Mathematical Background of Pairings

Tanja Lange

Department of Mathematics and Computer Science

Technische Universiteit Eindhoven

The Netherlands

tanja@hyperelliptic.org

03.05.2007

Overview

- Protocols
- Elliptic curves
  - Definition and group law
  - Divisor class group (explanation of group law, example hyperelliptic curves)
- Weil and Tate pairing on elliptic curves
- Supersingular and ordinary elliptic curves
- Distortion maps

Protocols

Diffie-Hellman Key exchange

Alice

1. secretly generates
   $a < |\langle P \rangle|$
2. computes $Q_1 = [a]P$
3. transmits Q_1
4. computes
   $[a]Q_2$

Bob

1. secretly generates
   $b < |\langle P \rangle|$
2. computes $Q_2 = [b]P$
3. transmits Q_2
4. computes
   $[b] \cdot Q_1$

$$[a]Q_2 = [ab]P = [b] \cdot Q_1$$

Common Key: the group element $k = [ab]P \in \langle P \rangle$
can be used in symmetric encryption.

Pairings

Let $(G_1, \oplus), (G_1', \oplus)$ and $(G, \cdot)$ be groups and let

$$e : G_1 \times G_1' \to G$$

be a map satisfying

- $e(P \oplus Q, R') = e(P, R')e(Q, R')$
- $e(P, R' \oplus S') = e(P, R')e(P, S')$
- The map is non-degenerate in the first argument, i.e. if $e(P, R') = 1$ for all $R' \in G_1'$ for some P then P is the identity in G_1

Then e is called a bilinear map or pairing.

In protocol papers often $G_1 = G_1'$.

Consequences

- Assume that $G_1 = G'_1$ and hence
$$e(P, P) \neq 1.$$
Then for all triples $(P_1, P_2, P_3) \in \langle P \rangle^3$ one can decide whether
$$\log_P(P_3) = \log_P(P_1)\log_P(P_2)$$
by comparing
$$e(P_1, P_2) \stackrel{?}{=} e(P, P_3).$$
Thus the Decision Diffie-Hellman Problem is easy.
- The DL system G_1 is at most as secure as the system G. Even if $G_1 \neq G'_1$ one can transfer the DLP in G_1 to a DLP in G, provided that one can find an element $P' \in G'_1$ such that the map $P \to e(P, P')$ is injective.

Positive Application of Pairings

Joux, ANTS 2000, one round tripartite key exchange

Let P, P' be generators of G_1 and G_1' respectively.
Users A, B and C compute joint secret from their secret contributions a, b, c as follows (A's perspective)

- Compute and send $[a]P, [a]P'$.
- Upon receipt of $[b]P$ and $[c]P'$ put $k = (e([b]P, [c]P'))^a$

The resulting element k is the same for each participant as

$$k = (e([b]P, [c]P'))^a = (e(P, P'))^{abc} = (e([a]P, [c]P'))^b = (e([a]P, [b]P'))^c.$$

- Obvious saving in first step if $G_1 = G_1'$.
- Only one user needs to do both computations.

Arithmetic on elliptic curves

Elliptic curve

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)},\ \ h, f \in \mathbb{F}_q[x].$$

Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \}$

Often $q = 2^r$ or $q = p$, prime. Isomorphic transformations lead to

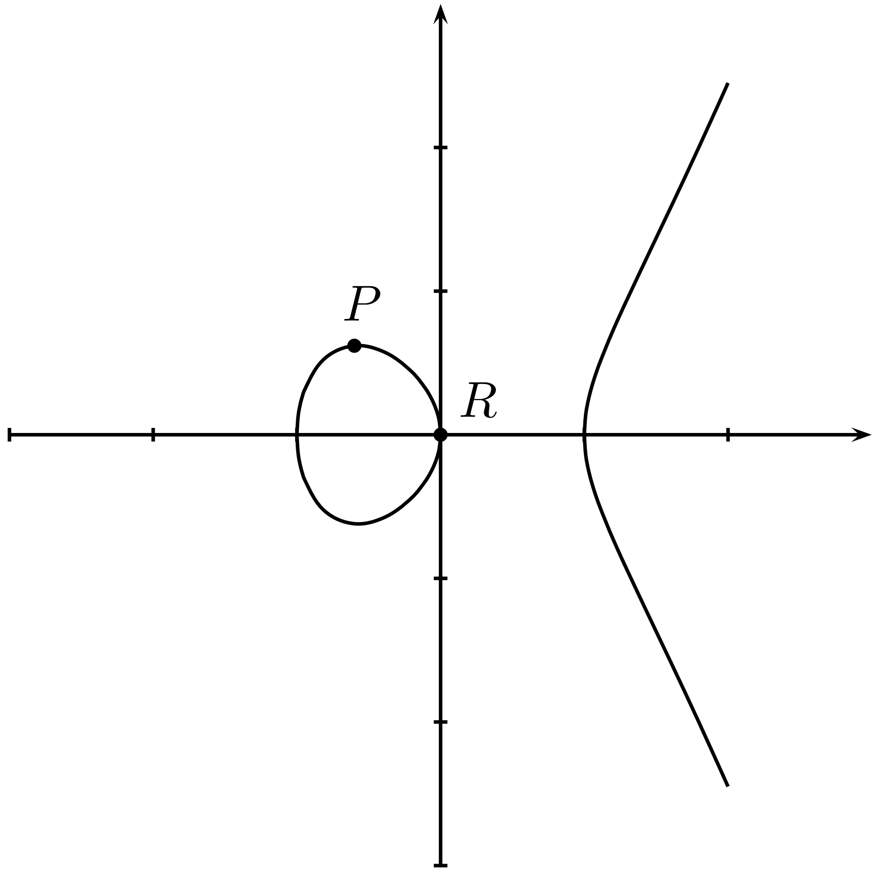
$y^2 = f(x)$ $\qquad$ q odd,

for

$$\begin{aligned} y^2 + xy &= x^3 + a_2 x^2 + a_6 \\ y^2 + y &= x^3 + a_4 x + a_6 \end{aligned} \qquad q = 2^r, \quad \begin{array}{l}\text{curve non-supersingular} \\ \text{curve supersingular}\end{array}$$

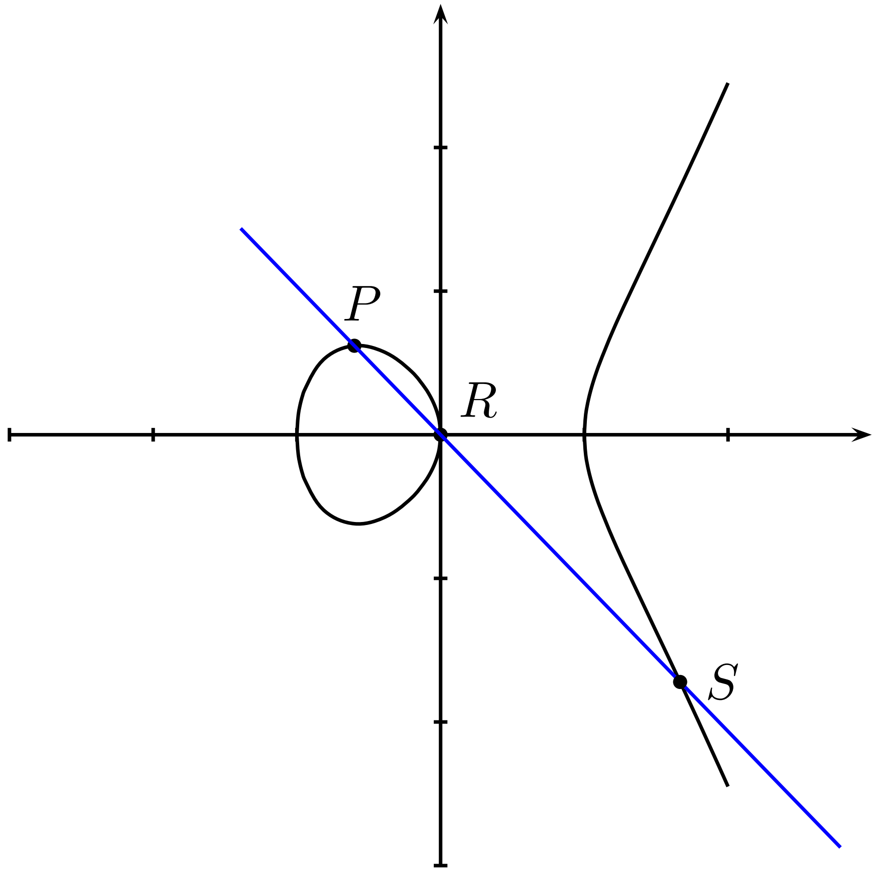
Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



