I Introduction

11.10.22

Plan: Have a "long" introduction in order to

- provide some motivation for the (partly) more "technical" content that will come later
- give those participants who were not in the Algebra 2 class last term a little more time to brush up their commutative algebra knowledge
  - (prime) ideals, quotients
  - localization
  - spectrum of a ring, Zariski topology

further references on moodle page

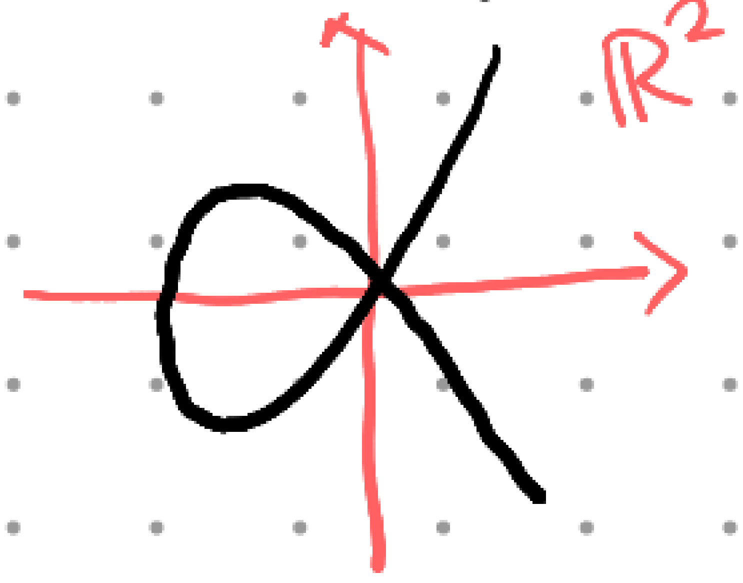
- What is algebraic geometry?
- (very) rough survey of this class
- I would like to know:
  What are your expectations?
  - practical/organizational
  - regarding content

  also: what is your background/knowledge so far?

What is algebraic geometry?

→ study "geometric properties" of solution sets of systems of polynomial equations (over a field, or more generally a commutative ring)

Example $\{(x,y)\in\mathbb{R}^2;\ y^2 = x^2(x+1)\}$



Compared to previous/other courses:

linear algebra	algebra	algebraic geometry	algebraic number th.
systems of linear equations	one polynomial equation, one variable	several pol. equations, several variables	coefficients/solutions in $\mathbb{Z}$, $\mathbb{Q}$, $K/\mathbb{Q}$ finite, $\mathbb{F}_q$ ...

What does the "algebraic" in "algebraic geometry" refer to?

→ look at solutions / zero sets of polynomials (rather than, e.g., of (convergent) power series, differentiable/holomorphic functions)

→ use algebraic methods (commutative algebra)

"in principle" can work over arbitrary field

We start with a simple example which illustrates how geometric methods can be useful:

An (algebro-) geometric view on the theorem of Cayley-Hamilton

Theorem k a field, $A \in M_n(k)$. Then $\mathrm{charpol}_A(A) = 0$

$(\in M_n(k))$.

Let us consider the following situation: $k = \mathbb{R}$, trace of A $\mathrm{tr}(A) = 0$

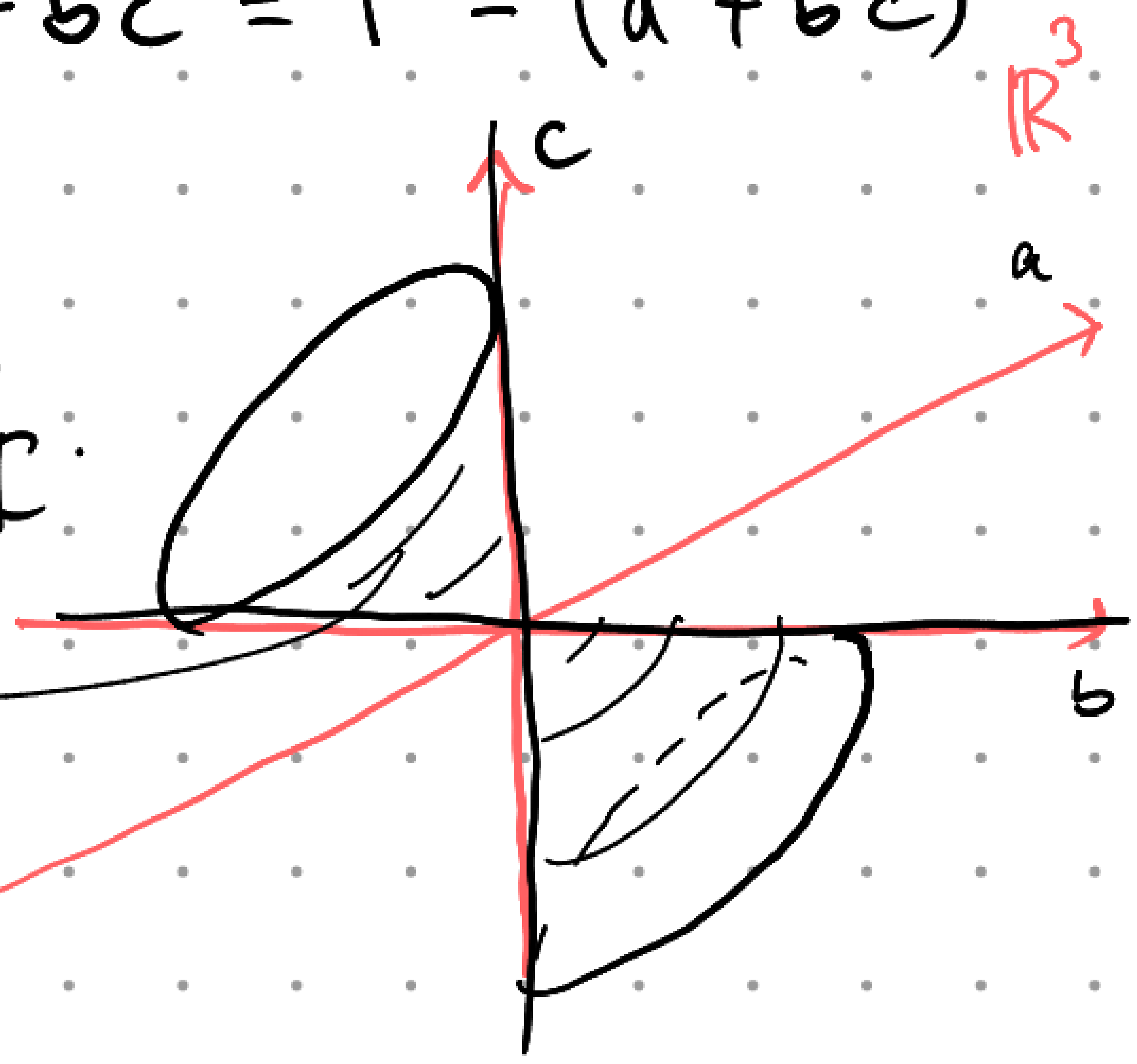
not really necessary, but simplifies the notation a little

Want to use that the theorem is obviously true for diagonal matrices, and hence for diagonalizable matrices. In fact, suffices to have diag-able/$\mathbb{C}$.

So consider $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in M_2(\mathbb{R})^{tr=0} \underset{\text{as } \mathbb{R}\text{-v.s.}}{\underline{= \mathbb{R}^3}}$

Have $\mathrm{charpol}_A = (T-a)(T+a) - bc = T^2 - (a^2+bc)$

⇝ all matrices $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ with $a^2+bc \neq 0$ are diagonalizable$/\mathbb{C}$.



cone where $a^2+bc=0$

To prove the result for matrices $A=\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ with $a^2+bc=0$, consider the map

$$M_2(\mathbb{R})^{tr=0} \xrightarrow{\Phi} M_2(\mathbb{R}), \quad A \mapsto \mathrm{charpol}_A(A).$$

Goal: $\Phi(A)=0$ for all A.

Can view Φ as a map $\mathbb{R}^3 \to \mathbb{R}^4$ given by polynomials, hence Φ is continuous.
Since $\{0\} \subset M_2(\mathbb{R})$ is closed, therefore $\Phi^{-1}(\{0\})$ is closed in $M_2(\mathbb{R})^{tr=0}$.

