Rational points on Jacobians of hyperelliptic curves I

Steffen Müller
Carl von Ossietzky Universität Oldenburg

September 2, 2014

Abelian varieties

Let k be a perfect field with fixed algebraic closure $\bar{k}$.

Informally, an abelian variety over k is a projective variety over k that carries a group structure, such that the group structure and the variety structure are compatible. More precisely:

Definition. An abelian variety A over k is a projective variety A/k such that

- $A(k')$ is a group for all field extensions $k \subset k'$;
- the group operation $A \times A \to A$ and the inversion $A \to A$ are regular functions (i.e. morphisms of algebraic varieties).

It turns out that the group law on an abelian variety is always commutative.

Examples of abelian varieties

Example. An abelian variety of dimension 1 is an elliptic curve.

Example. If A is an abelian variety of dimension g over $\mathbb{C}$, then $A(\mathbb{C})$ is isomorphic to a complex torus $\mathbb{C}^g/\Lambda$, where $\Lambda \cong \mathbb{Z}^{2g}$ is a lattice.

Every one-dimensional complex torus is an abelian variety, but in higher dimension this is no longer the case.

We're mostly interested in abelian varieties over $\mathbb{Q}$.

Theorem. (Mordell-Weil) Let $A/\mathbb{Q}$ be an abelian variety. Then the group $A(\mathbb{Q})$ is finitely generated. In other words, we have

$$A(\mathbb{Q}) \cong \mathbb{Z}^r \times A(\mathbb{Q})_{\mathrm{tors}}$$

where r is a nonnegative integer and the torsion subgroup $A(\mathbb{Q})_{\mathrm{tors}} \subset A(\mathbb{Q})$ is finite.

We call

- $A(\mathbb{Q})$ the Mordell-Weil group of $A/\mathbb{Q}$;
- r the rank of $A/\mathbb{Q}$.

The theorem holds in much greater generality, e.g. over number fields.

Proof of Mordell-Weil

The proof of Mordell-Weil can be broken down into 3 steps:

(i) $A(\mathbb{Q})/2A(\mathbb{Q})$ is a finite group (the "weak Mordell-Weil theorem").
(ii) There is a quadratic form $\hat{h} : A(\mathbb{Q}) \to \mathbb{R}$ such that for all $B \in \mathbb{R}$ the set $\{P \in A(\mathbb{Q}) : \hat{h}(P) \leq B\}$ is finite.
(iii) (i) and (ii) imply the theorem (the "descent lemma").

As a warm-up, let's prove (iii).
By (ii), $\hat{h}$ is nonnegative and vanishes precisely on torsion points. Let

- $P_1, \ldots, P_s \in A(\mathbb{Q})$ be a set of representatives for $A(\mathbb{Q})/2A(\mathbb{Q})$;
- $c = \max\{\hat{h}(P_i) : i \in \{1, \ldots, s\}\}$;
- $S = \{P \in A(\mathbb{Q}) : \hat{h}(P) \leq c\}$ (S is finite by (ii)).

We'll show that S generates $A(\mathbb{Q})$.

Proof of the descent lemma

Suppose not.
Then there is $Q_1 \in A(\mathbb{Q}) \setminus \langle S \rangle$ such that $\hat{h}(Q_1)$ is minimal for all such points.
We can write

$$Q_1 = P_i + 2Q_2$$

for some $i \in \{1, \ldots, s\}$ and $Q_2 \in A(\mathbb{Q})$. Then

$$4\hat{h}(Q_2) = \hat{h}(Q_1 - P_i) \leq 2\hat{h}(Q_1) + 2\hat{h}(P_i) < 4\hat{h}(Q_1),$$

since $\hat{h}$ is a quadratic form and since $\hat{h}(P_i) \leq c < \hat{h}(Q_1)$.

By minimality of $\hat{h}(Q_1)$, we have $Q_2 \in \langle S \rangle$, hence $Q_1 \in \langle S \rangle$. Contradiction!

Hyperelliptic curves

- k: perfect field of characteristic $\neq 2$
- C/k: hyperelliptic curve of genus $g \geq 1$, given by an equation $Y^2 = F(X, Z)$ in $\mathbb{P}^2_k(1, g+1, 1)$, where
  - $F \in k[X, Z]$ is a binary form of degree $2g + 2$,
  - $\mathrm{disc}(F) \neq 0$.

Usually we write $C : y^2 = f(x)$, where $f(x) = F(x, 1)$.

