Hyperelliptic Curves

Tanja Lange

Department of Mathematics

Technical University of Denmark

t.lange@mat.dtu.dk

15.08.2006

Overview

- Definition.
- Divisor class group.
- Elliptic curves (reminder).
- Pictorial description of group law.
- Mumford representation.
- Cantor's algorithm.

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. in no point $(a, b) \in C/\overline{\mathbb{F}_q}$ over the algebraic closure $\overline{\mathbb{F}_q}$ we have both partial derivatives vanishing, i.e.

$2b + h(a) = 0$ and $h'(a)b - f'(a) = 0$.

Otherwise (a, b) is called a singular point.

Try to mimic approach in elliptic curves, but first some examples.

Examples

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

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

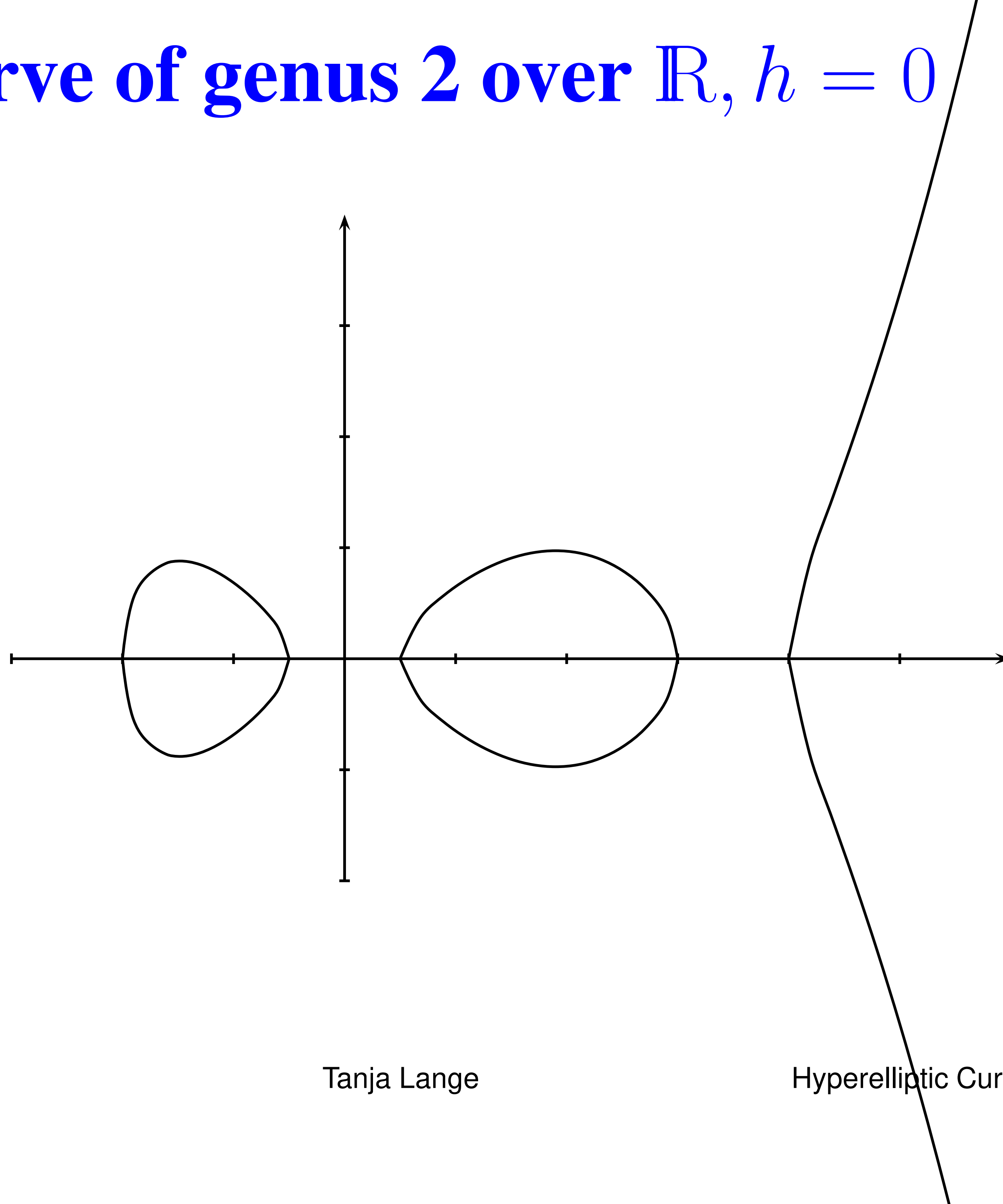
is considered as curve of genus one.

