

Le théorème de Tarski-Seidenberg

Deux preuves de ce résultat algébrique

Groupe de lecture entre nous

Éloan & Téofil

mercredi 24 février 2021

On part d'un constat : les ensembles algébriques de \mathbb{R}^n ne sont **pas** stables par projection. On prend, par exemple, l'hyperbole

$$V := V(XY - 1) = \{(x, y) \in \mathbb{R}^2 \mid xy = 1\}$$

et la projection $\pi: \mathbb{R}^2 \rightarrow \mathbb{R}$ sur la première coordonnée. Alors son image

$$\pi(V) = \mathbb{R}^*$$

n'est pas algébrique.

En fait, un ensemble algébrique de \mathbb{R}^n est de la forme

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \phi(x_1, \dots, x_n, a_{n+1}, \dots, a_{n+m})\}$$

où $(a_{n+1}, \dots, a_{n+m}) \in \mathbb{R}^m$ est un vecteur et $\phi(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m})$ est une formule sans quantificateurs faisant intervenir les symboles suivants :

- ▶ les symboles logiques usuels \wedge , \vee et \neg ;
- ▶ des constantes $0, 1$;
- ▶ l'égalité $=$;
- ▶ les opérations $+$, $-$ et \times .

On dit que la formule $\phi(x_1, \dots, x_n)$ est une formule sur le langage

$$\mathcal{L}_{\text{corps}} := \{0, 1, +, \times, -\}.$$

L'idée est d'enrichir le langage $\mathcal{L}_{\text{corps}}$ en \mathcal{L} pour que les ensembles de la forme

$$\{\bar{x} \in \mathbb{R}^n \mid \phi(\bar{x}, \bar{a})\}$$

où $\phi(\bar{x}, \bar{y})$ est une formule sans quantificateurs sur \mathcal{L} , soient stables par projections.

L'idée est d'enrichir le langage $\mathcal{L}_{\text{corps}}$ en \mathcal{L} pour que les ensembles de la forme

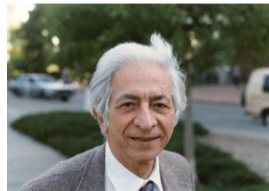
$$\{\bar{x} \in \mathbb{R}^n \mid \phi(\bar{x}, \bar{a})\}$$

où $\phi(\bar{x}, \bar{y})$ est une formule sans quantificateurs sur \mathcal{L} , soient stables par projections.

Ce langage va être celui des corps ordonnés : on va rajouter le symbole $<$.



Alfred Tarski (1901–1983)



Abraham Seidenberg (1916–1988)

1 Les trois formes du théorème

- 1.1 Énoncés
- 1.2 Équivalence entre les théorèmes
- 1.3 Une application

2 La preuve par le théorème de Sturm

- 2.1 Le théorème de Sturm
- 2.2 Preuve du théorème
- 2.3 Un exemple

3 Une preuve par la théorie des modèles

- 3.1 Théorie des modèles
- 3.2 Corps réels clos
- 3.3 Élimination des quantificateurs
- 3.4 Fin de la preuve

Partie 1

Les trois formes du théorème

Théorème de Tarski-Seidenberg, forme algébrique

Soient $n, m \in \mathbb{N}^*$ des entiers. Soient $S_1, \dots, S_m \in \mathbb{R}[T_1, \dots, T_n, X]$ des polynômes réels à $n + 1$ variables et $\diamond_1, \dots, \diamond_m \in \{>, =\}$ des symboles. Alors il existe des systèmes d'équations et d'inéquations polynomiales $R_1(T), \dots, R_k(T)$ d'inconnue T tels que, pour tout vecteur $t \in \mathbb{R}^n$, on ait l'équivalence

$$(\exists x \in \mathbb{R}, \forall i \in \llbracket 1, m \rrbracket, S_i(t, x) \diamond_i 0) \iff R_1(t) \vee \dots \vee R_k(t).$$

Théorème de Tarski-Seidenberg, forme algébrique

Soient $n, m \in \mathbb{N}^*$ des entiers. Soient $S_1, \dots, S_m \in \mathbb{R}[T_1, \dots, T_n, X]$ des polynômes réels à $n + 1$ variables et $\diamond_1, \dots, \diamond_m \in \{>, =\}$ des symboles. Alors il existe des systèmes d'équations et d'inéquations polynomiales $R_1(T), \dots, R_k(T)$ d'inconnue T tels que, pour tout vecteur $t \in \mathbb{R}^n$, on ait l'équivalence

$$(\exists x \in \mathbb{R}, \forall i \in \llbracket 1, m \rrbracket, S_i(t, x) \diamond_i 0) \iff R_1(t) \vee \dots \vee R_k(t).$$

Exemple. Soit $t \in \mathbb{R}$. L'équation $x^2 = t$ d'inconnue $x \in \mathbb{R}$ est équivalente à l'équation $t \geq 0$, c'est-à-dire

$$(\exists x \in \mathbb{R}, x^2 = t) \iff t \geq 0.$$

On considère le langage des corps ordonnés

$$\mathcal{L}_{\text{ord}} := \{0, 1, +, \times, -, <\}.$$

Une formule logique est une formule sur le langage \mathcal{L}_{ord} . Elle peut dépendre de variables $\bar{x} = (x_1, \dots, x_n)$, dites *libres*, comme la formule

$$\phi(\bar{x}) := \left(\exists t, \quad x_n t^n + \dots + x_1 t + x_0 = 0 \right).$$

On considère le langage des corps ordonnés

$$\mathcal{L}_{\text{ord}} := \{0, 1, +, \times, -, <\}.$$

Une formule logique est une formule sur le langage \mathcal{L}_{ord} . Elle peut dépendre de variables $\bar{x} = (x_1, \dots, x_n)$, dites *libres*, comme la formule

$$\phi(\bar{x}) := \left(\exists t, \quad x_n t^n + \dots + x_1 t + x_0 = 0 \right).$$

On dit qu'une formule est

- ▶ sans quantificateur si elle ne contient pas de quantificateur, comme

$$x_1 = x_3 + x_2^2 \vee x_2 < 0 ;$$

- ▶ *close* si elle ne dépend pas de variables libres, comme

$$\forall x, \quad \left[(x = 0) \vee (x > 0) \implies \exists t, t^2 = x \right].$$

Théorème de Tarski-Seidenberg, forme logique

Soit $\phi(\bar{t}, x_1, \dots, x_n)$ une formule sans quantificateur sur le langage

$$\mathcal{L}_{\text{ord}} := \{0, 1, +, \times, -, <\}.$$

Soient $\square_1, \dots, \square_n \in \{\forall, \exists\}$. Alors la formule

$$\square_1 x_1 \in \mathbb{R}, \dots, \square_n x_n \in \mathbb{R}, \quad \phi(\bar{t}, x_1, \dots, x_n)$$

est équivalente à une formule sans quantificateur.