Let $d = \deg(f)$. Then we have

- 1 point $\infty = (1 : 0 : 0) \in C$ at infinity if $d = 2g + 1$;
- 2 points $\infty_{\pm s} = (1 : \pm s : 0) \in C$ at infinity if $d = 2g + 2$.

In fact $\infty \in C(k)$ when d is odd.

Weierstrass points

Let $C : y^2 = f(x)$ be a hyperelliptic curve over k.

- The hyperelliptic involution w maps $(X : Y : Z)$ to $(X : -Y : Z)$.
- It has exactly $2g + 2$ fixed points, the Weierstrass points of C:
  - the points $(r, 0)$, where r is a root of f;
  - ∞, if d is odd.
- These are the ramification points of the 2-1 covering $C \to \mathbb{P}^1$ given by $(x, y) \mapsto x$.

Divisors

A divisor on C/k is a finite formal sum $D = \sum_{P \in C(\bar{k})} n_P P$, where $n_p \in \mathbb{Z}$ for all $P \in C(\bar{k})$.

We call $\mathrm{supp}(D) = \{P \in C(\bar{k}) : n_P \neq 0\}$ the support of D.

The absolute Galois group $G_k = \mathrm{Gal}(\bar{k}/k)$ acts on $C(\bar{k})$ via $(X : Y : Z)^\sigma := (X^\sigma : Y^\sigma : Z^\sigma)$.

If $\sigma \in G_k$ and $D = \sum_{P \in C} n_P P \in \mathrm{Div}_C$, then σ acts on D via

$$D^\sigma := \sum_{P \in C} n_P P^\sigma.$$

We say D is rational over k if D is invariant under the action of G_k.

Definition. $\mathrm{Div}(C/k)$ is the group of divisors on C/k rational over k.

Principal divisors

For $P \in C$, let $v_P : k(C)^\times \twoheadrightarrow \mathbb{Z}$ be the normalized discrete valuation w.r.t. P.
For $\varphi \in k(C)^\times$ we have

- $\varphi(P) = 0 \Leftrightarrow v_P(\varphi) > 0$,
- $\varphi^{-1}(P) = 0 \Leftrightarrow v_P(\varphi) < 0$.

We define

$$\mathrm{div}(\varphi) := \sum_P v_P(\varphi) P.$$

- Such divisors are called principal.
- They are always k-rational.
- They form a subgroup $\mathrm{Princ}(C/k)$ of $\mathrm{Div}(C/k)$.

$D_1, D_2 \in \mathrm{Div}(C/k)$ are called linearly equivalent (denoted by $D_1 \sim D_2$) if $D_1 - D_2$ is principal.

Picard group

The quotient $\mathrm{Pic}(C/k) := \mathrm{Div}(C/k)/\mathrm{Princ}(C/k)$ is called the Picard group or divisor class group of C.

- The degree of $D = \sum_{P \in C} n_P P \in \mathrm{Div}(C/k)$ is $\deg(D) = \sum_P n_P$.
- We define $\mathrm{Div}^0(C/k) := \ker(\deg : \mathrm{Div}(C/k) \to \mathbb{Z})$.

It turns out that $\deg(\mathrm{div}(\varphi)) = 0$ for every $\varphi \in k(C)^\times$.

Hence we can define $\mathrm{Pic}^0(C/k) := \mathrm{Div}^0(C/k)/\mathrm{Princ}(C/k)$.

Example. If C is an elliptic curve over k, then $C(k) \cong \mathrm{Pic}^0(C/k)$.

In general, $C(k)$ is not a group. Instead we use $\mathrm{Pic}^0(C/k)$.

The Jacobian

Theorem. (Weil) There is an abelian variety $J = J_C$ over k of dimension g such that $J(k') = \mathrm{Pic}^0(C/k')$ for every field $k \subset k' \subset \bar{k}$.

- We call J the Jacobian of C.
- J is birational to $\mathrm{Sym}^g(C) = C^g/\mathfrak{S}_g$.

Example. If $C = E$ is an elliptic curve, then $J = E$.

Example. For $g = 2$, an explicit embedding of J into $\mathbb{P}^{15}$ as an intersection of 72 quadrics was constructed by Cassels and Flynn.

- In general, J can be embedded into $\mathbb{P}^{4g-1}$ ($\mathbb{P}^{3g-1}$ when d is odd).
- For computational purposes, we'd like to avoid using this embedding.
- Instead, represent points by divisors on C of degree 0.

