Restrictions on endomorphism algebras of hyperelliptic jacobians

Pip Goodman

Jacobians

Given a (smooth, irreducible, projective) curve C, we may associate to it an abelian variety, $\mathrm{Jac}(C)$ called the jacobian of C.

This association is functorial, in particular a map $C \to C'$, induces a map $\mathrm{Jac}(C) \to \mathrm{Jac}(C')$.

Jacobians

Given a (smooth, irreducible, projective) curve C, we may associate to it an abelian variety, $\mathrm{Jac}(C)$ called the jacobian of C.

This association is functorial, in particular a map $C \to C'$, induces a map $\mathrm{Jac}(C) \to \mathrm{Jac}(C')$.

Let K be a number field and $f \in K[x]$ be a polynomial of degree $2g+2$ or $2g+1$ without multiple roots. Then the equation $y^2 = f(x)$ determines a curve of genus g. We call curves of this form *hyperelliptic*.

Notation

I'll write J_f to denote the jacobian of such a curve.

Notation

Endomorphism algebras

l-torsion

The l-torsion of a jacobian $J_f[l]$ is a $2g$-dimensional vector space over $\mathbb{F}_l$ with an action of $G_K := \mathrm{Gal}(\bar{K}/K)$.
We have $K(J_f[2]) = K(f)$ the splitting field of f.

Endomorphism algebras

l-torsion

The l-torsion of a jacobian $J_f[l]$ is a $2g$-dimensional vector space over $\mathbb{F}_l$ with an action of $G_K := \mathrm{Gal}(\bar{K}/K)$.
We have $K(J_f[2]) = K(f)$ the splitting field of f.

Question

How does $\mathrm{End}(J_f)$ relate to the fields $K(J_f[l])$?

In general, $K(J_f[2]) = K(f)$ doesn't tell us much about $\mathrm{End}(J_f)$. For example :

1. $f(x) = (x+1)(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}(J_f) \cong \mathbb{Z}$.
2. $f(x) = x(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}(J_f) \cong \mathbb{Z} \times \mathbb{Z}$.
3. $f(x) = (x-1)(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}(J_f) \cong \mathbb{Z}[\zeta_5]$.

Inverse Galois Theory

Theorem (Serre '72)

Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$.

Inverse Galois Theory

Theorem (Serre '72)

Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$. Then for all but finitely many primes l, we have $\mathrm{Gal}(K(E[l])/K) = \mathrm{GL}_2(\mathbb{F}_l)$.

Inverse Galois Theory

Theorem (Serre '72)

Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$. Then for all but finitely many primes l, we have $\mathrm{Gal}(K(E[l])/K) = \mathrm{GL}_2(\mathbb{F}_l)$.

Theorem (Hall '08)

Let $C_f : y^2 = f(x)$, where $\deg(f) = 2g + 1$. Let $J_f = \mathrm{Jac}(C_f)$. Suppose $\mathrm{End}(J_f) \cong \mathbb{Z}$, and f has a double root modulo some prime p. Then for all but finitely many primes l, we have $\mathrm{Gal}(K(J_f[l])/K) = \mathrm{GSp}_{2g}(\mathbb{F}_l)$.

Inverse Galois Theory

Theorem (Serre '72)

Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$. Then for all but finitely many primes l, we have $\mathrm{Gal}(K(E[l])/K) = \mathrm{GL}_2(\mathbb{F}_l)$.

Theorem (Hall '08)

Let $C_f : y^2 = f(x)$, where $\deg(f) = 2g+1$. Let $J_f = \mathrm{Jac}(C_f)$. Suppose $\mathrm{End}(J_f) \cong \mathbb{Z}$, and f has a double root modulo some prime p. Then for all but finitely many primes l, we have $\mathrm{Gal}(K(J_f[l])/K) = \mathrm{GSp}_{2g}(\mathbb{F}_l)$.

Theorem (Zarhin '00)

Let $f \in K[x]$ be a polynomial of degree $n \geq 5$ with Galois group containing A_n. Then J_f has trivial endomorphism ring.

Remark

To prove this result, it suffices to prove it for A_n.

Sketch proof

Theorem (Zarhin '00)

Let $f \in K[x]$ be a polynomial of degree $n \geq 5$ with Galois group containing A_n. Then J_f has trivial endomorphism ring.

What can we say for smaller Galois groups ?

