- Galois - theory (Artin)
- Representações de Grupos finitos (Serre).

- Três classes principais de corpos
  a) Number fields.
  b) Corpos finitos.
  c) Corpos de funções.

a) $K \subset \mathbb{C}$ $\mathbb{C}$ é uma extensão de K

$1 \in K$ $\Rightarrow$ $n \in K \ \forall n > 0$, $-n \in K \ \forall n \geq 0$ $\Rightarrow$ $\mathbb{Z} \subset K$

$\mathbb{Q} \subset K$

$\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\delta)$

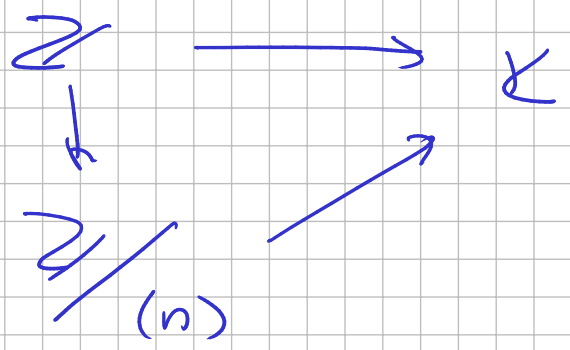
b) Corpos finitos:

$\varphi : \mathbb{Z} \longrightarrow K$ $\quad |K| < \infty \Rightarrow$

$1 \longmapsto 1 \in K$. $\quad \ker \varphi \neq 0$.

$\ker \varphi \subset \mathbb{Z}$ é um ideal

$\| \quad (n) \quad n \in \mathbb{Z}$.



K é corpo $\Leftrightarrow$ $n = p$ primo.

$\varphi : \mathbb{F}_p = \mathbb{Z}/(p) \longrightarrow K$

$\mathbb{Z}$

φ é injetivo. $K \in \mathbb{F}_p$-Vect.

Corpo finito. K é uma extensão $\mathbb{F}_p \subset K$

$\dim_{\mathbb{F}_p} K < \infty$.

Espaço vetorial. V / F é grupo Abeliano V,

$F \times V \longrightarrow V$. $\quad \alpha(v+w) = \alpha v + \alpha w$.

$\alpha, v \longmapsto \alpha \cdot v \quad (\alpha+\beta)v = \alpha v + \beta v$.

F corpo finito. $V \in F\text{-Vect}$.

$$\dim_F V < \infty \iff |V| < \infty.$$

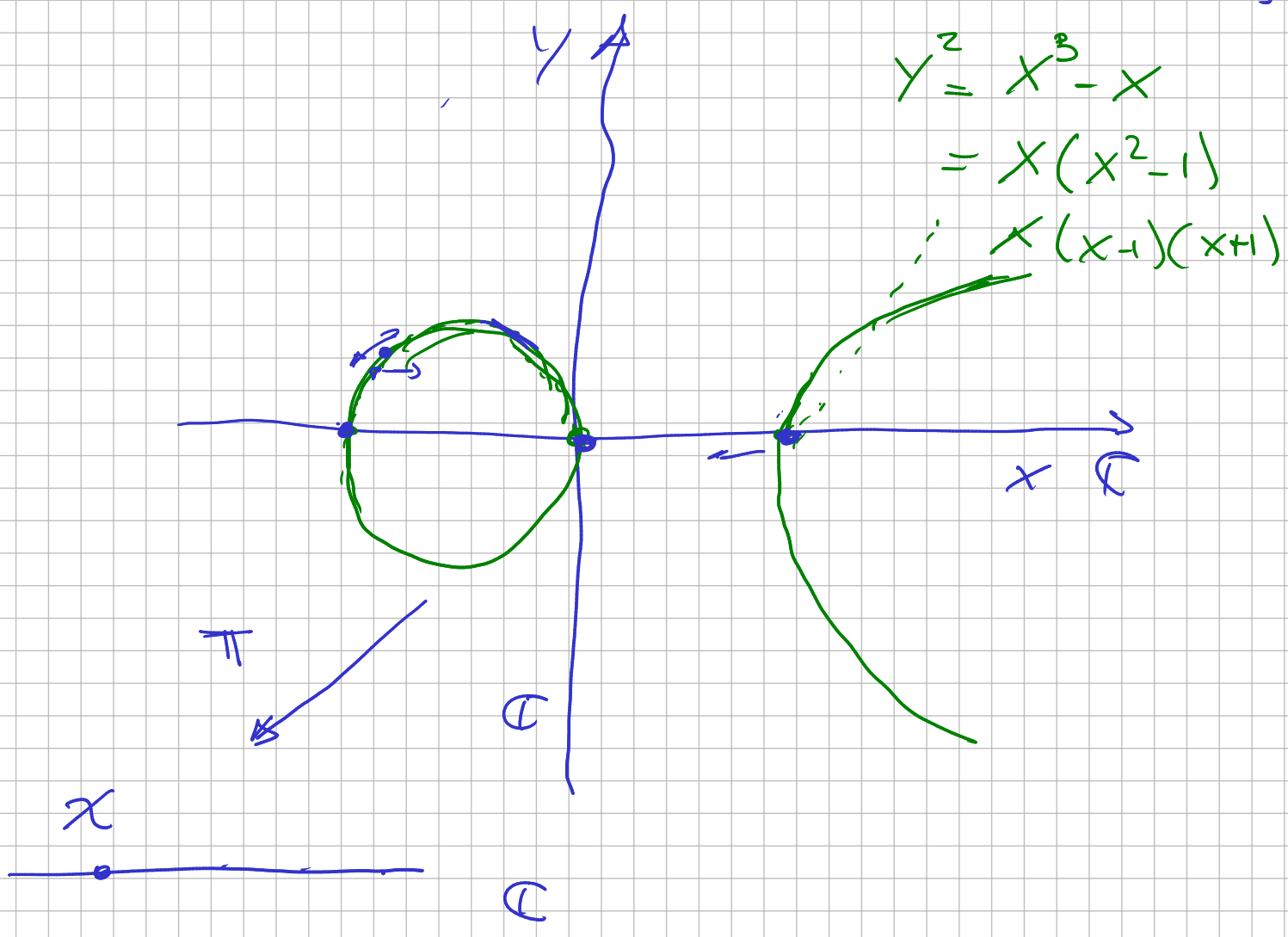
$$V \simeq F^{\oplus \dim V} \iff |V| = |F|^{(\dim V)}$$

---

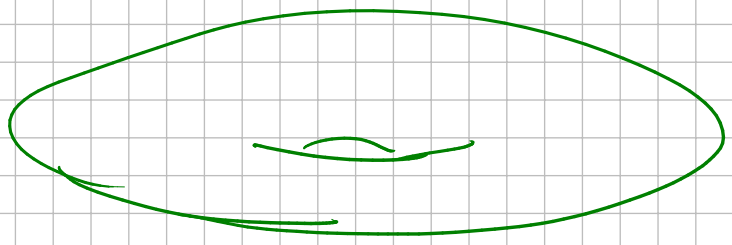
c) Corpos de funções

$$f \in \mathbb{C}[X, Y] \qquad f = Y^2 - X^3 + X$$

$$V(f) \subset \mathbb{C}^2 \qquad V(f) = \{ (x, y) \mid f(x, y) = 0 \}$$



$f(x,y)=0$ $\quad \begin{cases} \mathrm{Re} & f(x,y)=0 \\ \mathrm{im} & f(x,y)=0 \end{cases}$



$\mathbb{C}^2 = \mathbb{R}^4$

$\dim_{\mathbb{R}} V(f) = 2$. Superfície de Riemann.

$$\begin{array}{ccc} (x,y) & V(f) & \subset \mathbb{C}^2 \\ & \downarrow \pi & \\ x. & \mathbb{C} & \\ & \downarrow \varphi & \\ & \mathbb{C} & \end{array}$$

π é geralmente 2:1 exceto em $x = \pm 1, 0$ onde o mapa π é ramificado

$\pi^*(\varphi) := \varphi \circ \pi$.

(Funções em $\mathbb{C}$) $\longrightarrow$ (Funções em $V(f)$)

Funções racionais em $\mathbb{C}$.

$\mathbb{C}(x)$ = corpo de frações de $\mathbb{C}[x]$

$\mathbb{C}(x) = \left\{ \frac{P(x)}{q(x)} \;,\; P, q \in \mathbb{C}[x] \right\}$

$: V(f)$

$\swarrow$ 2:1

$f \in \mathbb{C}[x, y]$ dem lugar a uma extensão finita.

$\mathbb{C}(x) \longrightarrow K = \left(\begin{array}{c} \text{corpo de} \\ \text{funções} \\ \text{de } V(f) \end{array} \right)$

Em $V(f)$, posso expressar.

