{14}, (7)^4, (14)^2, (29)$		
	$(29, 6)$	$(2)^{14}, (4)^7, (7)^4, (14)^2$		

Polynomials with no real roots

What about polynomials $f(x) \in \mathbb{Q}[x]$ which have all non-real roots?

A polynomial $f(x) \in \mathbb{R}[x]$ with no real roots is called **totally complex**. Let $g(x)$ be given as

$$g(x) = \sum_{i=0}^{s} a_i x^i \in \mathbb{R}[x]$$

such that $a_s > 0$ and $\Delta_g \neq 0$. Let

$$f(x) = x^n + t \cdot g(x)$$

Theorem ((Otake and Shaska, 2018a))
$f(x)$ is totally complex for all

$$t > \max\{\alpha \mid \Delta_f(\alpha) = 0\}$$

If $g(x)$ satisfies the Eisenstein criteria, then $f(x)$ satisfies the Eisenstein criteria. In this case $f(x)$ is irreducible over $\mathbb{Q}$.

Lemma
If $f(x)$ as above is irreducible then

$$Gal_{\mathbb{Q}(t)}(f) \cong S_n.$$

Let $f(x)$ be as above. Then we have:

Theorem
i) The curve $\mathcal{C} : y^2 = f(x)$ has End $(J) = \mathbb{Z}$. Moreover, $\mathcal{J}(\mathcal{C})$ is absolutely simple.
ii) The curve $\mathcal{X} : y^p = f(x)$ has End $(J) = \mathbb{Z}[\varepsilon_p]$. Moreover, $\mathcal{J}(\mathcal{C})$ is absolutely simple.

Another family of polynomials:

Consider

$$f(x) = x^n + \xi(x^2 + ax + b)$$

where $a, b \in \mathbb{R}$ and ξ a parameter $\xi \in \mathbb{R}$. Then we have the following:

Theorem ((Otake and Shaska, 2018b))
The polynomial

$$f(x) = x^n + \xi(x^2 + ax + b)$$

is a totally complex polynomial for any even $n \geq 4$, such that $\xi \in (0, \infty)$, $b \neq 0$ and $b \geq \frac{(n-1)^2 a^2}{4n(n-2)}$.

Proof.
Quite tedious, using properties of Bezutians of polynomials. □

Proposition

If $n \leq 9$ then the Galois group of $f(x)$ over $\mathbb{Q}(\xi)$,

$$Gal_{\mathbb{Q}(\xi)} f(x) \cong S_n.$$

Conjecture

The Galois group of $f(x)$ over $\mathbb{Q}(\xi)$,

$$Gal_{\mathbb{Q}(\xi)} f(x) \cong S_n.$$

So we have created a family of curves of arbitrary large genus such that:

Theorem

i) The curve $\mathcal{C}$: $y^2 = f(x)$ has End $(J) = \mathbb{Z}$. Moreover, $\mathcal{J}(\mathcal{C})$ is absolutely simple.
ii) The curve $\mathcal{C}$: $y^p = f(x)$ has End $(J) = \mathbb{Z}[\varepsilon_p]$. Moreover, $\mathcal{J}(\mathcal{C})$ is absolutely simple.

References

Oort, Frans. 1988. *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, pp. 469–502. MR977774

Frey, Gerhard and Tony Shaska. 2018. *Abelian variaties and cryptography*, Algebraic curves and their applications.

Zarhin, Yuri G. 2017. *Endomorphism algebras of abelian varieties with special reference to superelliptic jacobians*, available at 1706.00110.

Otake, Shuichi and Tony Shaska. 2018a. *Some remarks on the non-real roots of polynomials*, available at 1802.02708.

_____. 2018b. *A family of totally complex polynomials and their discriminants*, Algebraic curves and their applications.