Curve of genus 2 over field of odd characteristic

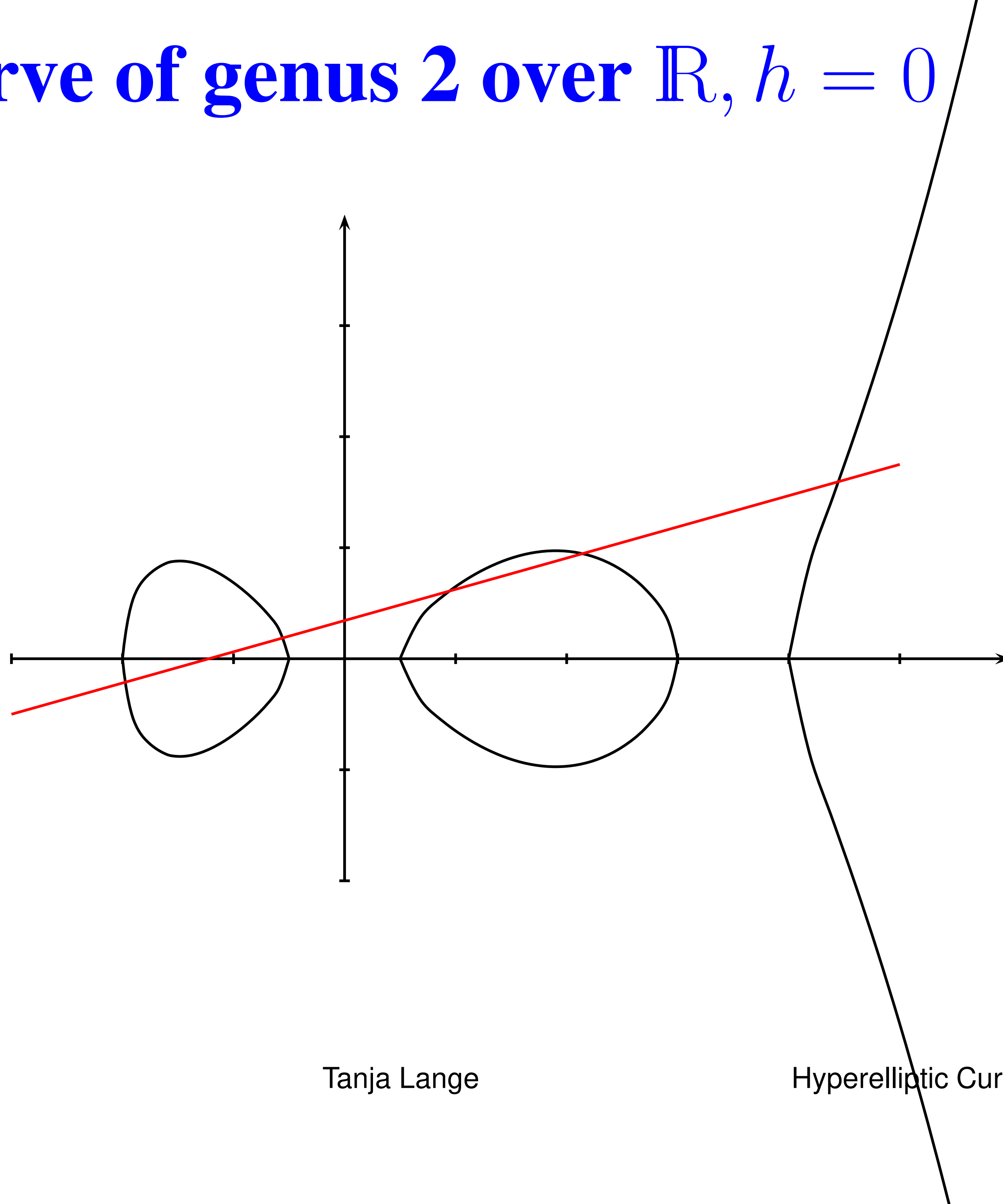
$$y^2 = x^5 + f_3 x^3 + f_2 x^2 + f_1 x + f_0,$$

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

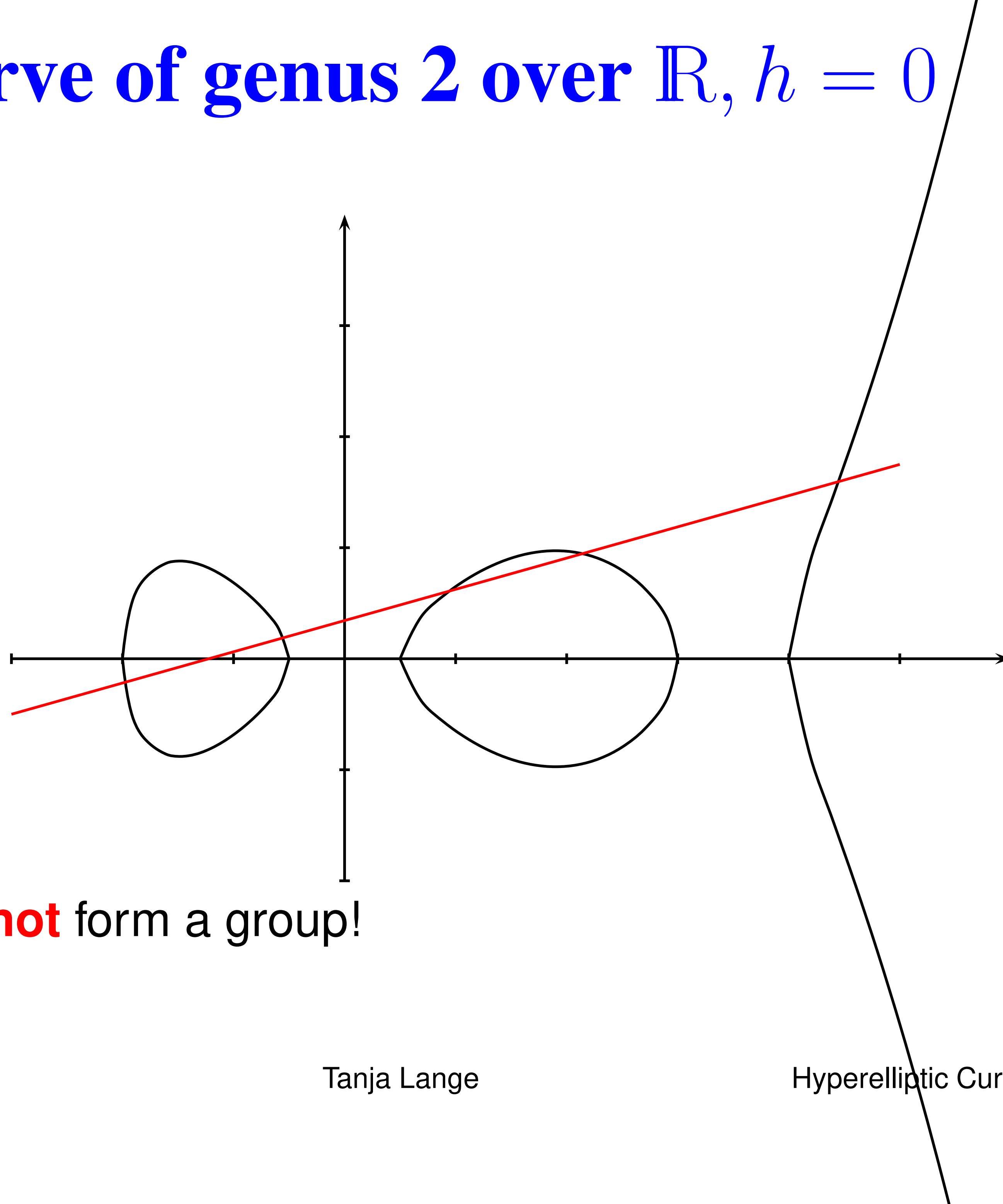
Curve of genus 2 over $\mathbb{R}, h = 0$