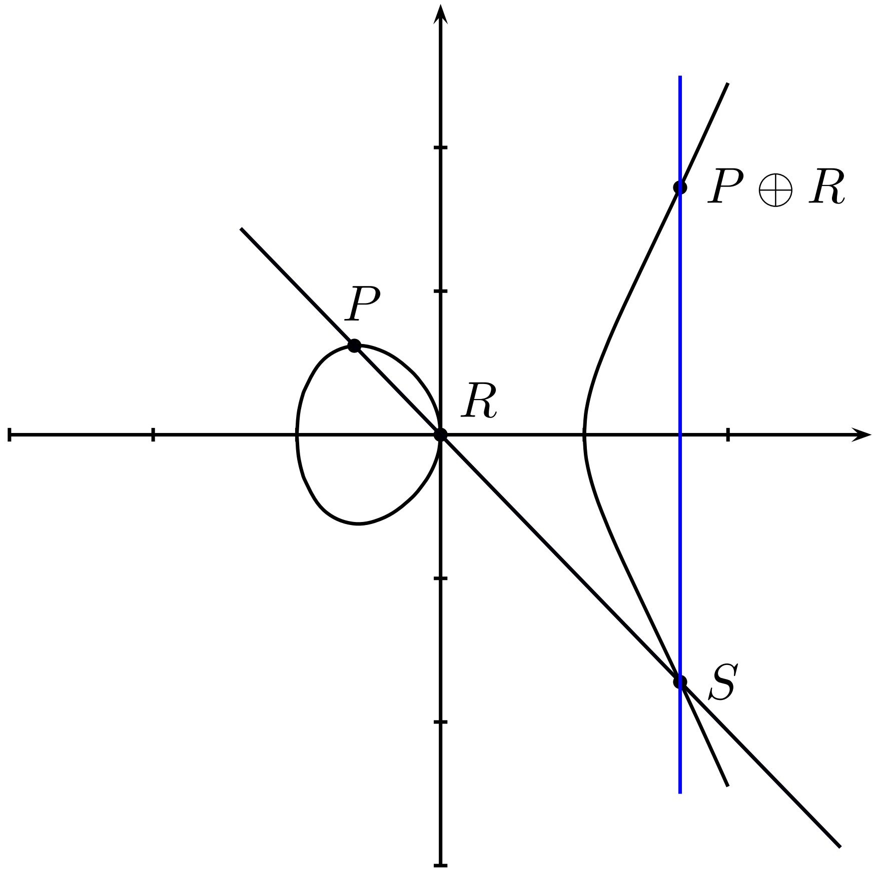
Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



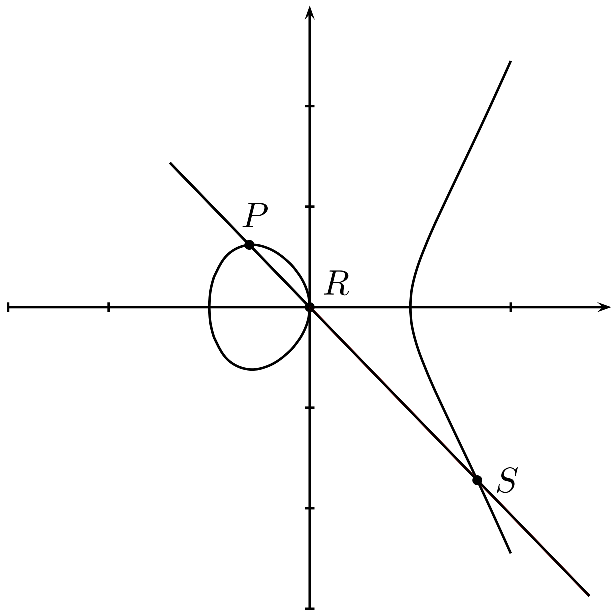
Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Line $y = \lambda x + \mu$ has slope

$$\lambda = \frac{y_R - y_P}{x_R - x_P}.$$

Equating gives

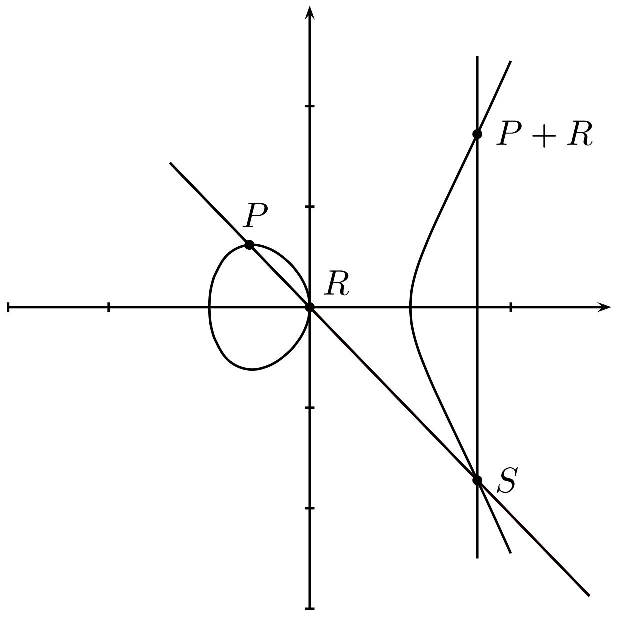
$(\lambda x + \mu)^2 = x^3 + a_4 x + a_6$.

This equation has 3 solutions, the x-coordinates of P, R and S, thus

$$\begin{aligned} (x - x_P)(x - x_R)(x - x_S) &= x^3 - \lambda^2 x^2 + (a_4 - 2\lambda\mu)x + a_6 - \mu^2 \\ x_S &= \lambda^2 - x_P - x_R \end{aligned}$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6, \ a_i \in \mathbb{F}_q$$



Point P is on line, thus

$y_P = \lambda x_P + \mu$, i.e.
$\mu = y_P - \lambda x_P$,

and

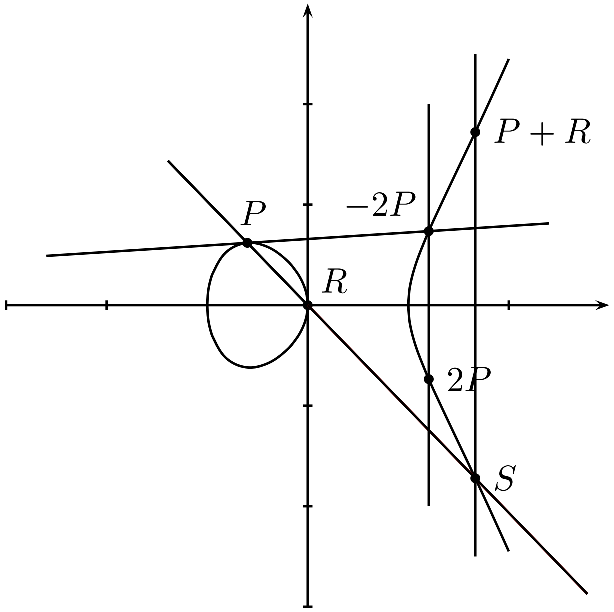
$$\begin{aligned} y_S &= \lambda x_S + \mu \\ &= \lambda x_S + y_P - \lambda x_P \\ &= \lambda(x_S - x_P) + y_P \end{aligned}$$

Point $P \oplus R$ has the same x-coordinate as S but negative y-coordinate:

$$x_{P\oplus R} = \lambda^2 - x_P - x_R, \quad y_{P\oplus R} = \lambda(x_P - x_{P\oplus R}) - y_P$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



In general, for $(x_P, y_P) \neq (x_R, -y_R)$:

$$\begin{aligned}(x_P, y_P) \oplus (x_R, y_R) &= \\ &= (x_{P\oplus R}, y_{P\oplus R}) = \\ &= (\lambda^2 - x_P - x_R, \lambda(x_P - x_{P\oplus R}) - y_P),\end{aligned}$$

where

$$\lambda = \begin{cases} (y_R - y_P)/(x_R - x_P) & \text{if } x_P \neq x_R, \\ (3x_P^2 + a_4)/(2y_P) & \text{else.} \end{cases}$$

$\Rightarrow$ Addition and Doubling need
1 I, 2M, 1S and 1 I, 2M, 2S, respectively

Weierstraß equation

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)}\, y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)},\ \ h, f \in \mathbb{F}_q[x].$$

- Negative of $P = (x_P, y_P)$ is given by $-P = (x_P, -y_P - h(x_P))$.
- $(x_P, y_P) \oplus (x_R, y_R) = (x_3, y_3) =$ $= (\lambda^2 + a_1\lambda - a_2 - x_P - x_R, \lambda(x_P - x_3) - y_P - a_1x_3 - a_3)$, where

$$\lambda = \begin{cases} (y_R - y_P)/(x_R - x_P) & \text{if } x_P \neq x_R, \\ \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_Px_P + a_3} & \text{else.} \end{cases}$$

Number of points

In cryptography we usually consider elliptic curves over finite fields $\mathbb{F}_q$.

Then the number of points is also finite, a bound is given by Hasse's theorem:

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

with

$$|t| \leq 2\sqrt{q}.$$

t is called the trace of E.

Each point has finite order dividing $\#E(\mathbb{F}_q)$. Due to the Pohlig-Hellman attack we want to work in (sub-)groups of prime order ℓ.