Points on the Jacobian

Suppose that

- d is odd,
- $P \in J(k)$.

Then there is a unique divisor $D = \sum_{i=1}^{n} P_i - n\infty \in \mathrm{Div}_C^0(k)$ such that

- D represents P,
- $0 \leq n \leq g$,
- $\infty \neq P_i$ for all i,
- $P_i \neq w(P_j)$ for all $j \neq i$.

We call such a divisor D a reduced divisor.

Mumford representation

Suppose that

- d is odd
- $P \in J(k)$
- $D = \sum_{i=1}^{n} P_i - n\infty \in \mathrm{Div}_C^0(k)$ is the reduced divisor representing P, where $P_i = (x_i, y_i) \in C(\bar{k})$.

Then there are unique polynomials $a, b \in k[x]$ such that

- a is monic of degree n and factors as $a(x) = \prod_{i=1}^{n}(x - x_i)$;
- b has degree at most $n-1$ and we have $b(x_i) = y_i$ for all i;
- there is a polynomial $c \in k[x]$ such that $b^2 - f = ac$.

We call the pair (a, b) the Mumford representation of P.

There is an algorithm for addition on J using the Mumford representation due to Cantor.

Embedding the curve

We can embed C into J as follows: Fix a divisor class $c \in \mathrm{Pic}(C/\bar{k})$ of degree 1 and define

$$\iota_c : C \hookrightarrow J, \quad P \mapsto [P] - c.$$

If $c \in \mathrm{Pic}(C/k)$, then ι_c is also defined over k and $\iota_c(C(k)) \subset J(k)$.

Example. Recall that if f has odd degree $d = 2g + 1$, then $\infty \in C(k)$. In this situation, we use the embedding

$$\iota : C \hookrightarrow J, \quad P \mapsto [P - \infty]$$

defined over k.

Idea. Use information on the group $J(k)$ to get information on $C(k)$. We'll concentrate on the case $k = \mathbb{Q}$.

Computational problems

By the Mordell-Weil theorem, we have

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \times J(\mathbb{Q})_{\mathrm{tors}},$$

where the rank r is a nonnegative integer and the torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}} \subset J(\mathbb{Q})$ is finite.

Problem. Given a hyperelliptic curve $C/\mathbb{Q}$, compute

- the rank r;
- generators of $J(\mathbb{Q})$.

The proof of the Mordell-Weil theorem is constructive in the following sense: It provides us with a method to compute these objects which often works in practice; however, the method is not currently effective.

Some Applications

- Chabauty's method to compute $C(\mathbb{Q})$ when $g \geq 2$
- Mordell-Weil sieve to compute $C(\mathbb{Q})$ when $g \geq 2$
- Computation of the set of integral points $\{(x, y) \in C(\mathbb{Q}) : x, y \in \mathbb{Z}\}$ (using work of Bugeaud-Mignotte-Siksek-Stoll-Tengely) when $g \geq 2$
- Numerical verification of the conjecture of Birch and Swinnerton-Dyer for $J/\mathbb{Q}$

Proof of Mordell-Weil: reminder

Recall the steps of the proof of the Mordell-Weil theorem:

(i) $J(\mathbb{Q})/2J(\mathbb{Q})$ is a finite group.
(ii) There is a quadratic form $\hat{h} : J(\mathbb{Q}) \to \mathbb{R}$ such that for all $B \in \mathbb{R}$ the set $\{P \in J(\mathbb{Q}) : \hat{h}(P) \leq B\}$ is finite.
(iii) (i) and (ii) imply the theorem.

We've already shown (iii). Today we discuss

- how to prove (i);
- how to compute (or at least bound) the rank r.

The 2-Selmer group

Theorem. There is an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}_2(J/\mathbb{Q}) \to Ш(J/\mathbb{Q})[2] \to 0,$$

where

- $\mathrm{Sel}_2(J/\mathbb{Q})$ is the 2-Selmer group of $J/\mathbb{Q}$,
- $Ш(J/\mathbb{Q})$ is the Shafarevich-Tate group of $J/\mathbb{Q}$,
- we write $G[2]$ for the elements of order dividing 2 of an abelian group G.

It turns out that

- $\mathrm{Sel}_2(J/\mathbb{Q})$ is finite, implying the finiteness of $J(\mathbb{Q})/2J(\mathbb{Q})$.
- $Ш(J/\mathbb{Q})$ is a torsion group which is conjectured (but in general not proved) to be finite.