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

- Effective divisors are divisors

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

  for which each $n_P \geq 0$.

- The degree of a divisor is

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

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

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

Principal divisors

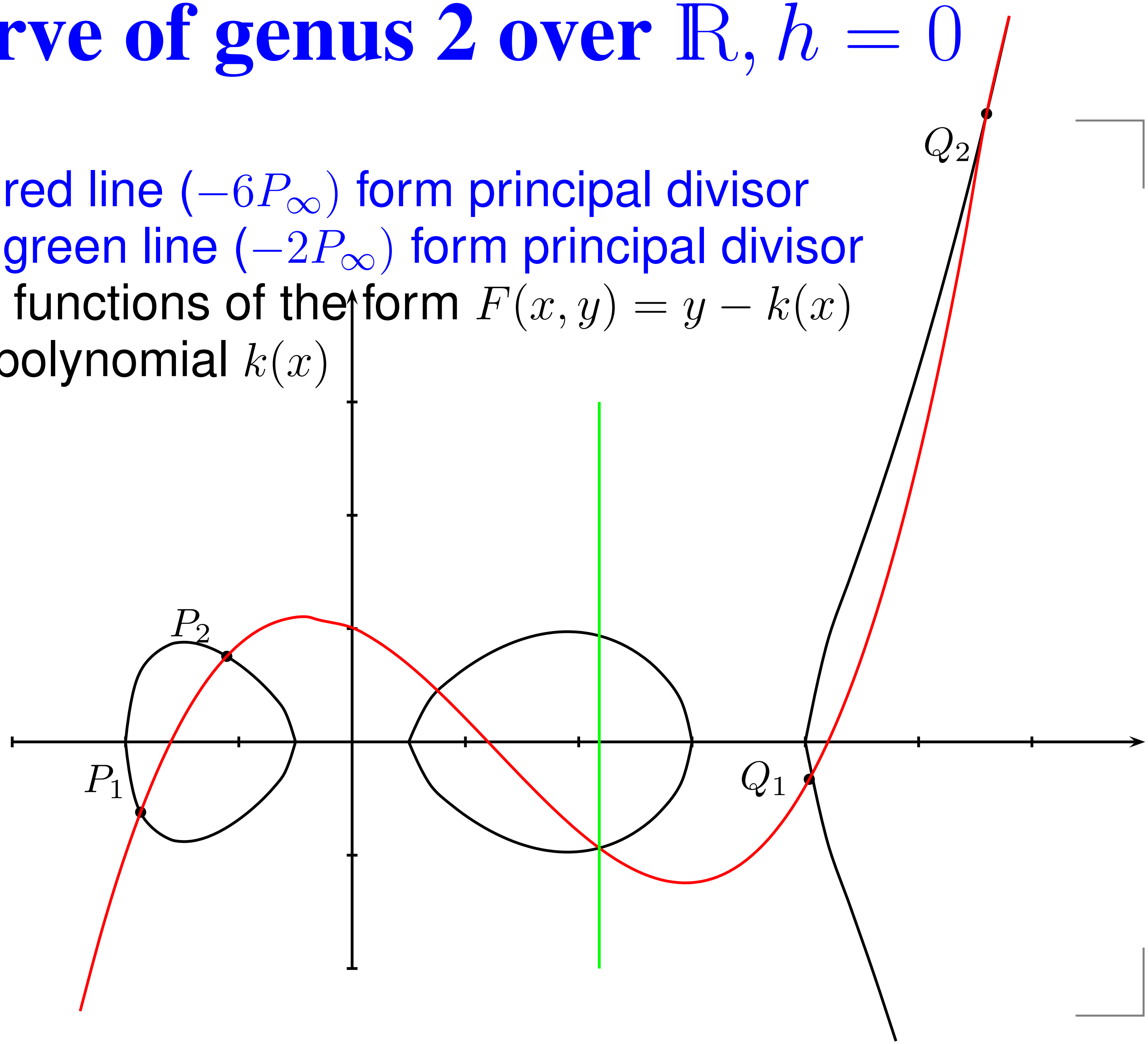
- For any function $F(x,y)$ the graph $F(x,y)=0$ intersects curve in some points of $C(\overline{\mathbb{F}_q})$.
- Let v_P be normalized valuation $P \in C(\overline{\mathbb{F}_q})$, thus $v_P(F)=n \geq 0$ iff F has intersection of multiplicity n with curve at P (simple intersection has $n=1$ while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

