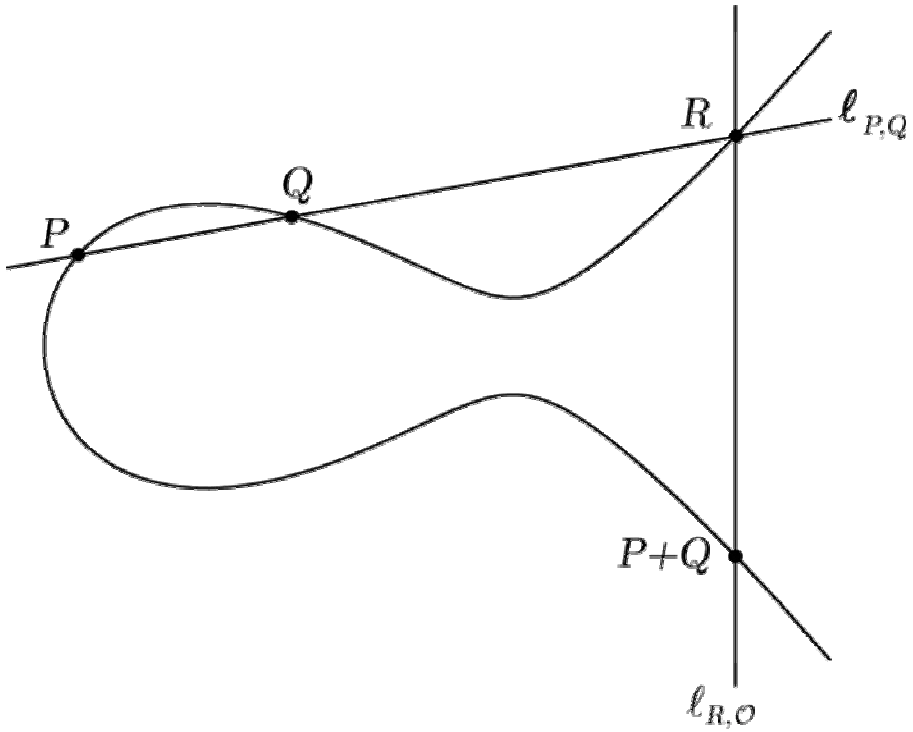
2004 ECRYPT Summer School on Elliptic Curve Cryptography

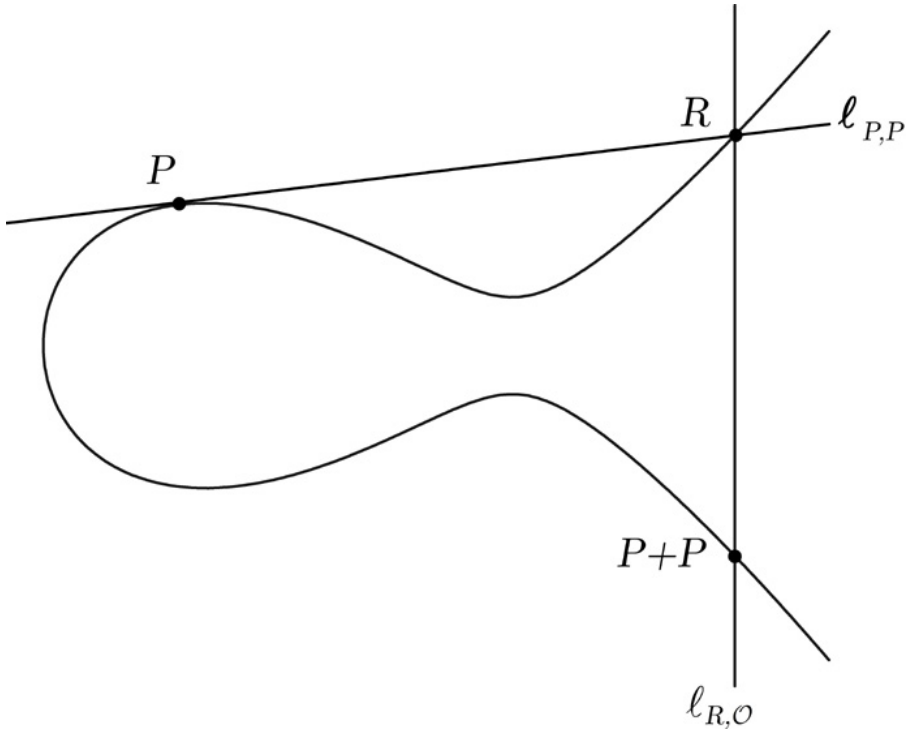
The Picard Group, or how to build a group from a set