Définition

Soit $n \in \mathbb{N}^*$ un entier. La classe des *ensembles semi-algébriques* est la plus petite classe de parties \mathcal{SA}_n de \mathbb{R}^n vérifiant

▶ si $P \in \mathbb{R}[X_1, \dots, X_n]$, alors

$$\{x \in \mathbb{R}^n \mid P(x) = 0\} \in \mathcal{SA}_n \quad \text{et} \quad \{x \in \mathbb{R}^n \mid P(x) > 0\} \in \mathcal{SA}_n ;$$

▶ la classe \mathcal{SA}_n est stable par union finie, intersection finie et différence.

Définition

Soit $n \in \mathbb{N}^*$ un entier. La classe des *ensembles semi-algébriques* est la plus petite classe de parties \mathcal{SA}_n de \mathbb{R}^n vérifiant

▶ si $P \in \mathbb{R}[X_1, \dots, X_n]$, alors

$$\{x \in \mathbb{R}^n \mid P(x) = 0\} \in \mathcal{SA}_n \quad \text{et} \quad \{x \in \mathbb{R}^n \mid P(x) > 0\} \in \mathcal{SA}_n ;$$

▶ la classe \mathcal{SA}_n est stable par union finie, intersection finie et différence.

Exemples. Les ensembles algébriques sont semi-algébriques. La demi-parabole

$$\{(x, y) \in \mathbb{R}^2 \mid y > x^2, x > 0\} \in \mathcal{SA}_2$$

est semi-algébrique. Les boules euclidiennes $\mathbb{B}^n \subset \mathbb{R}^n$ sont semi-algébriques.

Théorème de Tarski-Seidenberg, forme géométrique

Les ensembles semi-algébriques sur \mathbb{R} sont stables par projection. Plus précisément, si $\pi: \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$ désigne la projection sur les n premières coordonnées, alors

$$A \in \mathcal{SA}_{n+1} \implies \pi(A) \in \mathcal{SA}_n.$$

Théorème de Tarski-Seidenberg, forme géométrique

Les ensembles semi-algébriques sur \mathbb{R} sont stables par projection. Plus précisément, si $\pi: \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$ désigne la projection sur les n premières coordonnées, alors

$$A \in \mathcal{SA}_{n+1} \implies \pi(A) \in \mathcal{SA}_n.$$

Exemple. L'hyperbole $V := V(XY - 1) \subset \mathbb{R}^2$ est semi-algébrique et sa projection sur la première coordonnées est semi-algébrique car, si $\pi: \mathbb{R}^2 \rightarrow \mathbb{R}$ est la projection sur la première coordonnées, alors

$$\pi(V) = \mathbb{R}^* = \{x \in \mathbb{R} \mid x > 0\} \cup \{x \in \mathbb{R} \mid x < 0\} \in \mathcal{SA}_1.$$

- ▶ La forme logique implique clairement la forme géométrique : les ensembles semi-algébriques sont exactement les ensembles de la forme

$$\{\bar{x} \in \mathbb{R}^n \mid \phi(\bar{x})\}$$

pour une formule $\phi(\bar{x})$ sans quantificateur sur le langage \mathcal{L}_{ord} .

- ▶ La forme logique implique clairement la forme géométrique : les ensembles semi-algébriques sont exactement les ensembles de la forme

$$\{\bar{x} \in \mathbb{R}^n \mid \phi(\bar{x})\}$$

pour une formule $\phi(\bar{x})$ sans quantificateur sur le langage \mathcal{L}_{ord} .

- ▶ La forme géométrique implique clairement la forme algébrique.

- ▶ La forme logique implique clairement la forme géométrique : les ensembles semi-algébriques sont exactement les ensembles de la forme

$$\{\bar{x} \in \mathbb{R}^n \mid \phi(\bar{x})\}$$

pour une formule $\phi(\bar{x})$ sans quantificateur sur le langage \mathcal{L}_{ord} .

- ▶ La forme géométrique implique clairement la forme algébrique.
- ▶ La forme algébrique implique la forme logique en utilisant un nombre fini de fois

$$[\forall x \in \mathbb{R}, \phi(x)] \iff \neg[\exists x \in \mathbb{R}, \neg\phi(x)]$$

et on peut donc se ramener à un quantificateur existentiel en première place.

On se place dans l'espace euclidien \mathbb{R}^n .

Proposition

Soit $A \subset \mathbb{R}^n$ un ensemble semi-algébrique. Alors les ensembles \bar{A} et $\overset{\circ}{A}$ sont semi-algébriques.

En passant au complémentaire, il suffit de le faire pour l'adhérence \bar{A} qui vaut

$$\bar{A} := \left\{ x \in \mathbb{R}^n \mid \forall \varepsilon \in \mathbb{R}^*, \exists y \in \mathbb{R}^n, y \in A \wedge \sum_{i=1}^n (x_i - y_i)^2 < \varepsilon^2 \right\}.$$

Après calcul, on trouve

$$\bar{A} = \mathbb{R}^n \setminus \left[p_{n+1,n}(\mathbb{R}^{n+1} \setminus p_{2n+1,n+1}(B)) \right]$$

avec

$$B := [\mathbb{R}^n \times \mathbb{R} \times A] \cap \left\{ (x, \varepsilon, y) \in \mathbb{R}^n \times \mathbb{R}^* \times \mathbb{R}^n \mid \sum_{i=1}^n (x_i - y_i)^2 < \varepsilon^2 \right\} \in \mathcal{SA}_{2n+1}.$$

Par le théorème de Tarski-Seidenberg, on a $\bar{A} \in \mathcal{SA}_n$.

Partie 2

La preuve par le théorème de Sturm

Soit $P \in \mathbb{R}[X]$ un polynôme réel. On effectue l'algorithme d'Euclide et on obtient une suite (P_0, \dots, P_k) telle que

- ▶ $P_0 = P$ et $P_1 = P'$;
- ▶ pour tout $i \in \llbracket 2, k \rrbracket$, le polynôme P_i est l'**opposé** du reste de la division euclidienne de P_{i-2} par P_{i-1} ;
- ▶ le dernier polynôme P_k est non nul : c'est $\pm \text{pgcd}(P, P')$.

Soit $P \in \mathbb{R}[X]$ un polynôme réel. On effectue l'algorithme d'Euclide et on obtient une suite (P_0, \dots, P_k) telle que

- ▶ $P_0 = P$ et $P_1 = P'$;
- ▶ pour tout $i \in \llbracket 2, k \rrbracket$, le polynôme P_i est l'**opposé** du reste de la division euclidienne de P_{i-2} par P_{i-1} ;
- ▶ le dernier polynôme P_k est non nul : c'est $\pm \text{pgcd}(P, P')$.

Définition

La *suite de Sturm* associée au polynôme P est la suite (P_0, \dots, P_k) .