A formula for the rank

There is an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}_2(J/\mathbb{Q}) \to Ш(J/\mathbb{Q})[2] \to 0.$$

- All groups in this sequence are $\mathbb{F}_2$-vector spaces.
- Let $\dim$ denote the dimension of an $\mathbb{F}_2$-vector space.

Note that

$$\dim J(\mathbb{Q})/2J(\mathbb{Q}) = \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim Ш(J/\mathbb{Q})[2].$$

A formula for the rank

There is an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}_2(J/\mathbb{Q}) \to Ш(J/\mathbb{Q})[2] \to 0.$$

- All groups in this sequence are $\mathbb{F}_2$-vector spaces.
- Let $\dim$ denote the dimension of an $\mathbb{F}_2$-vector space.

Note that

$$\dim(\mathbb{Z}/2\mathbb{Z})^r + \dim J(\mathbb{Q})_{\mathrm{tors}}/2J(\mathbb{Q})_{\mathrm{tors}} = \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim Ш(J/\mathbb{Q})[2],$$

if we assume the Mordell-Weil Theorem.

A formula for the rank

There is an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}_2(J/\mathbb{Q}) \to Ш(J/\mathbb{Q})[2] \to 0.$$

- All groups in this sequence are $\mathbb{F}_2$-vector spaces.
- Let $\dim$ denote the dimension of an $\mathbb{F}_2$-vector space.

Note that

$$r + \dim J(\mathbb{Q})[2] = \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim Ш(J/\mathbb{Q})[2],$$

if we assume the Mordell-Weil Theorem.

Bounding the rank

We have

$$r = \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim Ш(J/\mathbb{Q})[2] - \dim J(\mathbb{Q})[2].$$

It turns out that

- $\dim \mathrm{Sel}_2(J/\mathbb{Q})$ is effectively computable;
- $\dim J(\mathbb{Q})[2] = m_{\mathbb{Q}} - 1$ is trivial to compute. E.g., $m_{\mathbb{Q}}$ is the number of irreducible factors of f over $\mathbb{Q}$, if d is odd.
- At present, no algorithm is known for the computation of $\dim Ш(J/\mathbb{Q})[2]$.

But we get an upper bound $r' := \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim J(\mathbb{Q})[2]$ for r.

We can complement this by a lower bound r'' for r, for instance by finding r'' independent non-torsion points in $J(\mathbb{Q})$.

If r' and r'' agree, then $r = r' = r''$.

Principal homogeneous spaces

Definition. A principal homogeneous space (phs) for J is a variety $V/\mathbb{Q}$ such that there is a simple transitive action of J on V.

Note that a phs for J is isomorphic to J over $\bar{\mathbb{Q}}$ (but not necessarily over $\mathbb{Q}$).

Every element of $\mathrm{Sel}_2(J/\mathbb{Q})$ and $Ш(J/\mathbb{Q})$ can be represented by a phs V.

- All of these V are everywhere locally soluble, i.e. $V(\mathbb{Q}_v) \neq \emptyset$ for all places v.
- V represents a nontrivial element of $Ш(J/\mathbb{Q})$ iff $V(\mathbb{Q}) = \emptyset$.
  - So $Ш(J/\mathbb{Q})$ measures the failure of the Hasse principle.
  - If $g = 1$, then such a phs V is a genus 1 curve.
  - If $g > 1$, then this interpretation isn't too helpful for computations.

Low-brow construction

$\mathrm{Sel}_2(J/\mathbb{Q})$ and $Ш(J/\mathbb{Q})$ can be defined in terms of Galois cohomology.

Instead, we give a construction of $\mathrm{Sel}_2(J/\mathbb{Q})$ that is

- more down-to-earth,
- amenable to explicit computations.

For simplicity, we restrict to the case of odd degree $d = \deg(f) = 2g + 1$.

By a change of variables over $\mathbb{Q}$, we can also assume that f is monic and has integral coefficients.

First we fix some notation.

Notation

For an extension field k of $\mathbb{Q}$ let

- $f = \prod_{i=1}^{m_k} f_{k,i}$ be the factorisation of f into irreducible factors over k,
- $A_{k,i} := k[x]/\langle f_{k,i}(x)\rangle$,
- $A_k := k[T] = k[x]/\langle f(x)\rangle \cong A_{k,1} \times \ldots \times A_{k,m_k}$.