We have seen that $M_2(\mathbb{R})^{tr=0} \setminus V(a^2+bc) \subseteq \Phi^{-1}(\{0\})$.
Since $M_2(\mathbb{R})^{tr=0} \setminus V(a^2+bc)$ is dense in $M_2(\mathbb{R})^{tr=0}$, it follows that $\Phi^{-1}(\{0\}) = M_2(\mathbb{R})^{tr=0}$, as desired.

Question: How to deal with other fields?
(See Problem sheets 1, 2.)

The Zariski topology on k^n (k a field)

Since we want to study solution sets of systems of polynomial equations, let us introduce some notation:

k field, $f_1, \dots, f_m \in k[T_1, \dots, T_n]$

$$\rightsquigarrow V(f_1, \dots, f_m) = \{ (t_i)_i \in k^n ;\ \forall j = 1, \dots, m : f_j(t_1, \dots, t_n) = 0 \}$$

Furthermore, if K/k is any field extension, we can also plug elements of K^n into the f_j and define

$$V(f_1, \dots, f_m)(K) = \{ (t_i)_i \in K^n ;\ \forall j : f_j(t_1, \dots, t_n) = 0 \}.$$

(V stands for vanishing set (or in German: Verschwindungsmenge).)

Prop. The sets $V(f_1,\dots,f_m)$, $f_j \in k[T_1,\dots,T_n]$, form the set of closed sets of a topology on k^n, the so-called Zariski topology, i.e.

- $\emptyset, k^n$ are of this form
- finite unions of sets of this form are of the same form
- arbitrary intersections of sets of this form are of this form.

Proof.
- $\emptyset = V(1)$, $k^n = V(0)$
- intersections:

For any subset $F \subseteq k[T_1,\dots,T_n]$ let

$$V(F) = \{ (t_i)_i \in k^n ; \text{ for all } f \in F : f(t_1,\dots,t_n) = 0 \}.$$

Then
- For $F_j \subseteq k[T_1,\dots,T_n]$, $j \in J$, we have

$$\bigcap_{j\in J} V(F_j) = V\Big(\bigcup F_j\Big)$$

- For $F \subseteq k[T_1,\dots,T_n]$, we have

$$V(F) = V(\underbrace{(F)}_{\text{ideal generated by } F})$$

- By Hilbert's basis theorem, the ring $k[T_1,\dots,T_n]$ is noetherian, i.e. every ideal is finitely generated.

Combining these statements, we get the desired conclusion about intersections of closed subsets.

- finite unions:

By induction, it is enough to consider the union of two closed subsets, say

$V(f_1 \ldots f_m)$, $V(g_1 \ldots g_r)$.

But $V(f_1 \ldots f_m) \cup V(g_1 \ldots g_r) = V\left(f_j g_k \,,\ \begin{matrix} j=1,\ldots m, \\ k=1,\ldots r \end{matrix}\right).$

The topological space k^n with the Zariski topology is denoted by $\mathbb{A}^n(k)$ and called "affine n-space" or "affine space of dimension n" over k.

Bézout's theorem k a field

12.10.22

For polynomial $f \in k[X,Y]$, as before we write

$$V(f) = \{(x,y) \in k^2 \,;\, f(x,y) = 0\}$$ "vanishing set of f"

We start from the following observation:

(1) For a polynomial $p \in k[X]$, $n = \deg(p) \geq 0$

$\#\{x \in k \,;\, p(x) = 0\} \leq n$.

If k algebraically closed and if we count zeros of p "with multiplicity", then we have equality: $\sum_{x \in k} \mathrm{ord}_x(p) = n$ (k alg. cl.)

($\mathrm{ord}_x(p) = \max\{r \,;\, (X-x)^r \mid p\}$

(2) For $p \in k[X]$, let $f = Y - p$, $g = Y$.

Then have bijection $\{x \in k \,;\, p(x) = 0\} \xrightarrow{1:1} V(f) \cap V(g)$

$$x \longmapsto (x, p(x))$$
$$(= (x,0))$$

More generally, given $f, g \in k[X,Y]$,

it is an interesting problem to determine $\#(V(f) \cap V(g))$

(much more generally: "intersection theory of algebraic varieties").

(3) Now consider $f, g \in k[X,Y]$. (Recall: $k[X,Y]$ UFD)

Easy: if f, g have common divisor h, $\deg h > 0$, and k alg. cl., then $V(f) \cap V(g)$ is infinite

So now suppose f, g are coprime.

Proposition Let k be a field, $f, g \in k[X,Y]$ coprime.

Then $\#\big(V(f) \cap V(g)\big) \leq \deg(f) \deg(g)$

"total degree", i.e. for $f = \sum a_{ij} X^i Y^j$, $\deg f = \max\{i+j \,;\, a_{ij} \neq 0\}$

Goal: more precise statement when we have equality

→ work over algebraically closed field k

→ count points with appropriate multiplicity $i_P(f,g)$

$P = (x,y)$, let $\mathfrak{m} := (X-x, Y-y) \subset k[X,Y]$ max'l ideal

Define $i_P(f,g) := \dim_k k[X,Y]_{\mathfrak{m}} / (f,g)$

localization at maximal ideal $\mathfrak{m}$

But this is not enough!

(e.g. $f = Y$, $g = Y-1 \rightsquigarrow V(f) \cap V(g) = \emptyset$)

(4) The projective plane $\mathbb{P}^2(k)$

Idea: Add points to k^2 to ensure that any two different lines intersect in a point.

$$\mathbb{P}^2(k) := \{ L \subseteq k^3 \text{ subvector space}; \dim L = 1 \}$$

$$\begin{tikzcd}
\mathbb{P}^2(k) & \text{line generated by } \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \\
k^2 \arrow[u, hook] & \ni (x,y) \arrow[u, mapsto]
\end{tikzcd}$$

Homogeneous coordinates

For $(x,y,z), (x',y',z') \in k^3 \setminus \{0\}$, define

$$(x,y,z) \sim (x',y',z') \iff \left\langle \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \right\rangle$$

$\iff$ there exists $\lambda \in k^\times$: $x' = \lambda x$, $y' = \lambda y$, $z' = \lambda z$.

This is an equivalence relation on $k^3 \setminus \{0\}$.

The equivalence class of (x,y,z) is denoted $(x:y:z)$.

Obtain bijection

$$\begin{aligned} (k^3 \setminus \{0\})/\sim \; &\longrightarrow \mathbb{P}^2(k) \\ (x:y:z) \; &\longmapsto \left\langle \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right\rangle \end{aligned}$$

We usually write points of $\mathbb{P}^2(k)$ as $(x:y:z)$ "homogeneous coordinates"

Want to define zero sets of polynomials in $\mathbb{P}^2(k)$.

Def A polynomial $f \in k[X_1, \ldots X_n]$ is called homogeneous of degree $d \in \mathbb{N}$ iff all monomials occurring in f with non-zero coefficient have degree d.

Examples $X^3 + X^2 + Y^3$ not homogeneous

$X^3 + X^2 Z + Y Z^2$ homogeneous of degree 3

Let $F \in k[X, Y, Z]$ be homogeneous of degree d.

Then $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z)$, $\lambda \in k$,

in particular, $F(\lambda x, \lambda y, \lambda z) = 0 \iff F(x, y, z) = 0$ for $\lambda \in k^\times$.

Therefore can define:

$F_j \in k[X, Y, Z]$ homogeneous

$\rightsquigarrow V_+(F_1, \ldots F_m) = \{(x : y : z) \in \mathbb{P}^2(k) ; \forall j : F_j(x, y, z) = 0\}$

The Zariski topology on $\mathbb{P}^2(k)$ is the topology whose closed sets are the sets of the form $V_+(F_1, \ldots F_m)$.

A <u>line</u> in $\mathbb{P}^2(k)$ is a subset of the form $V_+(F)$ for $F \neq 0$ homogeneous of degree 1.

