Le théorème de Tarski-Seidenberg

Deux preuves de ce résultat algébrique

Groupe de lecture entre nous

Éloan & Téofil

mercredi 24 février 2021

Introduction

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

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

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

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

n'est pas algébrique.

Introduction (ii)

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

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

où $(a_{n+1}, \ldots, a_{n+m}) \in \mathbb{R}^m$ est un vecteur et $\phi(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m})$ 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 le formule $\phi(x_1, \ldots, x_n)$ est une formule sur le langage

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

Introduction (iii)

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

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

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

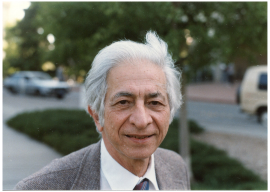
L'idée est d'enrichir le langage $\mathscr{L}_{\text{corps}}$ en $\mathscr{L}$ pour que les ensembles de la forme

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

où $\phi(\overline{x}, \overline{y})$ est une formule sans quantificateurs sur $\mathscr{L}$, 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)

Plan

Partie 1

Les trois formes du théorème

La forme algébrique

Théorème de Tarski-Seidenberg, forme algébrique

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

$$(\exists x \in \mathbb{R},\ \forall i \in [\![1, m]\!], \quad S_i(t, x) \diamond_i 0) \quad \Longleftrightarrow \quad R_1(t) \vee \cdots \vee R_k(t).$$

La forme algébrique

Théorème de Tarski-Seidenberg, forme algébrique

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

$$(\exists x \in \mathbb{R},\ \forall i \in [\![1, m]\!], \quad S_i(t, x) \diamond_i 0) \quad \Longleftrightarrow \quad R_1(t) \vee \cdots \vee R_k(t).$$

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

$$(\exists x \in \mathbb{R}, \quad x^2 = t) \quad \Longleftrightarrow \quad t \geqslant 0.$$

Formules logiques

On considère le langage des corps ordonnés

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

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

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

Formules logiques

On considère le langage des corps ordonnés

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

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

$$\phi(\overline{x}) := \Big(\exists t, \quad x_n t^n + \cdots + x_1 t + x_0 = 0\Big).$$

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

$$\forall x, \quad \Big[(x = 0) \vee (x > 0) \quad \Longrightarrow \quad \exists t,\ t^2 = x\Big].$$

Théorème de Tarski-Seidenberg, forme logique

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

$$\mathscr{L}_{\text{ord}} \coloneqq \{0, 1, +, \times, -, <\}.$$

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. Le classe des *ensembles semi-algébriques* est la plus petite classe de parties $\mathcal{SA}_n$ de $\mathbb{R}^n$ vérifiant

- si $P \in \mathbb{R}[X_1, \ldots, X_n]$, 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. Le 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.

La forme géométrique

Théorème de Tarski-Seidenberg, forme géométrique

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

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

La forme géométrique

Théorème de Tarski-Seidenberg, forme géométrique

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

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

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

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

Équivalences

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

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

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

Équivalences

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

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

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

- La forme géométrique implique clairement la forme algébrique.

Équivalences

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

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

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

- La forme géométrique implique clairement la forme algébrique.

- La forme algébrique implique la forme logique en usant un nombre fini de fois

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

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

Intérieur et adhérence d'un ensemble semi-algébrique

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

Proposition

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

Preuve

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

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

Après calcul, on trouve

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

avec

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

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

Partie 2

La preuve par le théorème de Sturm

Suite de Sturm d'un polynôme

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 $i \in [\![2, k]\!]$, 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 $\pm\,\mathrm{pgcd}(P, P')$.

Suite de Sturm d'un polynôme

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

- $P_0 = P$ et $P_1 = P'$;
- pour tout $i \in [\![2, k]\!]$, 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 $\pm\,\mathrm{pgcd}(P, P')$.