Then

- the $A_{k,i}$ are finite field extensions of k;
- A_k is a finite-dimensional commutative k-algebra.
  - If f is irreducible over k, then A_k is a field extension of k of degree d.
  - If f factors completely over k, then $A_k = k^{\times d} := k \times \ldots \times k$

Let

- k be an extension field of $\mathbb{Q}$,
- $D = \sum_P n_P P \in \mathrm{Div}^0(C/k)$ be a divisor whose support does not include a Weierstrass point.

We define

$$(x - T)(D) = \prod_P (x(P) - T)^{n_P} \in A_k^\times.$$

Let $D_1, D_2 \in \mathrm{Div}^0(C/k)$ such that D_1 and D_2 have no Weierstrass points in their support.
Then we have

$$(x - T)(D_1 + D_2) = (x - T)(D_1) \cdot (x - T)(D_2).$$

The Weil homomorphism δ

Lemma. Let $P \in J(k)$. Then there is a divisor $D \in \mathrm{Div}^0(C/k)$ representing P whose support does not include a Weierstrass point.

Proposition. (Schaefer) The map $x - T$ induces a group homomorphism $\delta_k : J(k) \to A_k^\times/(A_k^\times)^2$.

Sketch of proof. By the Lemma and the definition of $x - T$, it suffices to show that $(x - T)(D)$ is a square whenever $D \in \mathrm{Div}^0(C/k)$

- is principal and
- has no Weierstrass points in its support.

This follows using either

- Weil reciprocity or
- a direct computation.

The kernel of δ

Proposition. (Schaefer.) The kernel of δ_k is $2J(k)$.

Sketch of proof.

- $2J(k) \subset \ker \delta_k$: The codomain of δ_k has exponent 2, so its kernel must contain $2J(k)$.
- $\ker \delta_k \subset 2J(k)$: Given $P \in \ker(\delta_k)$, can explicitly construct a point $Q \in J(k)$ such that $2Q = P$.

So δ_k embeds $J(k)/2J(k)$ into $A_k^\times/(A_k^\times)^2$.

The norm

For $a \in A_k$ the map $m_a : A_k \to A_k,\ m_a(x) = a \cdot x$ is k-linear.

We define the norm of a by

$$N_{A_k/k}(a) = \det(m_a).$$

- If A_k is a field, then $N_{A_k/k}$ is the usual relative norm $A_k \to k$.
- $N_{A_k/k} : A_k^\times \to k^\times$ is a group homomorphism.

We set

$$H_k = \ker\left(N_{A_k/k} : A_k^\times/(A_k^\times)^2 \to k^\times/(k^\times)^2\right).$$

Proposition. (Schaefer.) The image of δ_k is contained in H_k.

Hence $J(k)/2J(k)$ embeds into H_k.

More notation

We'll drop all $\mathbb{Q}$'s in subscripts, denoting

- $A_{\mathbb{Q}} = \mathbb{Q}[T] = \mathbb{Q}[x]/\langle f(x)\rangle$ by A
- $H_{\mathbb{Q}}$ by H
- and so on...

We replace $\mathbb{Q}_v$ by v in subscripts, denoting

- $A_{\mathbb{Q}_v}$ by A_v
- $H_{\mathbb{Q}_v}$ by H_v
- and so on...

Concrete version of the 2-Selmer group

Let

- v be a place of $\mathbb{Q}$,
- ρ_v be the natural map $H \to H_v$ induced by the injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$.

The following diagram is commutative:

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{\delta} & H \\ \downarrow & & \downarrow{\scriptstyle \rho_v} \\ J(\mathbb{Q}_v) & \xrightarrow{\delta_v} & H_v \end{array}$$

Definition. The 2-Selmer group $\mathrm{Sel}_2(J/\mathbb{Q})$ is defined as

$$\mathrm{Sel}_2(J/\mathbb{Q}) := \{\xi \in H : \rho_v(\xi) \in \mathrm{im}(\delta_v) \text{ for all } v\}.$$

Finiteness of the 2-Selmer group I

Definition. The 2-Selmer group $\mathrm{Sel}_2(J/\mathbb{Q})$ is defined as

$$\mathrm{Sel}_2(J/\mathbb{Q}) := \{\xi \in H : \rho_v(\xi) \in \mathrm{im}(\delta_v) \text{ for all } v\}.$$

But we want to show that $\mathrm{Sel}_2(J/\mathbb{Q})$ is finite.

