$$Q(\underline{v}) = \sum_{i,j=0}^{n} X_{ij} v_i v_j, \quad X_{ij} = X_{ji} \ /\mathbb{F}; \quad \text{char } \mathbb{F} \neq 2$$

Diagonalization process

Step 1: by an invertible change of variables, can assume $X_{ii} \neq 0$

Step 2:

$$\sum_{i,j=0}^{n} X_{ij} v_i v_j = \underbrace{\frac{1}{X_{ii}}\Big(X_{ii} v_i + \sum_{i \neq j} X_{ij} v_j\Big)^2}_{\underbrace{X_{ii} v_i^2 + 2\sum_{i\neq j} X_{ij} v_j}_{\text{the only terms containing } v_i} + \sum_{j \neq i} \frac{X_{ij}^2}{X_{ii}} v_j^2} + \sum_{j,\ell \neq i} X'_{j\ell} v_j v_\ell$$

Step 3: now use induction

Lemma $B: V \times V \to \mathbb{F}$, $\dim V = 3$, B non-degenerate.
If $U \subseteq V$ is a 2-dimensional subspace, then $B|_U : U \times U \to \mathbb{F}$ cannot be identically 0.

Proof Suppose $B|_U \equiv 0$. Let $v \notin U$, consider $\langle \underline{v} \rangle^\circ = \{ \underline{w} \in V : B(\underline{v}, \underline{w}) = 0 \}$

$$B(\underline{v}, \underline{w}) = \underbrace{\underline{v}^t X}_{\neq 0} \underline{w}$$

(X matrix of $B \Rightarrow X$ invertible)

Then $\dim \langle \underline{v} \rangle^\circ = 2$, given by a single linear condition.

So $\dim(U \cap \langle v \rangle^\circ) \geq 1$; for any $\underline{w} \in U \cap \langle \underline{v} \rangle^\circ$, $\underline{w} \neq 0$,

but then $\forall\, \underline{w} \in U^\circ$, $\underline{w} \in \langle \underline{v} \rangle^\circ$, so $\underline{w} \in \langle U, \underline{v} \rangle^\circ = V^\circ$

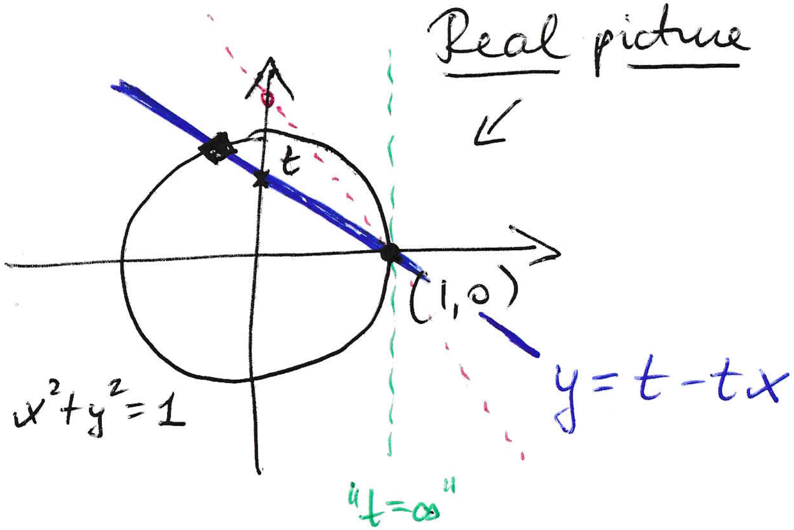
This contradicts the non-degeneracy of B.

$\square$

Concrete example $/\mathbb{F}$: "parametrize the unit circle over $\mathbb{F}$"

$$C = \{x^2+y^2=1\} \subseteq \mathbb{F}^2, \quad p=(1,0) \in C$$

Real picture



$$\left.\begin{aligned} x^2+y^2&=1 \\ y&=t-tx \end{aligned}\right\}$$

$$x^2+(t-tx)^2=1$$

$$x^2(t^2+1)-2t^2x+(t^2-1)=0$$

$$x_{1,2} = \frac{2t^2 \pm \sqrt{4t^4-(t^2+1)(t^2-1)}}{2(t^2+1)} = \frac{2t^2\pm 2}{2(t^2+1)}$$

$$= \begin{cases} 1 \\ t^2-1/t^2+1 \end{cases}$$

$\Rightarrow \quad (x,y) = (1,0)$ "expected" solution

$$(x,y) = \left(\frac{t^2-1}{t^2+1}, \frac{-2t}{t^2+1} \right)$$

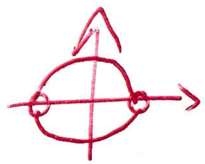
For $t = \infty$, we get $(1,0)$ again.