$y = y(x)$

$y^2 = x^3 - x \qquad y = \sqrt{x^3 - x}$

Pensar $f \in \mathbb{C}[x,y] \simeq (\underbrace{\mathbb{C}[x]}_{\| \; R})[y] = R[y]$

$f \notin R$. Imagine f irredutível.

$$V(gh) = V(g) \cup V(h).$$

$\Downarrow$

f é irredutível $F[y]$

$F =$ corpo de frações de R

$= \mathbb{C}(x)$

$$\frac{F[y]}{(f)} = K. \quad =: \text{"corpo de funções de } V(f)\text{"}$$

K é um corpo. Porque f é irredutível. (f) é um ideal primo. $\Rightarrow$ maximal.

$$\mathbb{C}(x) = F \subset K.$$

$V(f) \to \mathbb{C}$

$(y, x) \longrightarrow x$

2:1

$$\dim_F K = 2.$$

$$f = \underbrace{1}_{\in F} \cdot y^2 + \underbrace{(-x^3 + x)}_{\in F} y^0 \in F[y]$$

$K = F[Y]/(f)$ base de K como F-espaço vetorial está dada por $\{1, y\}$.

$$F[Y] \longrightarrow K$$
$$g \longmapsto g \bmod (f)$$

K é gerado pelas imagens de $\{1, y, y^2, \dots\}$ que é uma base de $F[Y]$ como F-vet.

$y^2 = x^3 - x \pmod f$

$\Rightarrow \{1, y\}$ base de K. $\square$

$\mathbb{C}(x) \subset K$ ext. $\dim_{\mathbb{C}(x)} K = 2$

$y \in K \setminus F$ satisfaz uma equação polynomial.

$$y^2 = x^3 - x$$

$F \subset K \Rightarrow \alpha$ que satisfaz.

$f(\alpha) = 0$ para algum

$$0 \neq f \in F[x]$$

é dito algébrico $F \subset K$

Uma extensão de corpos é algébrica se $\forall \alpha \in K$ é algébrico

$\mathbb{R} \subset \mathbb{C}$ é uma extensão algébrica

$\left.\begin{array}{l} \mathbb{Q} \subset \mathbb{R} \\ \mathbb{Q} \subset \mathbb{C} \end{array}\right\} \Rightarrow$ não são extensões algébricas.

$\pi, e \in \mathbb{R}$ não são algébricos.

i.e. são Transcendentes.

$F \subset K \quad \alpha \in K$.

$\varphi : F[x] \longrightarrow K \qquad x \longrightarrow \alpha$.

$\operatorname{im}\varphi = F[\alpha] \subset K$.

$F(\alpha)$ = corpo de frações de $F[\alpha]$ $\subset K$

$F \subset F(\alpha) \subset K$

$F[\alpha]$ é o menor subanel de K que contém F e α.

$F(\alpha)$ é menor subcorpo de K que contém F e α.

$f \in \operatorname{Ker}\varphi \subset F[x] \xrightarrow{\varphi} F[\alpha] \subset K$

$\operatorname{Ker}\varphi \neq 0$

$f \in \operatorname{Ker}\varphi \Rightarrow f(\alpha) = 0$.

$\Leftrightarrow \alpha$ é algébrico.

$\operatorname{Ker}\varphi = (f)$ → f é o único gerador mônico

f é dito o polynômio minimal de α.

f é irredutível.

$F(\alpha) = F[\alpha] = \operatorname{im}\varphi = F[x]/(f)$

$F(\alpha)$ é um corpo!

Corolário

$F \subset K \Rightarrow \alpha$ algébrico.

$\Rightarrow F[\alpha] = F(\alpha) \supset F$

Def $F \subset K$ o grau de K/F é $\dim_F K$.

se α é algébrico $F \subset F(\alpha)$ é finito. $\dim_F F(\alpha) = \deg(f)$

$1, \alpha, \alpha^2, \alpha^3, \ldots$

$f = x^{\deg f} + a_{\deg f - 1} x^{\deg f - 1} + a_{-2} \ldots + a_0$

$a_i \in F$ $f(\alpha) = 0 \Rightarrow$

$\alpha^{\deg(h)}$ é uma combinação linear de α^r $r < \deg h$ e coef. em F.

---

base de $F(\alpha)$ - $\{1, \alpha, \ldots, \alpha^{\deg h - 1}\}$

$F[x] \longrightarrow 1, x, \ldots x^{\deg h - 1}$

(h)

α é transcendente.

$\ker \varphi \hookrightarrow F[x] \xrightarrow{\varphi} K$

$0 \qquad\qquad x \longrightarrow \alpha$

$\dim = \infty$.

$F \subset F(x) \subset K$.

$F \subset F(\alpha) \subset K$ $\quad F(\alpha)$ = corp de Frações de $F[\alpha]$.

---

dim ∞.

$F \subset K$ não é algebrica.

$\dim_F K = \infty$.

$F \subset F(\alpha)$ é finito $\forall \alpha$.
α é algébrico.

$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \dots$

α algébrico.

$\mathbb{Q} \subset \mathbb{C}$

olhar. $\forall \sqrt[n]{s} \in \mathbb{R}$

$\alpha^n = s$

Pergunta) $\{ \alpha \in \mathbb{C}$ algébricos sobre $\mathbb{Q} \}$

é uma extensão algébrica

$\mathbb{Q} \subset K$

Pergunta $\underbrace{\mathbb{Q} \subset K}_{\text{dimensão } \infty} \subset \mathbb{R}$

algébrica.

Thiago ✓
acha que não.

Pergunta: $F \subset \mathbb{R}$

algébrico não enumerável.

Pergunta: ~~$\mathbb{R} \subset K \subset \mathbb{C}$~~

~~algébrico~~ infinito ?

$(\alpha_1, \ldots, \alpha_n)$ $\beta_1, \ldots \beta_m$ K-base

$F \subset K \subset L$

$$\dim_F L = \left(\dim_K L\right) \cdot \left(\dim_F K\right)$$

$$[L : F] = [L : K] \cdot [K : F]$$

então $\forall$ elemento de L.

$\ell = \sum_{i=1}^{m} \lambda_i \beta_i$ único.

$\lambda_i \in K$.

Como $\lambda_i \overset{!}{=} \sum_{j=1}^{n} (\lambda_{ij}) \alpha_j$ com $\lambda_{ij} \in F$

$\therefore \quad \ell = \sum (\lambda_{ij})(\alpha_j \cdot \beta_i)$

$\Rightarrow \{\alpha_i \beta_j\}$ são uma base de L como F-vect

$$\dim_F L = n \cdot m \qquad \square$$

$F \subset K$ finita α algébrico.

$\deg f_\alpha$ divide $[K:F]$.

heluani@potuz.net

Lectura 2: $F \subset K \subset L$

$$(*) \quad [L:F] = [L:K] \cdot [K:F]$$

$F \subset K \Rightarrow \alpha$ α algébrico.

$f_\alpha \in F[x]$ o polinômio minimal

- $[F[\alpha]:F] = \deg f_\alpha$
- $\deg f_\alpha \mid [K:F]$

se $[K:F]$ é finita então.

é algébrica e $\deg f_\alpha \mid [K:F]$

$\forall \alpha \in K$.

$[K:F] = p \in \mathbb{Z}_+$ p primo.

$\forall \alpha \in K \setminus F \quad F \subset F[\alpha] \subset K$

p

$[F[\alpha] : F] \mid p$

$\Downarrow$

$[F[\alpha] : F] = p \Rightarrow F[\alpha] = K.$

Pergunte do Caio: $\alpha \in K$ é algébrico

$F[\alpha] = F(\alpha) \subset K$

$\Vert$

é um corpo.

$\varphi : F[x] \longrightarrow K \qquad x \longmapsto \alpha$

$\ker \varphi = (f_\alpha) \qquad \operatorname{im} \varphi = F[\alpha] \subset K$

12

$F[x]/(f_\alpha)$

f_α irredutível. $\Rightarrow F[x]/(f_\alpha)$

é um corpo!

Categoria de extensões de F.

$F \subset K$

$K \xrightarrow{\varphi} K'$

$\cup \quad \circlearrowleft$

F

morfismos corp. fixando F.

Dadas duas extensões, quando são isomorfas?

$F \subset K$, α transcendente

$F[x] \xhookrightarrow{\varphi} K$ φ é injetiva.

K
$\cup$
$F[\alpha] = \operatorname{im}\varphi \cong F[x]$

$\Rightarrow F(\alpha) \simeq F(x)$

Cor. $\alpha, \beta \in K$ transcendentes.

$F(\alpha) \simeq F(\beta)$
$\cup \quad \cup$
F

$\pi, e \in \mathbb{R} \setminus \mathbb{Q}$

$\mathbb{R} \supset \mathbb{Q}(\pi) \simeq \mathbb{Q}(e) \subset \mathbb{R}$

Para extensões algébricas.

$K \simeq K'$ $\Rightarrow \dim_F K = \dim_F K'$
$\cup \quad \cup$
F

$[K:F] = [K':F]$

Observação: um morfismo de extensões $K \xrightarrow{\varphi} K'$ é um morfismo de corpos $a \to \varphi(a)$ tq $\varphi|_F = id_F$.