We'll find a subgroup H' of H such that

- H' is finite;
- H' contains $\mathrm{Sel}_2(J/\mathbb{Q})$.

Let S denote the set of places

$$S = \{\infty, 2\} \cup \{p : p \mid \mathrm{disc}(f)\}.$$

The prime numbers $p \in S$ are precisely the primes of bad reduction (more on this later).

Finiteness of the 2-Selmer group II

An element of $H \subset A^\times/(A^\times)^2$ is an equivalence class of tuples $(\xi_1, \ldots, \xi_m)$, where

- $\xi_i \in A_i = \mathbb{Q}[x]/\langle f_i(x)\rangle$,
- $f = \prod_{i=1}^m f_i$ is the factorisation of f into irreducibles over $\mathbb{Q}$.

We define H' as the subgroup of H consisting of elements ξ that have a representative $(\xi_1, \ldots, \xi_m)$ such that the following holds for all i:

ξ_i is a $\mathfrak{p}$-adic unit for all primes $\mathfrak{p}$ of A_i not above S.

Equivalently, an element $\xi \in H$ lies in H' if and only if every representative $(\xi_1, \ldots, \xi_m)$ of ξ satisfies:

For all i, $A_i(\sqrt{\xi_i})/A_i$ is ramified only at primes above S.

Finiteness of the 2-Selmer group III

Proposition. The group H' is finite.

Proposition. (Schaefer) $\mathrm{Sel}_2(J/\mathbb{Q})$ in H is contained in H':

$$\mathrm{Sel}_2(J/\mathbb{Q}) = \{\xi \in H' : \rho_v(\xi) \in \mathrm{im}(\delta_v) \text{ for all } v \in S\},$$

Corollary. $\mathrm{Sel}_2(J/\mathbb{Q})$ is finite.

Corollary. $J(\mathbb{Q})/2J(\mathbb{Q})$ is finite.

This proves the weak Mordell-Weil theorem for $J/\mathbb{Q}$.

Two-descent: The algorithm

Recall the commutative diagram

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{\delta} & H' \\ \downarrow & & \downarrow{\scriptstyle \rho_v} \\ J(\mathbb{Q}_v) & \xrightarrow{\delta_v} & H_v. \end{array}$$

We obtain the following algorithm for the computation of $\mathrm{Sel}_2(J/\mathbb{Q})$:

(1) Compute the set S.
(2) Compute generators for the group H'.
(3) For every $v \in S$, compute $\delta_v(J(\mathbb{Q}_v)) \subset H_v$.
(4) For every $v \in S$, compute $\ker(\rho_v : H' \to H_v)$.
(5) Compute $\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_{v \in S} \rho_v^{-1}(\delta_v(J(\mathbb{Q}_v)))$.

Two-descent: steps (1) and (2)

(1) Compute the set S.
(2) Compute generators for the group H'.
(3) For every $v \in S$, compute $\delta_v(J(\mathbb{Q}_v)) \subset H_v$.
(4) For every $v \in S$, compute $\ker(\rho_v : H' \to H_v)$.
(5) Compute

$$\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_{v \in S} \rho_v^{-1}(\delta_v(J(\mathbb{Q}_v))).$$

For (1) it suffices to factor the discriminant $\mathrm{disc}(f)$.

Since we have to factor f anyway to construct A, we can use the discriminants and resultants of the various factors.

We'll discuss (2) in detail below for the case where f factors completely over $\mathbb{Q}$.

Two-descent: step (3)

(1) Compute the set S.
(2) Compute generators for the group H'.
(3) For every $v \in S$, compute $\delta_v(J(\mathbb{Q}_v)) \subset H_v$.
(4) For every $v \in S$, compute $\ker(\rho_v : H' \to H_v)$.
(5) Compute $\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_{v \in S} \rho_v^{-1}(\delta_v(J(\mathbb{Q}_v)))$.

For (3) we use

$$\dim \delta_v(J(\mathbb{Q}_v)) = m_v - 1 + \begin{cases} g & \text{if } v = 2 \\ 0 & \text{if } v \notin \{2, \infty\} \\ -g & \text{if } v = \infty \end{cases},$$

where m_v is the number of irreducible factors of f over $\mathbb{Q}_v$.

We simply compute $\delta_v(P)$ for points $P \in J(\mathbb{Q}_v)$ until the group generated by these images has the correct dimension.

