Aplikace Bézoutovy věty

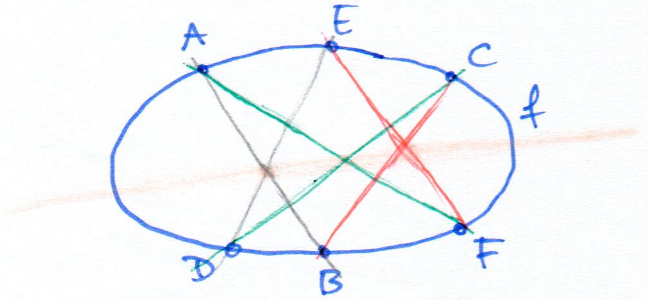
1) Pascalovo hexagrammum mysticum (1639, důkaz později)

(je to v zásadě hříčka, ale důležité je pochopit důkazovou techniku)

Věta: f kvadrika (tj. polynom st. 2), ireducibilní (tj. ne sjednocení dvou přímek)

A, B, C, D, E, F 6 různých bodů na f

$\Rightarrow$ body $AB \cap DE$, $EF \cap BC$, $CD \cap AF$ leží na přímce



[Pozn.: platí projektivně, tj. včetně případu $AB \parallel DE$ apod.]

[Pořadí bodů libovolné, průsečíky mohou být venku, ...]

Důkaz: $g :=$ součin přímek AB, CD, EF
$h :=$ součin přímek DE, BC, AF } formy stupně 3

projektivních!

zvol $P \in V(f)$, $P \neq A, \dots, F$

zvol λ t.ž. $k := g + \lambda h$ má nulu v bodě P ... $\lambda := -\frac{g(P)}{h(P)}$

k je forma st. 3, nuluje se i v $A, \dots, F$
i v těch třech průsečících

$\leadsto$ čili $|k \cap f| = 7$ $\not\Rightarrow$ SPOR s Bézoutem!

$\xRightarrow{\text{Bézout}}$ k, f mají společnou komponentu
ALE: f je ireducibilní } $\not\Rightarrow$ SPOR
$\Rightarrow$ společ. komp. je celé f

$\Longrightarrow$ $k = f \cdot l$ pro nějakou formu l st. 1

Čili $V(k) = V(f) \cup \underbrace{V(l)}_{\text{přímka}}$, ty tři průsečíky – leží na k
– neleží na f
$\Rightarrow$ leží na l $\square$

2) Cayley-Bacharachova věta (1886)

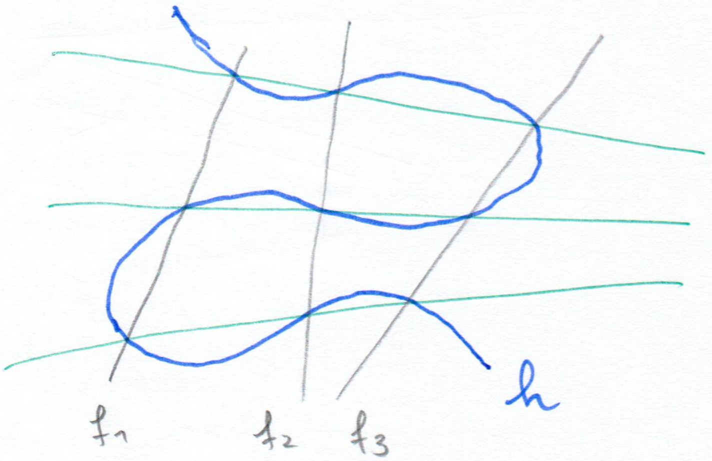
Věta: (v $\mathbb{P}^2 K$) f, g kubické křivky (projektivní!) – bez společné komponenty
– jednoduchá křížení $A_1, \dots, A_9$

h kubická křivka obsahující $A_1, \dots, A_8$

$\Rightarrow$ h obsahuje také A_9 & navíc $h = \lambda f + \mu g$ pro nějaká $\lambda, \mu \in K$

Speciální případ: Lemma o devíti bodech:

uvažujte f, g, které jsou součiny tří přímek, tj. 3x3 mříž

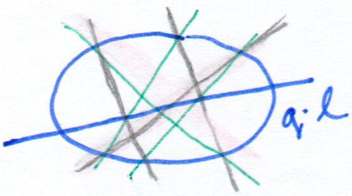


$f = f_1 \cdot f_2 \cdot f_3$

$g = g_1 \cdot g_2 \cdot g_3$

h prochází osmi body
$\Rightarrow$ i tím devátým

Důsledky: – Pascalův hexagram:



$f_{1,2,3}$ = jedna trojice přímek

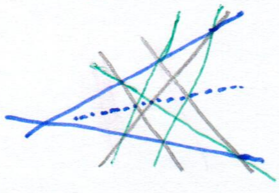
$g_{1,2,3}$ = druhá trojice přímek

$h = q \cdot l$

daná kvadrika ... přímka procházející dvěma průsečíky

$\Rightarrow$ i ten třetí průsečík tam leží, $\notin q \Rightarrow \in l$

– Pappova věta: to samé, ale q = součin dvou přímek
(~300 BC)



– původní důkaz vyžadoval q ired.
– argument výše to nepotřebuje!