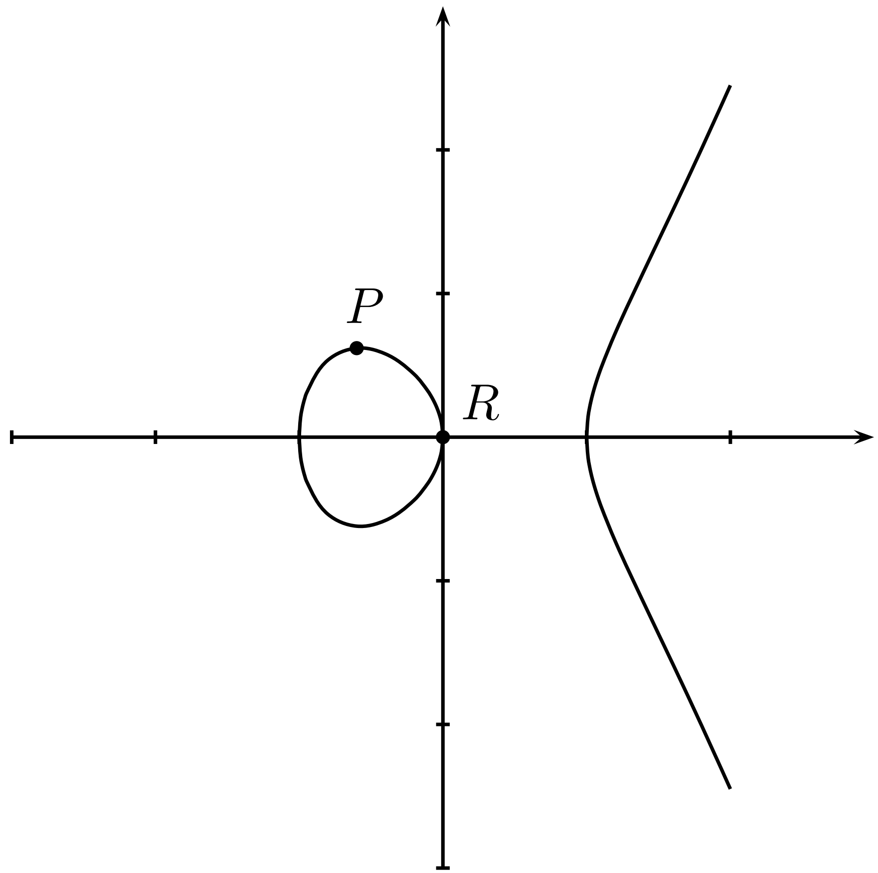
$$\mathrm{Pic}_C^0 = \mathrm{Div}_C^0/\mathrm{Princ}_C.$$

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 endomorphismus, i.e. computing q-th powers of all coordinates. Note that not each point needs to remain fixed for that (sum can be rearranged).

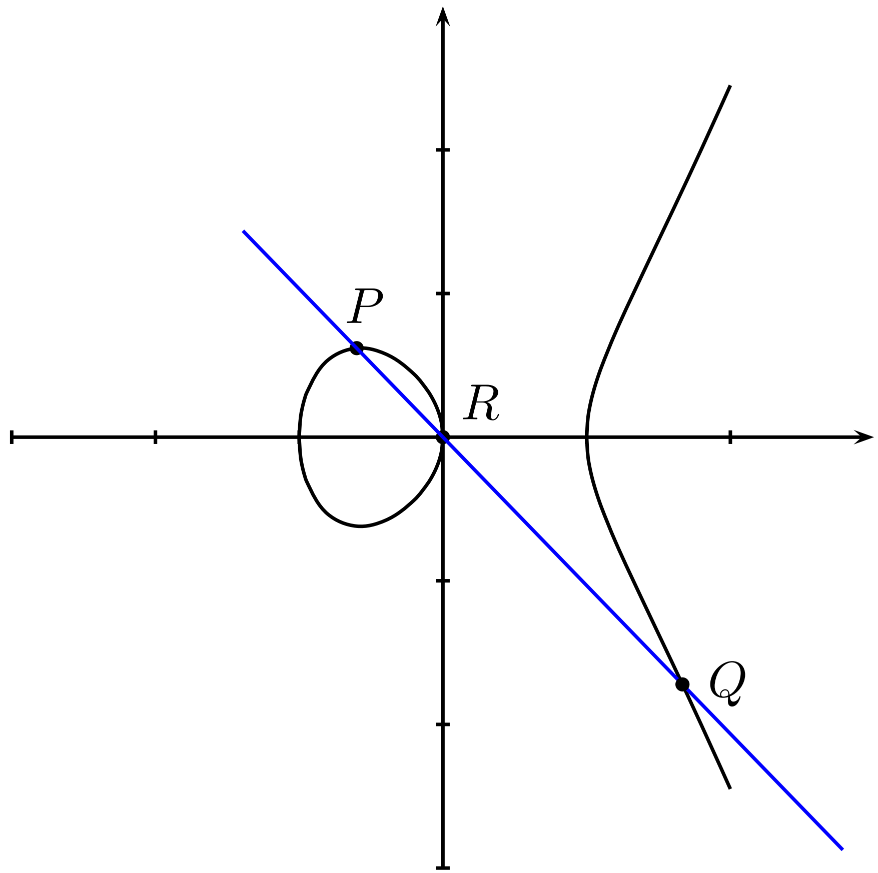
Example: $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