Converse teorema anterior é falso: $\mathbb{Q}(\delta)$ extensões quadráticas não são isomorfas.

Proposição Toda extensão quadrát. de F (char $\neq 2$!) é isomorfa a $F(\delta)$ onde $\delta^2 \in F$ e $\delta \notin F$.

$F \subset K \quad \delta \in K \setminus F \quad \delta^2 \in F$

$\Rightarrow F[\delta] = F(\delta) \supset F \quad x^2 - \delta^2$

$\uparrow$

extensão de grau 2.

Convera Suponha que

$F \subset K$ é de grau 2.

$\{1, \alpha\}$ base de K/F.

$\alpha \in K \setminus F$.

$2 < [F[\alpha] : F] \mid [K : F] = 2$

$\Rightarrow [F[\alpha] : F] = 2$

$F[\alpha] = K \quad \forall \alpha$.

$f_\alpha = x^2 + b \cdot x + c$

$(*) \quad \alpha^2 + b \cdot \alpha + c = 0$

$\boxed{\alpha(\alpha + b) = -c}$

Claim. $(2\alpha + b)^2 \in F$.

$4\alpha^2 + 4\alpha b + b^2 = 4\alpha(\alpha + b) + b^2$

$= -4c + b^2 \in F$.

$\delta := 2\alpha + b \in K \setminus F$.

$\Rightarrow \delta \in K \setminus F \quad \delta^2 \in F$

$F[\delta] = F[\alpha] = K$. $\square$.

$\frac{1}{2}\left(-b + \sqrt{b^2 - 4c}\right)$]

char F | $[K:F]$ coisas extranhas acontecem

$\mathbb{Q}$, $\sqrt[3]{2}$, $\sqrt[4]{5}$

α , β

$\alpha \in \mathbb{R}$, $\beta \in \mathbb{R}$

$x^3 - 2$

$x^4 - 5$

gr. 3 , gr. = ? = d'

$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \beta) \subset \mathbb{R}$

4

$\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha, \beta) \subset \mathbb{R}$

d' = gr. = ?

L

$[L:\mathbb{Q}] = ?$

$d \cdot 3 = d' \cdot 4 = [L:\mathbb{Q}]$

12) $[L:\mathbb{Q}]$

$\beta \notin \mathbb{Q}(\alpha)$

β é algébrico $\mathbb{Q}(\alpha)$

$x^4 - 5$ tem coef. em $\mathbb{Q}(\alpha)$

$\Rightarrow d \leq 4 \Rightarrow d = 4$

$[L : \mathbb{Q}] = 8$

$$\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha, \beta)$$

d' sobre $\mathbb{Q}$; α sobre $\mathbb{Q}(\beta)$

$\alpha \notin \mathbb{Q}(\beta)$

$x^3 - 2$ $\quad 1 < d_1' \leq 3$

Teorema $F \subset K$, $\overline{F} := \{\alpha \in K \mid \alpha \text{ algébrico sobre } F\}$ é um corpo

$\alpha, \beta \in \overline{F} \quad \alpha + \beta \in \overline{F}$.

α é algébrico / F. β é algébrico sobre $F(\alpha)$.

finito finito

$F \subset F(\alpha) \subset F(\alpha, \beta)$.

finito $\Rightarrow F \subset F(\alpha, \beta)$

é algébrico. $\Rightarrow$ $\alpha+\beta$, $-\alpha$, $\alpha\cdot\beta$, β^{-1}, α^{-1} $\Big\}$ $F(\alpha,\beta)$ são algébricos.

$\cap$

F. $\quad\cdot\quad$ Π

$\alpha=\sqrt{a}$ $\quad\beta=\sqrt{b}$. $\quad a,b\in F$.

$\alpha^2=a$ $\quad\beta^2=b$. $\quad x^2-a$ $\quad x^2-b$

$P(\alpha+\beta)=0$?

$\gamma=\alpha+\beta$

$2\alpha\beta=\gamma^2-(a+b)$

$\gamma^2=\alpha^2+2\alpha\beta+\beta^2=2\alpha\beta+(a+b)$

$\gamma^4=4\alpha^2\beta^2+4(a+b)\cdot\alpha\beta+(a+b)^2$

$=4ab+(a+b)^2+4(a+b)\cdot\alpha\beta$

$2\cdot(a+b)\,(\gamma^2-(a+b))$

$\gamma^4-2(a+b)\cdot\gamma^2=4ab+(a+b)^2-2(a+b)^2$

$\gamma^4-2(a+b)\gamma^2+\left[(a+b)^2-4ab\right]=0$

$(a-b)^2$

$\gamma^4-2(a+b)\gamma^2+(a-b)^2=0.$

$\alpha, \beta \in K$ algebricos. f_α f_β os minimais em $F[x]$. d_α d_β

$F(\alpha)$ tem como base.

$\{1, \alpha, \ldots, \alpha^{d_\alpha - 1}\}$

$F(\beta)$ $\{1, \beta, \ldots, \beta^{d_\beta - 1}\}$

$F(\alpha, \beta)$ é gerado

γ^k

$\{\alpha^i \beta^j\}$ $0 \le i \le d_\alpha - 1$

$0 \le j \le d_\beta - 1$

$\{1, \gamma, \gamma^2, \ldots, \gamma^{d_\alpha \cdot d_\beta - 1}\}$, $\gamma^{d_\alpha \cdot d_\beta}$

$\gamma^{d_\alpha \cdot d_\beta}$ é combinação linear de $1, \gamma, \gamma^2 \ldots, \gamma^{d_\alpha \cdot d_\beta - 1}$

$\Downarrow$

Isso dá um polynomio ϕ c/ f. em F tem γ como raiz.

Porém não necessariamente o polynômio minimal de γ.

Teorema $F \subset K \subset L \Rightarrow F \subset L$ é algeb.
(K alg., L alg.)

$\alpha \in L$. quero ver que é algébrico sobre F.

$$X^n + a_{n-1}X^{n-1} + \dots + a_0.$$

com $\{a_{n-1}, \dots, a_0\} \subset K$.

cada um dos $a_i \in K$ é algébrico sobre F.

$$F \subset F(a_0) \subset F(a_0, a_1) \dots \subset F(a_0, \dots, a_{n-1})$$

finita $\Rightarrow$ algébrica

$$F \subset F(a_0, \dots, a_{n-1}) \subset F(\alpha, a_0, \dots, a_{n-1})$$

é finita.

$\Rightarrow \alpha$ é algébrico sobre F. □.

$\alpha, \beta \in K$ algébricos sobre F.

$\gamma \in F(\alpha, \beta)$ (eg. $\gamma = \alpha + \beta$).

$$F(\alpha,\beta) = F[\alpha,\beta] \overset{(*)}{=} \{\alpha^i \beta^j\} \quad \begin{matrix} 0 \le i < d_\alpha \\ 0 \le j < d_\beta \end{matrix}$$

$d_\alpha = \deg f_\alpha \qquad d_\beta = \deg f_\beta$.

$\gamma \in F(\alpha,\beta)$ se escreve como combi. linear de $(*)$. Com coeff. em F.

$n = d_\alpha \cdot d_\beta$.

$$\left.\begin{aligned} 1 = \gamma^0 &= \alpha^0 \cdot \beta^0 \\ \to \gamma &= \sum a^1_{ij}\, \alpha^i \beta^j \\ \gamma^2 &= \sum a^2_{ij}\, \alpha^i \beta^j \\ &\vdots \\ \gamma^{n-1} &= \sum a^{n-1}_{ij}\, \alpha^i \beta^j \end{aligned}\right\}$$

$\alpha = e^{2\pi i/5} \qquad \beta = e^{2\pi i/7}$

$\mathbb{Q}(\beta) \not\ni \alpha \qquad (1 + X + \dots + X^6)$

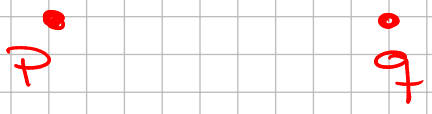
$\to (1 + X + \dots + X^4)$

$\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha, \beta) = L$

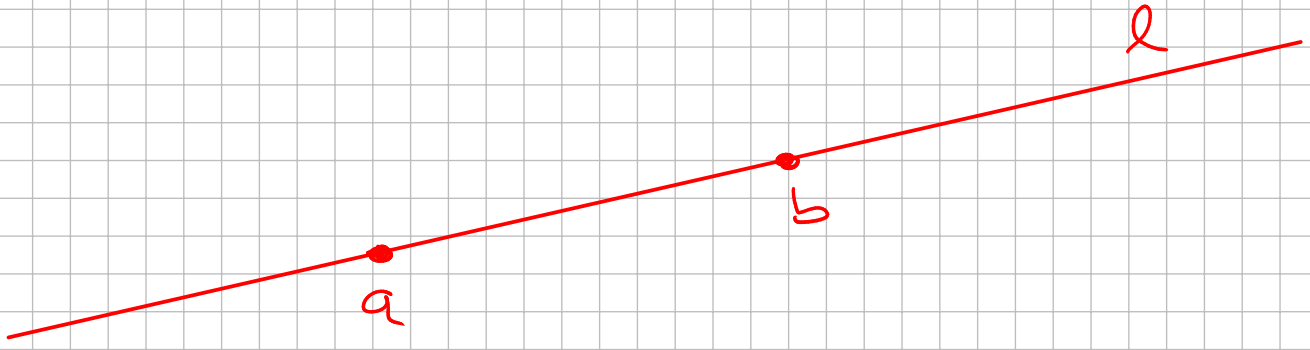
$=$

Construções com régua e compas.