– asociativita grupové operace na eliptických křivkách

Důkaz Lemmatu o 9 bodech:

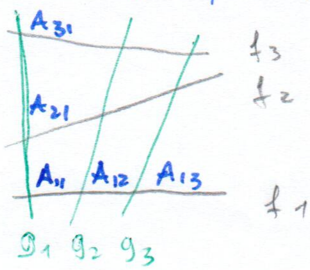
značení: $f = f_1 \cdot f_2 \cdot f_3$

$g = g_1 \cdot g_2 \cdot g_3$ kde $f_{1,2,3}$, $g_{1,2,3}$ po dvou různé přímky

$A_{ij} := f_i \cap g_j$

nechť h obsahuje A_{ij} $\forall (i,j) \neq (3,3)$

BÚNO: $f_1 = y$, $g_1 = x$ ... lze docílit projetivní změnou souřadnic



... $f(0,y)$ je poly. st. 3, má za kořeny y-ové souřadnice bodů A_{11}, A_{21}, A_{31}

ale $h(0,y)$ taky!

$\Longrightarrow$ $f(0,y) \,\|\, h(0,y)$ v $K[y]$

čili $h(0,y) = \boxed{\mu \cdot f(0,y)}$ pro něj. $\mu \in K$

... $g(x,0)$ je poly. st. 3, má za kořeny x-ové souřadnice bodů A_{11}, A_{12}, A_{13}

ale $h(x,0)$ taky

$\Longrightarrow$ $h(x,0) = \lambda \cdot g(x,0)$ pro něj. $\lambda \in K$

? $h = \mu \cdot f + \lambda \cdot g$?

... označ $k := h - \mu f - \lambda g \overset{?}{=} 0$ ... nuluje se ve všech A_{ij}, $(i,j) \neq (3,3)$

... $k(0,y) = \underbrace{h(0,y) - \mu f(0,y)}_{=0} - \lambda \underbrace{g(0,y)}_{=0\text{, protože } x \mid g}$

$\Rightarrow$ $x \mid k$

... analogicky: $y \mid k$

$\Rightarrow$ $k = x \cdot y \cdot l$, ale: • k obsahuje všechny A_{ij}, $(i,j) \neq (3,3)$

st. ≤ 3 $\Rightarrow$ st. ≤ 1 • A_{22}, A_{23}, A_{32} nenuluje x ani y

$\Rightarrow$ nuluje je l $\Big\}$ $\Rightarrow$ $l = 0$

ale ony neleží na přímce

3) Grupová operace na eliptické křivce

eliptická křivka $\equiv$ $y^2 = x^3 + ax + b$ t.ž. neobsahuje singulární body

$E_f := (V(f), +, -, O)$ kde O je libovolně zvolený bod

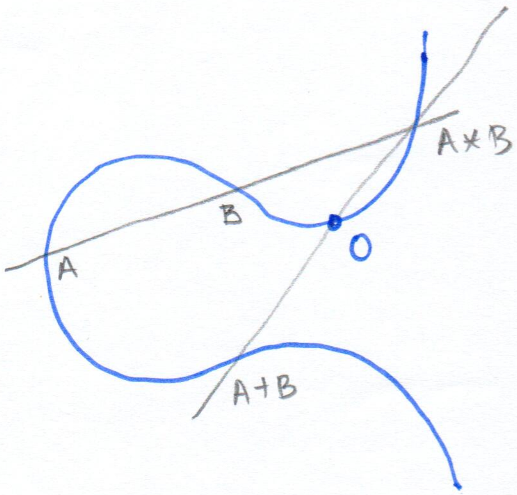
$$-A = (O * O) * A$$

$$A+B = O * (A * B)$$

kde $A * B$ = ten třetí bod v průniku $AB \cap f$ (Bézout!)
$(A+B)$

$A * A$ = ten ~~druhý~~ třetí bod na (jednoznačně určené) tečně v bodě A k f

($I_A(f \cap t) = 3 \Rightarrow A * A = A$, jinak t obsahuje jiné B)



$*, +$ jsou komutativní
... je to jen o přímce AB, resp. tečně v A

$$O + A = O * \underbrace{(O * A)}_{\text{ten třetí na } OA} = A$$

$$A + (-A) = O * (A * (-A))$$
$$= O * \underbrace{(A * ((O * O) * A))}_{O * O} = O$$

? asociativita ?