For example: $V_+(Z)$ "line at infinity",

$$\mathbb{P}^2(k) = \iota(k^2) \ \dot\cup\ V_+(Z).$$

$$F \text{ homog} \rightsquigarrow \quad V_+(F) = \underbrace{\left(V_+(F)\cap \iota(k^2)\right)}_{\substack{1{:}1 \Big\uparrow \iota \\ V_+(f)}} \ \dot\cup\ V_+(F,Z)$$

$f(X,Y) = F(X,Y,1) \in k[X,Y]$

<u>Proposition.</u>

(1) Let $P_1 \neq P_2 \in \mathbb{P}^2(k)$. Then there exists $F \in k[X,Y,Z]$ linear homog s.t. $P_1, P_2 \in V_+(F)$, and F unique up to $\lambda \in k^\times$.

(2) For linear homogeneous polynomials $F_1, F_2 \in k[X,Y,Z]$: $\quad V_+(F_1) = V_+(F_2) \iff \exists\, \lambda \in k^\times : F_2 = \lambda F_1$.

(3) Let $F_1, F_2 \in k[X,Y,Z]$ linear, homog s.t. $V_+(F_1) \neq V_+(F_2)$. Then $\#\left(V_+(F_1) \cap V_+(F_2)\right) = 1$.

Proof (1) Phrase the problem in terms of a system of linear equations on the coefficients of F.

(2) follows from (1)

(3) Consider points on $\mathbb{P}^2(k)$ as lines (1-dim'l subvector spaces) in k^3.

Remark Similarly, one can define projective n-space $\mathbb{P}^n(k) = \{\text{lines in } k^{n+1}\} = \left(k^{n+1} \setminus \{0\}\right) / k^\times$.

18.10.2022

Can now state the precise version of Bézout's theorem.

Theorem (Bézout) k algebraically closed

$F, G \in k[X, Y, Z]$ non-constant, homogeneous, coprime.

Then $\sum_{P \in \mathbb{P}^2(k)} i_P(F,G) = \deg(F)\deg(G)$,

in particular, $\#(V_+(F) \cap V_+(G)) \leq \deg(F)\deg(G)$.

Here, $i_P(F,G)$ is defined similarly as before.

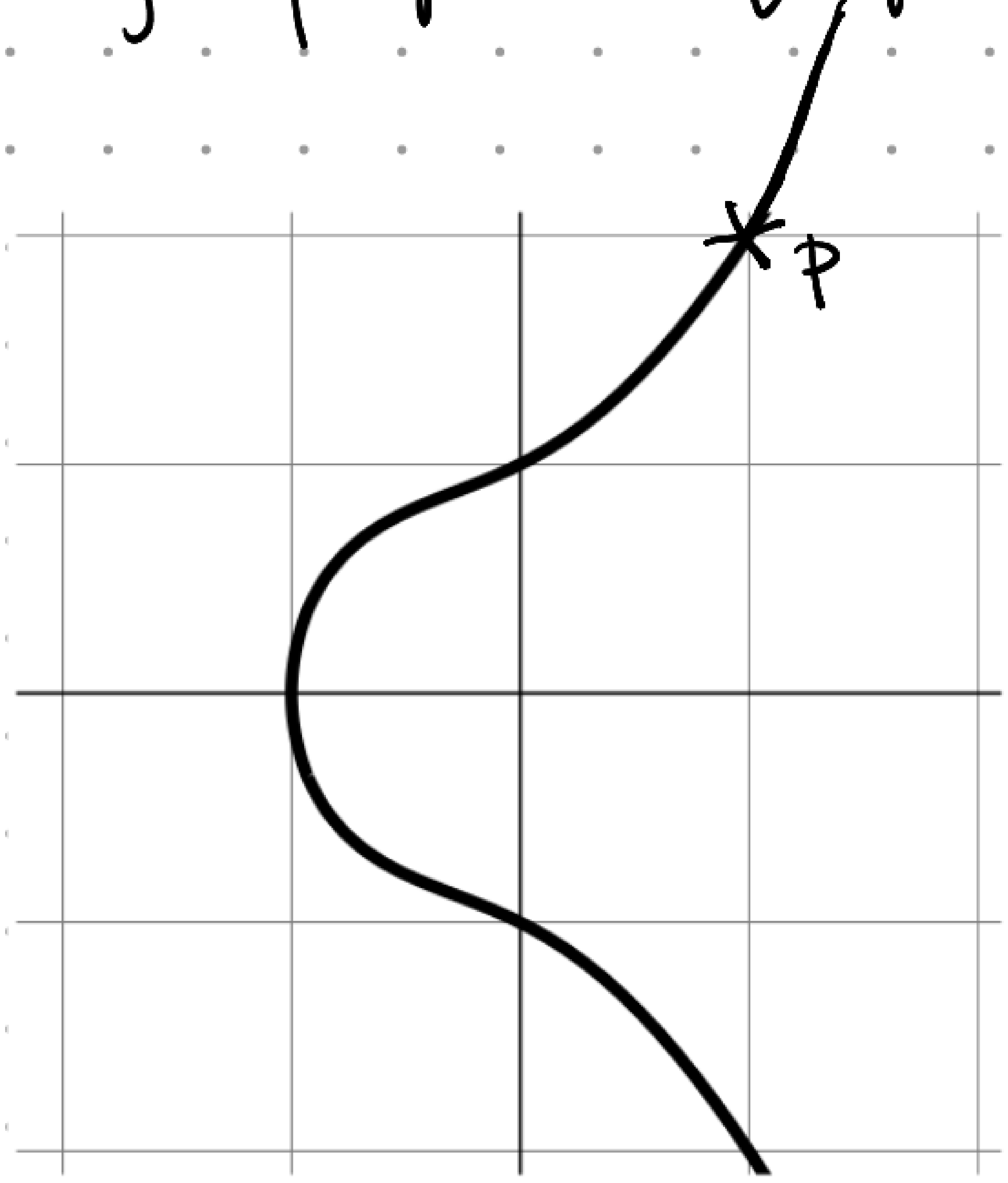
We will give a proof later in the course.

Let us look at some more examples.

Cubic curves

(i.e. "plane curves" defined by a polynomial of degree 3)

char $k \neq 2$



- $y^2 = (x+1)(x^2+1)$

$$f = y^2 - (x+1)(x^2+1)$$
$$= y^2 - x^3 - x^2 - x - 1$$
$$C = V(f)$$

$\frac{\partial f}{\partial x} = -3x^2 - 2x - 1$ $\quad \frac{\partial f}{\partial y} = 2y$