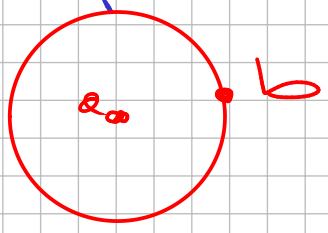
Regras: 1) Começamos com dois pontos desenhados no plano



2). a). Dois pontos construídos. A reta que contém os dois é construtível.



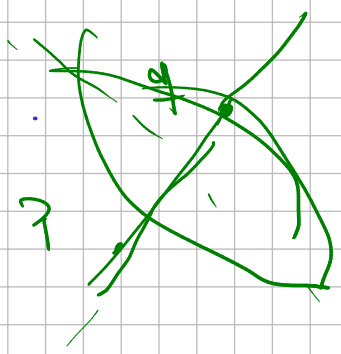
b) Dados dois pontos a, b. O círculo com centro em a, passando por b é construtível

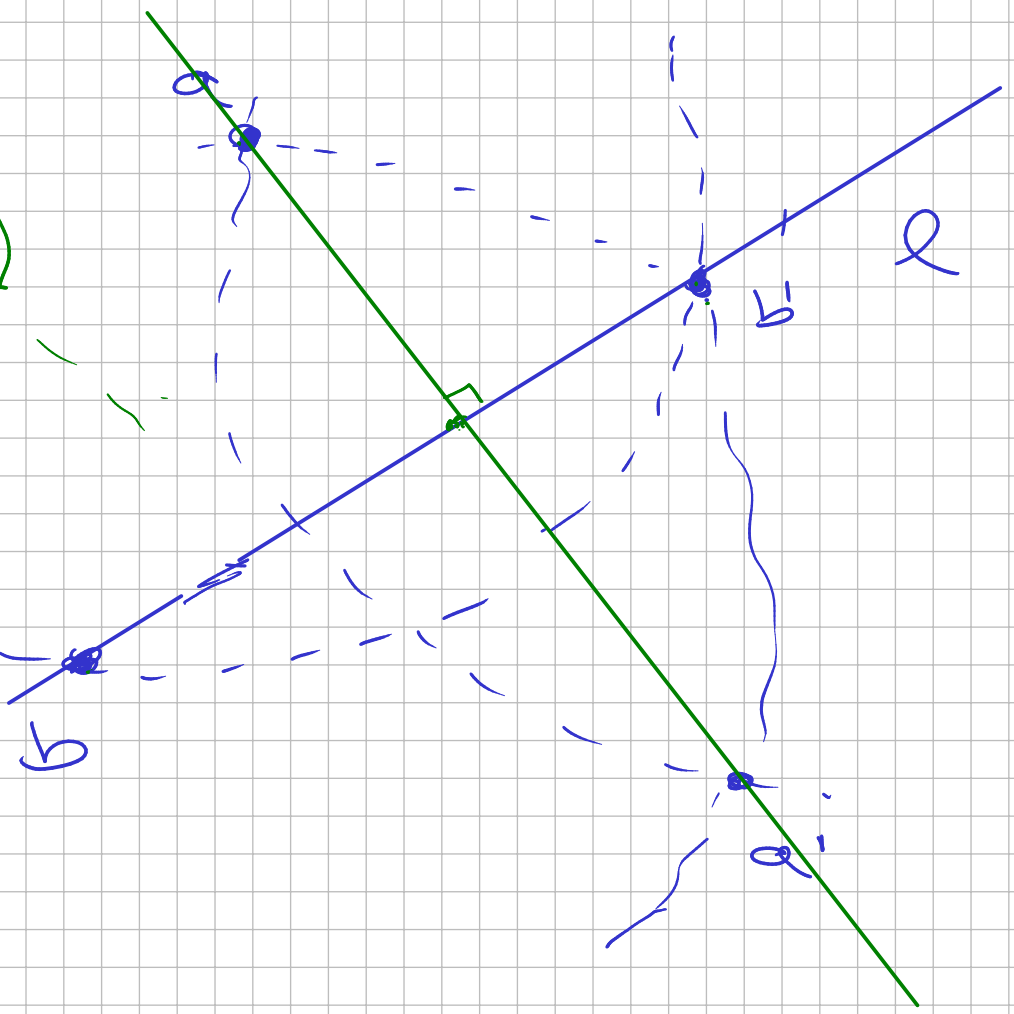


3). Dados Dois retos / círculos ou uma reta e um círculo as intersecções são construtíveis.

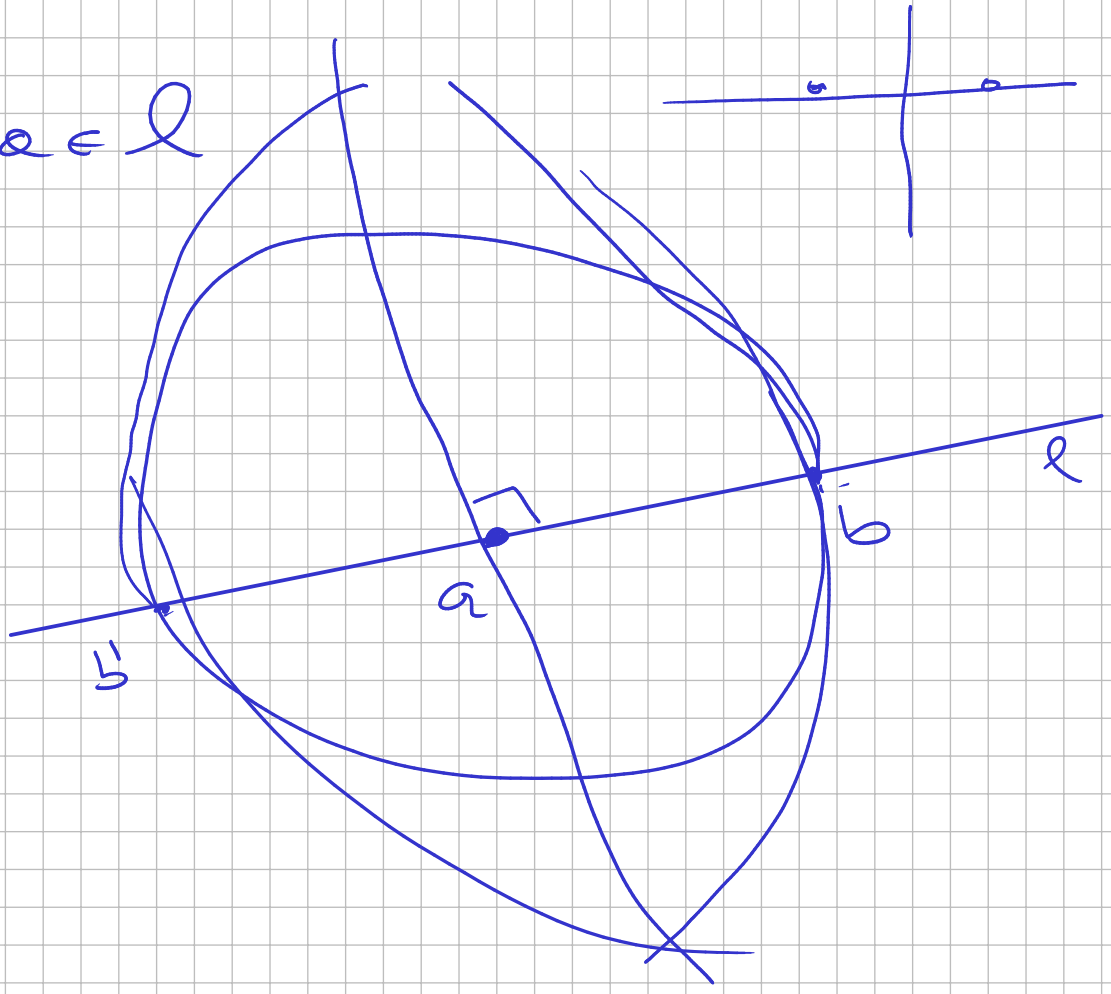
O conjunto de todos os pontos que podem ser construídos com as regras 1-3 são os pontos construtíveis do plano.