Pozn.: v kanonickém tvaru $y^2 = x^3 + ax + b$ je křivka symetrická podle osy x, obsahuje bod $[0:1:0]$ v nekonečnu

$\leadsto$ zpravidla se volí $O = [0:1:0]$

$\Rightarrow$ $O * O = O$ & ($-A$ = reflexe bodu A podle osy x

Důkaz asociativity :

$$? \quad A+(B+C) = (A+B)+C \quad ?$$

$\rightsquigarrow$ stačí $? \; A*(B+C) = C*(A+B) \; ?$

... uvažuj průsečík přímek $A(B+C) \cap C(A+B) =: X$

$? \; X$ leží na křivce f ? ... pak je to nutně výsledek obou operací $*$

Lemma o 9 bodech :

$f_1 = AB \qquad f_2 = O(B*C) \qquad f_3 = C(A+B)$

$g_1 = BC \qquad g_2 = O(A*B) \qquad g_3 = A(B+C)$

... na eliptické křivce leží určitě 8 z devíti průsečíků :

$$\begin{array}{cccccccc}
A, & B, & C, & A*B, & B*C, & O, & A+B, & B+C \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
f_1\cap g_3 & f_1\cap g_1 & f_3\cap g_1 & f_1\cap g_2 & f_2\cap g_1 & f_2\cap g_2 & f_3\cap g_2 & f_2\cap g_3
\end{array}$$

$\Rightarrow$ leží tam i ten devátý, tj. X

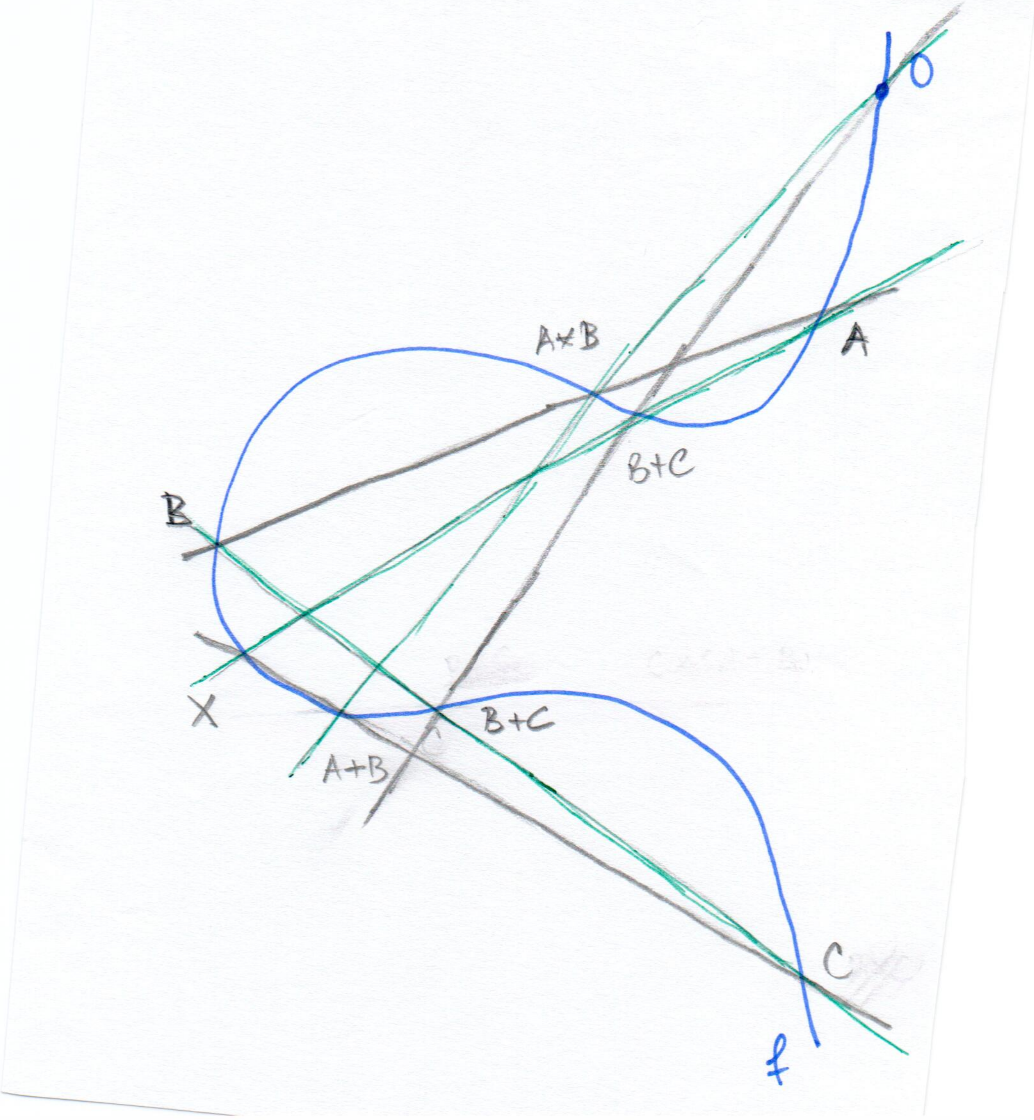
Pozn.: Často se uvažují grupy $E_f(K)$ pro různá K $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \dots)$

... Idea: A, B mají souřadnice v $K \Rightarrow A*B$ taky

$\rightsquigarrow$ využití v teorii čísel $(K=\mathbb{Q})$

v kryptografii $(K=\mathbb{F}_q)$

↳ Pozor! nemám Bézouta, takže není jistota, že je $*, +$ dobře def.



O
A*B
A
B+C
B
X
B+C
A+B
C
f