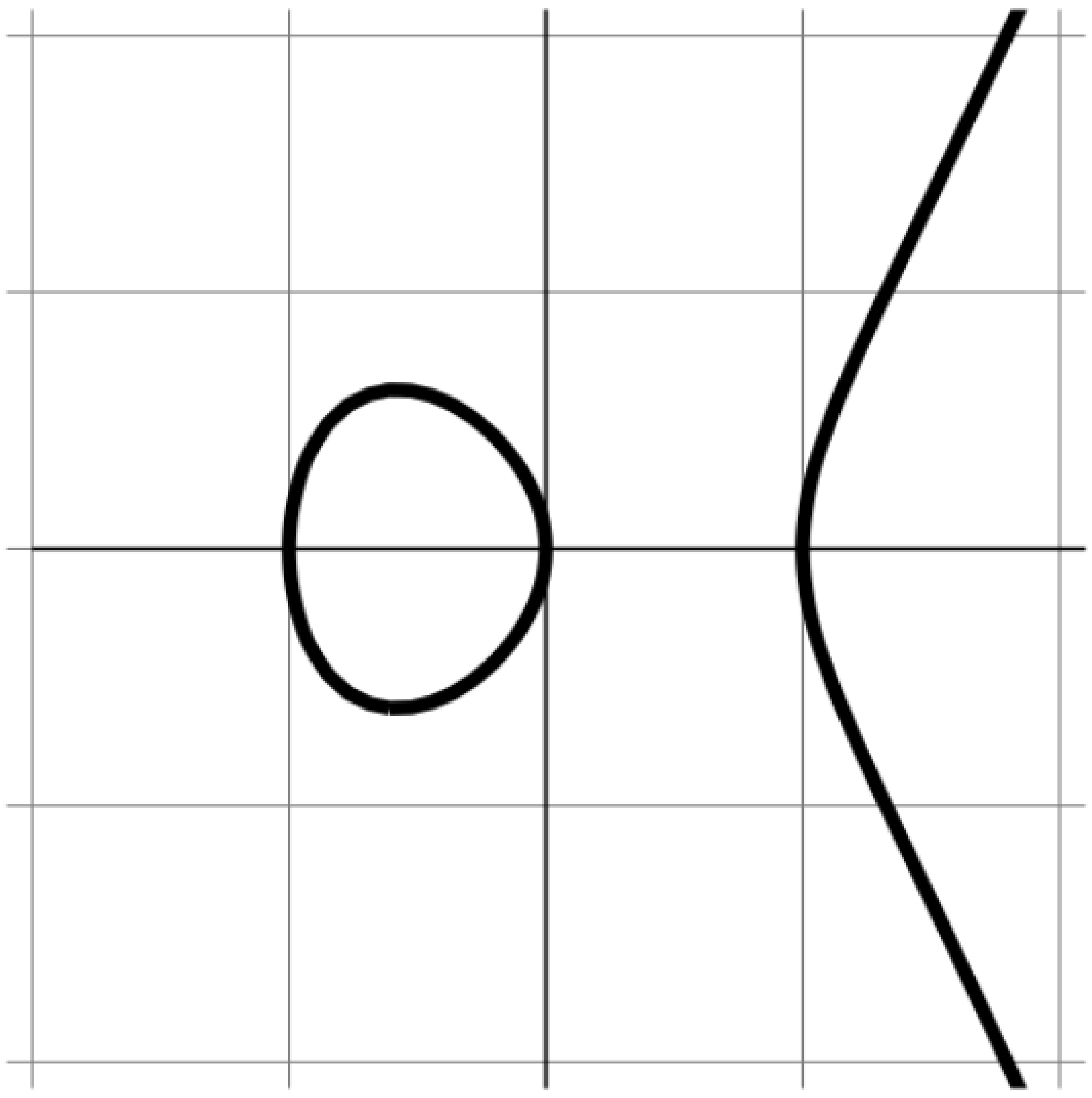
Consider

$P = (1,2) \in C$, $\quad \frac{\partial f}{\partial x}(1,2) = -6$, $\frac{\partial f}{\partial y}(1,2) = 4$ $\neq 0$ since $\mathrm{char}(k) \neq 2$

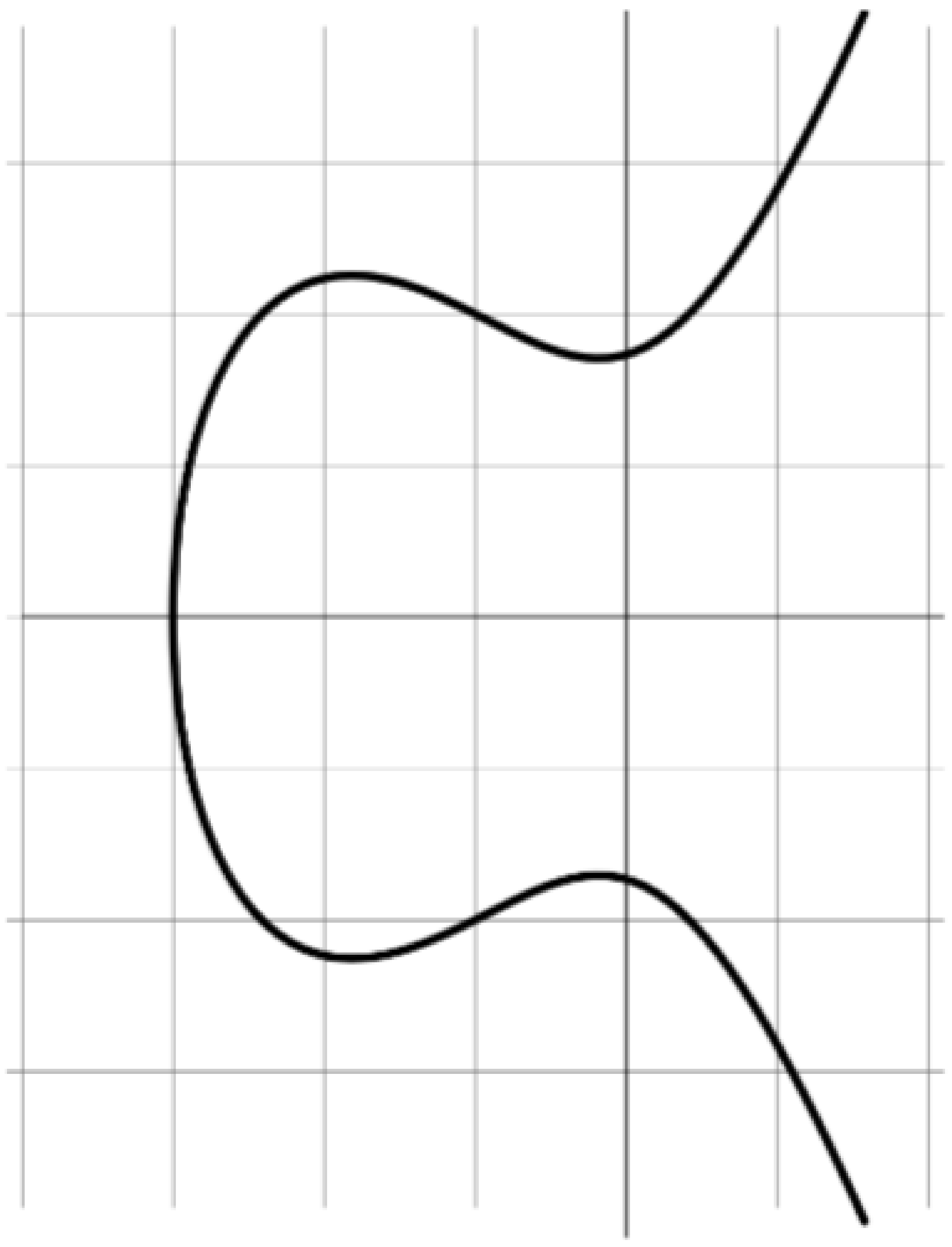
$\boxed{\text{over } \mathbb{R} \ (\text{or } \mathbb{C})}$ → at P, $(x,y) \mapsto f(x,y)$ is approximated well by the linear function $(x,y) \mapsto -6x + 4y \underbrace{-2}_{\text{to make the fct. vanish at } P}$

⇝ the zero set $V(f)$ is approximated "in a small neighborhood of P" by the zero set of the above linear function, i.e., by the line $V(-6x+4y-2)$ $\left(\Longleftrightarrow \ y = \frac{3}{2}x + \frac{1}{2}\right)$