Isabelle Déchène
Assistant Professor
Department of Mathematics and Statistics
University of Ottawa, Canada

Tutorial on Elliptic and
Hyperelliptic Curve Cryptography
University College Dublin, Ireland
September 3rd, 2007

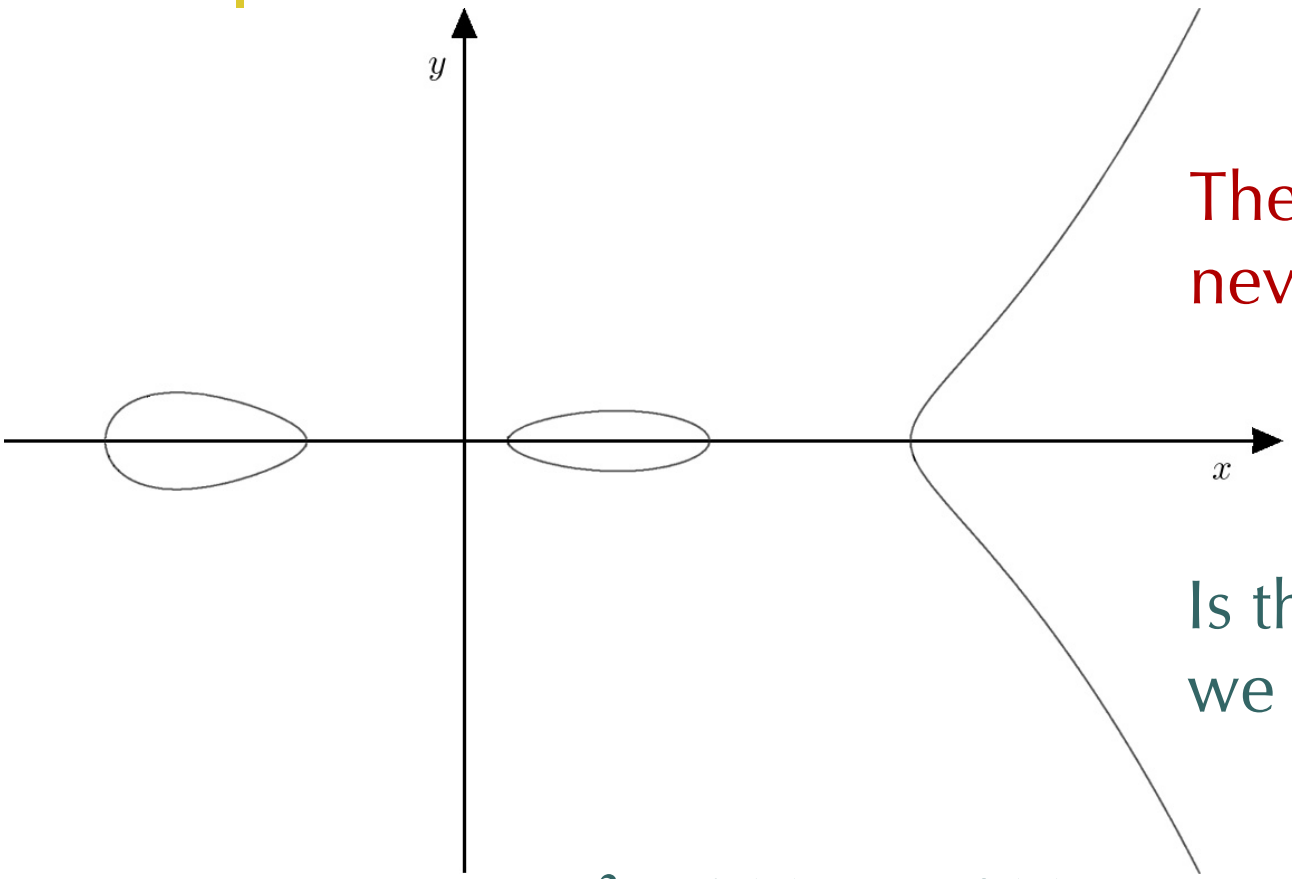
Chord-and-tangent Rule on Elliptic Curves





$$y^2 = x^3 + ax + b$$

Motivation: Hyperelliptic Curves



The points here will never form a group…

Is there something we can do?

$$y^2 + h(x)\,y = f(x),$$

plus some extra conditions on f and h that we'll see later on.