<u>Aside</u> (parametrize circle $/\mathbb{R}$)

$S^1 = \{x^2+y^2=1\}$ then • $(x,y) = (\cos\theta, \sin\theta)$ periodic, $S^1 = \mathbb{R}/2\pi\mathbb{Z}$

"topology"

• $y = \sqrt{1-x^2}$ bijection $(-1,1) \leftrightarrow$ upper semicircle, $\leftrightarrow$ lower semicircle



"analysis"

• $(x,y) = \left(\frac{t^2-1}{t^2+1}, \frac{-2t}{t^2+1} \right)$ bijection $\mathbb{R} \longleftrightarrow S^1 \setminus \{pt\}$

"affine algebraic geometry"

Over $\mathbb{F}$, can projectivize!

$$C_p = \{X^2+Y^2=Z^2\} \subset \mathbb{FP}^2$$
$$\begin{array}{c}\Psi\\ {[1:0:1]}\end{array}$$

Parameter t gets replaced by $[a:b]$, $t = a/b$ if $b \neq 0$.

We get:

$$[X:Y:Z] = [(a^2-b^2):(-2ab):(a^2+b^2)]$$

bijection $\quad \mathbb{FP}^1 \longleftrightarrow C_p$ projective conic (circle)

Aside (continued) bijection over $\mathbb{R}$

$$[X:Y:Z] = [(a^2-b^2):(-2ab):(a^2+b^2)]$$

$$\mathbb{RP}^1 \longleftrightarrow S^1$$

"projective algebraic geometry"

Application $\mathbb{F} = \mathbb{Q}$, in this case $\{x^2+y^2=1,\ x,y \in \mathbb{Q}\} \longleftrightarrow$ $t \in \mathbb{Q}$

$$(x,y) = \left(\frac{t^2-1}{t^2+1}, \frac{-2t}{t^2+1}\right)$$

$\longleftarrow$ obvious !

$\longrightarrow$

t = slope of line from $(1,0)$ to (x,y)

So $(x,y) \in \mathbb{Q}^2 \Rightarrow t \in \mathbb{Q}$

But also general theorem gives bijection

$$\mathbb{Q}\mathbb{P}^1 \longleftrightarrow C \subseteq \mathbb{Q}\mathbb{P}^2 \qquad (\mathbb{F} = \mathbb{Q})$$

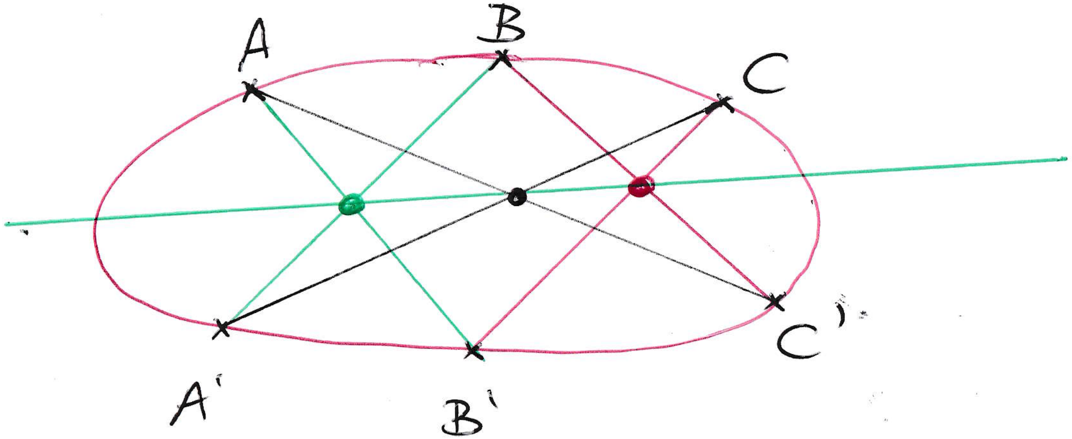
Now $a^2+b^2=c^2$ [redacted] over $\mathbb{Z}$, then $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$ over $\mathbb{Q}$, $\left(\frac{a}{c}, \frac{b}{c}\right) \in C$, and then $\frac{a}{c} = \frac{t^2-1}{t^2+1}$, $\frac{b}{c} = \frac{2t}{t^2+1}$, with $t = \frac{m}{n} \in \mathbb{Q}$.