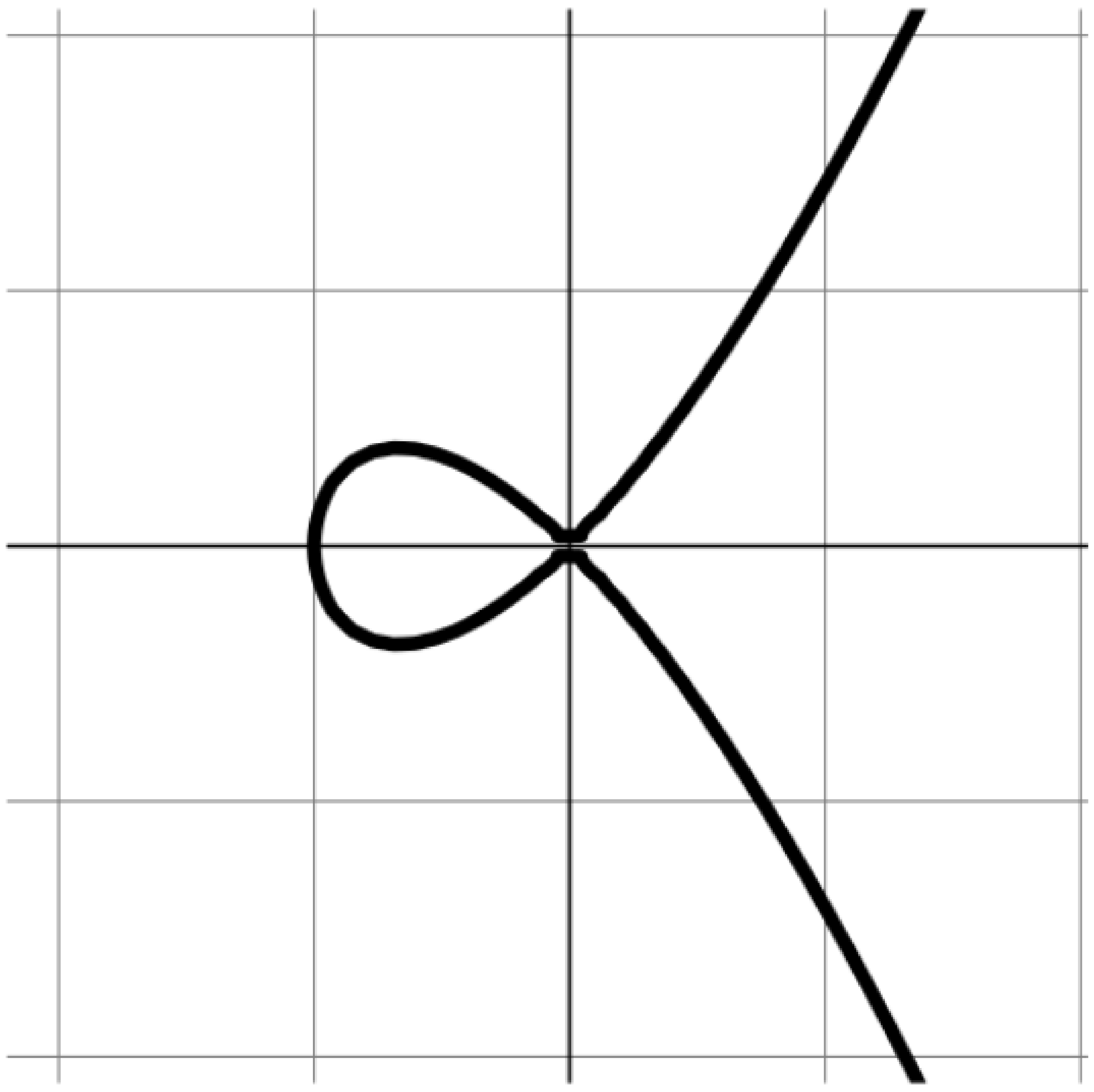
- $y^2 = x(x+1)(x-1)$



- $y^2 = (x+3)(x^2+1)$



- $y^2 = x^2(x+1)$



"node" at the origin

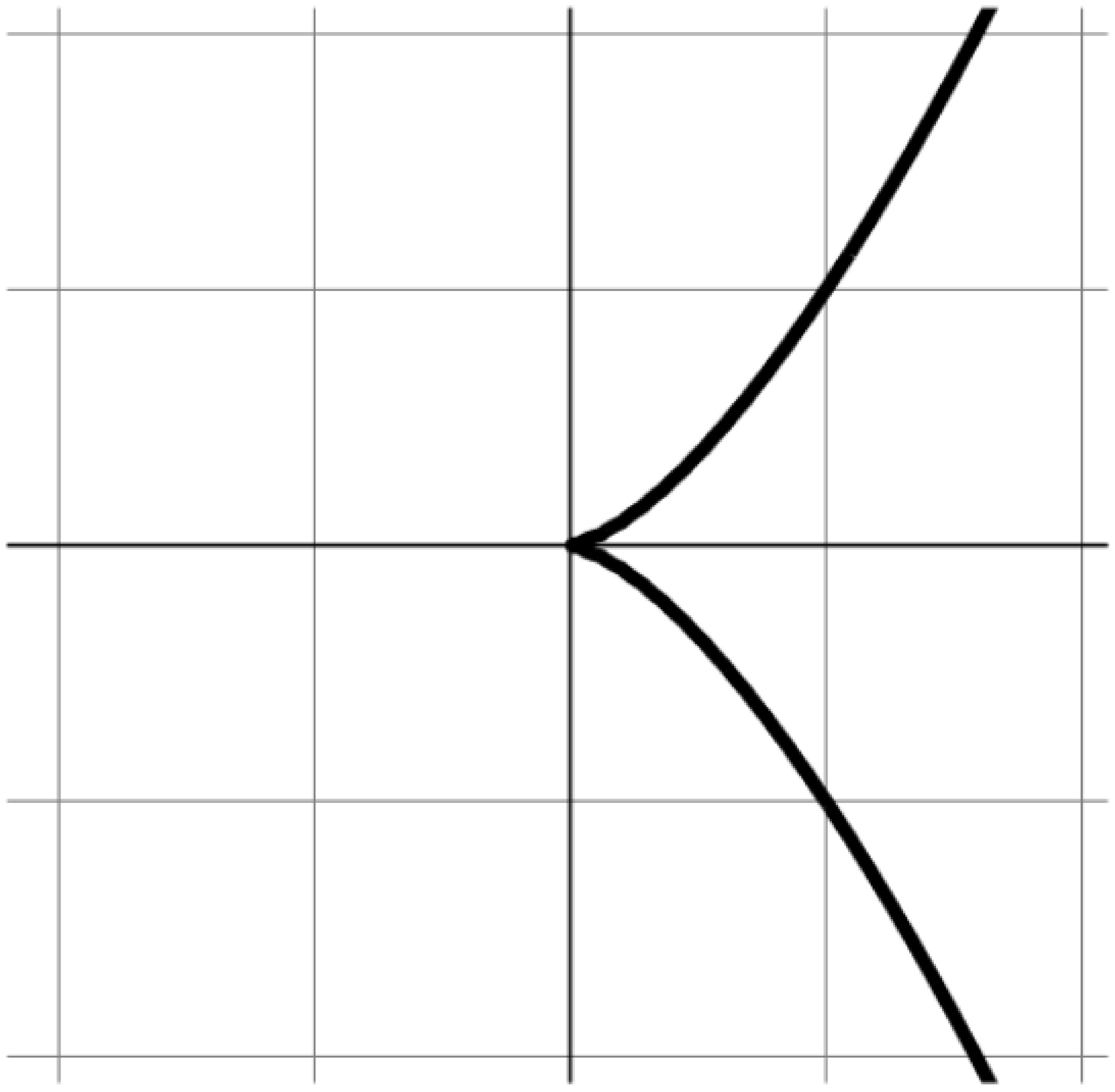
$$\frac{\partial f}{\partial x} = 3x^2+2x$$

$$\frac{\partial f}{\partial y} = 2y$$

both vanish at (0,0)

→ no well-def'd tangent line (as is evident from the pictures)

- $y^2=x^3$



$$\frac{\partial f}{\partial x} = 3x^2$$

$$\frac{\partial f}{\partial y} = 2y$$

"cusp" at the origin

Singular and non-singular points $\quad k$ a field

- Let $f \in k[x,y]$ non-constant,

  $P = (x_0, y_0) \in C := V(f)$.

  If $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) \neq (0,0)$, then we call the line

  $$V\left(\frac{\partial f}{\partial x}(P)\cdot\left(x-x_0\right) + \frac{\partial f}{\partial y}(P)\cdot\left(y-y_0\right)\right)$$

  the <u>tangent line</u> to C at P, and say that P is a smooth point of C.

  If $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) = (0,0)$, then we say that P is a singular point of C.

- We say that C is smooth if every point of $C(\bar{k})$ is smooth (where $\bar{k}$ is an algebraic closure of k).

- Now let $F \in k[X,Y,Z]$ be non-constant, homogeneous.

Let $P = (x:y:z) \in V_+(F) \subset \mathbb{P}^2(k)$.

We say that P is a smooth point of $V_+(F)$, if $\left(\frac{\partial F}{\partial X}(x,y,z), \frac{\partial F}{\partial Y}(x,y,z), \frac{\partial F}{\partial Z}(x,y,z)\right) \neq (0,0,0)$

and in this case call

$$V_+\left(\frac{\partial F}{\partial X}(x,y,z)\, X + \frac{\partial F}{\partial Y}(x,y,z)\, Y + \frac{\partial F}{\partial Y}(x,y,z)\right)$$

the tangent line to $V_+(F)$ at P. Otherwise we call P a singular point of $V_+(F)$.

We call $V_+(F)$ smooth, if every point of $V_+(F)(\bar{k})$ is smooth.