The Stamp Collector

A stamp collector takes his passion quite seriously.
Each collectible has a unique identification code.

D

F

G

R

The Stamp Collector

It is then an easy matter to write in a compact form an up to date inventory of his collection.

Date	Operation	D	F	G	R	…
Sept. 1st	Inventory	4	0	5	1	…
Sept. 3rd	Transaction	0	0	-2	1	…
Sept. 3rd	Inventory	4	0	3	2	…

For quick reference, this last state could also be symbolized by the shorthand

$$4(D)+3(G)+2(R)\ +\ \ldots$$

The Stamp Collector

So we started with a *set* consisting of the different stamps and we ended up with a *group* where a typical element consists of a list of integers, one for each stamp.

This idea is often used in mathematics.

Indeed, we just built a *free abelian group* on a set of stamps!

The identity element in this group is:

$$\mathbf{0} = 0(D) + 0(F) + 0(G) + 0(R) \; + \; \ldots$$

Divisors

Let C be your favorite smooth algebraic curve defined over a field K.

We now collect the points of $C(\overline{K})$ as a hobby:

$$\begin{array}{r} 3(P_1) - 5(P_2) + 0(P_3) - 9(P_4) + \ldots \\ + \; 0(P_1) - 3(P_2) - 1(P_3) + 3(P_4) + \ldots \\ \hline 3(P_1) - 8(P_2) - 1(P_3) - 6(P_4) + \ldots \end{array}$$

Each of these formal sums is called a *divisor*.

Divisors

A *divisor* on C is hence a formal sum of the form

$$D = \sum_{P \in C} n_P(P),$$

where each n_P is an integer and finitely many of them are nonzero.

The addition of two such divisors is thus given by

$$\sum_{P \in C} n_P(P) + \sum_{P \in C} m_P(P) = \sum_{P \in C} (n_P + m_P)(P).$$

Divisors

The group formed by these divisors is denoted $\mathrm{Div}(C)$, and its identity element is

$$\mathbf{0} = \sum_{P \in C} 0(P)$$

The *degree* of the divisor D is the integer

$$\deg(D) = \sum_{P \in C} n_P$$

The divisors of degree zero form a subgroup of $\mathrm{Div}(C)$ denoted by $\mathrm{Div}^0(C)$.

Divisors defined over K

Let $\mathrm{Gal}(\overline{K}/K)$ be the Galois group of $\overline{K}$ over K and let $D = \sum_{P \in C} n_P(P)$ be a divisor.

Definitions. For $\sigma \in \mathrm{Gal}(\overline{K}/K)$, let

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

Moreover, D is said to be *defined over* K if

$$D^\sigma = D \text{ for all } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

Principal Divisors

The *divisor of a function* $f \in \overline{K}(C)^*$ is

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)(P),$$

where $\operatorname{ord}_P(f)$ is the *order of vanishing* at P.

- If $\operatorname{ord}_P(f) < 0$, then f has a *pole* of order $-\operatorname{ord}_P(f)$ at P,
- If $\operatorname{ord}_P(f) = 0$, then f is defined and nonzero at P,
- If $\operatorname{ord}_P(f) > 0$, then f has a *zero* of order $\operatorname{ord}_P(f)$ at P.

These special divisors are called *principal divisors*.