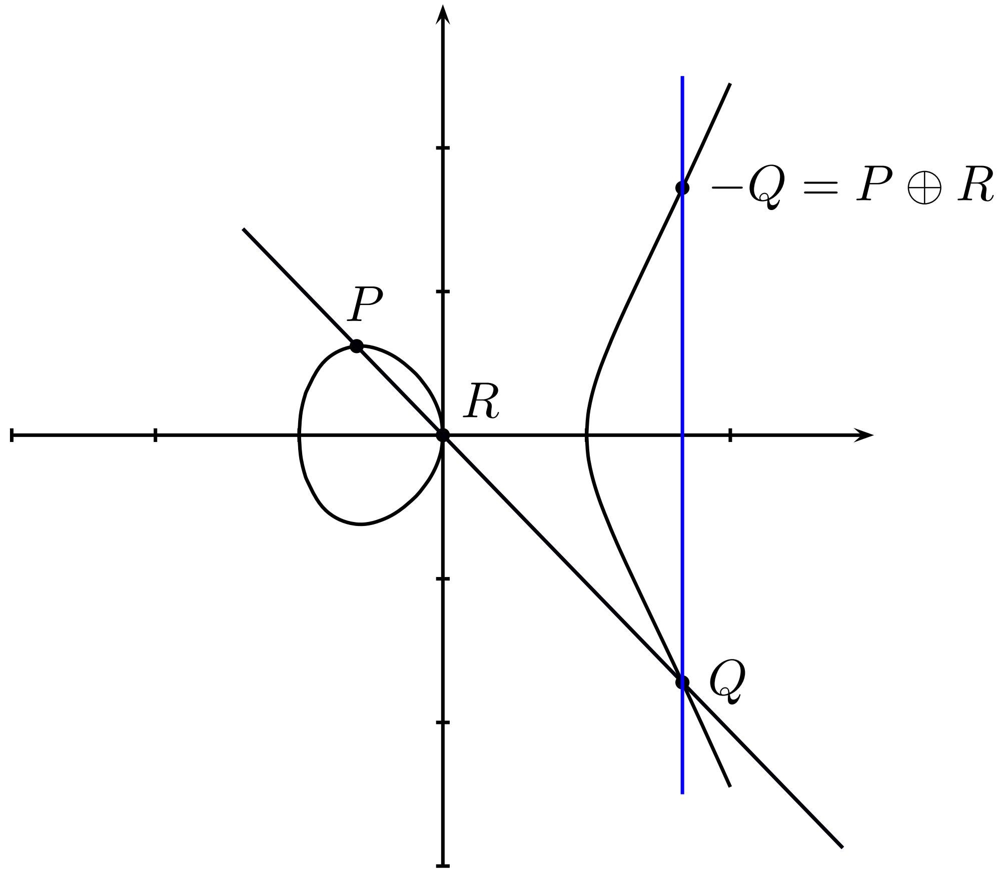
Example: $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