Définition

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

Exemple de suite de Sturm

Considérons le polynôme

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

Alors

$$\begin{aligned} P_0 &= X^3 - 6X^2 + 11X - 6, \\ P_1 &= 2X^2 - 12X + 11, \\ P_2 &= \tfrac{2}{3}X - \tfrac{4}{3}, \\ P_3 &= 1. \end{aligned}$$

Changement de signes dans la suite de Sturm

Définition

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

$$\mathfrak{s}_P(a) \coloneqq \sharp\{i \in [\![1, k]\!] \mid P_{i-1}(a)P_i(a) < 0\}.$$

Changement de signes dans la suite de Sturm

Définition

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

$$\mathfrak{s}_P(a) := \sharp\{i \in [\![1, k]\!] \mid P_{i-1}(a)P_i(a) < 0\}.$$

Exemple. Avec le polynôme précédent, on a

$$\begin{aligned}(P_0(-1), P_1(-1), P_2(-1), P_3(-1)) &= (-24, 25, -2, 1),\\ (P_0(4), P_1(4), P_2(4), P_3(4)) &= (6, 11, 4/3, 1).\end{aligned}$$

Alors

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

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

$$\mathfrak{s}_P(a) - \mathfrak{s}_P(b).$$

Le théorème de Sturm

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

$$\mathfrak{s}_P(a) - \mathfrak{s}_P(b).$$

Exemple. On a $\mathfrak{s}_P(4) - \mathfrak{s}_P(-1) = 3 - 0 = 3$ et le polynôme

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

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

Preuve : cas sans racine multiple

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.

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

Preuve : cas sans racine multiple

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.

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

$\Rightarrow$ Diminution du nombre de changements de signes !

Preuve : cas sans racine multiple (ii)

- Soient $i \in [\![1, k-1]\!]$ 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	
$\operatorname{sgn} P_{i-1}(x)$	$+$	$+$	$+$
$\operatorname{sgn} P_i(x)$	$+$	0	$+$
$\operatorname{sgn} P_{i+1}(x)$	$-$	$-$	$-$

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

Preuve : cas sans racine multiple (ii)

- Soient $i \in [\![1, k-1]\!]$ 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.

$$\begin{array}{l|ccc}
x & & r & \\
\operatorname{sgn} P_{i-1}(x) & + & + & + \\
\operatorname{sgn} P_{i}(x) & + & 0 & + \\
\operatorname{sgn} P_{i+1}(x) & - & - & -
\end{array}
\qquad
\begin{array}{l|ccc}
x & & r & \\
\operatorname{sgn} P_{i-1}(x) & - & - & - \\
\operatorname{sgn} P_{i}(x) & - & 0 & + \\
\operatorname{sgn} P_{i+1}(x) & + & + & +
\end{array}$$

$\Rightarrow$ Nombre de changements de signes constant !

Preuve : cas sans racine multiple (ii)

- Soient $i \in [\![1, k-1]\!]$ 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.

$$\begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P_{i-1}(x) & + & + & + \\ \operatorname{sgn} P_i(x) & + & 0 & + \\ \operatorname{sgn} P_{i+1}(x) & - & - & - \end{array} \qquad \begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P_{i-1}(x) & - & - & - \\ \operatorname{sgn} P_i(x) & - & 0 & + \\ \operatorname{sgn} P_{i+1}(x) & + & + & + \end{array}$$

$\Rightarrow$ 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.

Preuve : cas sans racine multiple (iii)

On va que la fonction $x \longmapsto \mathfrak{s}_P(x)$ 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

$$\mathfrak{s}_P(a) - \mathfrak{s}_P(b).$$

Preuve : cas général

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

$$\mathfrak{s}_P(a) = \mathfrak{s}_{P_0/P_k}(a).$$

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 !

Un corollaire utile

Corollaire

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

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

Alors le nombre de racines réelles de P est

$$\mathfrak{s}_P(-\infty) - \mathfrak{s}_P(+\infty).$$

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

$$\begin{aligned} p - n &= \mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b), \\ p &= \tfrac{1}{2}[\mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b) + \mathfrak{s}_{P,Q^2}(a) - \mathfrak{s}_{P,Q^2}(b)]. \end{aligned}$$

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

Preuve du lemme

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.