Considérons le polynôme

$$P := (X - 1)(X - 2)(X - 3) \in \mathbb{R}[X].$$

Alors

$$P_0 = X^3 - 6X^2 + 11X - 6,$$

$$P_1 = 2X^2 - 12X + 11,$$

$$P_2 = \frac{2}{3}X - \frac{4}{3},$$

$$P_3 = 1.$$

Définition

Soit $a \in \mathbb{R}$ un réel tel que $P(a) \neq 0$. On note $s_P(a) \in \mathbb{N}$ le nombre de changements de signe dans la suite $(P_0(a), \dots, P_k(a))$, c'est-à-dire

$$s_P(a) := \#\{i \in \llbracket 1, k \rrbracket \mid P_{i-1}(a)P_i(a) < 0\}.$$

Définition

Soit $a \in \mathbb{R}$ un réel tel que $P(a) \neq 0$. On note $s_P(a) \in \mathbb{N}$ le nombre de changements de signe dans la suite $(P_0(a), \dots, P_k(a))$, c'est-à-dire

$$s_P(a) := \#\{i \in \llbracket 1, k \rrbracket \mid P_{i-1}(a)P_i(a) < 0\}.$$

Exemple. Avec le polynôme précédent, on a

$$(P_0(-1), P_1(-1), P_2(-1), P_3(-1)) = (-24, 25, -2, 1),$$

$$(P_0(4), P_1(4), P_2(4), P_3(4)) = (6, 11, 4/3, 1).$$

Alors

$$s_P(-1) = 3 \quad \text{et} \quad s_P(4) = 0.$$

Théorème de Sturm (1829)

Soient $P \in \mathbb{R}[X]$ et $a, b \in \mathbb{R}$ avec $a < b$ tels que $P(a) \neq 0$ et $P(b) \neq 0$. Alors le nombre de racines réelles de P sur $[a, b]$ est

$$s_P(a) - s_P(b).$$

Théorème de Sturm (1829)

Soient $P \in \mathbb{R}[X]$ et $a, b \in \mathbb{R}$ avec $a < b$ tels que $P(a) \neq 0$ et $P(b) \neq 0$. Alors le nombre de racines réelles de P sur $[a, b]$ est

$$s_P(a) - s_P(b).$$

Exemple. On a $s_P(4) - s_P(-1) = 3 - 0 = 3$ et le polynôme

$$P = (X - 1)(X - 2)(X - 3)$$

a bien trois racines sur $[-1, 4]$.

On suppose que le polynôme P est sans racine multiple.

- ▶ Soit $r \in \mathbb{R}$ une racine de $P_0 = P$. Alors $P_1(r) = P'(r) \neq 0$: au voisinage de r , la fonction P' garde un signe constant forçant P à en changer.

$$\begin{array}{c|ccc} x & & r & \\ \text{sgn } P_0(x) & - & 0 & + \\ \text{sgn } P_1(x) & + & + & + \end{array}$$

$$\begin{array}{c|ccc} x & & r & \\ \text{sgn } P_0(x) & + & 0 & - \\ \text{sgn } P_1(x) & - & - & - \end{array}$$

On suppose que le polynôme P est sans racine multiple.

- ▶ Soit $r \in \mathbb{R}$ une racine de $P_0 = P$. Alors $P_1(r) = P'(r) \neq 0$: au voisinage de r , la fonction P' garde un signe constant forçant P à en changer.

$$\begin{array}{c|ccc} x & & r & \\ \text{sgn } P_0(x) & - & 0 & + \\ \text{sgn } P_1(x) & + & + & + \end{array} \qquad \begin{array}{c|ccc} x & & r & \\ \text{sgn } P_0(x) & + & 0 & - \\ \text{sgn } P_1(x) & - & - & - \end{array}$$

⇒ Diminution du nombre de changements de signes !

- Soient $i \in \mathbb{J}1, k-1\mathbb{K}$ et $r \in \mathbb{R}$ une racine de P_i . Alors $P_{i-1}(r) \neq 0$ et $P_{i+1}(r) \neq 0$ car sinon on aurait $P(r) = P'(r) = 0$ en remontant l'algorithme d'Euclide. De plus, on a $P_{i-1}(r) = -P_{i+1}(r)$. Par exemple, on est dans un des cas suivants.

$$\begin{array}{c|ccc}
 x & & & \\
 \hline
 \text{sgn } P_{i-1}(x) & + & + & + \\
 \text{sgn } P_i(x) & + & 0 & + \\
 \text{sgn } P_{i+1}(x) & - & - & -
 \end{array}$$

$$\begin{array}{c|ccc}
 x & & & \\
 \hline
 \text{sgn } P_{i-1}(x) & - & - & - \\
 \text{sgn } P_i(x) & - & 0 & + \\
 \text{sgn } P_{i+1}(x) & + & + & +
 \end{array}$$

- Soient $i \in \mathbb{J}1, k-1\mathbb{K}$ et $r \in \mathbb{R}$ une racine de P_i . Alors $P_{i-1}(r) \neq 0$ et $P_{i+1}(r) \neq 0$ car sinon on aurait $P(r) = P'(r) = 0$ en remontant l'algorithme d'Euclide. De plus, on a $P_{i-1}(r) = -P_{i+1}(r)$. Par exemple, on est dans un des cas suivants.

$$\begin{array}{c}
 x \\
 \text{sgn } P_{i-1}(x) \\
 \text{sgn } P_i(x) \\
 \text{sgn } P_{i+1}(x)
 \end{array}
 \left| \begin{array}{ccc}
 r \\
 + & + & + \\
 + & 0 & + \\
 - & - & -
 \end{array} \right.
 \qquad
 \begin{array}{c}
 x \\
 \text{sgn } P_{i-1}(x) \\
 \text{sgn } P_i(x) \\
 \text{sgn } P_{i+1}(x)
 \end{array}
 \left| \begin{array}{ccc}
 r \\
 - & - & - \\
 - & 0 & + \\
 + & + & +
 \end{array} \right.$$

⇒ Nombre de changements de signes constant !

- ▶ Soient $i \in \mathbb{J}1, k - 1\mathbb{K}$ et $r \in \mathbb{R}$ une racine de P_i . Alors $P_{i-1}(r) \neq 0$ et $P_{i+1}(r) \neq 0$ car sinon on aurait $P(r) = P'(r) = 0$ en remontant l'algorithme d'Euclide. De plus, on a $P_{i-1}(r) = -P_{i+1}(r)$. Par exemple, on est dans un des cas suivants.

x	r		x	r
$\text{sgn } P_{i-1}(x)$	+ + +		$\text{sgn } P_{i-1}(x)$	- - -
$\text{sgn } P_i(x)$	+ 0 +		$\text{sgn } P_i(x)$	- 0 +
$\text{sgn } P_{i+1}(x)$	- - -		$\text{sgn } P_{i+1}(x)$	+ + +

⇒ Nombre de changements de signes constant !

- ▶ Au voisinage d'un réel qui n'est pas racine des polynômes P_i , le nombre de changements de signe reste constant.

On va que la fonction $x \mapsto s_P(x)$ ne varie qu'au voisinage d'une racine de P et qu'elle diminue d'une unité à chaque passage. Donc le nombre de racines réelles de P sur $[a, b]$ est bien

$$s_P(a) - s_P(b).$$

On ne suppose plus que le polynôme P est sans racine multiple. Dans ce cas, on considère le polynôme P_0/P_k . Sa suite de Sturm associée est la suite

$$\left(\frac{P_0}{P_k}, \dots, \frac{P_{k-1}}{P_k}, 1 \right)$$

qui, évaluée en $a \in \mathbb{R}$, a le même nombre de changement de signes que la suite

$$(P_0(a), \dots, P_k(a)).$$

D'où

$$s_P(a) = s_{P_0/P_k}(a).$$

Comme le polynôme P_0/P_k est sans racine multiple, on est ramené au cas précédent et, comme les polynômes P_0/P_k et P_0 partagent les mêmes racines, on a terminé !

