# CURVAS ELÍPTICAS E LEI DE GRUPO:

## → Integrais:

- Consideremos a circunferência unitária, existem duas estruturas de grupo equivalentes:

  - multiplicação em $\mathbb{C}$, $\{z \in \mathbb{C} : |z| = 1\}$, $(u,v) = e^{i\theta}$, (maneira algébrica)

  - Adição em $(\mathrm{mod}\ 2\pi)$; (maneira analítica).

- define-se $(u,v) = (u,-v)$, $id = (1,0)$, na versão algébrica;
  ↑ reflexão

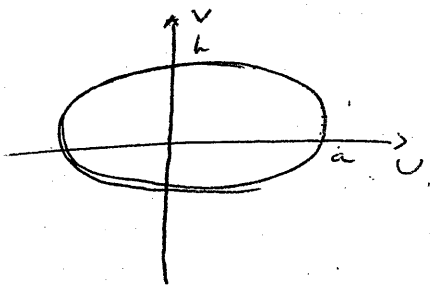
  $(u,v)\cdot(u',v') = (uu' - vv',\ uv' + vu')$;

- De uma maneira analítica, seja $\Theta(u,v) = \int_1^u \frac{1}{\sqrt{1+x^2}}\,dx$,

  se $I(t) = \int_1^t \frac{1}{\sqrt{1+x^2}}\,dt$, e de alguma modo

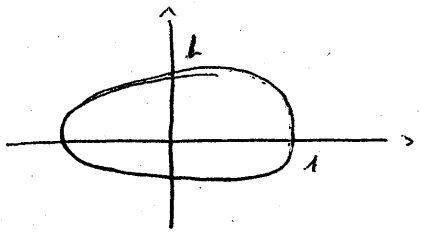
  conseguirmos inverter $I(t)$ obtemos um cos, ficando assim parametrizada a circunferência;

- Consideremos agora a elipse e o seu comprimento de arco;



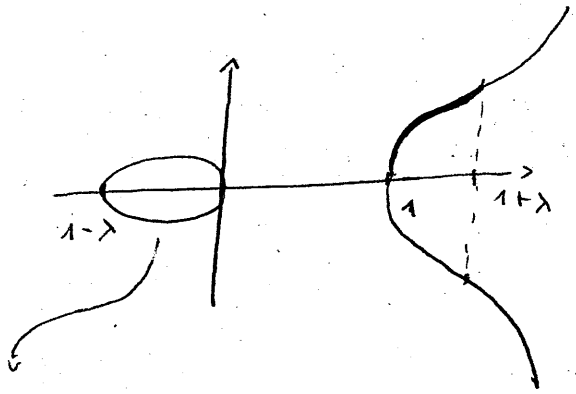

$\frac{u^2}{a^2} + \frac{v^2}{b^2} = 1$, com $0 < b < a$, $b, a \in \mathbb{R}$.

• fazendo a transformação $x \mapsto \frac{1}{a}$ de modo a obter




$0 < k < 1$, $k \in \mathbb{R}$.

• uma circunferência é o integral ao longo de




$k = \sqrt{1-k^2}$

$\lambda = \left(\frac{1+k}{1-k}\right)^2 > 1$

$y = \pm \sqrt{x(x-1)(x-(1-\lambda))}$

• O estudo destes integrais levou à descoberta que as curvas $\left(y^2 = x(x-1)(x-(1-\lambda))\right)$ têm uma lei de grupo, algébrica e analítica.

Notação

• <u>Nota</u>: o grupo analítico é melhor observado nas soluções de $y^2 = x(x-1)(x-(1-\lambda))$;

• Vamos assim estudar o grupo "algébrico" das curvas $y^2 = x(x-1)(x-(1-\lambda))$, de modo a relacionar o que foi visto em Lectura 1;

## → Curvas elípticas:

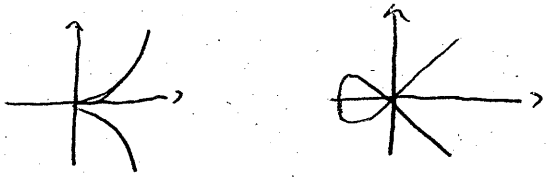
• Seja $\mathbb{K}$ um corpo de característica diferente de 2 ou 3; Admitamos que existe $L$ corpo t.q $\mathbb{K} \subseteq L$ e $L$ é algebricamente fechado ($\mathbb{K}$ é subcorpo de $L$; isto é, $\forall p \in \mathbb{K}[x]$, $\deg(p) = n \Rightarrow p$ tem $n$ soluções em $L$).