Preuve du lemme

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

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

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

$$\begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & - & 0 & + \\ \operatorname{sgn} P'(x) & + & + & + \\ \operatorname{sgn} P'Q(x) & + & + & + \end{array} \qquad \begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & + & 0 & - \\ \operatorname{sgn} P'(x) & - & - & - \\ \operatorname{sgn} P'Q(x) & - & - & - \end{array}$$

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

$$\begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & - & 0 & + \\ \operatorname{sgn} P'(x) & + & + & + \\ \operatorname{sgn} P'Q(x) & - & - & - \end{array} \qquad \begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & + & 0 & - \\ \operatorname{sgn} P'(x) & - & - & - \\ \operatorname{sgn} P'Q(x) & + & + & + \end{array}$$

Preuve du lemme (ii)

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

Preuve du lemme (ii)

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

En conclusion, la fonction $\mathfrak{s}_{P,Q}$ 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

$$p - n = \mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b).$$

Preuve du lemme (ii)

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

En conclusion, la fonction $\mathfrak{s}_{P,Q}$ 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

$$p - n = \mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b).$$

Pour la seconde égalité, avec ce qui précède, la quantité $\mathfrak{s}_{P,Q^2}(a) - \mathfrak{s}_{P,Q^2}(b)$ 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

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

Cas d'un système général

Maintenant, on considère, plus généralement, le système

$$\begin{cases} R_i(x) = 0, & i \in [\![1, m]\!], \\ Q_j(x) \diamond_j 0, & j \in [\![1, \ell]\!] \end{cases} \tag{S}$$

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

$$\begin{cases} P(x) = 0, & \\ Q_j(x) > 0, & j \in [\![1, \ell]\!]. \end{cases} \tag{Σ}$$

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

Cas d'un système général (ii)

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

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

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

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

Cas d'un système général (ii)

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

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

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

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

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

$$\begin{cases} P(x) = 0, \\ (-1)^{\mu_j} Q_j(x) > 0, \quad j \in [\![1, \ell]\!]. \end{cases} \tag{Σ^μ}$$

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

Calcul des quantités σ^μ

On considère les matrices

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

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

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

Calcul des quantités σ^μ

On considère les matrices

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

Alors pour tout $\ell \geqslant 1$, 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 $S_1, \ldots, S_\ell \in \mathbb{R}[T_1, \ldots, T_n, X]$ et $\diamond_1, \ldots, \diamond_\ell \in \{>, =\}$. Alors il existe des systèmes d'équations et d'inéquations polynomiales $R_1(T)$, ..., $R_k(T)$ d'inconnue T tels que, pour tout vecteur $t \in \mathbb{R}^n$, on ait l'équivalence

$$(\exists x \in \mathbb{R},\ \forall i \in [\![1, \ell]\!],\quad S_i(t, x) \diamond_i 0) \quad\Longleftrightarrow\quad R_1(t) \vee \cdots \vee R_k(t).$$

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 $R_1(T)$, ..., $R_k(T)$ d'inconnue T tels que, pour tout vecteur $t \in \mathbb{R}^n$, on ait l'équivalence

$$(\exists x \in \mathbb{R},\ \forall i \in [\![1, \ell]\!], \quad S_i(t, x) \diamond_i 0) \quad \Longleftrightarrow \quad R_1(t) \vee \cdots \vee R_k(t).$$

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

$$P(T_1, \dots, T_n, x) = 0 \quad \text{et} \quad Q_j(T_1, \dots, T_n, x) > 0 \qquad (j \in [\![1, \ell]\!] \text{ fixé})$$

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.

L'exemple du trinôme

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

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

Premier cas : $a \neq 0$

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

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

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

Premier cas : $a \neq 0$ (ii)

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

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

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

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

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

Premier cas : $a \neq 0$ (iii)

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

$$\begin{array}{lcc}
\operatorname{sgn}[\mathrm{c}(P_0(-X))] = \operatorname{sgn}(a) & + & - \\
\operatorname{sgn}[\mathrm{c}(P_1(-X))] = \operatorname{sgn}(-2a) & - & + \\
\hline
\mathfrak{s}_{P_0}(-\infty) & 1 & 1
\end{array}
\qquad
\begin{array}{lcc}
\operatorname{sgn}[\mathrm{c}(P_0(X))] = \operatorname{sgn}(a) & + & - \\
\operatorname{sgn}[\mathrm{c}(P_1(X))] = \operatorname{sgn}(2a) & + & - \\
\hline
\mathfrak{s}_{P_0}(+\infty) & 0 & 0
\end{array}$$