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

$y^2 = x^3 - x$



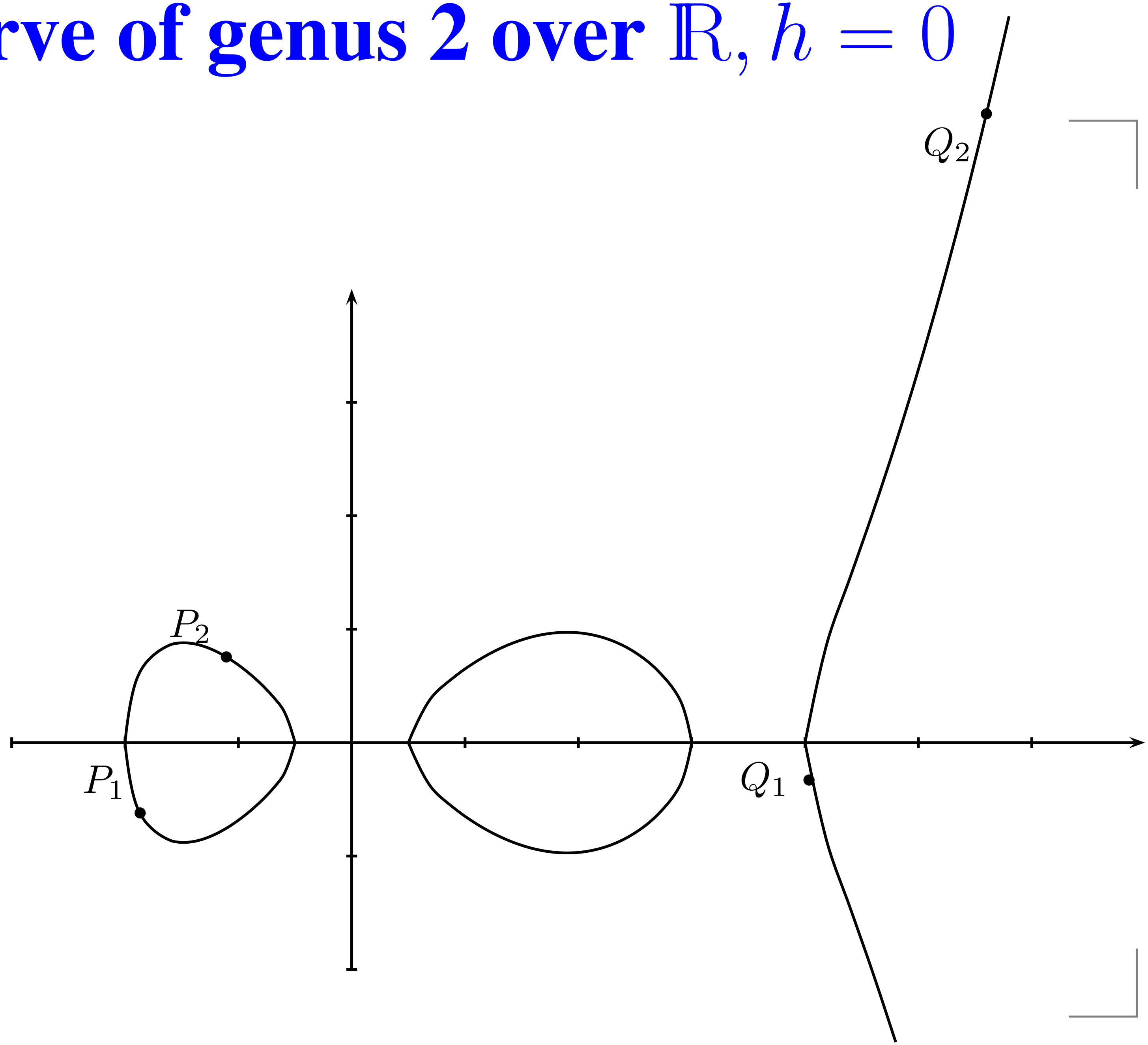
Reduced divisors

- Divisor D is semi-reduced if

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

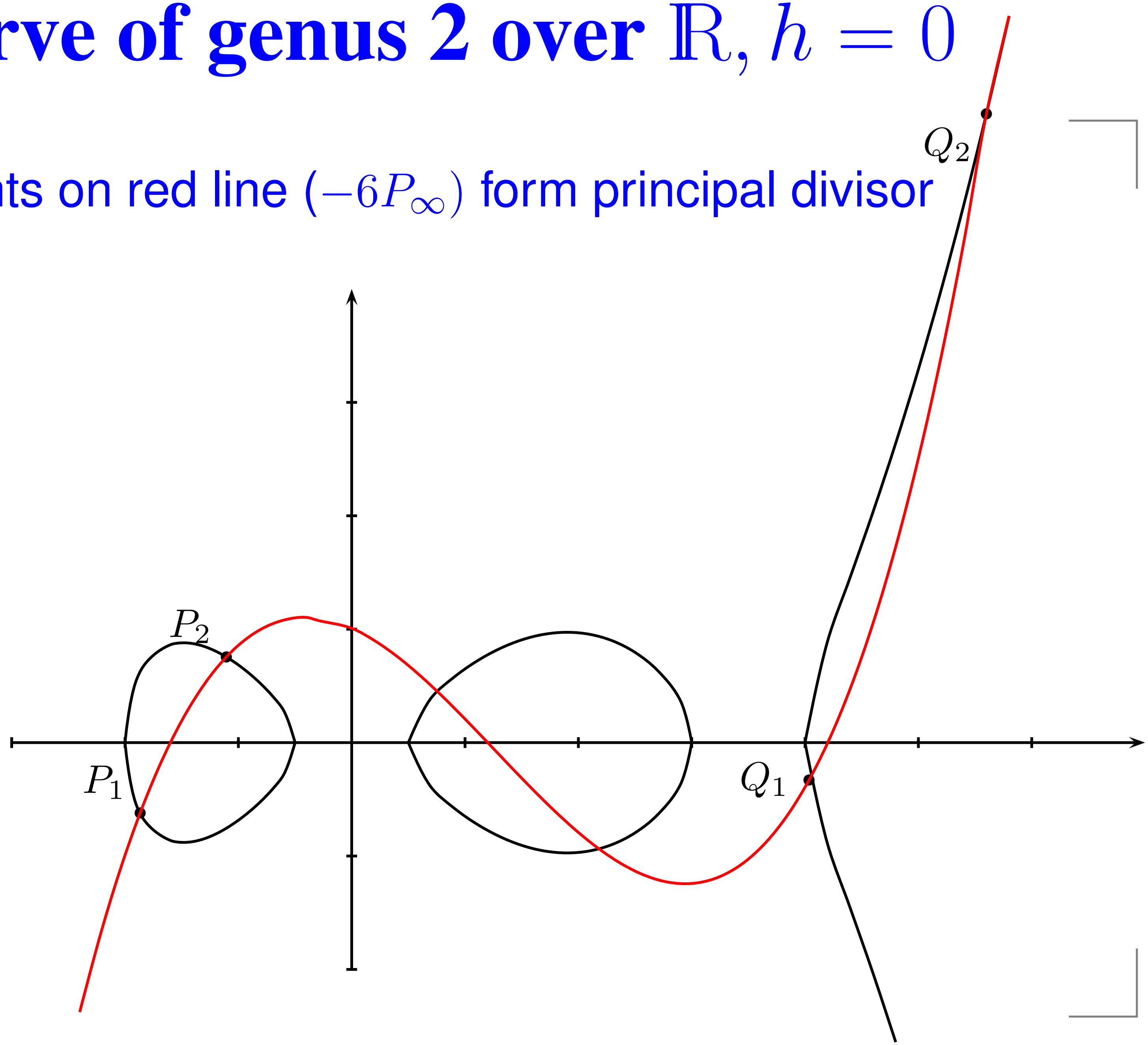
  and $P_i \neq -P_j$ for $i \neq j$ (no restriction on the number of points)
- Divisor D is reduced if it is semi-reduced and $m \leq g$.
- Important result on representation:
  Each divisor class has a unique reduced representative.