Zarhin has done a lot of work on this for large insoluble Galois groups. The “smallest” he considers is the following :

Theorem (Elkin, Zarhin ’06,’08)

Suppose $n = q + 1$, where $q \geq 5$ is a prime power congruent to ± 3 or 7 modulo 8. Suppose that $f(x)$ is irreducible and $\mathrm{Gal}(f) \cong \mathrm{PSL}_2(\mathbb{F}_q)$. Then one of the following holds :

1. $\mathrm{End}^0(J_f) = \mathbb{Q}$ *or a quadratic field.*
2. $q \equiv 3, 7 \mod 8$ *and J_f is isogenous over $\bar{K}$ to a self-product of an elliptic curve with CM by $\mathbb{Q}(\sqrt{-q})$.*

A result of Lombardo

Theorem (Lombardo '19)

Let $f \in K[x]$ be an irreducible degree 5 polynomial. Then $\mathrm{End}^0(J_f)$ is a division algebra.

Can we improve Lombardo's result?

Example

Jacobians with trivial endomorphism rings are easy to find, so let's see some non trivial examples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$

Can we improve Lombardo's result ?

Example

Jacobians with trivial endomorphism rings are easy to find, so let's see some non trivial examples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$
D_5	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$x^5 - 19x^4 + 107x^3 + 95x^2 + 88x - 16$
F_5	R	$52x^5 + 104x^4 + 104x^3 + 52x^2 + 12x + 1$

where R is the maximal order of the CM number field with defining polynomial $x^4 + x^3 + 2x^2 - 4x + 3$. We note that this field is cyclic, ramified only at 13, and 2 generates a maximal ideal.

Can we improve Lombardo's result?

Example

Jacobians with trivial endomorphism rings are easy to find, so let's see some non trivial examples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$
D_5	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$x^5 - 19x^4 + 107x^3 + 95x^2 + 88x - 16$
F_5	R	$52x^5 + 104x^4 + 104x^3 + 52x^2 + 12x + 1$

where R is the maximal order of the CM number field with defining polynomial $x^4 + x^3 + 2x^2 - 4x + 3$. We note that this field is cyclic, ramified only at 13, and 2 generates a maximal ideal.

Note also, when $\mathrm{Gal}(f) \cong F_5$ and J_f is of CM type, $\mathrm{End}^0(J_f)$ is isomorphic to the unique degree 4 extension of $\mathbb{Q}$ contained in $\mathbb{Q}(f)$.

Improvements in genus 2

Theorem (G. '19)

Let $f(x) \in K[x]$ be a polynomial of degree 5 or 6, with $\mathrm{Gal}(f)$ containing an element of order 5. Then one of the following holds :

1. $\mathrm{End}(J_f) \cong \mathbb{Z}$.
2. $\mathrm{End}(J_f) \cong \mathbb{Z}\left[\frac{1+r\sqrt{D}}{2}\right]$, *where* $D \equiv 5 \mod 8$, $D > 0$ *and* $2 \nmid r$.
3. $\mathrm{End}(J_f) \cong R$, *where* R *is a 2-maximal order in a degree 4 CM field, which is totally inert at 2.*

Remark

Specifying $\mathrm{Gal}(f)$, we can give more information on $\mathrm{End}(J_f)$.

Higher genus

Theorem (G.'19)

Let $f(x) \in K[x]$ be a polynomial of degree $2g+1$ or $2g+2$, with $\mathrm{Gal}(f)$ containing an element of prime order $p = 2g+1$, and g satisfying some additional conditions.
Then one of the following holds :

1. $\mathrm{End}^0(J_f)$ *is a number field, with restrictions on the primes above 2 ;*
2. J_f *is isogenous over $\overline{K}$ to the self product of an absolutely simple abelian variety with CM by a proper subfield of $\mathbb{Q}(\zeta_p)$.*

Satisfied by $g = 1, 2, 3, 5, 6, 9, 11, 14, 18, 23, 26, 29, 30, 33, 35, 39, 41, \ldots$

Sketch proof

Let's consider the case $\mathrm{Gal}(f)$ acts irreducibly on $J[2]$. We may assume $|\mathrm{Gal}(f)| = p$.

Sketch proof

Let's consider the case $\mathrm{Gal}(f)$ acts irreducibly on $J[2]$. We may assume $|\mathrm{Gal}(f)| = p$. Our first goal is to show $\mathrm{End}_K^0(J_f)$ is a field.

Restrictions on the endomorphism field

Let A/K be an abelian variety of dimension g. Denote by L/K the minimal extension over which all endomorphisms of A are defined.
E.g. $E : y^2 = x^3 - 2$ has $g = 1$ and $L = \mathbb{Q}(\zeta_3)$.

Theorem (G.'19)

Suppose $p = 2g + 1$ is a prime divisor of $[L : K]$. Then A is isogenous over $\bar{K}$ to the self product of an absolutely simple abelian variety with complex multiplication by a proper subfield of $\mathbb{Q}(\zeta_p)$.