Divisor class groups

(Arithmetic on hyperelliptic curves)

Example: Hyperelliptic Curves

Affine equation of hyperelliptic curve of genus g (with $\mathbb{F}_q$-rational Weierstraß-point at infinity)

$$C : y^2 + h(x)y = f(x)$$

$h(x), f(x) \in \mathbb{F}_q[x]$, f monic, $\deg f = 2g + 1, \deg h \leq g$
non singular, i. e. not both partial derivatives

$$(2y + h(x) \text{ and } h'(x)y - f'(x))$$

vanish in any in $(a, b) \in C/\overline{\mathbb{F}_q}$

Examples

Concerning the arithmetic properties one can consider elliptic curves as hyperelliptic curves, i. e.

$$y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6$$

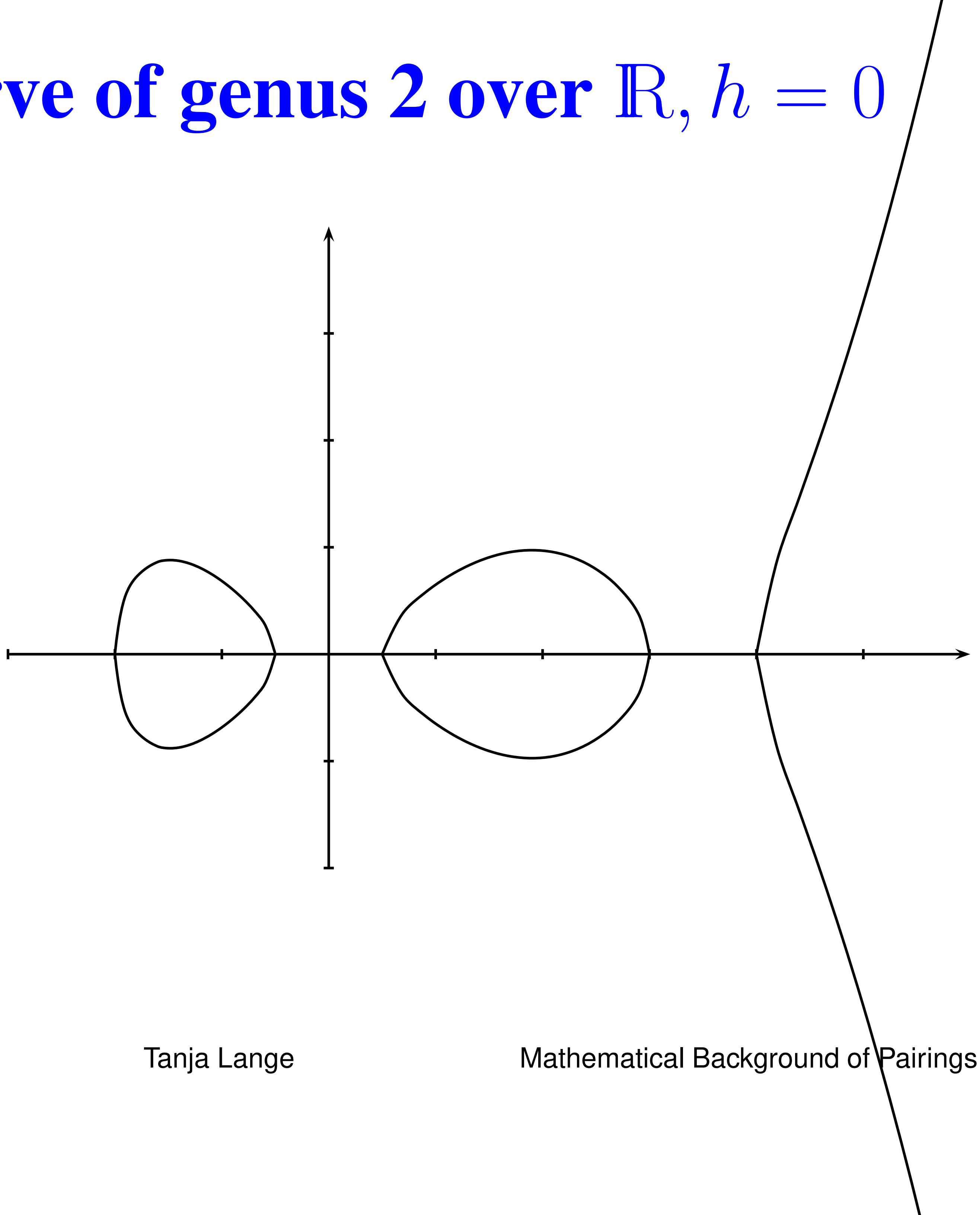
is considered as curve of genus one.

Curve of genus 2 over field of odd characteristic

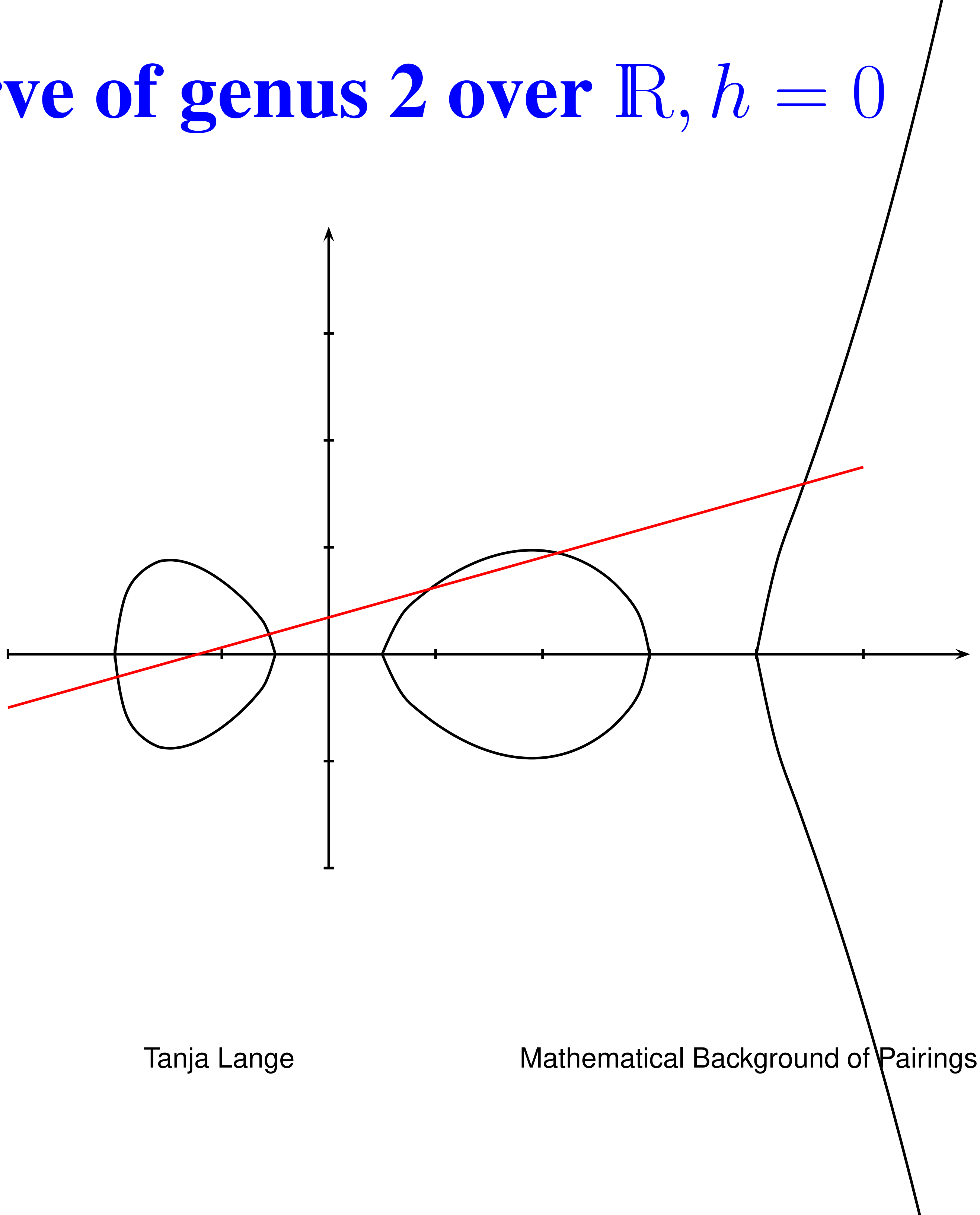
$$y^2 = x^5 + f_3 x^3 + f_2 x^2 + f_1 x + f_0,$$

provided $f(x)$ has no multiple roots.

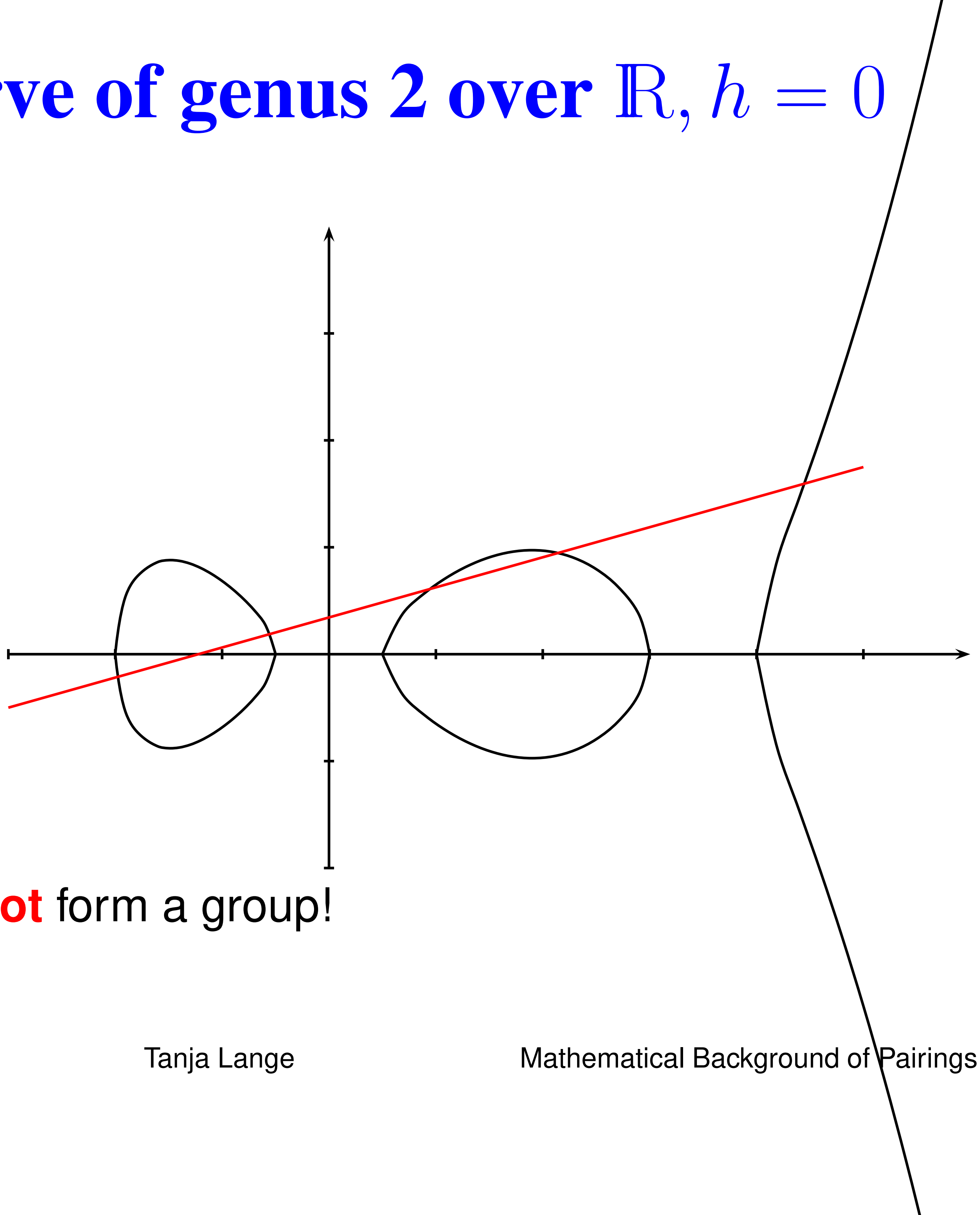
Curve of genus 2 over $\mathbb{R}, h = 0$