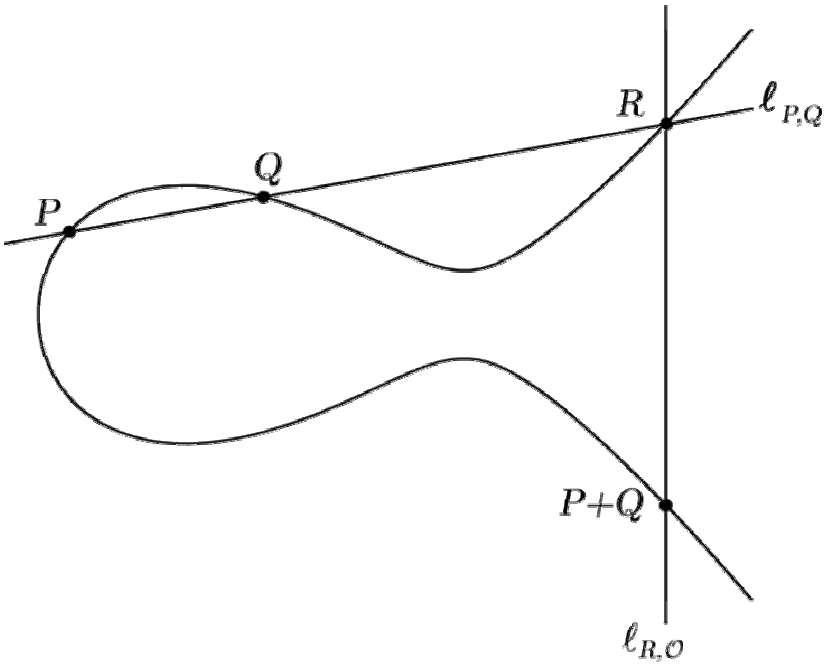
Properties of Principal Divisors

Theorem. Let C be a smooth algebraic curve defined over K and $f, g \in \overline{K}(C)^*$ be given. Then,

- $\operatorname{div}(f) = \mathbf{0}$ iff $f \in \overline{K}^*$
- $\deg(\operatorname{div}(f)) = 0$
- $\operatorname{div}(f \cdot g) = \operatorname{div}(f) + \operatorname{div}(g)$
- $\operatorname{div}(f / g) = \operatorname{div}(f) - \operatorname{div}(g)$
- $\operatorname{div}(f^n) = n \cdot \operatorname{div}(f)$ for all integers $n \geq 1$.
- $\operatorname{div}(f) = \operatorname{div}(g)$ iff $f = c \cdot g$ for some $c \in \overline{K}^*$.

Important Examples

$$\operatorname{div}\left(\frac{\ell_{P,Q}}{Z}\right) = (P) + (Q) + (R) - 3(\mathcal{O})$$



$$\operatorname{div}\left(\frac{\ell_{P+Q,\mathcal{O}}}{Z}\right) = (R) + (P+Q) - 2(\mathcal{O})$$

$$\operatorname{div}\left(\frac{\ell_{P,Q}}{\ell_{P+Q,\mathcal{O}}}\right) = \operatorname{div}\left(\frac{\ell_{P,Q}}{Z}\right) - \operatorname{div}\left(\frac{\ell_{P+Q,\mathcal{O}}}{Z}\right) = (P) + (Q) - (P+Q) - (\mathcal{O})$$

This observation is at the heart of pairing computations!

Constructing the Picard Group

✓ 1. Start with your favorite algebraic curve.

✓ 2. Consider its divisors of degree zero.

3. (Cleverly) define an equivalence relation on them.

4. Find a canonical representative for each class.

Linear Equivalence

Now let $D_1, D_2 \in \mathrm{Div}(C)$ be given.

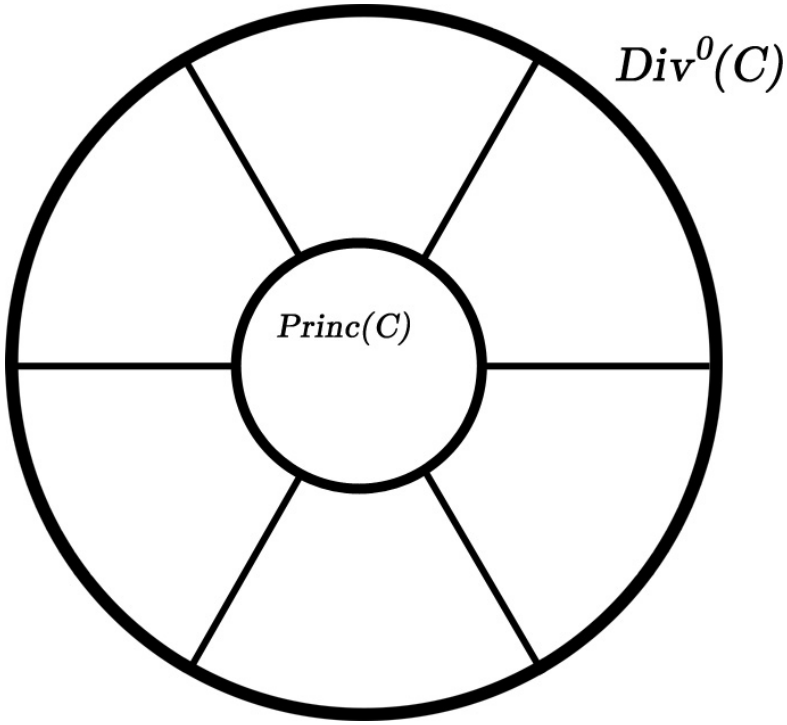
If $D_1 - D_2$ is a principal divisor, then we say that D_1 and D_2 are *linearly equivalent*, and we write

$$D_1 \sim D_2.$$

The whole idea behind this equivalence relation is to somehow measure how much D_1 differs from D_2.