Two-descent: steps (4) and (5)

(1) Compute the set S.
(2) Compute generators for the group H'.
(3) For every $v \in S$, compute $\delta_v(J(\mathbb{Q}_v)) \subset H_v$.
(4) For every $v \in S$, compute $\ker(\rho_v : H' \to H_v)$.
(5) Compute $\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_{v \in S} \rho_v^{-1}(\delta_v(J(\mathbb{Q}_v))$.

(4) and (5) are simply linear algebra over $\mathbb{F}_2$.

The totally split case

Now suppose that

$$f(x) = \prod_{i=1}^{d} (x - e_i),$$

where $e_i \in \mathbb{Z}$ for all i. Then we have:

- $A = \mathbb{Q}^{\times d}$
- The canonical map $\mathbb{Q}[x] \to A$ is $t \mapsto (t(e_1), \ldots, t(e_d))$.
- $N_{A/\mathbb{Q}}(\xi_1, \ldots, \xi_d) = \xi_1 \cdots \xi_d$

We find

$$\begin{aligned} H &= \ker(N_{A/\mathbb{Q}} : A^\times/(A^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \\ &= \{[(\xi_1, \ldots, \xi_d)] \in (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2))^{\times d} : \xi_1 \cdots \xi_d \in (\mathbb{Q}^\times)^2\} \\ &\cong (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2))^{\times (d-1)} \\ &= (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2))^{\times 2g}. \end{aligned}$$

Generators of H'

Note that every element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ can be represented by a unique squarefree integer.

So if $\xi \in H$ is represented by $(\xi_1, \ldots, \xi_{2g})$, where all $\xi_i \in \mathbb{Z}$ are squarefree, then

$$\xi \in H' \Leftrightarrow p \nmid \xi_i \quad \text{for all} \quad i = 1, \ldots, 2g \quad \text{and} \quad p \notin S.$$

Hence, if $S = \{\infty, p_1, \ldots, p_m\}$, then

$$H' = \langle -1, p_1, \ldots, p_m \rangle^{\times 2g}.$$

This immediately shows that H' is finite.

Example: Setup

Consider the genus 2 curve

$$C : y^2 = f(x) = \prod_{i=1}^{5}(x - e_i) = x(x-2)(x+2)(x+3)(x+7).$$

Then $\mathrm{disc}(f) = 2^{12} \cdot 3^6 \cdot 5^4 \cdot 7^2$, so

- $S = \{2, 3, 5, 7, \infty\}$,
- $H' = \langle -1, 2, 3, 5, 7 \rangle^{\times 4} \subset (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^4$.

We have

$$J(k)[2] = \langle [(e_i, 0) - \infty)] : i \in \{1, \ldots, 4\} \rangle \cong (\mathbb{Z}/2\mathbb{Z})^4$$

for all fields k extending $\mathbb{Q}$.

Example: Known points

Consider

$$C : y^2 = f(x) = x(x-2)(x+2)(x+3)(x+7).$$

We find the non-Weierstrass points

$$(-1, \pm 6), (-4, \pm 12), (3, \pm 30), (-6, \pm 24), (-7, \pm 210) \in C(\mathbb{Q}).$$

Let $G = \langle J(\mathbb{Q})[2], Q_1, Q_2 \rangle \subset J(\mathbb{Q})$, where

- $Q_1 = [(-1, 6) - \infty]$,
- $Q_2 = [(-4, 12) - \infty]$.

We'll compute the image of G under the maps

- $\delta : J(\mathbb{Q}) \to H$ (the map induced by the "$x - T$-map"),
- its v-adic analogues $\delta_v : J(\mathbb{Q}_v) \to H_v$ for $v \in S$.

Example: Computing δ

If $P = (x_P, y_P) \in C(\mathbb{Q})$, then $\delta(P - \infty)$ can be computed as follows:

If $y_P \neq 0$, then

$$\delta(P - \infty) = [(x_p - e_1, \ldots, x_p - e_5)] \in (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^5.$$

If $y_P = 0$, then $x_P = e_i$ for some i and

$$\delta(P - \infty) = [(l_1, \ldots, l_5)] \in (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^5,$$

where

- $l_j = e_i - e_j$ if $j \neq i$ and
- l_i is determined by the condition that the product of the l_i is a square.