Curve of genus 2 over $\mathbb{R}, h = 0$



Curve of genus 2 over $\mathbb{R}, h = 0$



points do **not** form a group!

Group of Divisors

- Construct group from points on curve. Free abelian groups are in particular groups, and so associativity etc. follow immediately.
- Construction uses Divisors, i. e. finite sums of points (elements of the free abelian group),

$$\sum_{P \in C(\overline{\mathbb{F}_q})} n_P P,\ n_P \in \mathbb{Z}$$

  with $n_P = 0$ for almost all P.
- Addition works component-wise:

$$(P_1 + 2P_2 - P_3) + (P_1 + P_2 + P_4) = 2P_1 + 3P_2 - P_3 + P_4.$$

Divisors

- The degree of a divisor is

$$\deg(D) = \sum_{P \in C(\overline{\mathbb{F}_q})} n_P.$$

- The degree is a homomorphism, i.e.

$$\deg(D_1) + \deg(D_2) = \deg(D_1 + D_2),$$

  like
  $\deg(P_1 + 2P_2 - P_3) = 1 + 2 - 1 = 2, \deg(P_1 + P_2 + P_4) = 3,$
  $\deg(2P_1 + 3P_2 - P_3 + P_4) = 5$.

- Divisors of degree zero form a group Div_C^0 with component-wise addition. This is a subgroup of Div_C.

Principal divisors

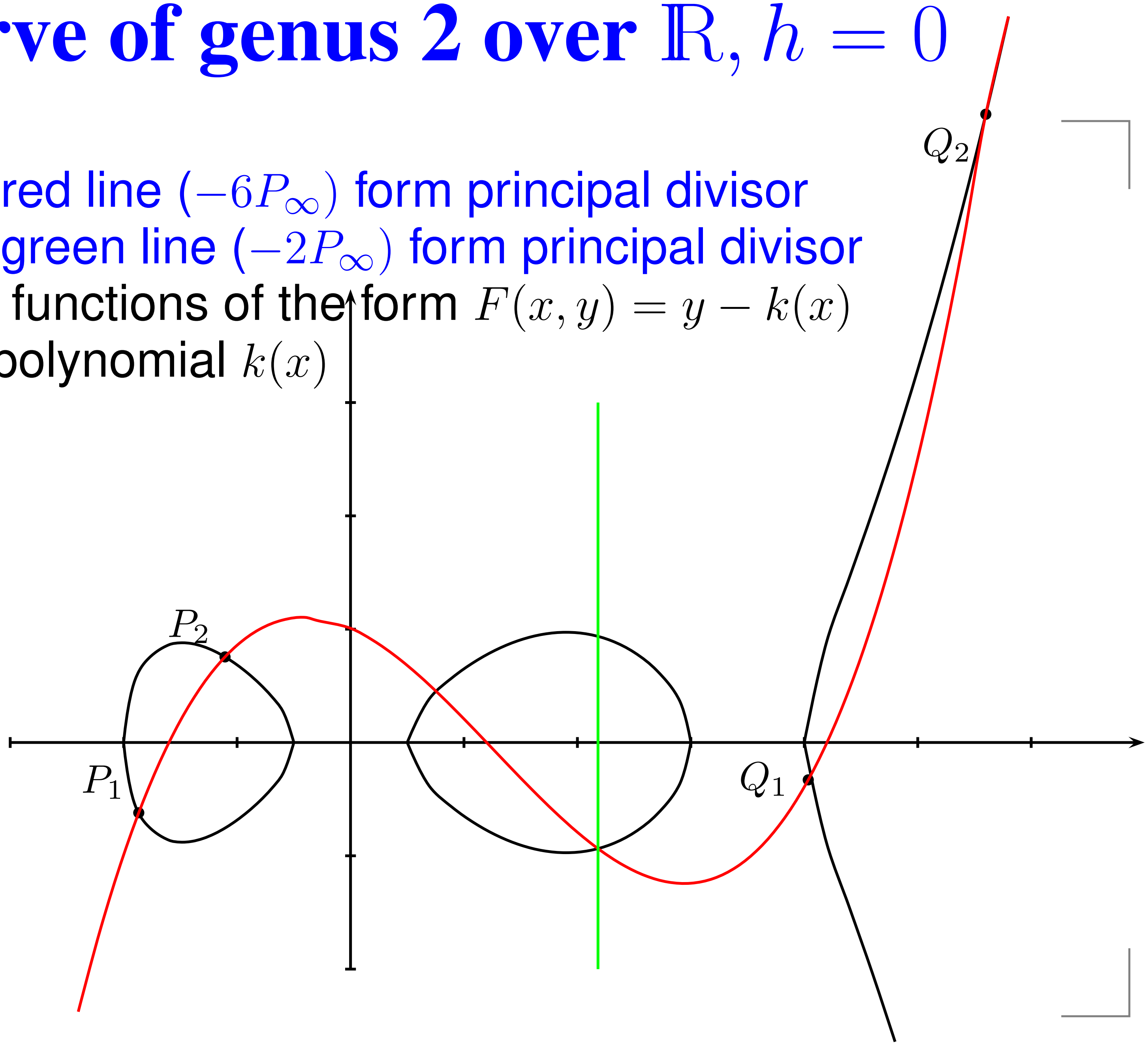
- For any function $F(x, y)$ the graph $F(x, y) = 0$ intersects curve in some points of $C(\overline{\mathbb{F}_q})$.
- Let v_P be normalized valuation $P \in C(\overline{\mathbb{F}_q})$, thus $v_P(F) = n \geq 0$ iff F has intersection of multiplicity n with curve at P (simple intersection has $n = 1$ while tangent has multiplicity $n \geq 2$).
- Negative values for multiplicity of poles.
- Associate divisor

$$\operatorname{div}(F) = \sum_{P \in C(\overline{\mathbb{F}_q})} v_P(F) P$$

to function $F \in \mathbb{F}_q(C)$.
- Such divisors are called principal divisors Princ_C. One can show that they have degree zero.

Curve of genus 2 over $\mathbb{R}$, $h = 0$

points on red line $(-6P_\infty)$ form principal divisor
points on green line $(-2P_\infty)$ form principal divisor
Here only functions of the form $F(x,y) = y - k(x)$
for some polynomial $k(x)$



Divisor class group

Consider the factor group of the group of divisors of degree zero Div_C^0 modulo the principal divisors. This way one constructs the divisor class group of degree zero.

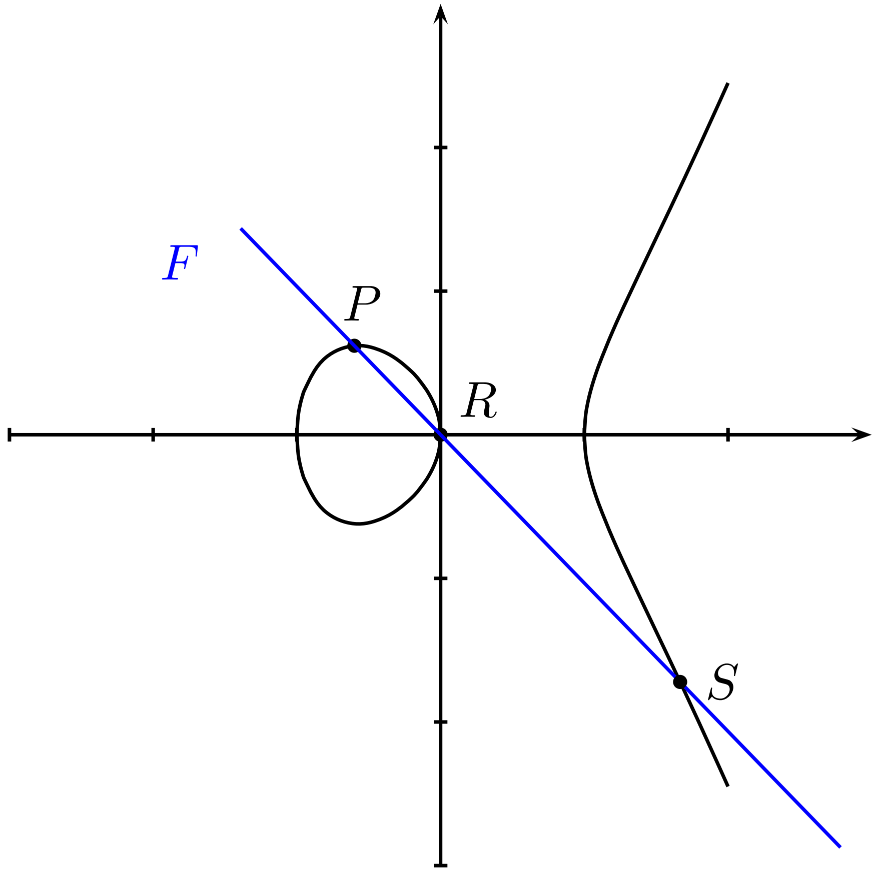
$$\mathrm{Pic}_C^0 = \mathrm{Div}_C^0/\mathrm{Princ}_C.$$

Meaning will become clear soon. First example ECC.