Finally $\frac{a}{c} = \frac{m^2-n^2}{m^2+n^2}$, $\frac{b}{c} = \frac{2mn}{m^2+n^2}$, $\boxed{(a,b,c) = (m^2-n^2,\ 2mn,\ m^2+n^2)}$

Pascal's theorem Let $\mathcal{C}$ be a non-degenerate conic in $\mathbb{FP}^2$.

Let (A, B, C) and (A', B', C') be two triples of points on $\mathcal{C}$.

Then $(AB' \wedge A'B)$, $(AC' \wedge A'C)$, $(BC' \wedge B'C)$ are collinear.



Instead of <u>non-degenerate conics</u>, could consider <u>line pairs</u>.

Then this becomes Pappus' theorem.

<u>Over $\mathbb{R}$</u>, non-degenerate conic in $\mathbb{RP}^2$ (with points) $\underset{PGL(3)}{\overset{\text{proj. equivalent}}{\longleftrightarrow}}$ unit circle $\subset \mathbb{R}^2 \subset \mathbb{RP}^2$

<u>Proposition</u> Pascal's theorem over $\mathbb{R}$ $\longleftrightarrow$ Pascal's theorem in unit circle

This has elementary proof
based on angles, triangles,
sine theorem.

Higher-degree plane curves $d \geq 3$

Note: $a^2+b^2=c^2$ ∞ly many solutions

$a^3+b^3=c^3$ only the trivial solutions

$\vdots$

Fact (not hard to prove for $d=3$)

There do not exist polynomials (for $d \geq 3$) [redacted]
[redacted] $p(t), q(t), r(t) \in \mathbb{F}[t]$ such that

$$p(t)^d + q(t)^d = r(t)^d$$

Equivalently, no non-constant rational functions

$$\left(\frac{p(t)}{r(t)}\right)^d + \left(\frac{q(t)}{r(t)}\right)^d = 1$$

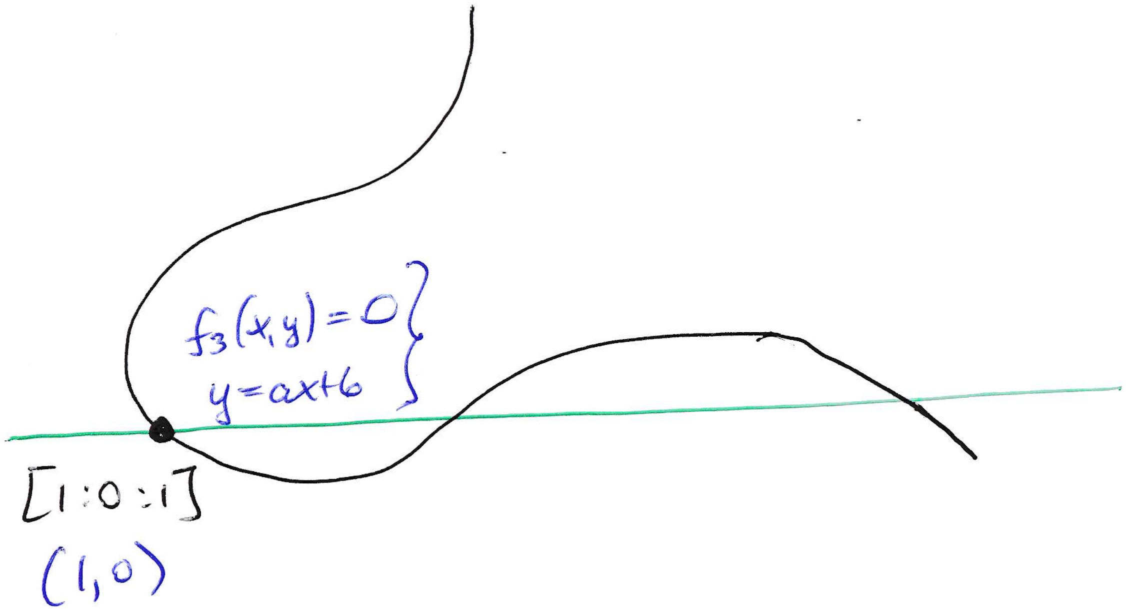
Geometrically this means: there is no polynomial parametrization of

- $\{x^d+y^d=1\} \subset \mathbb{F}^2$ by [redacted] $t \in \mathbb{F}$
- $\{X^d+Y^d=Z^d\} \subset \mathbb{P}\mathbb{F}^2$ by $\mathbb{F}\mathbb{P}^1$.