Example: Lower bound

We compute $\delta(G)$:

$$\begin{aligned}
\delta((0,0)-\infty) &= (-21,-2,2,3)\\
\delta((2,0)-\infty) &= (2,10,1,5)\\
\delta((-2,0)-\infty) &= (-2,-1,10,1)\\
\delta((-3,0)-\infty) &= (-3,-5,-1,-15)\\
\delta((-1,6)-\infty) &= (-1,-3,1,2)\\
\delta((-4,12)-\infty) &= (-1,-6,-2,-1)
\end{aligned}$$

Since the tuples on the RHS are independent elements of the $\mathbb{F}_2$-vector space H', we get

$$\dim \mathrm{Sel}_2(J/\mathbb{Q}) \geq 6.$$

Example: What's left?

We claim that

$$\delta(G) = \mathrm{Sel}_2(J/\mathbb{Q}).$$

Recall the diagram

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{\delta} & H' \\ \downarrow & & \downarrow{\scriptstyle \rho_v} \\ J(\mathbb{Q}_v) & \xrightarrow{\delta_v} & H_v \end{array}$$

and the remaining steps

(3) For every $v \in S$, compute $\delta_v(J(\mathbb{Q}_v)) \subset H_v$.
(4) For every $v \in S$, compute $\ker(\rho_v : H' \to H_v)$.
(5) Compute $\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_{v \in S} \rho_v^{-1}(\delta_v(J(\mathbb{Q}_v)))$.

Example: $v = 3$

For $v = 3$, we have $\mathbb{Q}_3^\times/(\mathbb{Q}_3^\times)^2 = \langle 1, -1, 3, -3\rangle$. We find that

$$\begin{aligned}\delta_3((0,0) - \infty) &= (3, 1, -1, 3)\\ \delta_3((2,0) - \infty) &= (-1, 1, 1, -1)\\ \delta_3((-2,0) - \infty) &= (1, -1, 1, 1)\\ \delta_3((-1,6) - \infty) &= (-1, -3, 1, -1)\end{aligned}$$

are independent elements of H_3.

Since $\dim(\delta_3(J(\mathbb{Q}_3))) = 4$, these generate $\delta_3(J(\mathbb{Q}_3))$.
Note that $\delta_3(J(\mathbb{Q}_3)) = \delta_3(G)$, so

$$\rho_3^{-1}(\delta_3(J(\mathbb{Q}_3))) = \langle \ker \rho_3, \delta(G)\rangle.$$

Example: Finishing up

We can also compute $\operatorname{im}\delta_v$ and $\ker\rho_v$ for $v = \infty, 2, 5, 7$.

We get $\delta_v(J(\mathbb{Q}_v)) = \delta_v(G)$ in all cases, hence

$$\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_{v\in S} \rho_v^{-1}(\delta_v(J(\mathbb{Q}_v))) = \bigcap_{v\in S} \langle \ker\rho_v, \delta(G)\rangle.$$

Using linear algebra, we obtain

$$\bigcap_{v\in S} \langle \ker\rho_v, \delta(G)\rangle = \delta(G),$$

so that

$$\mathrm{Sel}_2(J/\mathbb{Q}) = \delta(G).$$

Example: Conclusion

Let's summarize what we've shown:

- $\dim \mathrm{Sel}_2(J/\mathbb{Q}) = 6$,

$\Rightarrow$ $r \leq r' = \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim J(\mathbb{Q})[2] = 6 - 4 = 2$,

- $Q_1, Q_2 \in J(\mathbb{Q})$ are independent nontorsion points, because their images under δ are independent.

$\Rightarrow$ $r = 2$ and $Ш(J/\mathbb{Q})[2] = 0$

Note that we were only able to determine r because we found $2 = r'$ independent nontorsion points in $J(\mathbb{Q})$.

Question. What if we

- have computed $r' = \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim J(\mathbb{Q})[2]$, but we
- haven't managed to find r' independent nontorsion points in $J(\mathbb{Q})$?

Answer. We can

- spend more time searching for points;
- give up;
- use more refined techniques:
  - If $g = 1$, can try an N-descent for $N > 2$.
  - If there is a nontrivial isogeny $\varphi : J \to J'$ defined over $\mathbb{Q}$, can try a φ-descent.
  - If $Ш(J/\mathbb{Q})$ is finite, then $r' - r$ is even.
  - The conjecture of Birch and Swinnerton-Dyer predicts

$$r = \operatorname{ord}_{s=1} L_C(s),$$

where L_C is the L-function of $C/\mathbb{Q}$; $\operatorname{ord}_{s=1} L_C(s)$ can often be computed in practice.