Can show: for $f \mapsto F$ as above,

$$P \in \begin{array}{ccc} V(f) & \subseteq & V_+(F) \\ \cap & & \cap \\ k^2 & \subset & \mathbb{P}^2(k) \end{array}$$

have P smooth $\in V(f) \Leftrightarrow$ smooth $\in V_+(F)$,

and in this case $T_P V(f) \subset T_P V_+(F)$ "same line"

Smoothness for cubic curves

19.10.2022

Let us understand the notion of smoothness in the following special case (compare the above examples): Assume char$(k) \neq 2$.

(1) $$f = y^2 - \underbrace{(x^3 + ax^2 + bx + c)}_{g(x)} = y^2 - g(x)$$

$$\frac{\partial f}{\partial x} = -g'(x), \quad \frac{\partial f}{\partial y} = 2y$$

$\rightarrow$ the points $(x_0,y_0) \in V(f)$ with $\frac{\partial f}{\partial x}(x_0,y_0) = \frac{\partial f}{\partial y}(x_0,y_0) = 0$

are those with $y = g(x) = g'(x) = 0$,

i.e. $y=0$ and x is a multiple zero of g.

Prop. For f as above,

$V(f)$ smooth $\Longleftrightarrow$ g separable

(i.e. g does not have multiple zeros in $\overline{k}$)

(2) Now consider the projective situation:

$$F = Y^2Z - (X^3 + aX^2Z + bXZ^2 + cZ^3).$$

Then $\dfrac{\partial F}{\partial X} = -(3X^2 + 2aXZ + bZ^2)$ ①

$$\frac{\partial F}{\partial Y} = 2YZ \qquad ②$$

$$\frac{\partial F}{\partial Z} = Y^2 - aX^2 + 2bXZ + 3cZ^2 \qquad ③$$

By ②, for singular pts $(x:y:z)$, $y=0$ or $z=0$.

1st case $z=0$. Then $x=0$ since $F(x,y,z)=0$. Then ③ implies $y=0$, but $(0,0,0)$ is not a point of $\mathbb{P}^2(k)$. So $V_+(F)$ has no singular points lying on the line $V_+(Z)$

[note: $V_+(F) \cap V_+(Z) = \{(0:1:0)\}$, and we have seen that $(0:1:0)$ is always a smooth point. The tangent line at this point is $V_+(Z)$.]

2nd case $z \neq 0$, $y = 0$ Then may assume $z = 1$

Similarly as before, let $g(X) = X^3 + aX^2 + bX + c$.

Then ① $\iff g'(x) = 0$

$F(x,y,z) = 0 \iff g(x) = 0$

these cond (together with ②) imply ③ by Euler's identity

$$3F = \frac{\partial F}{\partial X} X + \frac{\partial F}{\partial Y} Y + \frac{\partial F}{\partial Z} Z$$

$\rightsquigarrow$ Prop. The singular pts of $V_+(F)(\bar{k})$ are the points of the form $(x:0:1)$, where $x \in \bar{k}$ is a multiple zero of g.

In particular: $V_+(F)$ smooth $\iff$ g seperable.

Fact Let k be a field, $A, B \in k$. Then [cf. homework Problem 4]

$$X^3 + AX + B \text{ separable} \iff 4A^3 + 27B^2 \neq 0$$

Def A smooth cubic curve E together with a fixed point $O \in E$ is called an elliptic curve.

The group law on smooth cubic curves

k alg. closed

in some sense this assumption can be removed ..

$E = V_+(F) \subset \mathbb{P}^2(k)$ smooth,
$\deg F = 3$, $\mathcal{O} \in E$ a fixed point.

$P, Q \in E$. Let $L \subset \mathbb{P}^2(k)$ be the unique line through P, Q

(in case $P = Q$: the tangent to E at $P = Q$)

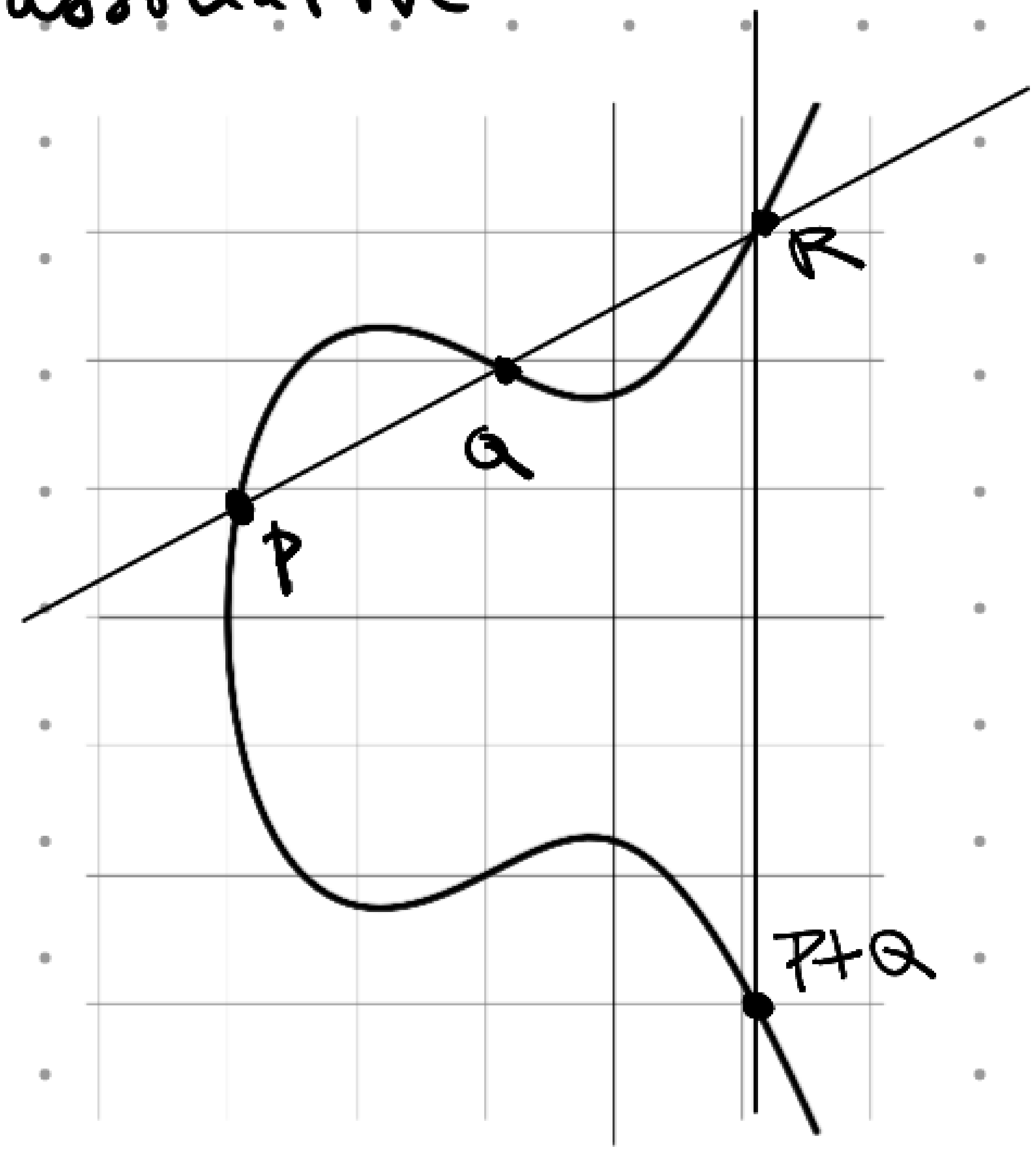
Bézout: $E \cap L = \{\{P, Q, R\}\}$ as a multiset

Let M be the line through $\mathcal{O}, R$ and define $P+Q$ by $E \cap M = \{\{\mathcal{O}, R, P+Q\}\}$

$\rightsquigarrow$ $E \times E \longrightarrow E$, $(P,Q) \mapsto P+Q$, commutative, neutral elt $\mathcal{O}$, inverse elts exist

Can show (more difficult): $+$ is associative

$\rightsquigarrow$ $(E,+)$ commutative group.