The Picard Group

Equivalence classes of divisors of degree zero form a group denoted $\mathrm{Pic}^0(C)$.



In other words,

$$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C) \,/\, \mathrm{Princ}(C),$$

where $\mathrm{Princ}(C)$ denotes the subgroup of principal divisors.

Lastly, $\mathrm{Pic}^0_K(C)$ is the subgroup of $\mathrm{Pic}^0(C)$ fixed by $\mathrm{Gal}(\overline{K}/K)$.

Constructing the Picard Group

✓ 1. Start with your favorite algebraic curve.

✓ 2. Consider its divisors of degree zero.

✓ 3. (Cleverly) define an equivalence relation on them.

4. Find a canonical representative for each class.

Canonical Representatives for Elliptic Curves

Let E be an elliptic curve defined over a field K.

We first want to associate a divisor to each point of E.

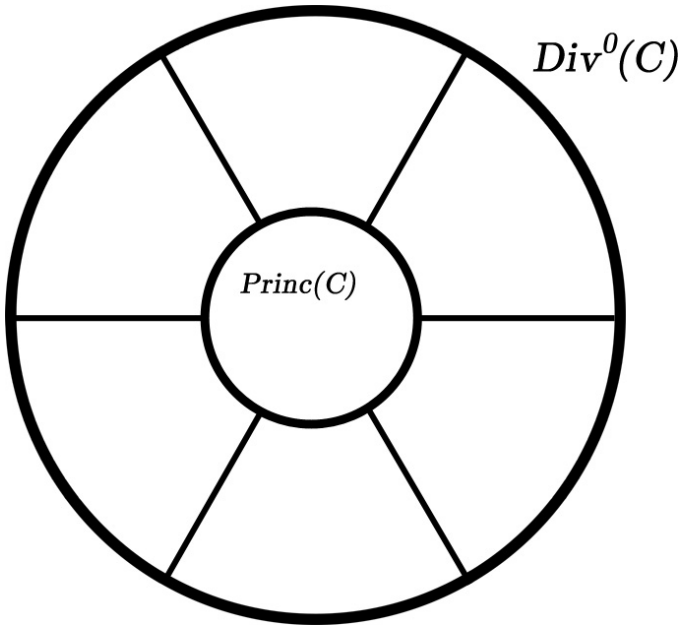
$$E \quad \Longleftrightarrow \quad \mathrm{Div}^0(E)$$

$$P \qquad\qquad (P) - (\mathcal{O})$$

$$\mathcal{O} \qquad\qquad \mathbf{0} = (\mathcal{O}) - (\mathcal{O})$$

$$E \quad \Longleftrightarrow \quad \mathrm{Pic}^0(E)$$

$$P \qquad\qquad [(P) - (\mathcal{O})]$$



The Abel-Jacobi Theorem

Theorem. Let E be an elliptic curve defined over a field K and let $D = \sum_{P \in E} n_P(P) \in \mathrm{Div}(E)$ be given. Then,