A distância $\overline{P-Q}$ é: 1

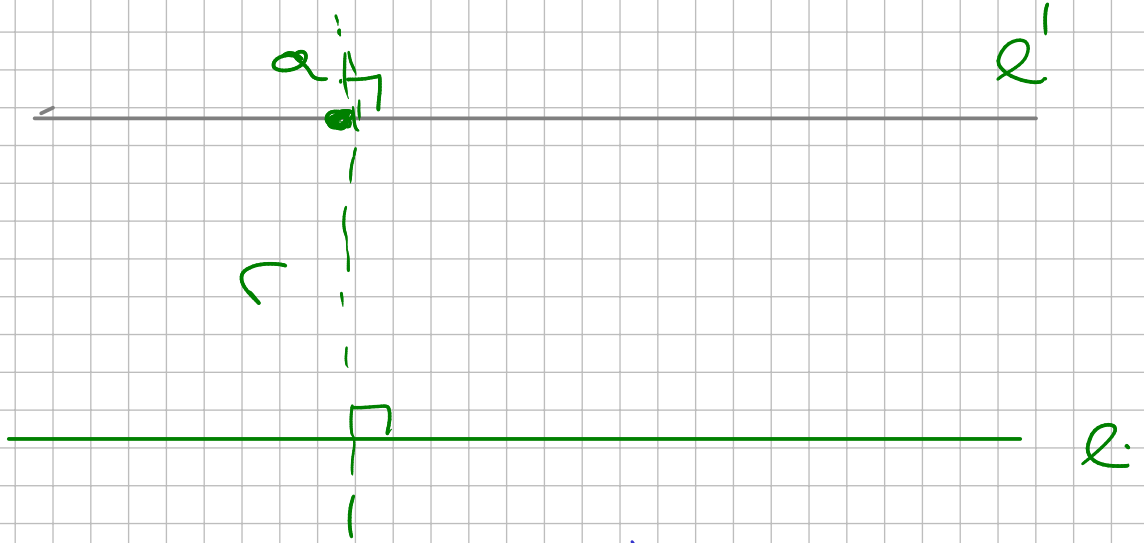




Caso $a \in l$

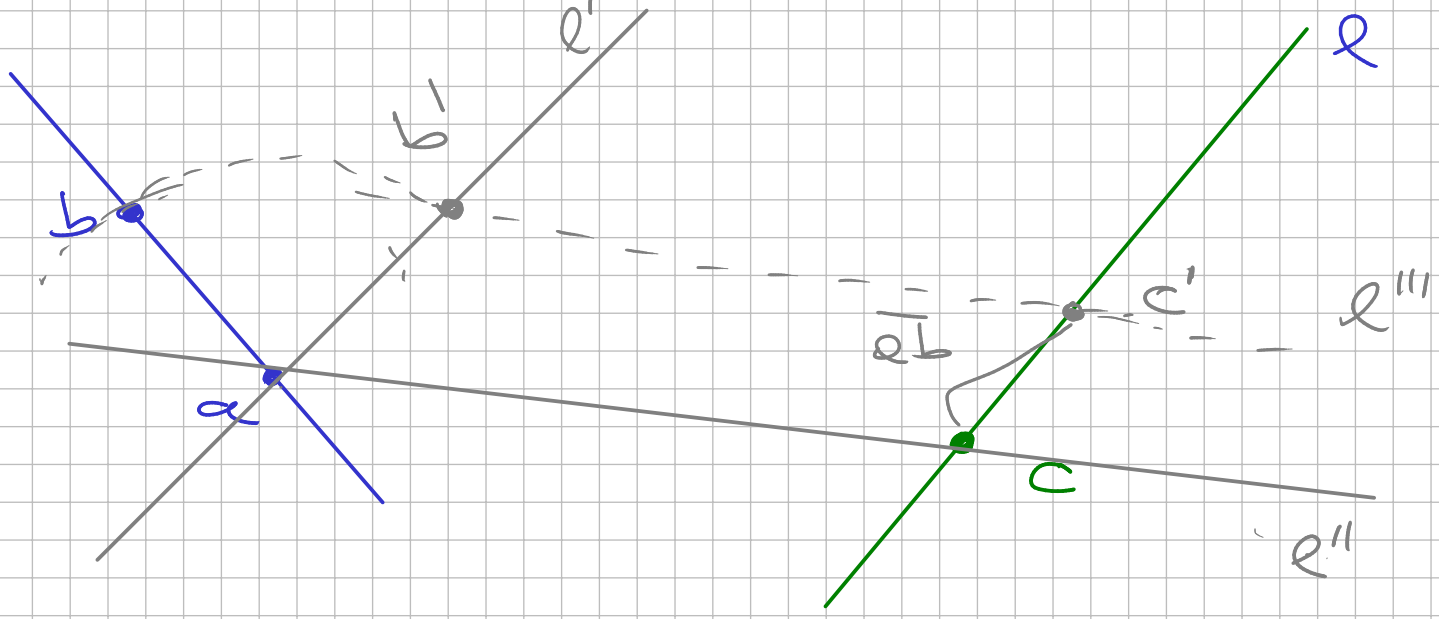


2). Dado l e a podemos construir $l' \parallel l$ $a \in l'$



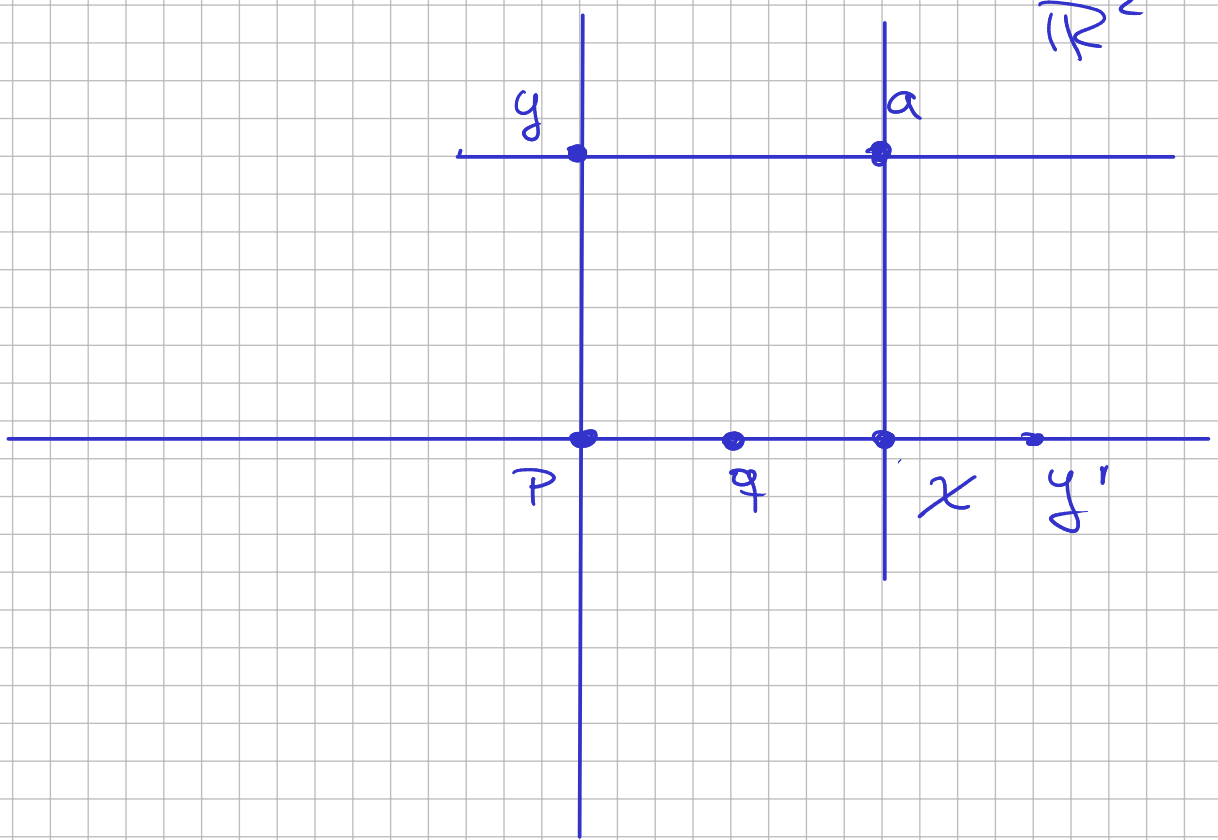
Dados dois pontos a b construídos. Diremos que existe $\overline{ab}$ é construível.

3). Suponha dada uma distância construída. e $l \ni c$



Podemos construir um ponto $d \in l$ a distância $\overline{cb}$ de c.