So far working over algebraic closure.
First definition: The $\mathbb{F}_q$-rational group elements $\mathrm{Pic}_C^0(\mathbb{F}_q)$ are those which remain fixed under applying the Frobenius endomorphisms, i.e. computing q-th powers of all coordinates. Note that not each point needs to remain fixed for that (sum can be rearranged).

Example: $E(\mathbb{R}), h = 0$

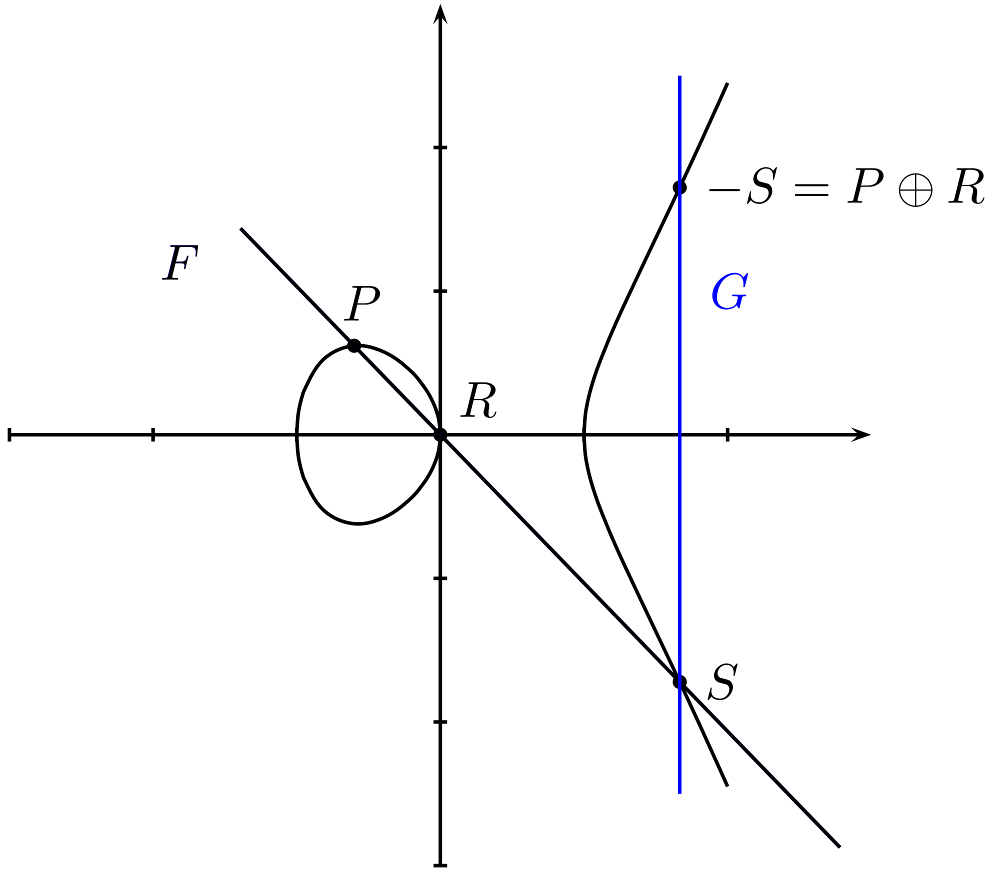
$y^2 = x^3 - x$



$\mathrm{div}(F(x,y)) = P + S + R - 3P_\infty$

Example: $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



$\mathrm{div}(F(x,y)) = P + S + R - 3P_\infty$ $\quad$ $\mathrm{div}(G(x,y)) = S + (-S) - 2P_\infty$

Representation of group elements

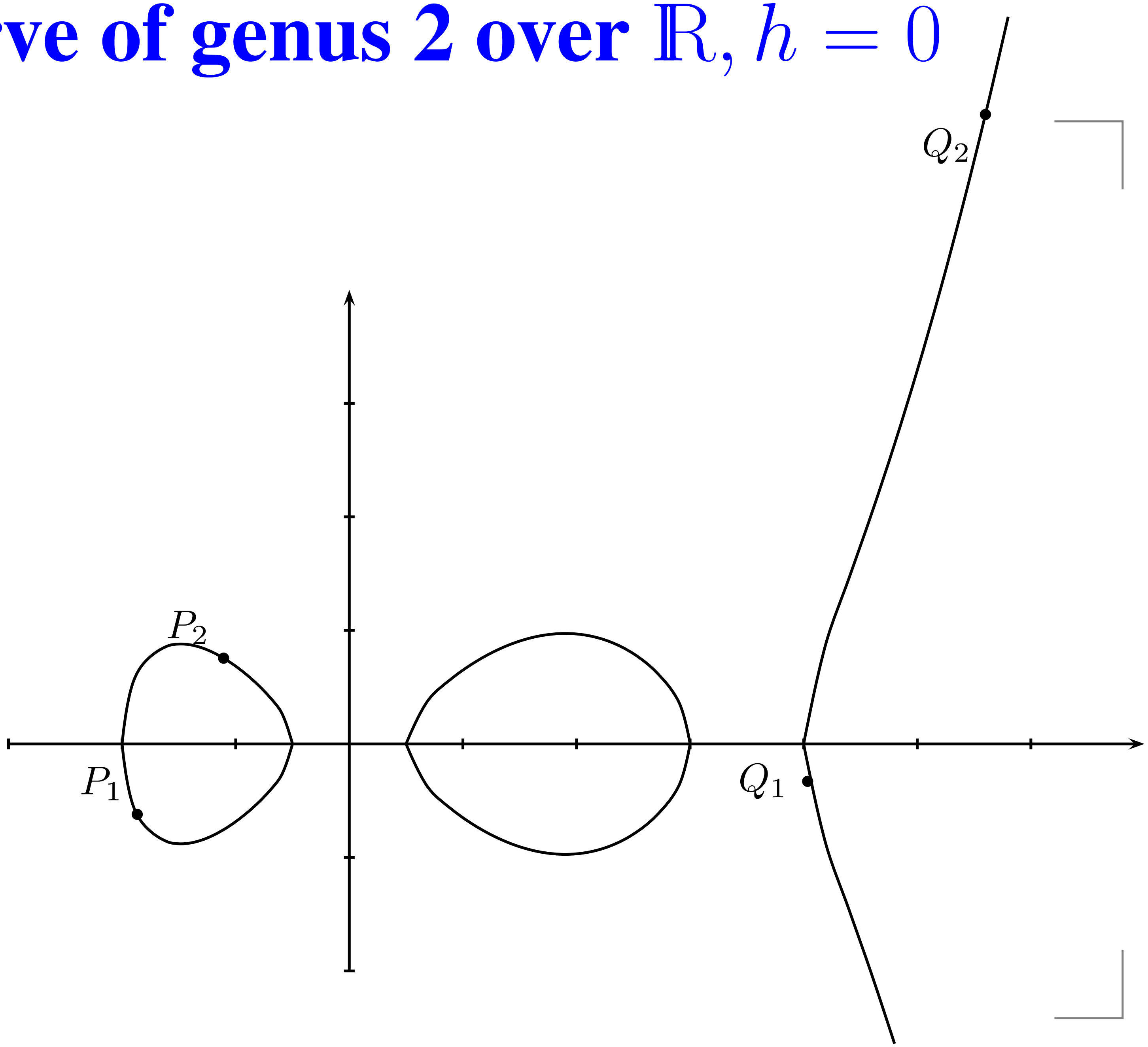
General:
Riemann-Roch allows to find a unique reduced representation by means of a divisor of degree zero with $m \leq g$

$$\bar{D} = \sum_{\substack{i=1 \\ P_i \in C(\overline{\mathbb{F}_q}) \setminus \{P_\infty\}}}^{m} P_i - mP_\infty$$

and $P_i \neq -P_j$ for $i \neq j$.