$$D \text{ is principal}$$

$$\text{if and only if}$$

$$\deg(D) = 0 \text{ and } \sum_{P \in E} n_P P = \mathcal{O}.$$

Important Tool

Corollary. Let E be an elliptic curve defined over a field K and let

$$D_1 = \sum_{P \in E} n_P(P), D_2 = \sum_{P \in E} m_P(P) \in \mathrm{Div}(E)$$

be given. Then,

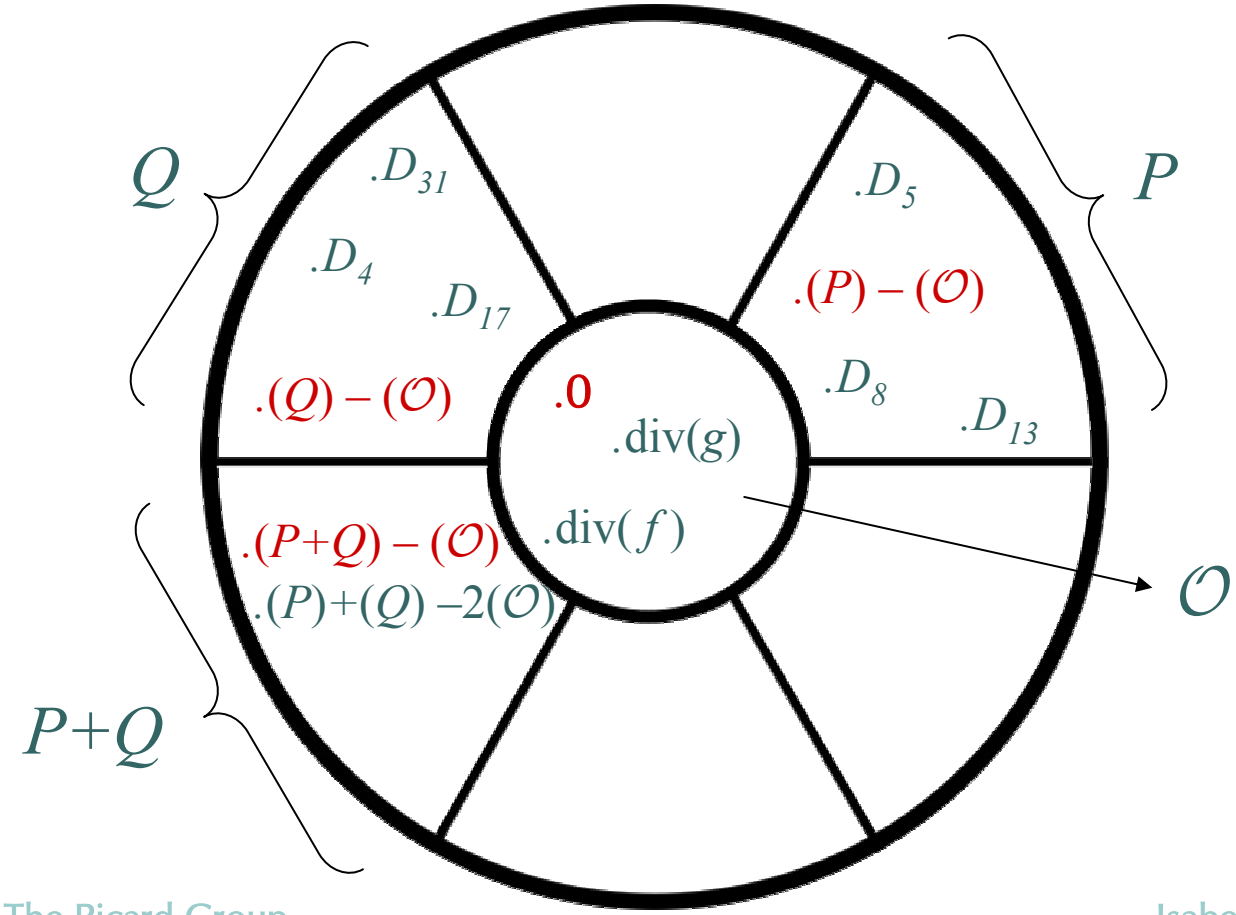
$$D_1 \sim D_2$$

if and only if

$$\deg(D_1) = \deg(D_2) \text{ and } \sum_{P \in E} n_P P = \sum_{P \in E} m_P P.$$

In other words...

For an elliptic curve E, the picture looks like this:



The Jacobian of an Elliptic Curve

Theorem. Let E be an elliptic curve defined over a field K. Then the map

$$E \to \mathrm{Pic}^0(E)$$

$$P \mapsto [(P) - (\mathcal{O})]$$

is a group isomorphism with well-defined inverse

$$\mathrm{Pic}^0(E) \to E$$

$$\left[\sum_{P \in E} n_P (P)\right] \mapsto \sum_{P \in E} n_P P.$$

The Jacobian Variety

Theorem. Let C be a smooth algebraic curve of genus g defined over an algebraically closed field.

Then there exists an abelian variety $J(C)$ of dimension g which is isomorphic (as a group) to $\mathrm{Pic}^0(C)$.

Definition. The variety $J(C)$ is called the *Jacobian* of C.

We just saw that the Jacobian of an elliptic curve is itself!

What about the Jacobian of a hyperelliptic curve???