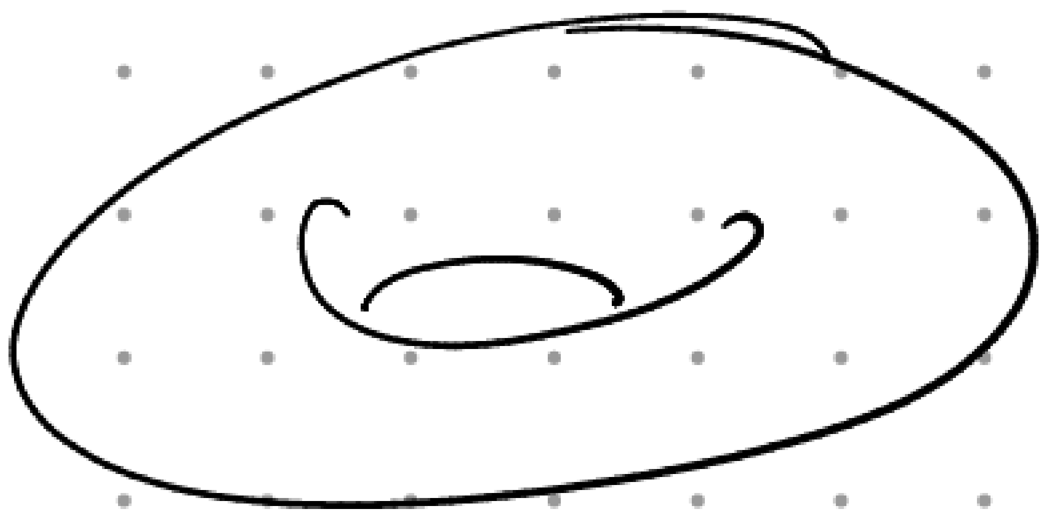
$\mathcal{O} = (0:1:0)$
$\in$
$\mathbb{P}^2(\mathbb{R})$

"at infinity", not in the picture

Remark (Elliptic curves / $\mathbb{C}$)

$\Lambda \subset \mathbb{C}$ a "lattice" (i.e. an additive subgp generated by two $\mathbb{R}$-linear indep elements)

$\rightsquigarrow \mathbb{C}/\Lambda$ a "torus" (homeomorphic to $S^1 \times S^1$)



Weierstraß $\wp$-function: (holom on $\mathbb{C} \setminus \Lambda$, double pole at each $\lambda \in \Lambda$)

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

$$\boxed{\begin{array}{l} g_2(\Lambda) = 60 \sum\limits_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \frac{1}{\lambda^4} \\ g_3(\Lambda) = 140 \sum\limits_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \frac{1}{\lambda^6} \end{array}}$$

$$\rightsquigarrow (\wp'_\Lambda)^2 = 4\wp^3 - g_2(\Lambda)\wp - g_3$$

$$\rightsquigarrow \quad \mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$$

induces a bijection $\mathbb{C}/\Lambda \xrightarrow{\sim} V_+(F) \leftarrow$ smooth cubic curve

for $F = Y^2 - (4X^3 - g_2(\Lambda)X - g_3)$

With a bit more work, this can

- be made more precise regarding the geometric structure on both sides
- be shown to be a group isomorphism (note: group structure is obvious on LHS)

25.10.2022

The Mordell conjecture (Faltings's theorem, Fields medal 1986)

Theorem Let $K/\mathbb{Q}$ be a finite field extension.

Let C/K be a smooth projective curve

of genus ≥ 2. Then $C(K)$ is a finite set.

Let us restrict to the case we have considered so far:

$C = V_+(F) \subset \mathbb{P}^2(K)$, $F \in K[X,Y,Z]$ non-constant, smooth

Remark (1) It is clear that for some F,

$V_+(F)(K)$ is infinite (e.g. if $\deg F = 1$)

(2) In the special case, the genus g of C can

computed by the genus-degree formula:

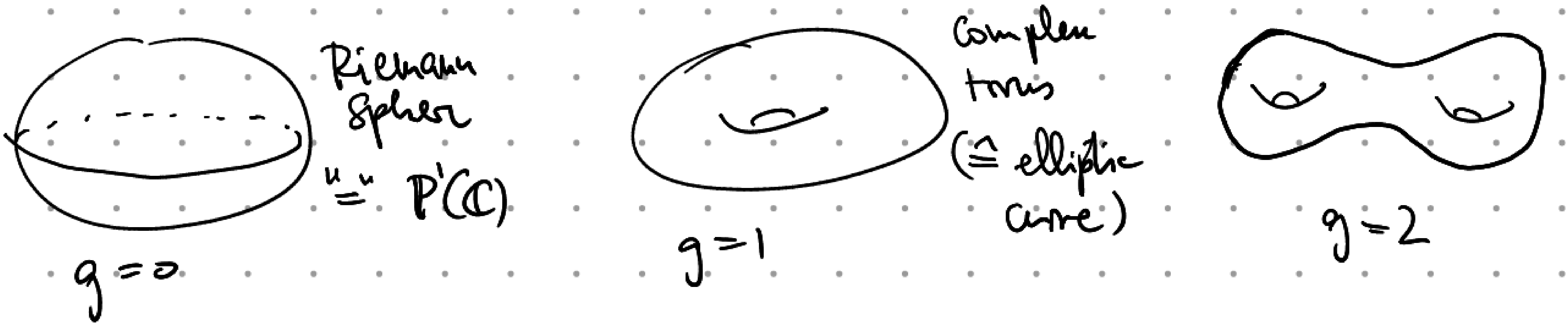
$$g = \frac{(d-1)(d-2)}{2}, \quad d = \deg F$$

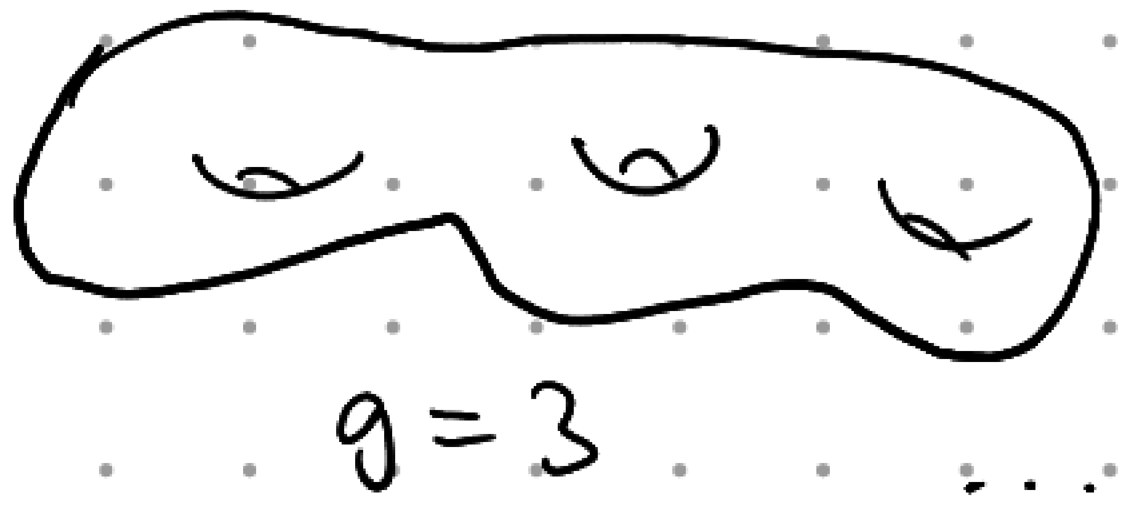
In particular, in the special case the

theorem applies whenever $\deg F \geq 4$.

(3) For $\deg F = 3$, the case of smooth cubic curves, so $g=1$, there are examples when $C(K)$ is finite, as well as examples when it is infinite.