Corollaire

Soit $P \in \mathbb{R}[X]$. On note $s_P(+\infty)$ et $s_P(-\infty)$ les nombres de changements de signe dans les suites

$$(c(P_0(X)), \dots, c(P_k(X))) \quad \text{et} \quad (c(P_0(-X)), \dots, c(P_k(-X))).$$

Alors le nombre de racines réelles de P est

$$s_P(-\infty) - s_P(+\infty).$$

Moralement, on prend un réel a assez petit et un réel b assez grand de sorte que le polynôme P ne change plus de signe sur les intervalles $]-\infty, a[$ et $]b, +\infty[$ et on utilise le théorème de Sturm.

Lemme : comptage des racines pour un système simple

Soient $P, Q \in \mathbb{R}[X]$ et $a, b \in \mathbb{R}$ avec $a < b$ tels que $P(a) \neq 0$ et $P(b) \neq 0$.

On note $p, n \in \mathbb{N}$ respectivement le nombre de solutions sur $[a, b]$ des systèmes

$$\begin{cases} P(x) = 0, \\ Q(x) > 0 \end{cases} \quad \text{et} \quad \begin{cases} P(x) = 0, \\ Q(x) < 0. \end{cases}$$

On note (P_0, \dots, P_k) la suite de Sturm avec $P_0 = P$ et $P_1 = P'Q$ et, pour $a \in \mathbb{R}$, on note $s_{P,Q}(a)$ le nombre de changements de signe de cette suite. Alors

$$p - n = s_{P,Q}(a) - s_{P,Q}(b),$$

$$p = \frac{1}{2}[s_{P,Q}(a) - s_{P,Q}(b) + s_{P,Q^2}(a) - s_{P,Q^2}(b)].$$

Les mêmes relations sont valables avec $a = -\infty$ et $b = +\infty$.

On peut supposer que les polynômes $P_0 = P$ et $P_1 = P'Q$ sont premiers entre eux. Soit $r \in \mathbb{R}$ une racine de P . Alors $P'(r) \neq 0$ et $Q(r) \neq 0$, donc $P_0 = P$ change de signe au voisinage de r .

On peut supposer que les polynômes $P_0 = P$ et $P_1 = P'Q$ sont premiers entre eux. Soit $r \in \mathbb{R}$ une racine de P . Alors $P'(r) \neq 0$ et $Q(r) \neq 0$, donc $P_0 = P$ change de signe au voisinage de r .

- ▶ Si $Q > 0$ au voisinage de r , alors on est dans un des deux cas

x	r		x	r		
$\text{sgn } P(x)$	-	0	+	+	0	-
$\text{sgn } P'(x)$	+	+	+	-	-	-
$\text{sgn } P'Q(x)$	+	+	+	-	-	-

On peut supposer que les polynômes $P_0 = P$ et $P_1 = P'Q$ sont premiers entre eux. Soit $r \in \mathbb{R}$ une racine de P . Alors $P'(r) \neq 0$ et $Q(r) \neq 0$, donc $P_0 = P$ change de signe au voisinage de r .

- ▶ Si $Q > 0$ au voisinage de r , alors on est dans un des deux cas

x	r		x	r		
$\text{sgn } P(x)$	-	0	+	+	0	-
$\text{sgn } P'(x)$	+	+	+	-	-	-
$\text{sgn } P'Q(x)$	+	+	+	-	-	-

- ▶ Si $Q < 0$ au voisinage de r , alors on est dans un des deux cas

x	r		x	r		
$\text{sgn } P(x)$	-	0	+	+	0	-
$\text{sgn } P'(x)$	+	+	+	-	-	-
$\text{sgn } P'Q(x)$	-	-	-	+	+	+

Comme dans la preuve du théorème de Sturm, au voisinage d'une racine d'un polynôme P_i , la fonction $s_{P,Q}$ est constante.

Comme dans la preuve du théorème de Sturm, au voisinage d'une racine d'un polynôme P_i , la fonction $s_{P,Q}$ est constante.

En conclusion, la fonction $s_{P,Q}$ ne varie qu'au voisinage d'une racine $r \in \mathbb{R}$ de P et

- ▶ décroît d'une unité au voisinage lorsque $Q(r) > 0$;
- ▶ croît d'une unité au voisinage lorsque $Q(r) < 0$.

D'où

$$p - n = s_{P,Q}(a) - s_{P,Q}(b).$$

Comme dans la preuve du théorème de Sturm, au voisinage d'une racine d'un polynôme P_i , la fonction $s_{P,Q}$ est constante.

En conclusion, la fonction $s_{P,Q}$ ne varie qu'au voisinage d'une racine $r \in \mathbb{R}$ de P et

- ▶ décroît d'une unité au voisinage lorsque $Q(r) > 0$;
- ▶ croît d'une unité au voisinage lorsque $Q(r) < 0$.

D'où

$$p - n = s_{P,Q}(a) - s_{P,Q}(b).$$

Pour la seconde égalité, avec ce qui précède, la quantité $s_{P,Q^2}(a) - s_{P,Q^2}(b)$ correspond au nombre de racines de P non racines de Q sur $[a, b]$, c'est $n + p$. Par une bonne combinaison linéaire, on trouve

$$p = \frac{1}{2}[s_{P,Q}(a) - s_{P,Q}(b) + s_{P,Q^2}(a) - s_{P,Q^2}(b)].$$

Maintenant, on considère, plus généralement, le système

$$\begin{cases} R_i(x) = 0, & i \in J1, m\mathbb{K}, \\ Q_j(x) \diamond_j 0, & j \in J1, \ell\mathbb{K} \end{cases} \quad (\text{S})$$

avec $\diamond_j \in \{\geq, >\}$. On peut se ramener au cas $m = 1$ et $\diamond_j = >$, c'est-à-dire

$$\begin{cases} P(x) = 0, \\ Q_j(x) > 0, & j \in J1, \ell\mathbb{K}. \end{cases} \quad (\Sigma)$$

On cherche à savoir, en fonction des coefficients des polynômes P et Q_j , si le système (Σ) admet ou non des solutions.