How much of "elementary" projective geometry survives? Some for $d=3$.

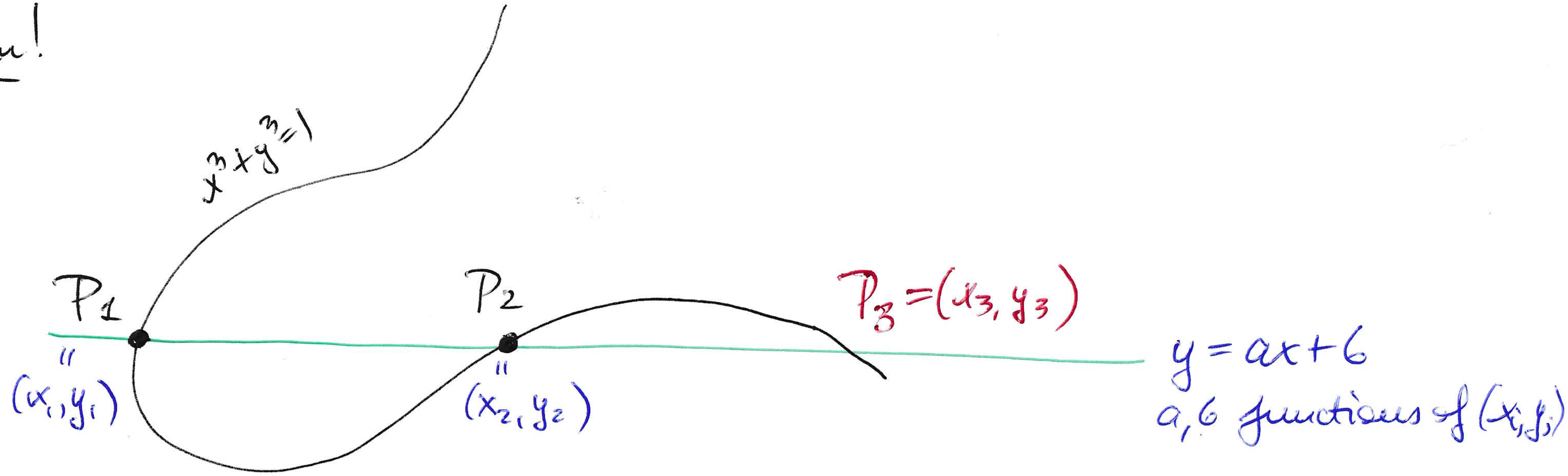
Consider $\{ f_3(X,Y,Z) = 0 \} \subset \mathbb{FP}^2$.

e.g. $X^3 + Y^3 - Z^3 = 0$



(one point, one line) $\Longrightarrow$?

Try again!



$P_1, P_2 \in \mathbb{F}^2 / \mathbb{FP}^2$. Consider $L = P_1 P_2$ projective line.

For intersection $\left\{ \begin{array}{l} y = ax + b \\ x^3 + y^3 = 1 \end{array} \right\} \Rightarrow$ cubic for x with <u>two</u> known roots (x_1, x_2),

and a <u>third</u> root $x_3 =$ rational expression (x_1, x_2, y_1, y_2)

$y_3 = \ldots.$

Get a "machine": given $(P_1, P_2) \in C \subset \mathbb{FP}^2$, get $P_3 \in C \subset \mathbb{FP}^2$.

<u>the operation</u>: $(P_1, P_2) \longrightarrow P_3$

We get an <u>abelian group structure</u> on points of $C \subset \mathbb{FP}^2$.

$$(P_1, P_2) \longmapsto P_3 = P_1 \boxplus P_2$$

(lying here a little bit)

$\Longrightarrow$ Cubic curve cryptography