Sketch of the proof

Proof sketch

1. First prove $A \sim B^n$ over $\bar{K}$ for some absolutely simple abelian variety B and integer $n > 1$.

Sketch of the proof

Proof sketch

1. First prove $A \sim B^n$ over $\bar{K}$ for some absolutely simple abelian variety B and integer $n > 1$.
2. Then observe that $\mathrm{Gal}(L/K)$ acts faithfully on $\mathrm{End}^0(B^n) \cong M_n(D)$ by automorphisms, where $D = \mathrm{End}^0(B)$ is a finite dimensional divison algebra satisfying $[D : \mathbb{Q}]n \leq 2g = p - 1$.
3. The Skolem-Noether Theorem then tells us we have a faithful representation

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{PGL}_n(D)$$

4. This restricts D to be a subfield of $\mathbb{Q}(\zeta_p)$ and $[D : \mathbb{Q}]n = p - 1$. Which in turn implies B has CM by a proper subfield of $\mathbb{Q}(\zeta_p)$.

Frobenius groups

Theorem (G. '19)

Let q be an odd prime power. Let $f \in K[x]$ be a polynomial of degree q with Galois group $\mathbb{F}_q \rtimes \mathbb{F}_q^\times \cong \mathrm{AGL}(1,q)$. Suppose $E = \mathrm{End}^0(J_f)$ is a number field.
Then $E/\mathbb{Q}$ is cyclic Galois, and L/K is the unique extension of degree $[E:\mathbb{Q}]$ contained in $K(f)$.
Furthermore, if $[E:\mathbb{Q}] = q-1$, then $L = EK$.

Frobenius groups

Theorem (G. '19)

Let q be an odd prime power. Let $f \in K[x]$ be a polynomial of degree q with Galois group $\mathbb{F}_q \rtimes \mathbb{F}_q^{\times} \cong \mathrm{AGL}(1, q)$. Suppose $E = \mathrm{End}^0(J_f)$ is a number field.
Then $E/\mathbb{Q}$ is cyclic Galois, and L/K is the unique extension of degree $[E : \mathbb{Q}]$ contained in $K(f)$.
Furthermore, if $[E : \mathbb{Q}] = q - 1$, then $L = EK$.

Sketch proof

Lower bound

- Use permutation groups and representation theory to show $\dim_{\mathbb{Q}} \mathrm{End}^0_{F'}(J_f) \leq [F' \cap K(f) : K]$.
- This allows us to show L, the minimal field of definition for the endomorphisms, contains some field $K \subseteq F \subseteq K(f)$ with $[F : K] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.
- This gives us a “lower bound” on L, so now we want to find an “upper bound”.

Upper bound

- $\mathrm{Gal}(\bar{K}/K)$ acts on $E := \mathrm{End}^0(J_f)$. This action factors through $\mathrm{Gal}(L/K)$.
- Moreover, as abstract groups, $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(E)$.
- As E is number field, we have $|\mathrm{Aut}(E)| \leq [E : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.

Sketch proof

Lower bound

- Use permutation groups and representation theory to show $\dim_{\mathbb{Q}} \mathrm{End}^0_{F'}(J_f) \leq [F' \cap K(f) : K]$.
- This allows us to show L, the minimal field of definition for the endomorphisms, contains some field $K \subseteq F \subseteq K(f)$ with $[F : K] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.
- This gives us a “lower bound” on L, so now we want to find an “upper bound”.

Upper bound

- $\mathrm{Gal}(\bar{K}/K)$ acts on $E := \mathrm{End}^0(J_f)$. This action factors through $\mathrm{Gal}(L/K)$.
- Moreover, as abstract groups, $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(E)$.
- As E is number field, we have $|\mathrm{Aut}(E)| \leq [E : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.

Sketch proof

Lower bound

- Use permutation groups and representation theory to show $\dim_{\mathbb{Q}} \operatorname{End}^0_{F'}(J_f) \leq [F' \cap K(f) : K]$.
- This allows us to show L, the minimal field of definition for the endomorphisms, contains some field $K \subseteq F \subseteq K(f)$ with $[F : K] = \dim_{\mathbb{Q}} \operatorname{End}^0(J_f)$.
- This gives us a “lower bound” on L, so now we want to find an “upper bound”.

Upper bound

- $\operatorname{Gal}(\bar{K}/K)$ acts on $E := \operatorname{End}^0(J_f)$. This action factors through $\operatorname{Gal}(L/K)$.
- Moreover, as abstract groups, $\operatorname{Gal}(L/K) \hookrightarrow \operatorname{Aut}(E)$.
- As E is number field, we have $|\operatorname{Aut}(E)| \leq [E : \mathbb{Q}] = \dim_{\mathbb{Q}} \operatorname{End}^0(J_f)$.