Hyperelliptic Curves

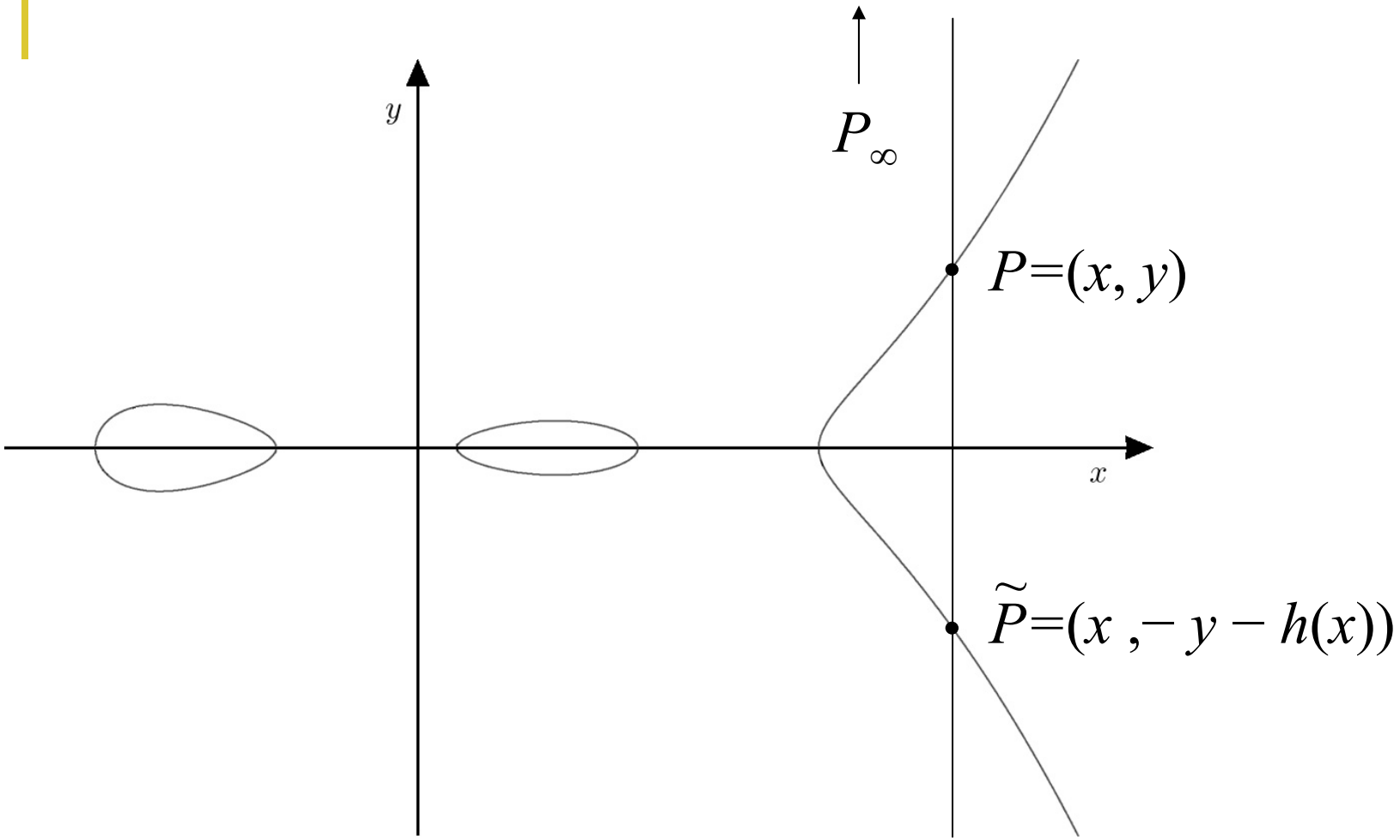
Definition. A *hyperelliptic curve* of genus g over a field K is a smooth algebraic curve C given by an equation of the form

$$y^2 + h(x)\, y = f(x),$$

where $h, f \in K[x]$, $\deg(f) = 2g + 1$, $\deg(h) \leq g$, and f is a monic polynomial.

To ensure that C is smooth, it suffices to verify that the partial derivatives $2y + h$ and $f' - h'y$ do not simultaneously vanish at any point of $C(\bar{K})$.

Hyperelliptic Curve



Is there a way to see the group law on the Jacobian here?

Constructing the Picard Group of a Hyperelliptic Curve

✓ 1. Start with your favorite hyperelliptic curve C.

✓ 2. Consider its divisors of degree zero $\mathrm{Div}^0(C)$.

✓ 3. Linear equivalence will yield $\mathrm{Pic}^0(C)$.