Soit $\mu := (\mu_1, \dots, \mu_\ell) \in \{0, 1\}^\ell$. On pose

$$s^\mu := s_{P, Q^\mu}(-\infty) - s_{P, Q^\mu}(+\infty) \quad \text{avec} \quad Q^\mu := Q_1^{2-\mu_1} \dots Q_\ell^{2-\mu_\ell}$$

qu'on sait calculer « facilement » : il s'agit de la quantité

$$\#\{r \in \mathbb{R} \mid P(r) = 0, Q^\mu(r) > 0\} - \#\{r \in \mathbb{R} \mid P(r) = 0, Q^\mu(r) < 0\}.$$

Soit $\mu := (\mu_1, \dots, \mu_\ell) \in \{0, 1\}^\ell$. On pose

$$s^\mu := s_{P, Q^\mu}(-\infty) - s_{P, Q^\mu}(+\infty) \quad \text{avec} \quad Q^\mu := Q_1^{2-\mu_1} \dots Q_\ell^{2-\mu_\ell}$$

qu'on sait calculer « facilement » : il s'agit de la quantité

$$\#\{r \in \mathbb{R} \mid P(r) = 0, Q^\mu(r) > 0\} - \#\{r \in \mathbb{R} \mid P(r) = 0, Q^\mu(r) < 0\}.$$

On pose $\sigma^\mu \in \mathbb{N}$ le nombre de solutions du système

$$\begin{cases} P(x) = 0, \\ (-1)^{\mu_j} Q_j(x) > 0, \quad j \in \llbracket 1, \ell \rrbracket. \end{cases} \quad (\Sigma^\mu)$$

Pour cela, on cherche une relation entre les quantités σ^μ et s^μ . La quantité qui nous intéresse est $\sigma^{(0, \dots, 0)}$.

On considère les matrices

$$A_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \quad \text{et} \quad A_{\ell+1} \in \begin{pmatrix} A_\ell & A_\ell \\ A_\ell & -A_\ell \end{pmatrix} \in \mathrm{GL}_{2^{\ell+1}}(\mathbb{Z}), \quad \ell \geq 1.$$

Alors pour tout $\ell \geq 1$, on a

$$\begin{pmatrix} s^{(0,\dots,0,0)} \\ s^{(0,\dots,0,1)} \\ s^{(0,\dots,1,0)} \\ \vdots \\ s^{(1,\dots,1,1)} \end{pmatrix} = A_\ell \begin{pmatrix} \sigma^{(0,\dots,0,0)} \\ \sigma^{(0,\dots,0,1)} \\ \sigma^{(0,\dots,1,0)} \\ \vdots \\ \sigma^{(1,\dots,1,1)} \end{pmatrix}$$

On considère les matrices

$$A_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \quad \text{et} \quad A_{\ell+1} \in \begin{pmatrix} A_\ell & A_\ell \\ A_\ell & -A_\ell \end{pmatrix} \in \mathrm{GL}_{2^{\ell+1}}(\mathbb{Z}), \quad \ell \geq 1.$$

Alors pour tout $\ell \geq 1$, on a

$$\begin{pmatrix} s^{(0,\dots,0,0)} \\ s^{(0,\dots,0,1)} \\ s^{(0,\dots,1,0)} \\ \vdots \\ s^{(1,\dots,1,1)} \end{pmatrix} = A_\ell \begin{pmatrix} \sigma^{(0,\dots,0,0)} \\ \sigma^{(0,\dots,0,1)} \\ \sigma^{(0,\dots,1,0)} \\ \vdots \\ \sigma^{(1,\dots,1,1)} \end{pmatrix}$$

\Rightarrow On sait calculer la quantité $\sigma^{(0,\dots,0)}$ qui est exactement celle qui nous intéresse. Elle dépend linéairement des quantités s^μ et ces dernières dépendent uniquement des signes des coefficients des polynômes P et Q_j . On est trop content !

Théorème de Tarski-Seidenberg, forme système

Soient $n, \ell \in \mathbb{N}^*$. Soient $S_1, \dots, S_\ell \in \mathbb{R}[T_1, \dots, T_n, X]$ et $\diamond_1, \dots, \diamond_\ell \in \{>, =\}$. Alors il existe des systèmes d'équations et d'inéquations polynomiales $R_1(T), \dots, R_k(T)$ d'inconnue T tels que, pour tout vecteur $t \in \mathbb{R}^n$, on ait l'équivalence

$$(\exists x \in \mathbb{R}, \forall i \in \{1, \dots, \ell\}, S_i(t, x) \diamond_i 0) \iff R_1(t) \vee \dots \vee R_k(t).$$

Théorème de Tarski-Seidenberg, forme système

Soient $n, \ell \in \mathbb{N}^*$. Soient $S_1, \dots, S_\ell \in \mathbb{R}[T_1, \dots, T_n, X]$ et $\diamond_1, \dots, \diamond_\ell \in \{>, =\}$. Alors il existe des systèmes d'équations et d'inéquations polynomiales $R_1(T), \dots, R_k(T)$ d'inconnue T tels que, pour tout vecteur $t \in \mathbb{R}^n$, on ait l'équivalence

$$(\exists x \in \mathbb{R}, \forall i \in \mathbb{J}1, \ell\mathbb{K}, S_i(t, x) \diamond_i 0) \iff R_1(t) \vee \dots \vee R_k(t).$$

Preuve. On se ramène à un système de la forme (Σ) . On calcul toutes les suites de Sturm nécessaires à la recherche d'existence de solutions aux systèmes simples

$$P(T_1, \dots, T_n, x) = 0 \quad \text{et} \quad Q_j(T_1, \dots, T_n, x) > 0 \quad (j \in \mathbb{J}1, \ell\mathbb{K} \text{ fixé})$$

et on utilise le procédé algorithmique précédent qui nous donne l'existence de solution au système (Σ) . Ce calcul se fait dans $\mathbb{R}(T)[X]$. On divise à chaque fois en deux étapes en fonction de la nullité des coefficients dominants des polynômes.

Soient $a, b, c \in \mathbb{R}$ trois réels. Considérons l'équation

$$ax^2 + bx + c = 0 \tag{E}$$

d'inconnue $x \in \mathbb{R}$. Retrouvons, à l'aide de notre algorithme, le résultat bien connu pour qu'elle admette au moins une solution réelle.

Pour cela, on pose

$$P_0 := aX^2 + bX + c \in \mathbb{R}[X].$$

On suppose $a \neq 0$. Alors la suite de Sturm associée à P_0 est (P_0, P_1, P_2) avec

$$P_1 := P' = 2aX + b \quad \text{et} \quad P_2 := \frac{\Delta}{4a} \quad \text{avec} \quad \Delta := b^2 - 4ac$$

car

$$P_0 = \left(\frac{X}{2} + \frac{b}{4a} \right) P_1 - P_2.$$

Premier sous-cas. On suppose $\Delta/4a \neq 0$. Pour rappel, on a

$$P_0 = aX^2 + bX + c, \quad P_1 = 2aX + b \quad \text{et} \quad P_2 = \Delta/4a.$$

Alors

$\text{sgn}(\Delta)$	+	-	+	-	$\text{sgn}(\Delta)$	+	-	+	-
$\text{sgn}[c(P_0(-X))] = \text{sgn}(a)$	+	+	-	-	$\text{sgn}[c(P_0(X))] = \text{sgn}(a)$	+	+	-	-
$\text{sgn}[c(P_1(-X))] = \text{sgn}(-2a)$	-	-	+	+	$\text{sgn}[c(P_1(X))] = \text{sgn}(2a)$	+	+	-	-
$\text{sgn}[c(P_2(-X))] = \text{sgn}(\Delta/4a)$	+	-	-	+	$\text{sgn}[c(P_2(X))] = \text{sgn}(\Delta/4a)$	+	-	-	+
<hr/>					<hr/>				
$\mathfrak{s}_{P_0}(-\infty)$	2	1	2	1	$\mathfrak{s}_{P_0}(+\infty)$	0	1	0	1