• Defina-se uma curva elíptica sobre $\mathbb{K}$ é o conjunto de soluções:

$$E = \{(x,y) \in L^2 : y^2 = F(x)\} \cup \{\infty\},$$

onde $F \in \mathbb{K}[x]$ e tem raízes distintas em $L$;

Ex:



$y^2 = x^3$ $\qquad$ $y^2 = x^2(x+1)$

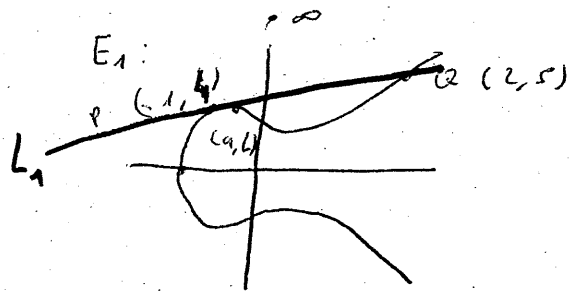
• Note-se que se $F$ tem raízes distintas, todo o ponto de $E$ tem uma "tangente";

• Estamos assim interessados em

$$E(\mathbb{K}) = \{(x,y) \in E : x, y \in \mathbb{K}\} \cup \{\infty\}.$$

• Vejamos a título de exemplos,

$E_1 = (y^2 = x^3 + 17)_{/\mathbb{Q}}$ e $E_2 = (y^2 = x^3 - 25x)_{/\mathbb{Q}}$




$L_1 : y = \frac{x}{3} + \frac{13}{3}$

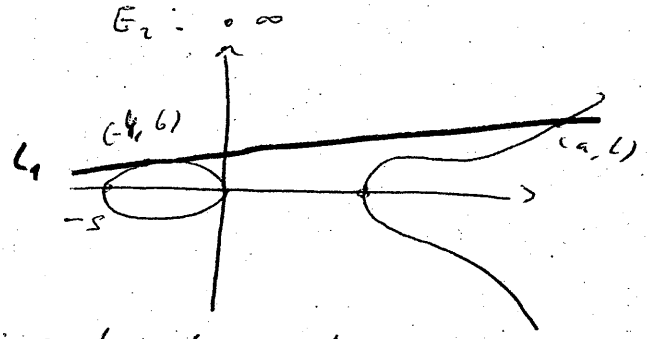
$\left(\frac{x}{3} + \frac{13}{3}\right)^2 = x^3 + 17$, logo

$0 = x^3 - \frac{x^2}{9} + (\dots) =$

$= (x+1)(x-2)(x-a) \Rightarrow$

$\Rightarrow a = -\frac{8}{9}$,

utilizando $L_1$, $h = \frac{109}{27}$




$L_1$ - recta tangente,

$y = \frac{23}{12}x + \frac{41}{3}$, note-se que sempre que se toma uma recta tangente, a raiz é dupla;

$\left(\frac{23}{12}x + \frac{41}{3}\right)^2 = x^3 - 25x \Leftrightarrow$

$\Leftrightarrow 0 = x^3 - \left(\frac{23}{12}\right)^2 x^2 + (\dots) \Leftrightarrow$

$\Leftrightarrow (x+4)^2(x-a) \Rightarrow a = \frac{41^2}{2^4 \times 3^2}$,

recorrendo a $L_1$,

$h = \frac{41 \times 1519}{2^6 \times 3^3}$;

- Note-se que a recta tangente é vista de um ponto de vista puramente algébrico;

- Seja $E \cap \overline{PQ} = \{P, Q, R\}$, $P, Q \in E$, defina-se $P \oplus Q = (a, -b)$, $R = (a, b)$; Prove-se que $\oplus$ é indutor uma estrutura de grupo comutativo, com inverso $(x, y) \longmapsto (x, -y)$ e $\hat{0} = \infty$;

• Define-se $O = Id.(?)$.

• Ex $2P = P \oplus P = O \Rightarrow P = (x, 0) \iff x \in$ lhe pertence $F(x) = 0$ ;

$3P = P \oplus P \oplus P \iff 2P = -P$, $2P$ é $T_P(E)$ (tangente), vê-se onde a tangente intersecta E e faz-se um "flip"

$y^2 = x^3 + 16$, $P = (0, 4)$

$T_P(E) = \{ y = 4 \}$,

$4^2 = x^3 + 16 \Rightarrow x^3 = 0$

• Voltemos a considerar $E_1$ :

$(2, 5) \oplus (4, 9) = (-2, 3)$ ; $2(-1, 4) = \left( \frac{132}{64} ; \frac{-265}{512} \right)$

$(8, -23) \oplus (-2, 3) \oplus (2, -5) = (5\frac{1}{4}, 375)$

• Coloca-se assim a questão, $E_1(\mathbb{R})$ é finito ou infinito?
Se é infinito, o grupo é finitamente gerado?
Poderá $E_1(\mathbb{Z})$ ser finito?

~~Seria E~~

• Considera-se $E(\mathbb{F}_p)$, grupo finito, poderá este grupo "controlar" $E(\mathbb{R})$?