4). podemos desenhar um sistema de coordenadas. $\mathbb{R}^2$



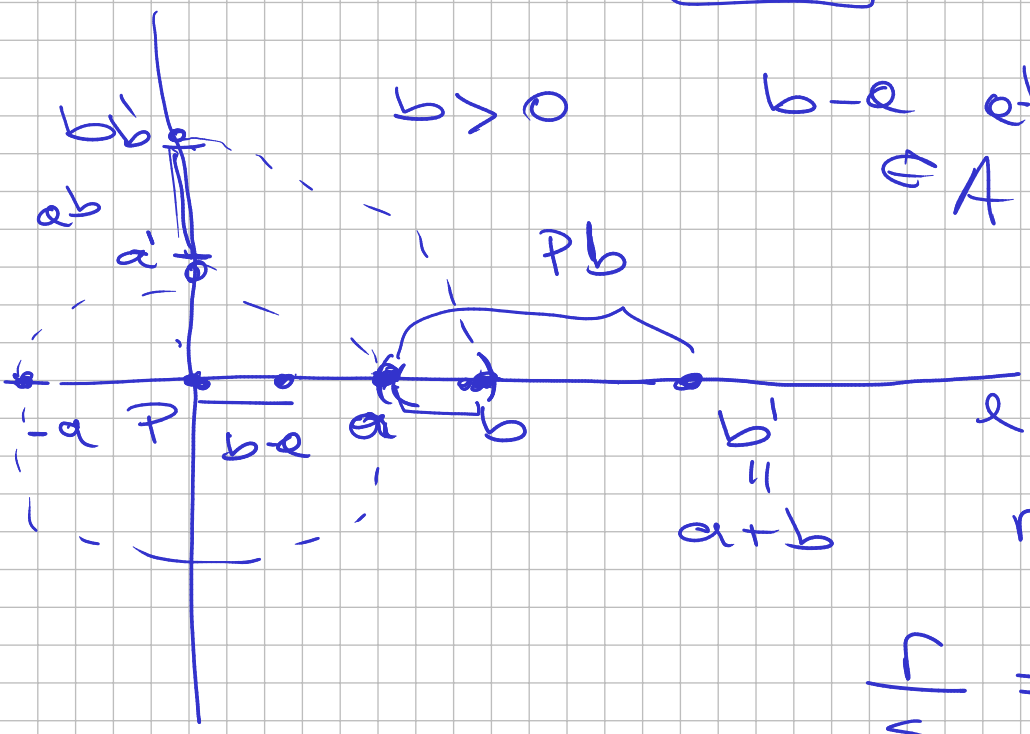
Def. Um número $x \in \mathbb{R}$ é dito construtível se é a coord. x de algum ponto $a \in \mathbb{R}^2$ construtível

$a \in \mathbb{R}^2$ é construtível $\iff$ x, y são construtíveis.
$\|$
(x, y)

Lemma: O conjunto $A \subset \mathbb{R}$ números construtíveis. é um sub corpo de $\mathbb{R}$.

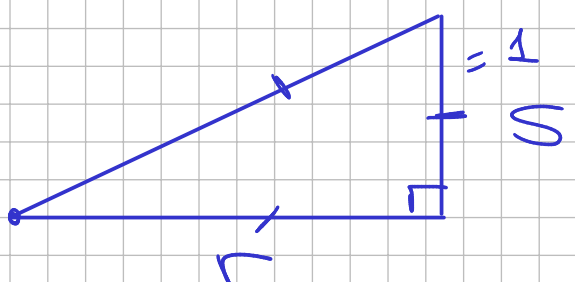
$p = 0 \in A$ $\quad q = 1 \in A$.

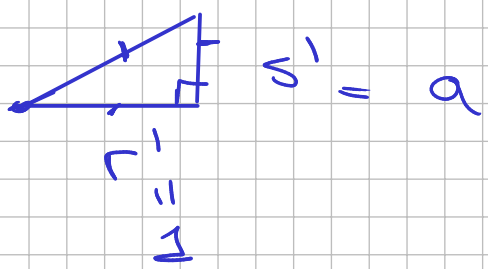
$a, b \in A$ $\quad a+b$ $\quad -a$ $\quad ab$ $\quad a^{-1} \in A$



$rs' = r's$

$\frac{r}{s} = \frac{r'}{s'}$





$1, a, b \in A$

$s' = 1 \quad r' = a \quad s = b$

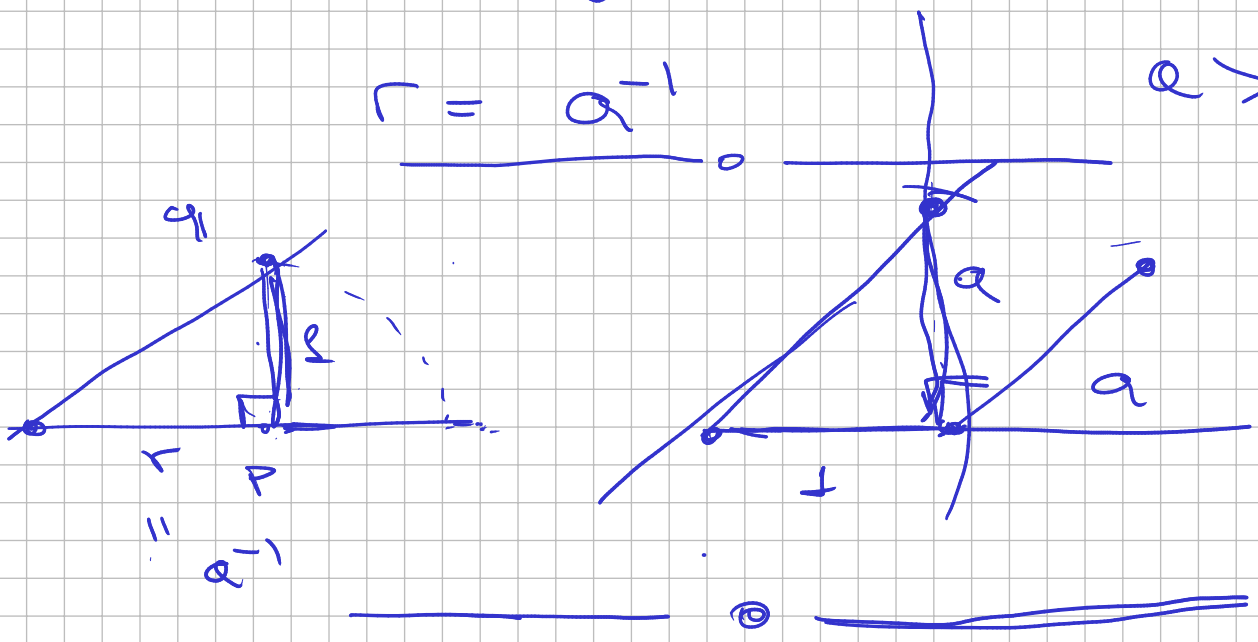
$\Downarrow$

$r = a \cdot b$ $\qquad a, b > 0$

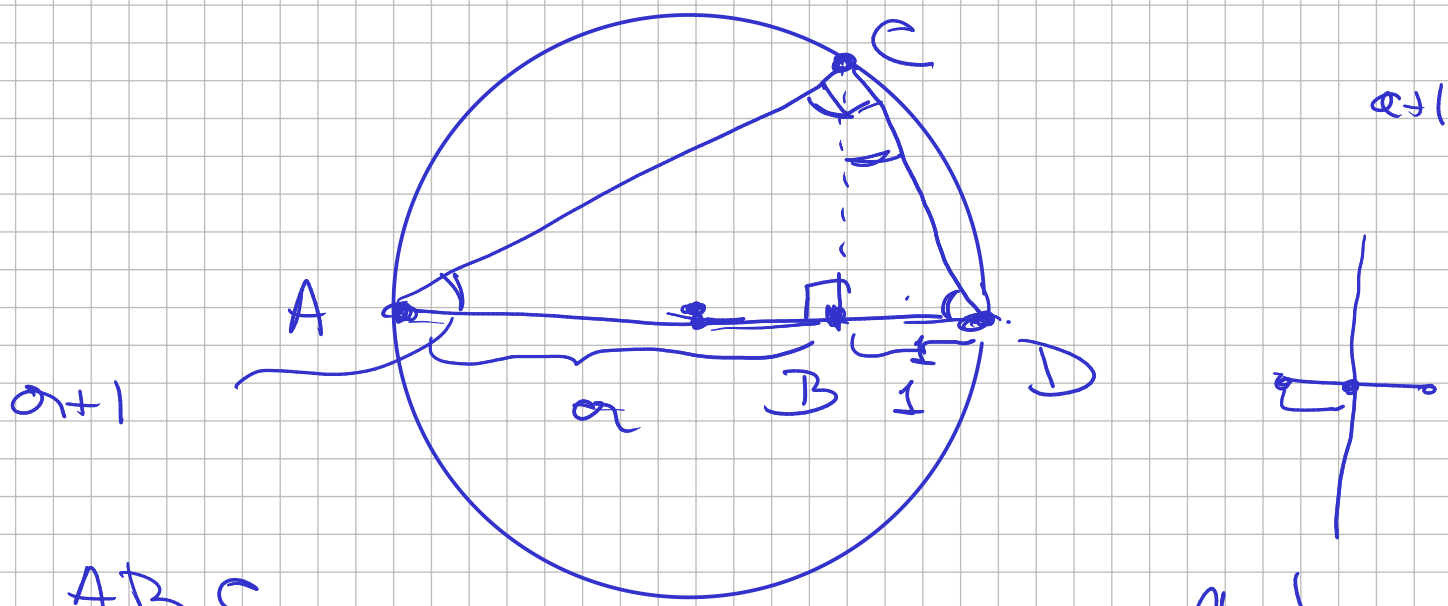
$s' = a \quad r' = 1 \quad s = 1$

$\Downarrow$

$r = a^{-1}$ $\qquad a > 0$



Theorem. $0 < a \in A \Rightarrow \sqrt{a} \in A$.