(4) The origin of the notion of genus is topological, the genus "counts the number of holes" of a "Riemann surfaces", as illustrated by the following picture:

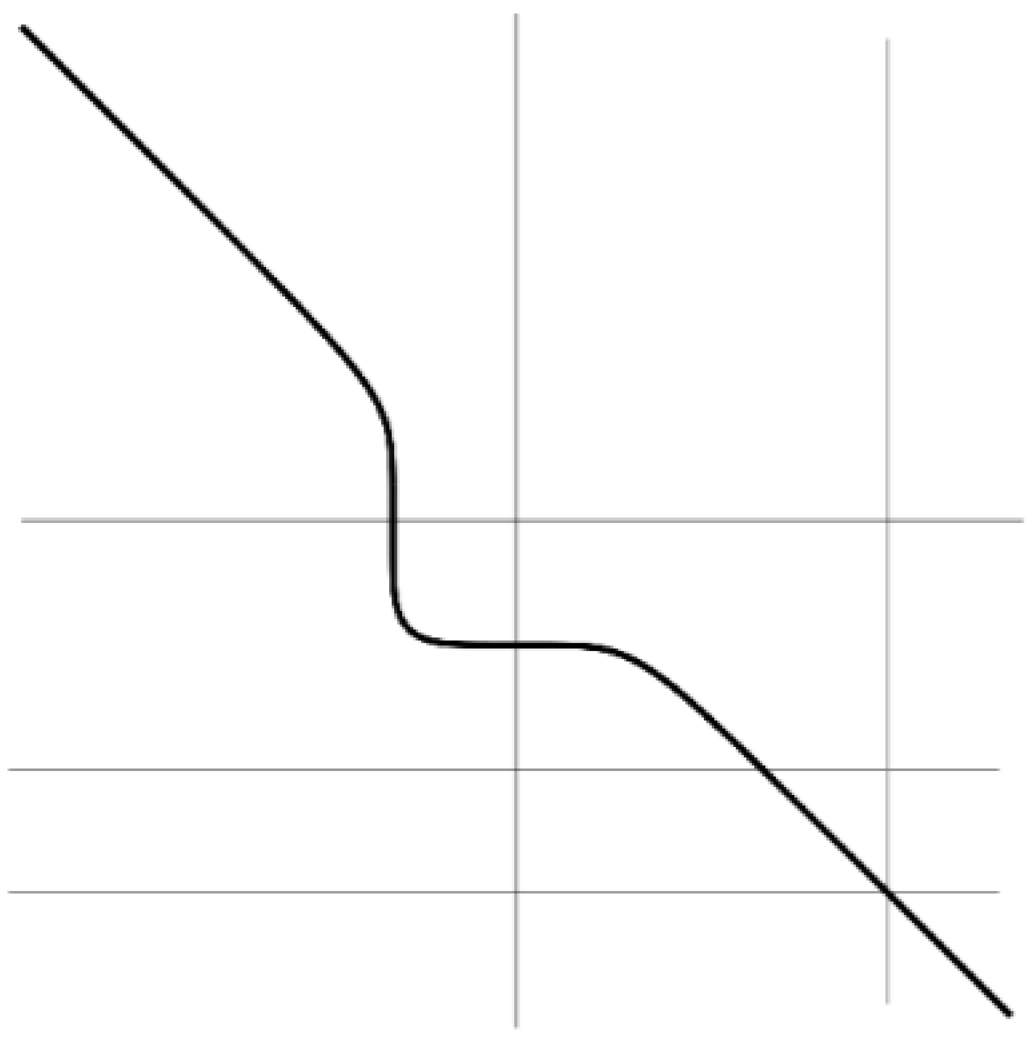




Specific example $n \in \mathbb{Z}$, $n \geq 4$

$$F = X^n + Y^n + Z^n, \quad C = V_+(F)$$

$k = \mathbb{R}$, $n = 5$



Fermet's last theorem (Wiles's theorem, 1995)

Let $p>2$ be prime. Then

$$\underbrace{V_+(x^p+y^p+z^p)(\mathbb{Q})}_{\text{(a finite set by Faltings's theorem)}} = \{(0:1:1),\ (1:0:1),(1:1:0)\}$$

only the "trivial" (= obvious) solutions

What Wiles (and Taylor ...) showed:

Theorem Every elliptic curve E over $\mathbb{Q}$ is modular.

Previously, Ribet had shown (based on an idea of Frey) that this theorem (which had been conjectured by Taniyama, Shimura and Weil) implies "Fermat's last theorem".

roughly: assume E given by $Y^2=X^3-AX-B$ with $A,B\in\mathbb{Z}$

Saying that E is a modular amounts to a (very precise) regularity statement about the numbers

$$\#\{(x,y)\in\mathbb{F}_q\ ;\ y^2=x^3+Ax+B\}$$

(q any prime power)

Rmk This indicates that it will be useful to have a theory that does not only work over a single base field, but "over $\mathbb{Z}$".

The abc conjecture

$$n \in \mathbb{N}_{>0} \rightsquigarrow \overset{\text{"radical"}}{\mathrm{rad}(n)} = \prod_{\substack{p \mid n \\ \text{prime}}} p$$

<u>Conjecture</u> (Masser, Oesterlé) Let $\varepsilon > 0$.

There exist only finitely many triples (a,b,c) of coprime positive integers with $a+b=c$ and $c > \mathrm{rad}(abc)^{1+\varepsilon}$

<u>Example</u>. $3 + 125 = 128 = c > 30 = \mathrm{rad}(3 \cdot 125 \cdot 128)$

Variant:

<u>abc-conjecture, explicit form:</u>

Let $a,b,c \in \mathbb{Z}_{>0}$ be coprime with $a+b=c$.

Then $c \leq \mathrm{rad}(abc)^2$.

Equivalent:

<u>Conjecture</u> (Szpiro) For every $\varepsilon > 0$ there ex. $C > 0$ s.t.:

For all $A, B \in \mathbb{Z}$ with

(a) $4A^3 + 27B^2 \neq 0$ (so $Y^2 - (X^3 + AX + B)$ defines an elliptic curve $/\mathbb{Q}$)

(b) there is no $u \in \mathbb{Z}$ s.t. $u^4 | A$, $u^6 | B$,

we have $\max(A^3, B^2) \leq C \cdot f^{6+\varepsilon}$,

where f is the conductor of the elliptic curve $V_+(Y^2Z - (X^3 + AXZ^2 + BZ^3))$

Here the conductor of the above elliptic curve is defined as $f = \prod_{p \text{ prime}} p^{f_p}$

where
$$f_p = \begin{cases} 0 & \text{if } p \neq 2,3 \text{ and } 4A^3 + 27B^2 \not\equiv 0 \bmod p \\ & \text{(ie. } Y^2 - (X^3 + AX + b) \text{ defines ell.c.} / \mathbb{F}_p) \\ 1 & \text{if } p \neq 2,3 \text{ and } V(Y^2 - (X^3 + AX + B)) \text{ has a node} \\ 2 & \text{if } p \neq 2,3 \text{ and } V(Y^2 - (X^3 + AX + B)) \text{ has a cusp} \\ \in \{0, 1, \ldots, 8\} & \text{if } p = 2 \text{ or } p = 3 \end{cases}$$

in this case the definition of f_p is more complicated...

The abc-conjecture is a very elementary statement. But it is very powerful. In fact it implies several famous (and famously difficult) theorems in number theory. For example:

Remark (the (above explicit version of the) abc-conjecture implies Fermat's Last thm).

Suppose there exist $n \in \mathbb{N}$ and positive integers x, y, z such that $x^n + y^n = z^n$.

Then
$$\underbrace{\mathrm{rad}(xyz)^2}_{\overset{\wedge}{z^6}} = \mathrm{rad}(x^n y^n z^n)^2 \underset{\overset{\uparrow}{\text{explicit abc}}}{\geq} z^n$$

$\rightsquigarrow n < 6$

But the cases $n = 3, 4, 5$ are (relatively) easy to check and have been known for a long time.

Problems with our approach so far

What we have discussed was not very systematic, but besides that, there are some further "defects". Some of them are easy to deal with, but for others a good solution is more involved.

So let us list some things that are needed / desirable.

- more systematic use of commutative algebra

- definition of morphisms (and hence isomorphisms) of sets of the form $V(f_1, \dots, f_m)$

  (Note that in the way we have phrased things, this only has a chance of working well over alg. closed fields k. In fact, over general fields, we may have $V_+(F) = \emptyset$ for 'many different' polynomials F.)

- theory which works well over non-alg. closed fields (or even over arbitrary commutative rings)

- attach a more transparent geometric meaning to intersection multiplicities $i_p(V_+(F), V_+(G))$ in Bézout's theorem.