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



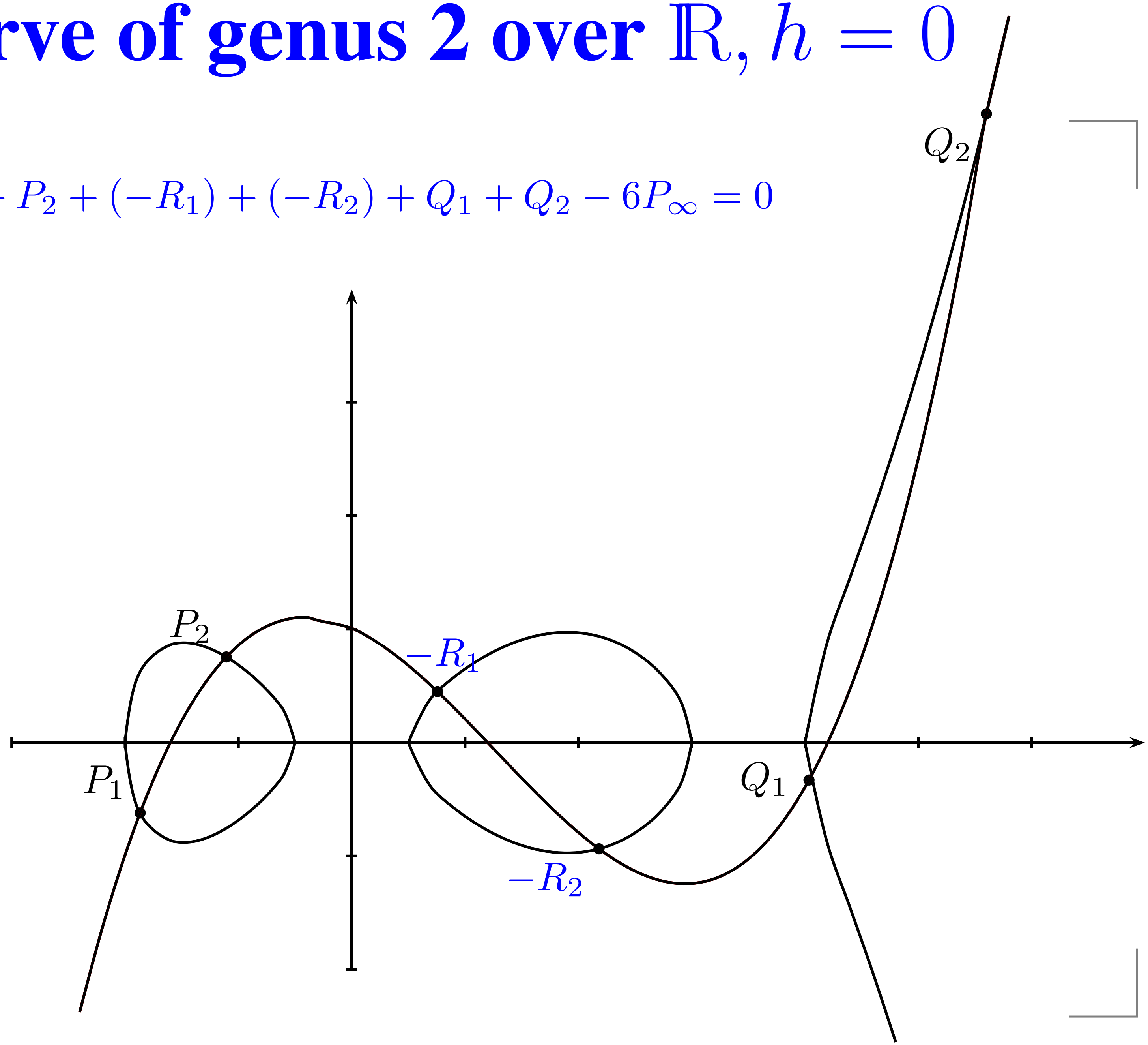
Curve of genus 2 over $\mathbb{R}, h = 0$