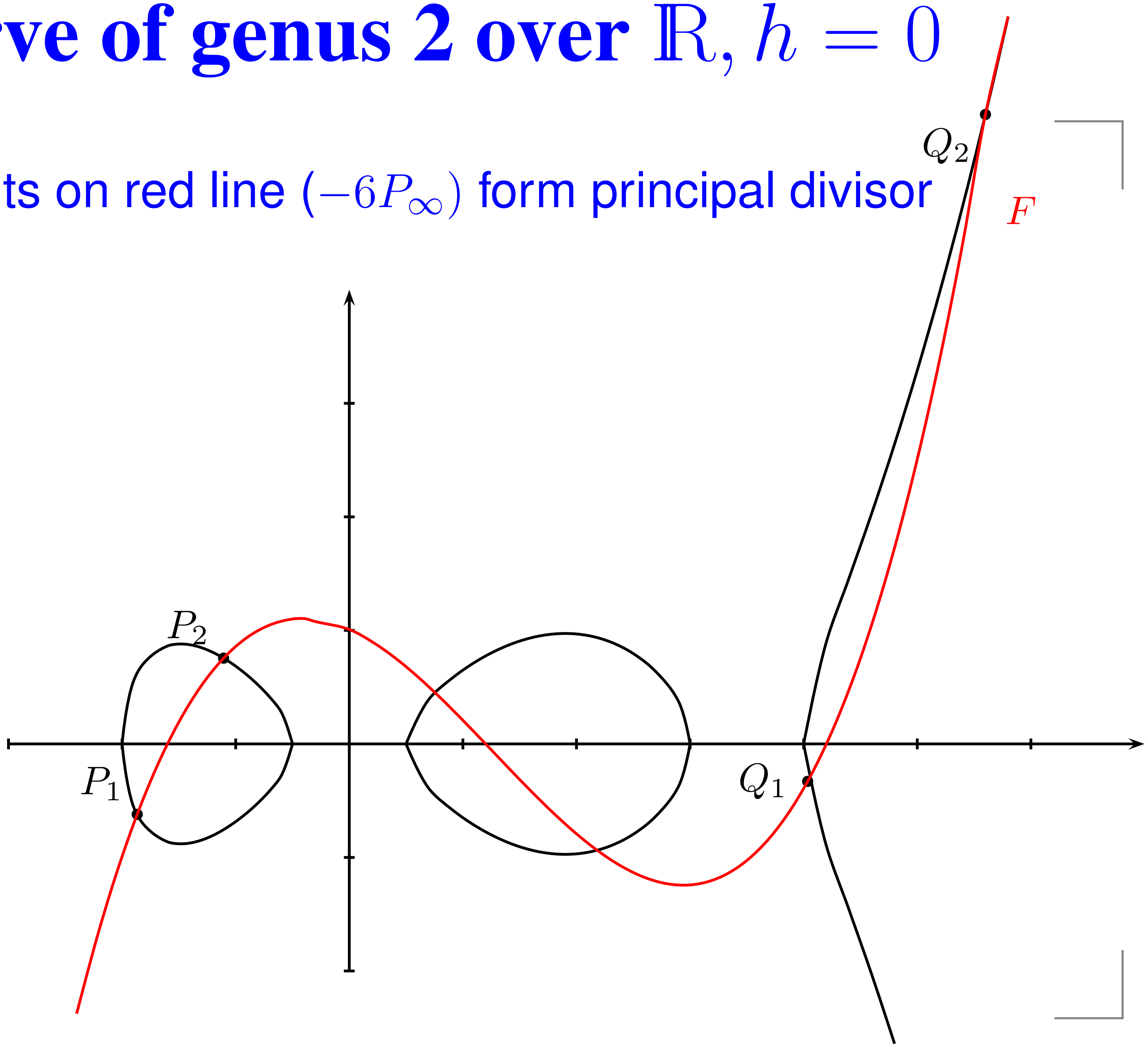
If $\bar{D}$ is defined over $\mathbb{F}_q$, the extension degree of the field of definition of the P_i is bounded, e. g. at most 2 for $g = 2$.

Curve of genus 2 over $\mathbb{R}, h = 0$



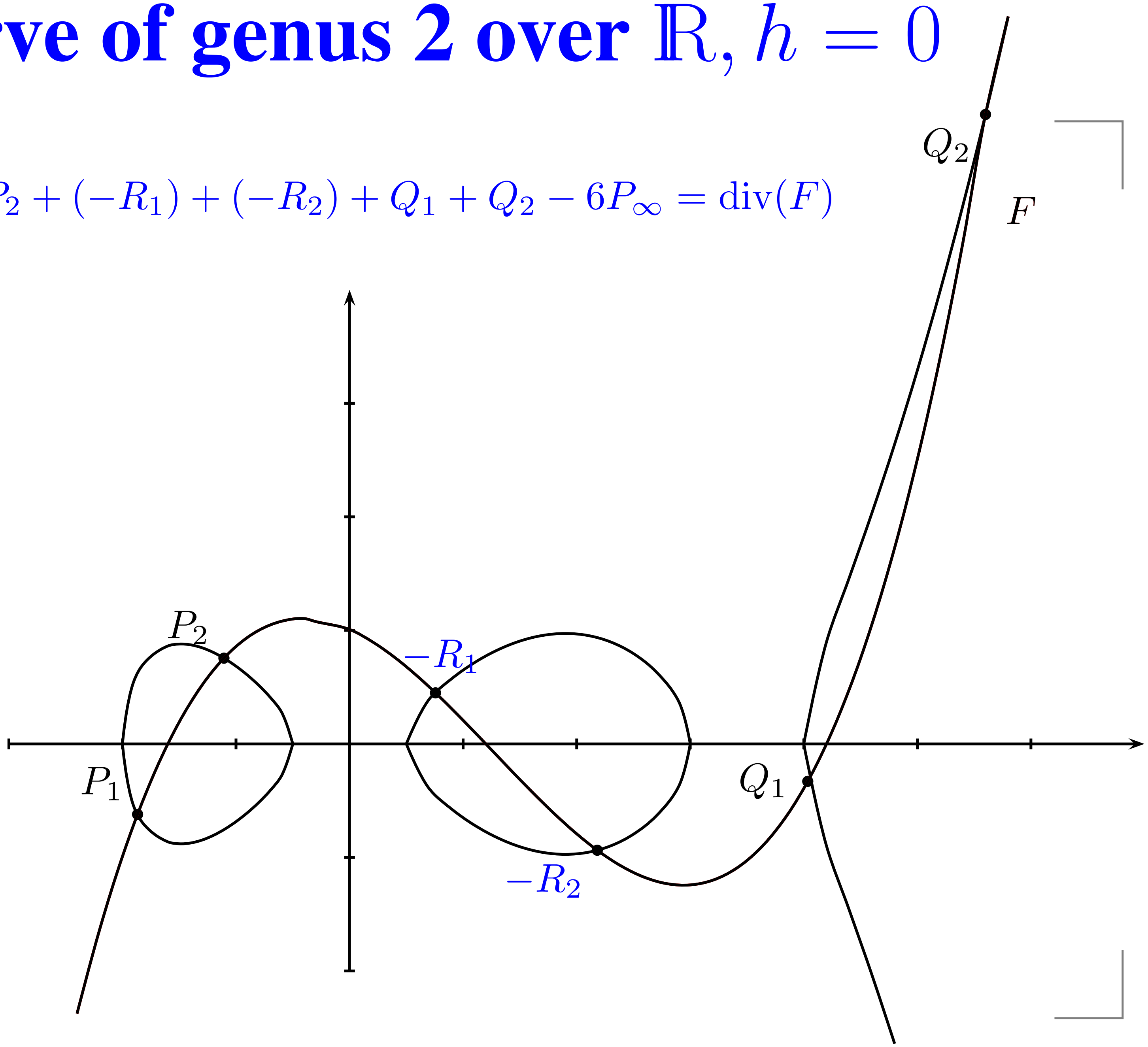
Curve of genus 2 over $\mathbb{R}$, $h = 0$

points on red line $(-6P_\infty)$ form principal divisor



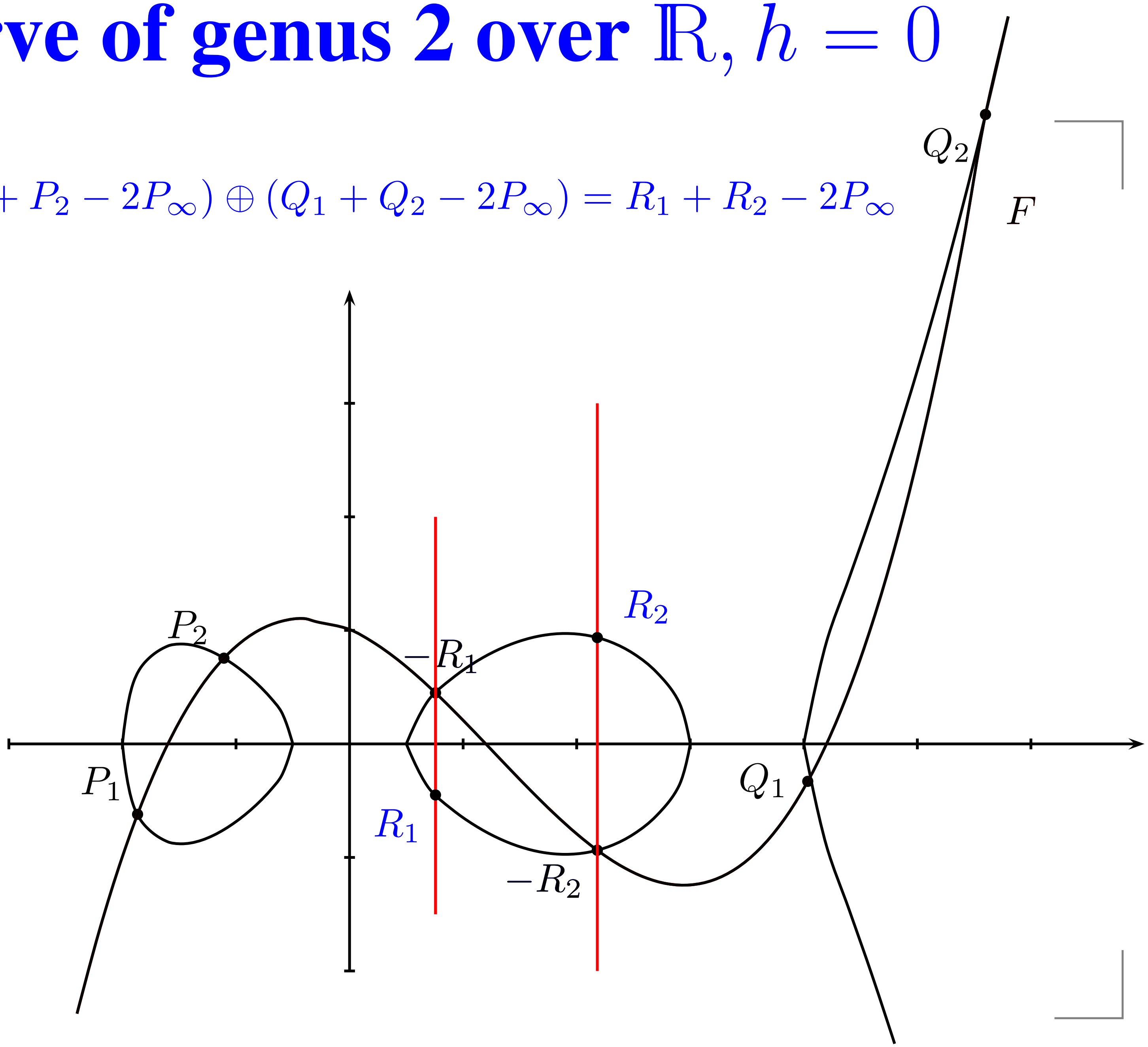
Curve of genus 2 over $\mathbb{R}$, $h = 0$