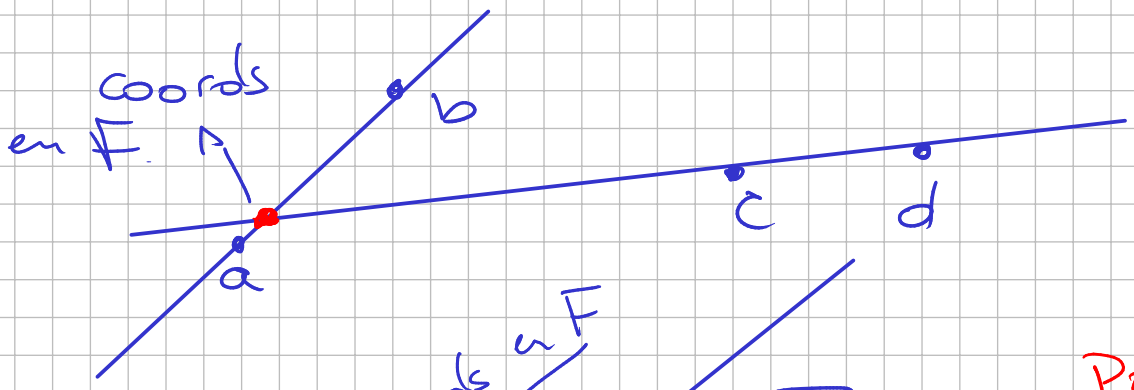
ABC e CBD são semelhantes.

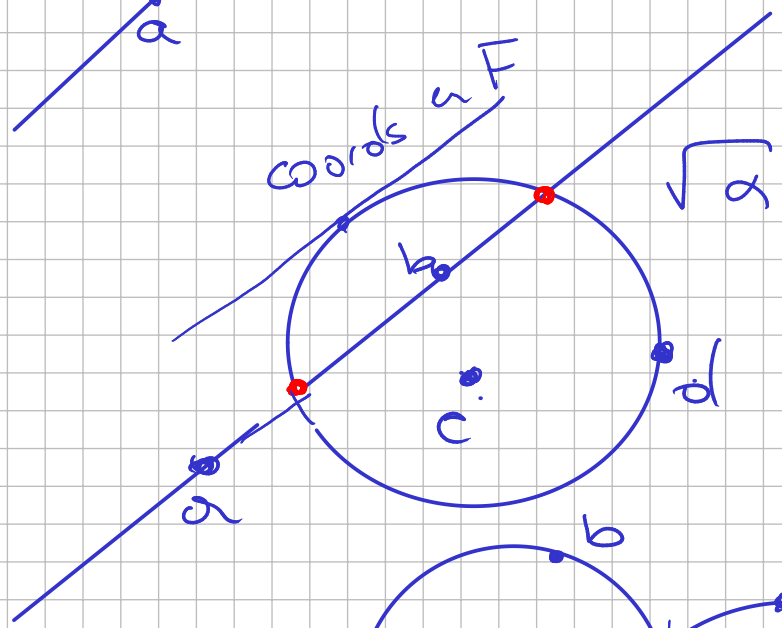
$$\frac{a}{BC} = \frac{AB}{BC} = \frac{BC}{BD} = \frac{BC}{1} \Rightarrow (BC)^2 = a$$

$$BC = \sqrt{a} \qquad \square$$

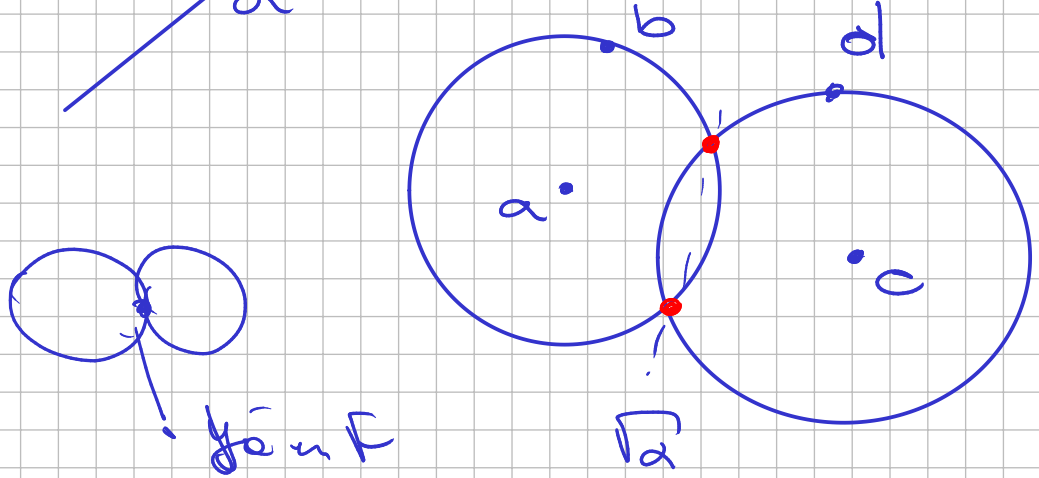
<u>Cor.</u> Corpo A é fechado por todas as $\sqrt{\alpha}$.

"<u>Converse</u>" Dados 4 pontos em $\mathbb{R}^2$ com coords em $F \subset A$.



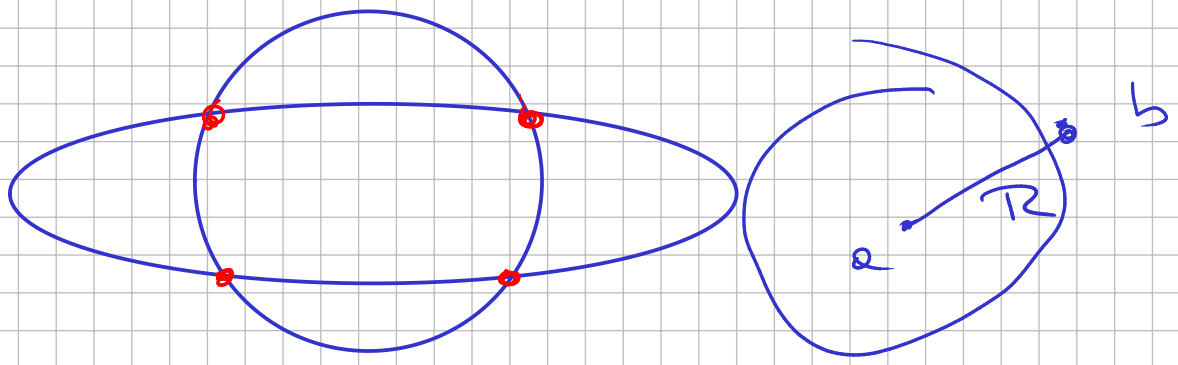


Posso ter 2, 1, 0 pontos na interseção.



2, 1, 0

as coord. dos pontos de interseção se obtem das de a, b, c, d agregando $\sqrt{\alpha}$, $\alpha \in F$.



$a = (x_a, y_a)$ $\quad b = (x_b, y_b)$ $\quad R^2 = \|\cdot\|^2$

$(y - y_a)^2 + (x - x_a)^2 = (y_b - y_a)^2 + (x_b - x_a)^2$

$\deg^2$ ← em X coeff. em F. $\qquad \in F$

$c = (x_c, y_c)$ $\quad d = (x_d, y_d)$ $\quad \in F$

$(y - y_c)^2 + (x - x_c)^2 = (y_d - y_c)^2 + (x_d - x_c)^2$

$(y - y_a)^2 - (y - y_c)^2 = (2y - y_a - y_c)(y_c - y_a)$

$(x - x_a)^2 - (x - x_c)^2 = (2x - x_a - x_c)(x_c - x_a)$

$(y_c - y_e) \cdot (2y - y_a - y_c) + (x_c - x_a)(2x - x_a - x_c)$

$\vec{F}$ $\cap$ F $\quad$ F

y é uma combinação linear de x e 1 com coeff. em F.

solução dem uma quadrática se obtem Tirando $\sqrt{\alpha}$ $\square$.

Teorema. Sejam $a_1, \ldots, a_n \in A$. Existe cadeia de extensões de corpos.

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_m \subset \mathbb{R}$$

$\sqrt{\alpha_1}$ $\quad$ $\sqrt{\alpha_2}$

$K_i \subset \mathbb{R}$ são subcorpos.