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



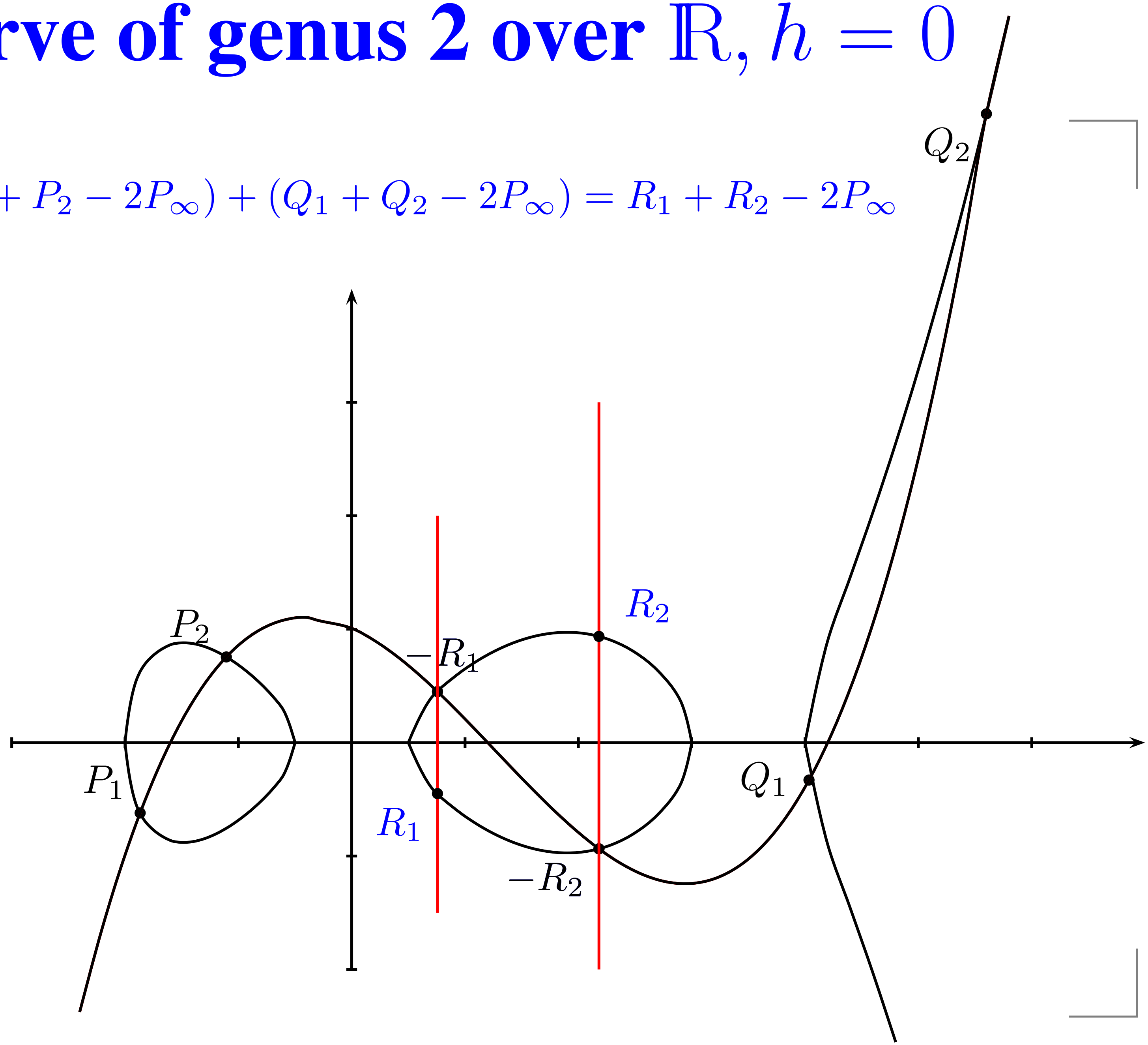
Curve of genus 2 over $\mathbb{R}$, $h = 0$

$$P_1 + P_2 + (-R_1) + (-R_2) + Q_1 + Q_2 - 6P_\infty = 0$$



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

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



Representation

- Still need a compact representation.
- Idea: use polynomials to represent divisors, ignore P_∞ – multiplicity dictated by affine part.
- Let semi-reduced $D = \sum_{i=1}^{m} P_i - mP_\infty$ with $P_i = (x_i, y_i)$. Put

  $$u(x) = \prod_{i=1}^{m}(x - x_i) \text{ and define } v \text{ by } v(x_i) = y_i \text{ with multiplicity}$$

  (latter gives conditions on derivative of v).
- $\deg(v) < \deg(u) = m$.
- Reduced divisors have $\deg(u) \leq g$.

Mumford Representation

- Easy characterization for field of definition!
  Divisor classes defined over $\mathbb{F}_q$ have $u, v \in \mathbb{F}_q[x]$.
- Divisor classes can be represented by reduced divisors
  $\Rightarrow$ each class can be represented by two polynomials

  $$[u(x), v(x)]; u, v \in \mathbb{F}_q[x],$$

  u monic, $\deg v < \deg u \leq g, \quad u | v^2 + vh - f.$

  $\Rightarrow$ compact representation.
- Alternative viewpoint:

  We define group on elements $[u(x), v(x)]$ with conditions as above according to algorithm on next slide.
- That's all we really need to do crypto on hyperelliptic curves.

Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor/Koblitz)

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$
`OUT:` $D = [u, v]$ reduced with $D \sim D_1 + D_2$

1. compute $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$
3. let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
4. $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$

This result $[u, v]$ corresponds to a semireduced divisor.

Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor/Koblitz)

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$
`OUT:` $D = [u, v]$ reduced with $D \sim D_1 + D_2$

1. compute $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$
3. let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
4. $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
5. let $u' = \frac{f - vh - v^2}{u} \quad v' = (-h - v) \bmod u'$
6. if $\deg u' > g$ put $u := u', v := v'$ goto step 5
7. make u monic

This result $[u, v]$ corresponds to a reduced divisor.

More in the afternoon.