$$P_1 + P_2 + (-R_1) + (-R_2) + Q_1 + Q_2 - 6P_\infty = \mathrm{div}(F)$$



Curve of genus 2 over $\mathbb{R}$, $h = 0$

$$(P_1 + P_2 - 2P_\infty) \oplus (Q_1 + Q_2 - 2P_\infty) = R_1 + R_2 - 2P_\infty$$



Representation – elliptic curves

In the introduction we computed explicitly that there is always a third point on a non-vertical line.

By reduction modulo principal divisors (lines) one can thus reduce any divisor to just $P - P_\infty$ or the neutral element.

The isomorphism

$$\mathrm{Pic}^0_E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k}), \qquad \begin{array}{rcl} P - P_\infty & \mapsto & P \\ 0 & \mapsto & P_\infty \end{array}$$

shows that the above construction gives a group on the points of E together with the point at infinity.

Pairings

Prerequisites I

We want to define pairings

$$G_1 \times G_2 \to G_T$$

preserving the group structure.

- Tate and the Weil pairing both use abelian varieties as the first argument. Assume that $\ell \big| |\mathrm{Pic}_C^0(\mathbb{F}_q)|$ and $\ell^2 \not| \ |\mathrm{Pic}_C^0(\mathbb{F}_q)|$.
- Let ℓ be a prime, let C be a (hyper)elliptic curve over $\mathbb{F}_q$.
- G_1 is the group of $\mathbb{F}_q$-rational ℓ-torsion points of Pic_C^0,
- i.e. $G_1 = E[\ell](\mathbb{F}_q)$, $\mathbb{F}_q$-rational points on elliptic curve $C = E$ of order ℓ
- or $G_1 = \mathrm{Pic}_C^0[\ell](\mathbb{F}_q)$, $\mathbb{F}_q$-rational divisor classes of order ℓ.

Prerequisites II

- The pairings we use map to the multiplicative group of a finite extension field $\mathbb{F}_{q^k}$.
- G_T has order ℓ, so by Lagrange ℓ must divide the group order of $\mathbb{F}^*_{q^k}$, this happens if $\ell \mid q^k - 1$.
- The embedding degree k is defined to be the minimal extension degree of $\mathbb{F}_q$ so that the ℓ-th roots of unity are in $\mathbb{F}^*_{q^k}$, i.e.

  $$k \text{ minimal with } \ell \mid q^k - 1.$$

- Attention: if q is not prime then the group of ℓ-th roots of unity can be in a a smaller extension of the prime field!
- For $k > 1$ Tate-Lichtenbaum pairing is degenerate on linear dependent points, i.e. $T_\ell(P, P) = 1$.

Tate-Lichtenbaum pairing I

- We now use the whole machinery of divisors and divisor classes in the “easy” case of elliptic curves.
- Denote by $E(\mathbb{F}_{q^k})[\ell]$ the points on E of order ℓ defined over $\mathbb{F}_{q^k}$.
- Using the embedding of E into Pic_E^0, i.e.

$$P \mapsto P - P_\infty$$

we have:

$$P \in E(\mathbb{F}_{q^k})[\ell] \Rightarrow \exists F_P \text{ such that } \ell(P - P_\infty) \sim \mathrm{div}(F_P),$$

i.e. $\ell(P - P_\infty)$ is a principal divisor.

Tate-Lichtenbaum pairing II

- Given $Q \in E(\mathbb{F}_{q^k})$, find $S \in E(\mathbb{F}_{q^k})$ so that $Q \oplus S, S \notin \{\pm P, P_\infty\}$. (A random choice of S will do.)
- Note that $Q \oplus S - S \sim Q - P_\infty$.
- Tate-Lichtenbaum pairing

$$T_\ell(P,Q) = F_P(Q \oplus S - S) = \frac{F_P(Q \oplus S)}{F_P(S)}.$$

- This map is actually bilinear – easy to see for second argument; slightly harder for first.
- The value is independent of the choices of F_P and S – up to ℓ-th powers.

Tate-Lichtenbaum pairing III

This T_ℓ defines a bilinear and non-degenerate map

$$T_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*\ell}$$

as ℓ-folds are in the kernel of T_ℓ.
To achieve unique value in $\mathbb{F}_{q^k}$ rather than class do final exponentiation

$$\tilde{T}_\ell = T_\ell(P,Q)^{(q^k-1)/\ell}.$$

Often

$$T_\ell : E(\mathbb{F}_{q})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*\ell}.$$

The function F_P is built iteratively and evaluated in each round. This is known as Miller's algorithm.

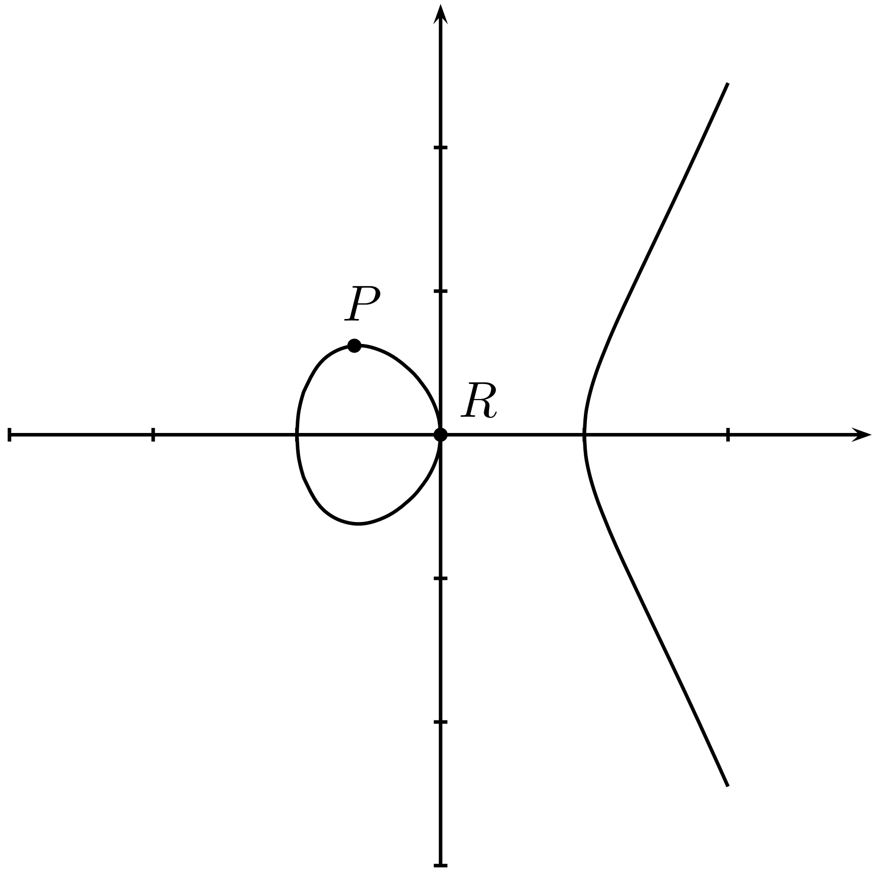
Miller's algorithm

In: $\ell = \sum_{i=0}^{n-1} \ell_i 2^i$, $P, Q \oplus S, S$
Out: $T_\ell(P, Q)$

1. $T \leftarrow P$, $F \leftarrow 1$
2. for $i = n-2$ downto 0 do
   (a) Calculate lines l and v in doubling
   $T \leftarrow [2]T$
   $F \leftarrow F^2 \cdot l(Q \oplus S)v(S)/(l(S)v(Q \oplus S))$
   (b) if $\ell_i = 1$ then
   Calculate lines l and v in addition $T \oplus P$
   $T \leftarrow T \oplus P$
   $F \leftarrow F \cdot l(Q \oplus S)v(S)/(l(S)v(Q \oplus S))$
3. return F