Sketch proof

Lower bound

- Use permutation groups and representation theory to show $\dim_{\mathbb{Q}} \mathrm{End}^0_{F'}(J_f) \leq [F' \cap K(f) : K]$.
- This allows us to show L, the minimal field of definition for the endomorphisms, contains some field $K \subseteq F \subseteq K(f)$ with $[F : K] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.
- This gives us a "lower bound" on L, so now we want to find an "upper bound".

Upper bound

- $\mathrm{Gal}(\bar{K}/K)$ acts on $E := \mathrm{End}^0(J_f)$. This action factors through $\mathrm{Gal}(L/K)$.
- Moreover, as abstract groups, $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(E)$.
- As E is number field, we have $|\mathrm{Aut}(E)| \leq [E : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.

Sketch proof

Lower bound

- Use permutation groups and representation theory to show $\dim_{\mathbb{Q}} \operatorname{End}^0_{F'}(J_f) \leq [F' \cap K(f) : K]$.
- This allows us to show L, the minimal field of definition for the endomorphisms, contains some field $K \subseteq F \subseteq K(f)$ with $[F : K] = \dim_{\mathbb{Q}} \operatorname{End}^0(J_f)$.
- This gives us a “lower bound” on L, so now we want to find an “upper bound”.

Upper bound

- $\operatorname{Gal}(\bar{K}/K)$ acts on $E := \operatorname{End}^0(J_f)$. This action factors through $\operatorname{Gal}(L/K)$.
- Moreover, as abstract groups, $\operatorname{Gal}(L/K) \hookrightarrow \operatorname{Aut}(E)$.
- As E is number field, we have $|\operatorname{Aut}(E)| \leq [E : \mathbb{Q}] = \dim_{\mathbb{Q}} \operatorname{End}^0(J_f)$.

Sketch proof

Lower bound

- Use permutation groups and representation theory to show $\dim_{\mathbb{Q}} \mathrm{End}^0_{F'}(J_f) \leq [F' \cap K(f) : K]$.
- This allows us to show L, the minimal field of definition for the endomorphisms, contains some field $K \subseteq F \subseteq K(f)$ with $[F : K] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.
- This gives us a “lower bound” on L, so now we want to find an “upper bound”.

Upper bound

- $\mathrm{Gal}(\bar{K}/K)$ acts on $E := \mathrm{End}^0(J_f)$. This action factors through $\mathrm{Gal}(L/K)$.
- Moreover, as abstract groups, $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(E)$.
- As E is number field, we have $|\mathrm{Aut}(E)| \leq [E : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathrm{End}^0(J_f)$.

Conclusion

- We have shown $[E:\mathbb{Q}] = [F:K] \leq [L:K] \leq |\mathrm{Aut}(E)| \leq [E:\mathbb{Q}]$.
- Hence we have equality, and so $E/\mathbb{Q}$ is Galois with $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(L/K) = \mathrm{Gal}(F/K)$.

Thus we've shown that if $\mathrm{Gal}(f) \cong \mathbb{F}_q \rtimes \mathbb{F}_q^{\times}$ and $E = \mathrm{End}^0(J_f)$ is a field, then $E/\mathbb{Q}$ is cyclic Galois and L/K is the unique extension of degree $[E:\mathbb{Q}]$ in $K(f)$.

Conclusion

- We have shown $[E:\mathbb{Q}] = [F:K] \leq [L:K] \leq |\mathrm{Aut}(E)| \leq [E:\mathbb{Q}]$.
- Hence we have equality, and so $E/\mathbb{Q}$ is Galois with $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(L/K) = \mathrm{Gal}(F/K)$.

Thus we've shown that if $\mathrm{Gal}(f) \cong \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ and $E = \mathrm{End}^0(J_f)$ is a field, then $E/\mathbb{Q}$ is cyclic Galois and L/K is the unique extension of degree $[E:\mathbb{Q}]$ in $K(f)$.

Conclusion

- We have shown $[E:\mathbb{Q}] = [F:K] \leq [L:K] \leq |\mathrm{Aut}(E)| \leq [E:\mathbb{Q}]$.
- Hence we have equality, and so $E/\mathbb{Q}$ is Galois with $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(L/K) = \mathrm{Gal}(F/K)$.

Thus we've shown that if $\mathrm{Gal}(f) \cong \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ and $E = \mathrm{End}^0(J_f)$ is a field, then $E/\mathbb{Q}$ is cyclic Galois and L/K is the unique extension of degree $[E:\mathbb{Q}]$ in $K(f)$.