Premier sous-cas. On suppose $\Delta/4a \neq 0$. Pour rappel, on a

$$P_0 = aX^2 + bX + c, \quad P_1 = 2aX + b \quad \text{et} \quad P_2 = \Delta/4a.$$

Alors

$\text{sgn}(\Delta)$	+	-	+	-	$\text{sgn}(\Delta)$	+	-	+	-
$\text{sgn}[c(P_0(-X))] = \text{sgn}(a)$	+	+	-	-	$\text{sgn}[c(P_0(X))] = \text{sgn}(a)$	+	+	-	-
$\text{sgn}[c(P_1(-X))] = \text{sgn}(-2a)$	-	-	+	+	$\text{sgn}[c(P_1(X))] = \text{sgn}(2a)$	+	+	-	-
$\text{sgn}[c(P_2(-X))] = \text{sgn}(\Delta/4a)$	+	-	-	+	$\text{sgn}[c(P_2(X))] = \text{sgn}(\Delta/4a)$	+	-	-	+
<hr/>					<hr/>				
$\mathfrak{s}_{P_0}(-\infty)$	2	1	2	1	$\mathfrak{s}_{P_0}(+\infty)$	0	1	0	1

Conclusion. L'équation admet des solutions si et seulement si

$$\mathfrak{s}_{P_0}(-\infty) - \mathfrak{s}_{P_0}(+\infty) > 0, \quad \text{i. e.} \quad \Delta > 0.$$

Deuxième sous-cas. On suppose $\Delta/4a = 0$. Alors la suite de Sturm est

$$P_0 = aX^2 + bX + c \quad \text{et} \quad P_1 = 2aX + b.$$

Alors

$$\begin{array}{rcc} \text{sgn}[c(P_0(-X))] = \text{sgn}(a) & + & - \\ \text{sgn}[c(P_1(-X))] = \text{sgn}(-2a) & - & + \\ \hline \mathfrak{s}_{P_0}(-\infty) & 1 & 1 \end{array}$$

$$\begin{array}{rcc} \text{sgn}[c(P_0(X))] = \text{sgn}(a) & + & - \\ \text{sgn}[c(P_1(X))] = \text{sgn}(2a) & + & - \\ \hline \mathfrak{s}_{P_0}(+\infty) & 0 & 0 \end{array}$$

Deuxième sous-cas. On suppose $\Delta/4a = 0$. Alors la suite de Sturm est

$$P_0 = aX^2 + bX + c \quad \text{et} \quad P_1 = 2aX + b.$$

Alors

$\text{sgn}[c(P_0(-X))] = \text{sgn}(a)$	+ -	$\text{sgn}[c(P_0(X))] = \text{sgn}(a)$	+ -
$\text{sgn}[c(P_1(-X))] = \text{sgn}(-2a)$	- +	$\text{sgn}[c(P_1(X))] = \text{sgn}(2a)$	+ -
$\mathfrak{s}_{P_0}(-\infty)$	1 1	$\mathfrak{s}_{P_0}(+\infty)$	0 0

Conclusion. Dans tous les cas, on a $\mathfrak{s}_{P_0}(-\infty) - \mathfrak{s}_{P_0}(+\infty) = 1 > 0$, donc l'équation admet des solutions.

On suppose $a = 0$. Alors la suite de Sturm est

$$P_0 = bX + c \quad \text{et} \quad P_1 = b.$$

Premier sous-cas. On suppose $b \neq 0$. Alors

$\text{sgn}[c(P_0(-X))] = \text{sgn}(-b)$	+	-	$\text{sgn}[c(P_0(X))] = \text{sgn}(b)$	+	-
$\text{sgn}[c(P_1(-X))] = \text{sgn}(b)$	-	+	$\text{sgn}[c(P_1(X))] = \text{sgn}(b)$	+	-
$\mathfrak{s}_{P_0}(-\infty)$	1	1	$\mathfrak{s}_{P_0}(+\infty)$	0	0

Conclusion. Dans tous les cas, on a $\mathfrak{s}_{P_0}(-\infty) - \mathfrak{s}_{P_0}(+\infty) = 1 > 0$, donc l'équation admet des solutions.

Second sous-cas. On suppose $b = 0$. Alors il est clair que l'équation admet des solutions si et seulement si $c = 0$.

On a ainsi traité tous les cas. Finalement, on peut savoir quand notre équation

$$ax^2 + bx + c = 0 \quad (\text{E})$$

admet des solutions et les calculs précédents montrent

$$\exists x \in \mathbb{R}, \quad ax^2 + bx + c = 0$$



$$(a \neq 0 \wedge b^2 - 4ac > 0) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0).$$

Partie 3

Une preuve par la théorie des modèles

Si $\phi(\bar{x})$ est une formule sur \mathcal{L}_{ord} , \mathcal{S} une \mathcal{L}_{ord} -structure, $\bar{a} \in \mathcal{S}^n$, on note :

$$\mathcal{S} \models \phi(\bar{a})$$

si ϕ est vrai en interprétant \bar{x} comme \bar{a} , les lois du corps ordonné comme celles de \mathcal{S} et en quantifiant sur \mathcal{S} .

Soit T un ensemble de formules closes. On appelle *modèle* de T une structure \mathcal{S} telle que $\mathcal{S} \models \phi$ pour tout $\phi \in T$.

Si ψ est une formule close, on note :

$$T \models \psi$$

si ψ est vrai dans tout modèle de T .

Si $T(\bar{x})$ est un ensemble de formules et $\psi(\bar{x})$ est une formule, on note $T(\bar{x}) \models \psi(\bar{x})$ si pour toute structure \mathcal{S} et $\bar{a} \in \mathcal{S}$ tels que $\mathcal{S} \models T(\bar{a})$, on a $\mathcal{S} \models \psi(\bar{a})$.

Théorème de compacité

Soit T, U deux ensembles de formules closes, ϕ une formule close. Si $T, U \models \phi$, il existe $\psi_1, \dots, \psi_k \in U$ tels que $T \models \left(\bigwedge_{i=1}^k \psi_i \right) \rightarrow \phi$.

Théorème

Soit \mathbb{K} un corps ordonné. Il y a équivalence entre :

- ▶ \mathbb{K} n'a pas d'extension algébrique propre ordonnée ;
- ▶ tout élément positif est un carré et tout polynôme unitaire de degré impair est irréductible ;
- ▶ $\mathbb{K}[X]/(X^2 + 1)$ est un corps algébriquement clos.

Définition

Dans le cas précédant, \mathbb{K} est un *corps réel clos*.

Exemples : \mathbb{R} , $\overline{\mathbb{Q}} \cap \mathbb{R}$, $\mathbb{R}((X^{1/N}))$, $\overline{\mathbb{Q}} \cap \mathbb{R}((X^{1/N}))$

- ▶ tout élément positif est un carré ;
- ▶ tout polynôme unitaire de degré impair est irréductible.