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

$$\begin{array}{lcc} \mathrm{sgn}[\mathrm{c}(P_0(-X))] = \mathrm{sgn}(a) & + & - \\ \mathrm{sgn}[\mathrm{c}(P_1(-X))] = \mathrm{sgn}(-2a) & - & + \\ \hline \mathfrak{s}_{P_0}(-\infty) & 1 & 1 \end{array} \qquad \begin{array}{lcc} \mathrm{sgn}[\mathrm{c}(P_0(X))] = \mathrm{sgn}(a) & + & - \\ \mathrm{sgn}[\mathrm{c}(P_1(X))] = \mathrm{sgn}(2a) & + & - \\ \hline \mathfrak{s}_{P_0}(+\infty) & 0 & 0 \end{array}$$

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 cas : $a = 0$

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

$$\begin{array}{lcc} \mathrm{sgn}[\mathrm{c}(P_0(-X))] = \mathrm{sgn}(-b) & + & - \\ \mathrm{sgn}[\mathrm{c}(P_1(-X))] = \mathrm{sgn}(b) & - & + \\ \hline \mathfrak{s}_{P_0}(-\infty) & 1 & 1 \end{array} \qquad \begin{array}{lcc} \mathrm{sgn}[\mathrm{c}(P_0(X))] = \mathrm{sgn}(b) & + & - \\ \mathrm{sgn}[\mathrm{c}(P_1(X))] = \mathrm{sgn}(b) & + & - \\ \hline \mathfrak{s}_{P_0}(+\infty) & 0 & 0 \end{array}$$

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 $c = 0$.

Conclusion de l'exemple

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

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

admet des solutions et les calculs précédents montrent

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

$$\Updownarrow$$

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

Partie 3

Une preuve par la théorie des modèles

Notations

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

$$\mathscr{S} \models \phi(\overline{a})$$

si ϕ est vrai en interprétant $\overline{x}$ comme $\overline{a}$, les lois du corps ordonné comme celles de $\mathscr{S}$ et en quantifiant sur $\mathscr{S}$.
Soit T un ensemble de formules closes. On appelle *modèle* de T une structure $\mathscr{S}$ telle que $\mathscr{S} \models \phi$ 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 $T(\overline{x})$ est un ensemble de formules et $\psi(\overline{x})$ est une formule, on note $T(\overline{x}) \models \psi(\overline{x})$ si pour toute structure $\mathscr{S}$ et $\overline{a} \in \mathscr{S}$ tels que $\mathscr{S} \models T(\overline{a})$, on a $\mathscr{S} \models \psi(\overline{a})$.

Théorème de compacité

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

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

Corps réels clos

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

Cela s'exprime par un ensemble de formules :

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

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

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

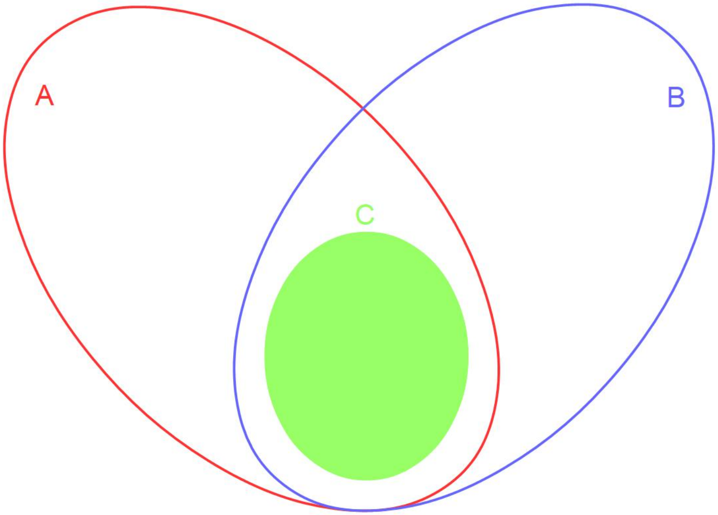
On note CRC l'ensemble des axiomes des corps ordonnés et de ces formules.

Objectif

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

$$\mathsf{CRC} \models \forall \overline{x}, \phi(\overline{x}) \leftrightarrow \psi(\overline{x})$$

Critère d'élimination des quantificateurs



Critère d'élimination des quantificateurs

Théorème

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

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

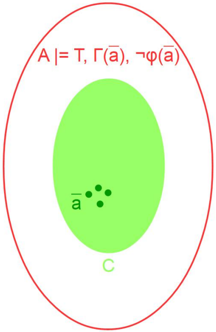
Preuve.