4. Find a canonical representative for each class.

Reduced Divisors

Theorem. Let C be a hyperelliptic curve of genus g over K. Then each divisor class can be *uniquely* represented by a divisor of the form

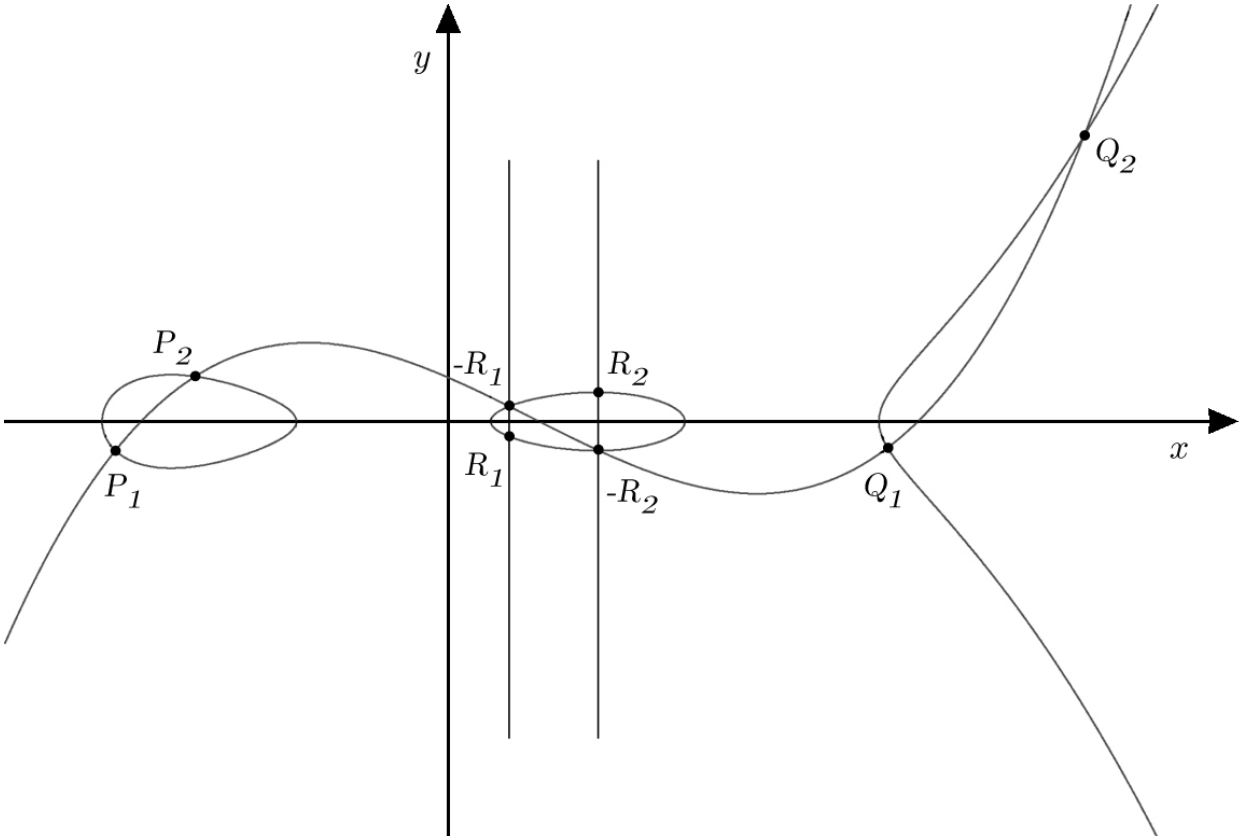
$$D = \sum_{i=1}^{r} (P_i) - r(P_\infty),$$

where $r \leq g$, each $P_i \neq P_\infty$, and $P_i \neq \widetilde{P}_j$ as soon as $i \neq j$.

Note. We do not require the P_i's to be distinct.

Definition. Such a divisor D is said to be *reduced*.

Group Law on the Jacobian of a Hyperelliptic Curve of Genus 2



$$(P_1) + (P_2) - 2(\mathcal{O}) \quad + \quad (Q_1) + (Q_2) - 2(\mathcal{O}) \quad = \quad (R_1) + (R_2) - 2(\mathcal{O}).$$

Mumford Representation

Theorem. Let C be a hyperelliptic curve of genus g over K. Then each nontrivial divisor class over K can be represented by a *unique* pair of polynomials $u, v \in K[x]$ satisfying:

- u is monic
- $\deg(v) < \deg(u) \leq g$
- $u \mid (v^2 + vh - f)$

Great News!

You are now ready for the talks of tomorrow morning!

✓ Pairing background	Tanja Lange
✓ Fast arithmetic on ECC and HECC	Peter Birkner
✓ Pairing implementation	Mike Scott

Good Luck!