$a_1, \ldots, a_n \in K_m$

$K_i = K_{i-1}(\alpha_i)$ $\quad$ $\alpha_i^2 \in K_{i-1}$, $\alpha_i \notin K_{i-1}$

Converse Dada cadeia como

$$\mathbb{Q} \subset K_1 \subset \cdots \subset K_m$$

$\Rightarrow$ $K_m \subset A$. $\longrightarrow$ $\sqrt{\alpha} \in A$ $\forall \alpha \in A$.

Primeira parte segue da "conversa" anterior. por indução. □

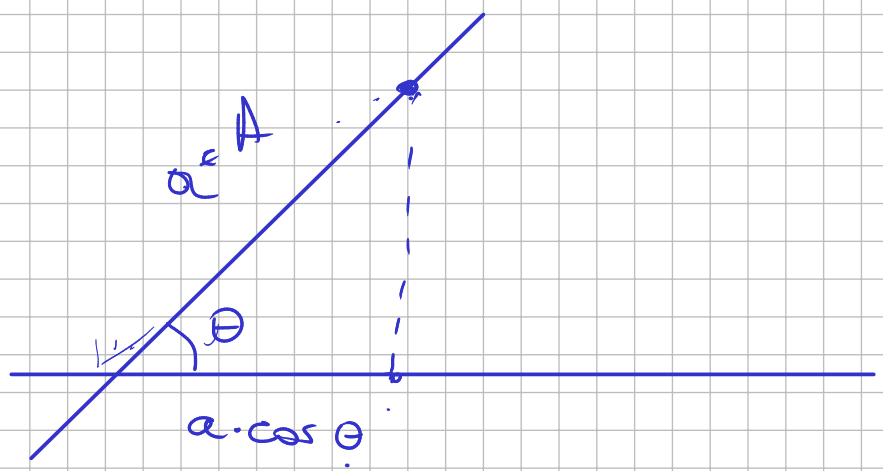
$\mathbb{Q} \subset A \subset \mathbb{R}$

$\alpha \Rightarrow \alpha$ é algébrico

é $[K(\alpha) : \mathbb{Q}] = 2^n$

Teorema. Não existe algoritmo com régua e "compasso" pra trisecar um ângulo.

Def ângulo θ é construtível se $\cos\theta \in K$ é construtível.



Ex θ tq. é construtível.

$\frac{1}{3}\theta$ não é construtível.

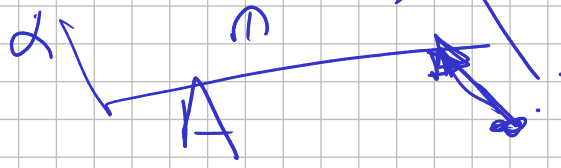
" $\operatorname{sen}(\alpha+\beta) = \operatorname{sen}(\alpha)\cos(\beta) + \operatorname{sen}(\beta)\cos(\alpha)$ "

$\cos(2\beta) = \cos(\beta)^2 - \operatorname{sen}^2(\beta)$

$\cos(3\beta) = 4\cos^3(\beta) - 3\cos(\beta)$

$\cos(\theta) = 4\cos^3(\beta) - 3\cos(\beta)$

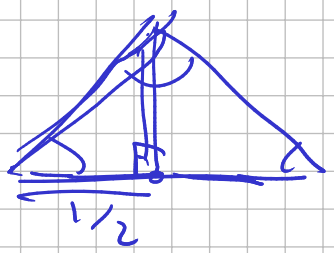
x



$\mathbb{Q}[x]$ $\quad x^3 - \frac{3}{4}x - \frac{\alpha}{4} = 0$

é irredutível sobre $\mathbb{Q}$.

$\theta = 60^\circ \qquad \alpha = \frac{1}{2} \in \mathbb{Q}.$



$\beta = 20^\circ \qquad \cos(\beta) = x$ satisfaz.

$x^3 - \frac{3}{4}x - \frac{1}{8} = 0$

$\Downarrow$ irred. sobre $\mathbb{Q}$.

$8x^3 - 3x - 1$ é irredutível.

$ax+b$ $\quad a, b \in \mathbb{Z}$.

grau de α é 3 / $\mathbb{Q}$.

$$[\mathbb{Q}(x) : \mathbb{Q}] = 3$$

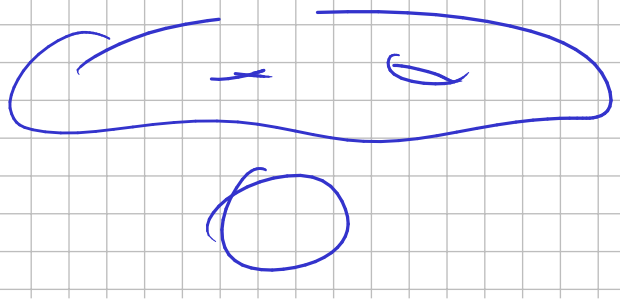
$x \in A$ grau série 2^n *

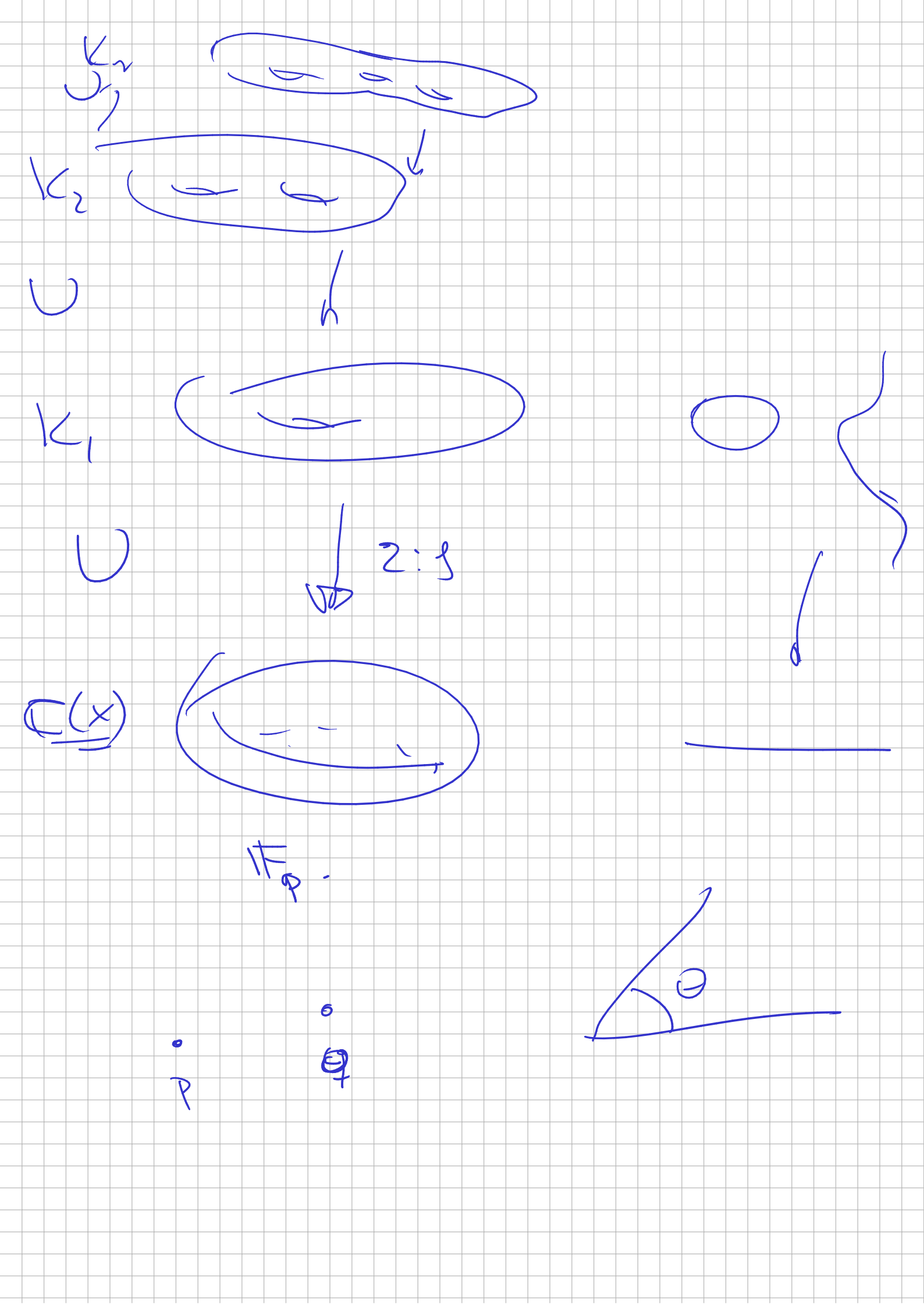
"30° é Trisecável."

Qual é o corpo plástico por agregar interseção de retas. círculos quadrática cúbicas.

em Arnaldo Garcia

Torres de corpos.




K_2
K_2
K_1
K_1
$\mathbb{C}(x)$
$\mathbb{F}_q$.
P
Q
θ