Cela s'exprime par un ensemble de formules :

$$\forall x, (x > 0 \rightarrow \exists y, x = y^2)$$

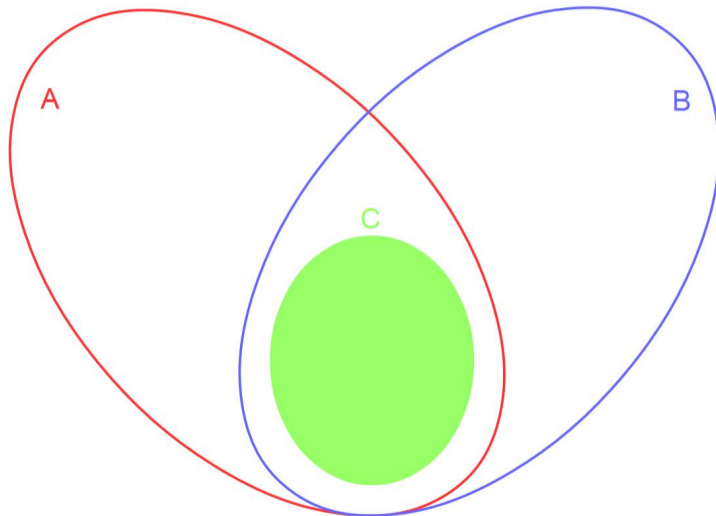
et pour $n \in \mathbb{N}$ impair :

$$\forall a_0, \dots, \forall a_{n-1}, \exists x, x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$$

On note CRC l'ensemble des axiomes des corps ordonnés et de ces formules.

Montrer que, pour toute formule $\phi(\bar{x})$ sur \mathcal{L}_{ord} , il existe une formule sans quantificateurs $\psi(\bar{x})$ telle que :

$$\text{CRC} \models \forall \bar{x}, \phi(\bar{x}) \leftrightarrow \psi(\bar{x})$$



Théorème

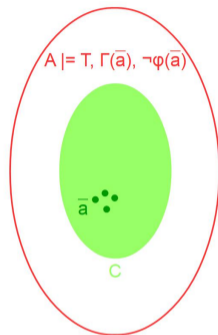
Soit T un ensemble de formules closes, $\phi(\bar{x})$ une formule. Il y a équivalence entre :

- ▶ il existe une formule sans quantificateurs $\psi(\bar{x})$ telle que $T \models \forall \bar{x}, \phi(\bar{x}) \leftrightarrow \psi(\bar{x})$;
- ▶ pour tous modèles \mathcal{A}, \mathcal{B} de T avec une sous-structure commune \mathcal{C} , pour tout $\bar{a} \subset \mathcal{C}$, on a $\mathcal{A} \models \phi(\bar{a})$ si et seulement si $\mathcal{B} \models \phi(\bar{a})$.

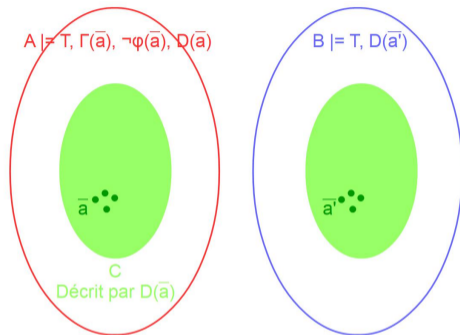
Preuve.

\Rightarrow OK

⊆ Supposons que pour tous modèles \mathcal{A}, \mathcal{B} de T avec une sous-structure commune \mathcal{C} , pour tout $\bar{a} \subset \mathcal{C}$, on a $\mathcal{A} \models \phi(\bar{a})$ si et seulement si $\mathcal{B} \models \phi(\bar{a})$.
Soit $\phi(\bar{x})$ une formule. Soit $\Gamma(\bar{x})$ l'ensemble des formules $\psi(\bar{x})$ sans quantificateur telles que $T \models \forall \bar{x}, \phi(\bar{x}) \rightarrow \psi(\bar{x})$.
Commençons par montrer $T \cup \Gamma(\bar{x}) \models \phi(\bar{x})$.



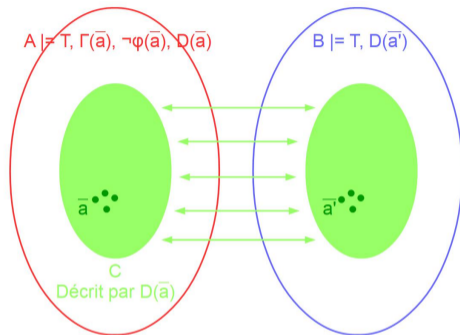
Par l'absurde, supposons qu'il existe $\mathcal{A}, \bar{a} \subset S$ tels que $\mathcal{A} \models T \cup \Gamma(\bar{a}) \cup \{\neg\phi(\bar{a})\}$.
Soit \mathcal{C} la sous-structure engendrée par \bar{a} .



Par l'absurde, supposons qu'il existe \mathcal{A} , $\bar{a} \subset S$ tels que $\mathcal{A} \models T \cup \Gamma(\bar{a}) \cup \{\neg\phi(\bar{a})\}$.

Soit \mathcal{C} la sous-structure engendrée par \bar{a} .

Soit $D(\bar{x})$ l'ensemble des formules sans quantificateur $\psi(\bar{x})$ telles que $\mathcal{C} \models \psi(\bar{a})$. Soit \mathcal{B} , $\bar{a}' \subset \mathcal{B}$ tel que $\mathcal{B} \models T \cup D(\bar{a}')$.



Par l'absurde, supposons qu'il existe \mathcal{A} , $\bar{a} \subset S$ tels que $\mathcal{A} \models T \cup \Gamma(\bar{a}) \cup \{\neg\phi(\bar{a})\}$.

Soit \mathcal{C} la sous-structure engendrée par \bar{a} .

Soit $D(\bar{x})$ l'ensemble des formules sans quantificateur $\psi(\bar{x})$ telles que $\mathcal{C} \models \psi(\bar{a})$. Soit \mathcal{B} , $\bar{a}' \subset \mathcal{B}$ tel que $\mathcal{B} \models T \cup D(\bar{a}')$.

La sous-structure engendrée par \bar{a}' est isomorphe à \mathcal{C} !

Avec l'hypothèse : $\mathcal{B} \models \neg\phi(\bar{a}')$.

Ainsi $T \cup D(\bar{x}) \models \neg\phi(\bar{x})$.

Par compacité, il existe $\psi_1(\bar{x}), \dots, \psi_k(\bar{x}) \in D(\bar{x})$ telles que :

$$T \models \forall \bar{x}, \left(\bigwedge_{i=1}^k \psi_i(\bar{x}) \right) \rightarrow \neg\phi(\bar{x})$$

$$T \models \forall \bar{x}, \phi(\bar{x}) \rightarrow \left(\bigvee_{i=1}^k \neg\psi_i(\bar{x}) \right).$$

Ainsi $\bigvee_{i=1}^k \neg\psi_i(\bar{x}) \in \Gamma(\bar{x})$. En particulier $\mathcal{A} \models \neg \bigwedge_{i=1}^k \psi_i(\bar{a})$. Mais $\mathcal{A} \models D(\bar{a})$, donc $\mathcal{A} \models \bigwedge_{i=1}^k \psi_i(\bar{a})$ ce qui est absurde.