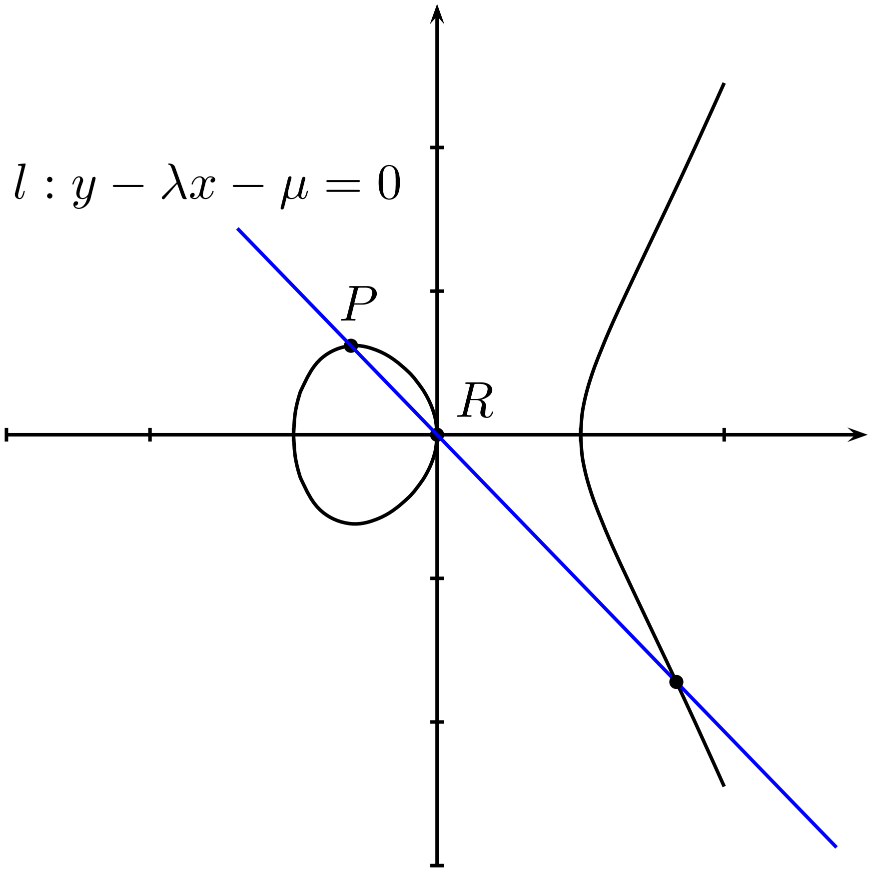
Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$

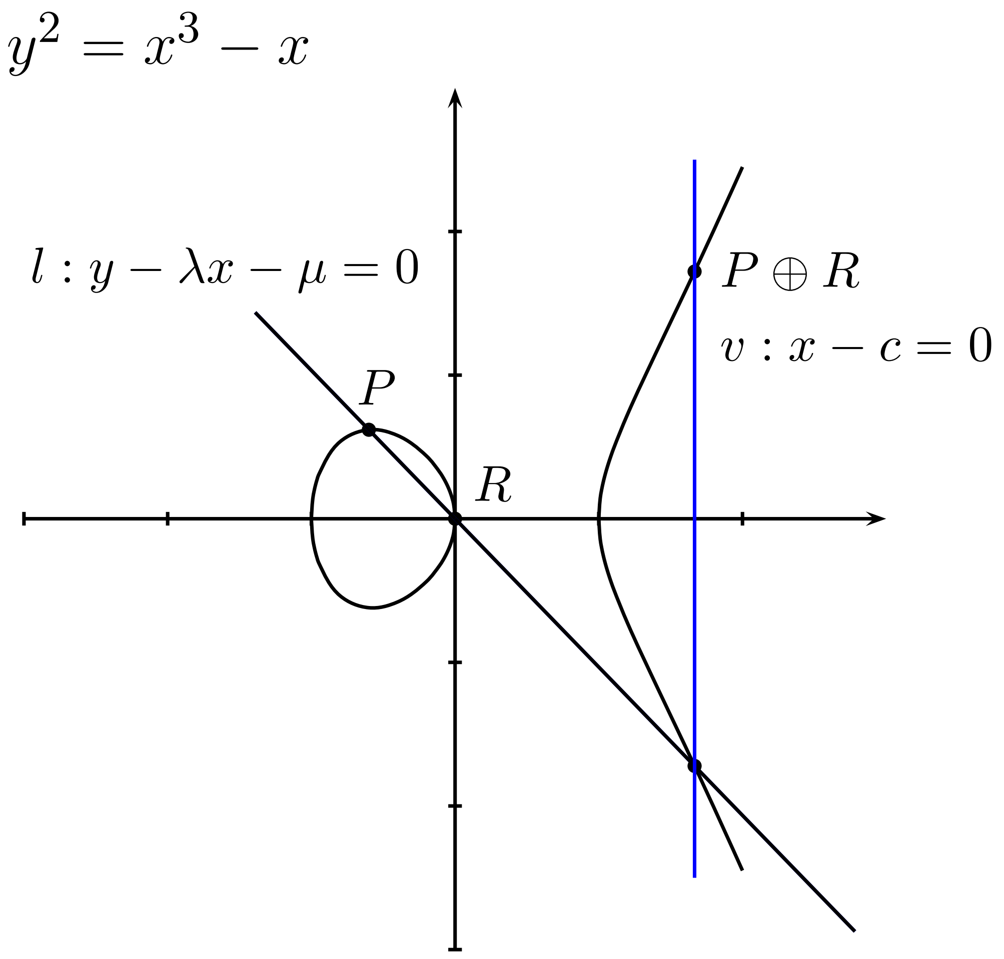


Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



Group Law in $E(\mathbb{R}), h = 0$



Weil pairing

For an elliptic curve E define

$$W_\ell : E(\overline{\mathbb{F}}_q)[\ell] \times E(\overline{\mathbb{F}}_q)[\ell] \rightarrow \mu_\ell$$
$$(P,Q) \mapsto \frac{F_P(D_Q)}{F_Q(D_P)},$$

where μ_ℓ is the multiplicative groups of the ℓ-th roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ and D_P and D_Q are divisors isomorphic to $P - P_\infty$ or $Q - P_\infty$, respectively. Obviously, $W_\ell(P,P) = 1$.

Weil pairings can be seen as two-fold application of the Tate-Lichtenbaum pairing, note $Q \in E(\mathbb{F}_{q^k})$.

Needs full group of order ℓ in $E(\mathbb{F}_{q^k})$, if $k = 1$ then the Weil pairing is trivial & one needs to use larger field.

Supersingular and ordinary

Definition

Let E be an elliptic curve defined over $\mathbb{F}_q, q = p^r$.
E is supersingular if

- $E[p^s](\overline{\mathbb{F}}_q) = \{P_\infty\}$.
- $|E(\mathbb{F}_q)| = q - t + 1$ with $t \equiv 0 \bmod p$.
- End_E is order in quaternion algebra.

Otherwise it is ordinary and one has $E[p^s](\overline{\mathbb{F}}_q) \cong \mathbb{Z}/p^s\mathbb{Z}$.

These statements hold for all s if they hold for one.
End_E order in quaternion algebra means that there are maps which are linearly independent of the Frobenius endomorphism. They are called distortion maps.

Example

Consider

$$y^2 + y = x^3 + a_4 x + a_6 \text{ over } \mathbb{F}_{2^r},$$

so $q = 2^r$.

Negative of $P = (a, b)$ is $-P = (a, b + 1)$,
$\Rightarrow$ no affine point with $P = -P$ since $b \neq b + 1$,
$\Rightarrow$ even number of affine points, one point P_∞,

$\Rightarrow |E(\mathbb{F}_q)| = q - t + 1 = 2^r - t + 1$ is odd, so t is even.

This curve is supersingular (using the second criterion).

Distortion map I

For supersingular curves it is possible to find maps $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$ that map to a linearly independent subgroup, i.e.

$$T'_\ell(P,P) \neq 1 \text{ for } T'_\ell(P,P) = T_\ell(P,\phi(P)).$$

(This needs that there are independent endomorphisms, so no chance for ordinary curves).
Examples:

- $y^2 = x^3 + a_4 x$, for $p \equiv 3 \pmod 4$.
  Distortion map $(x,y) \mapsto (-x, iy)$ with $i^2 = -1$
- $y^2 = x^3 + a_6$, for $p \equiv 2 \pmod 3$.
  Distortion map $(x,y) \mapsto (jx, y)$ with $j^3 = 1, j \neq 1$,

In both cases, $\#E(\mathbb{F}_p) = p+1$, $k = 2$.

Distortion maps II

- Over $\mathbb{F}_{2^d}$ consider
$$y^2 + y = x^3 + x + a_6, \text{ with } a_6 = 0 \text{ or } 1$$
and distortion map
$$(x, y) \mapsto (x+s^2, y+sx+t),\ s, t \in \mathbb{F}_{2^{4d}},\ s^4+s = 0,\ t^2+t+s^6+s^2 = 0.$$
$$\#E(\mathbb{F}_{2^d}) = 2^d + 1 \pm 2^{(d+1)/2},\ k = 4.$$
- Over $\mathbb{F}_{3^d}$ consider
$$y^2 = x^3 + x + a_6, \quad \text{with} \quad a_6 = \pm 1$$
and distortion map
$$(x, y) \mapsto (-x + s, iy) \ \text{ with } \ s^3 + 2s + 2a_6 = 0 \ \text{ and } \ i^2 = -1.$$
$$\#E(\mathbb{F}_{3^d}) = 3^d + 1 \pm 3^{(d+1)/2},\ k = 6.$$

Outlook and literature

- Efficient implementation of pairings in Mike Scott's talk
- More applications and protocols involving pairings tomorrow in the talks by Kenny Paterson and Benoit Libert.
- Chapter 6. Background on Pairings of the Handbook of Elliptic and Hyperelliptic Curve Cryptography currently online as sample chapter at `http://www.hyperelliptic.org/HEHCC`
- Advances in Elliptic Curve Cryptography by I. F. Blake, G. Seroussi, and N. P. Smart (Eds.) has chapter on pairings by Steven D. Galbraith.
- Pairings for Cryptographers by S. D. Galbraith, K. G. Paterson, and N. P. Smart; ePrint Archive: Report 2006/165