Ainsi $T \cup \Gamma(\bar{x}) \models \phi(\bar{x})$ et on conclut par compacité.

Théorème

Soit $\phi(\bar{x})$ une formule. Alors pour tous corps réels clos \mathbb{K}, \mathbb{L} avec un sous-anneau commun A , pour tout $\bar{a} \subset A$, on a $\mathbb{K} \models \phi(\bar{a})$ si et seulement si $\mathbb{L} \models \phi(\bar{a})$.

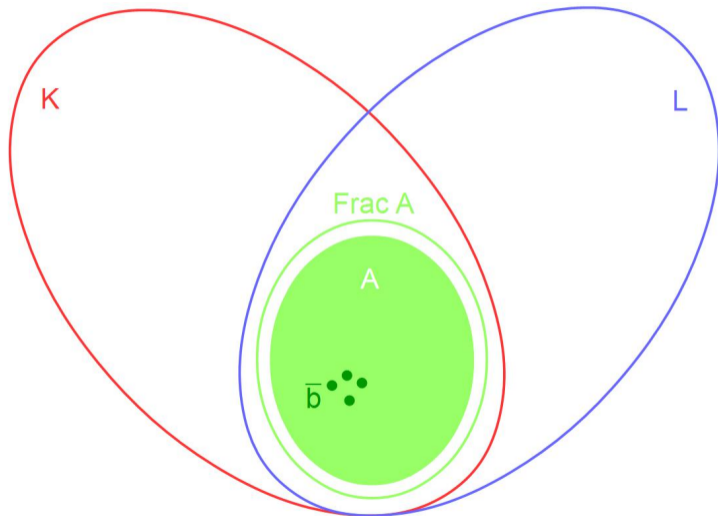
Preuve.

On pose $\phi(\bar{y}) := \exists x, \psi(x, \bar{y})$ avec

$$\psi(x, \bar{y}) := \exists x, \bigwedge_{i=1}^k (P_i(x, \bar{y}) = 0) \wedge \bigwedge_{i=1}^l (Q_i(x, \bar{y}) > 0).$$

On pose \mathbb{K} et \mathbb{L} deux corps réels clos avec un sous-anneau commun A , et $\bar{b} \subset A$ tel que $\mathbb{K} \models \phi(\bar{b})$. Montrons que $\mathbb{L} \models \phi(\bar{b})$.

Il existe $a \in \mathbb{K}$ tel que $\mathbb{K} \models \psi(a, \bar{b})$.



Théorème

Soit \mathbb{K} un corps ordonné. Il existe une extension \mathbb{L}/\mathbb{K} telle que \mathbb{L} est algébrique sur \mathbb{K} et réel clos.

Cette extension est unique à isomorphisme près.

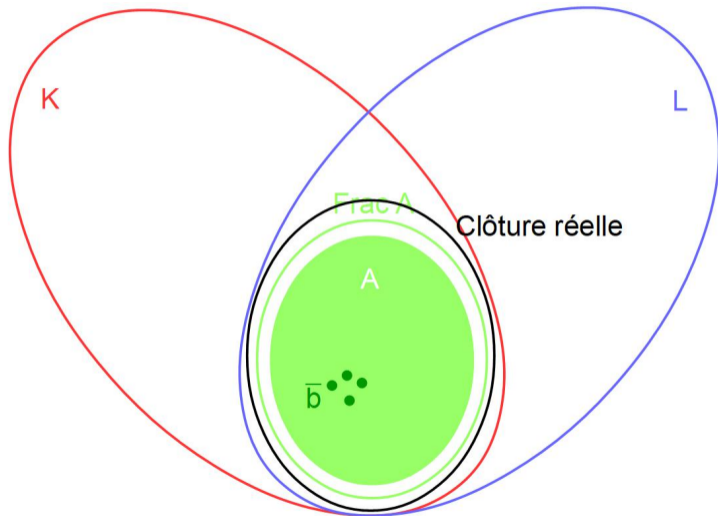
Enfin, toute extension réelle close de \mathbb{K} contient \mathbb{L} .

Définition

Dans le cas précédant, \mathbb{L} est la *clôture réelle* de \mathbb{K} .

Exemple : $\overline{\mathbb{Q}} \cap \mathbb{R}$ est la clôture réelle de \mathbb{Q} .

La clôture réelle de \mathbb{K} dans \mathbb{L} inclut les éléments algébriques sur \mathbb{K} .



$$\phi(\bar{y}) = \exists x, \psi(x, \bar{y}) = \exists x, \bigwedge_{i=1}^k (P_i(x, \bar{y}) = 0) \wedge \bigwedge_{i=1}^l (Q_i(x, \bar{y}) > 0)$$

Si il existe i tel que $P_i(X, \bar{b}) \neq 0$. Alors a est algébrique sur $\mathbb{Q}(\bar{b})$, donc est dans \mathbb{L} .
D'où $\mathbb{L} \models \phi(\bar{b})$.
Sinon...

$$\phi(\bar{y}) = \exists x, \psi(x, \bar{y}) = \bigwedge_{i=1}^l (Q_i(x, \bar{y}) > 0)$$

Les $Q_i(X, \bar{b})$ sont strictement positifs sur un intervalle $] -\infty, c[$, $]c, c'[$ ou $]c, +\infty[$ avec c, c' des zéros d'un des $Q_i(X, \bar{b})$. Donc c, c' sont algébriques sur $\mathbb{Q}(\bar{b})$.

Alors $c - 1, \frac{c + c'}{2}, c + 1$ sont algébriques sur $\mathbb{Q}(\bar{b})$, donc dans \mathbb{L} et tous les $Q_i(X, \bar{b})$ y sont positifs. D'où la conclusion.

- ▶ La généralité de la preuve : par exemple, quasiment la même preuve montre que la théorie des corps algébriquement clos élimine les quantificateurs.
- ▶ La généralisation au corps réels clos : par exemple, on déduit de ce qui précède que pour $\phi(\bar{x})$ une formule et $\bar{a} \subset \overline{\mathbb{Q}} \cap \mathbb{R}$:

$$\overline{\mathbb{Q}} \cap \mathbb{R} \models \phi(\bar{a}) \text{ ssi } \mathbb{R} \models \phi(\bar{a})$$

Partie 4

Conclusion

Merci pour votre attention !

Références.

George COMTE. *Géométrie algébrique*. 2016. URL :
<http://gcomte.perso.math.cnrs.fr/M2/CoursM2RGeometrieAlgebrique.pdf>.

Michel COSTE. *An Introduction to O-minimal Geometry*. 1999. URL :
<https://perso.univ-rennes1.fr/michel.coste/polyens/OMIN.pdf>.

Michel COSTE. *An Introduction to Semialgebraic Geometry*. 2000. URL :
<https://perso.univ-rennes1.fr/michel.coste/polyens/SAG.pdf>.

Françoise POINT. *Théorie des modèles 1*. 2015. URL :
<http://www.logique.jussieu.fr/~point/papiers/Bac3-2014-2015.pdf>.

Goulwen « le S » FICHOU. *Lecture on real closed fields*. 2021. URL :
<https://perso.univ-rennes1.fr/goulwen.fichou/RAG2.pdf>.