$\boxed{\Rightarrow}$ OK

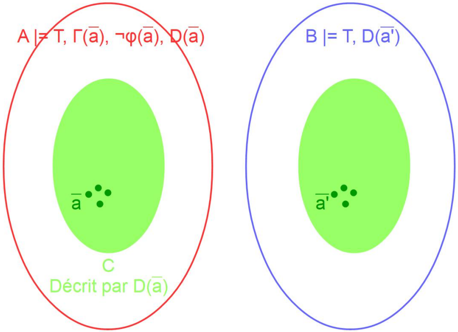
Critère d'élimination des quantificateurs

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

Critère d'élimination des quantificateurs

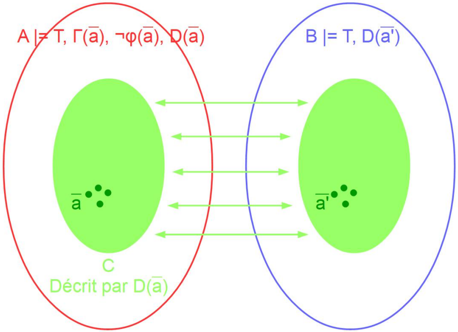


Par l'absurde, supposons qu'il existe $\mathcal{A}$, $\bar{a} \subset S$ tels que $\mathcal{A} \vDash T \cup \Gamma(\bar{a}) \cup \{\neg\phi(\bar{a})\}$.
Soit $\mathcal{C}$ la sous-structure engendrée par $\bar{a}$.



Par l'absurde, supposons qu'il existe $\mathcal{A}$, $\overline{a} \subset S$ tels que $\mathcal{A} \vDash T \cup \Gamma(\overline{a}) \cup \{\neg\phi(\overline{a})\}$.
Soit $\mathcal{C}$ la sous-structure engendrée par $\overline{a}$.
Soit $D(\overline{x})$ l'ensemble des formules sans quantificateur $\psi(\overline{x})$ telles que $\mathcal{C} \vDash \psi(\overline{a})$. Soit $\mathcal{B}$, $\overline{a'} \subset \mathcal{B}$ tel que $\mathcal{B} \vDash T \cup D(\overline{a'})$.

Critère d'élimination des quantificateurs



Par l'absurde, supposons qu'il existe $\mathcal{A}$, $\bar{a} \subset S$ tels que $\mathcal{A} \vDash T \cup \Gamma(\bar{a}) \cup \{\neg\phi(\bar{a})\}$.
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 $\mathcal{C} \vDash \psi(\bar{a})$. Soit $\mathcal{B}$, $\overline{a'} \subset \mathcal{B}$ tel que $\mathcal{B} \vDash T \cup D(\overline{a'})$.
La sous-structure engendrée par $\overline{a'}$ est isomorphe à $\mathcal{C}$!

Critère d'élimination des quantificateurs

Avec l'hypothèse : $\mathcal{B} \vDash \neg\phi(\overline{a'})$.
Ainsi $T \cup D(\overline{x}) \vDash \neg\phi(\overline{x})$.
Par compacité, il existe $\psi_1(\overline{x}), \ldots, \psi_k(\overline{x}) \in D(\overline{x})$ telles que :

$$T \vDash \forall \overline{x}, \left(\bigwedge_{i=1}^{k} \psi_i(\overline{x}) \right) \to \neg\phi(\overline{x})$$

$$T \vDash \forall \overline{x}, \phi(\overline{x}) \to \left(\bigvee_{i=1}^{k} \neg\psi_i(\overline{x}) \right).$$

Ainsi $\bigvee_{i=1}^{k} \neg\psi_i(\overline{x}) \in \Gamma(\overline{x})$. En particulier $\mathcal{A} \vDash \neg \bigwedge_{i=1}^{k} \psi_i(\overline{a})$. Mais $\mathcal{A} \vDash D(\overline{a})$, donc $\mathcal{A} \vDash \bigwedge_{i=1}^{k} \psi_i(\overline{a})$ ce qui est absurde.
Ainsi $T \cup \Gamma(\overline{x}) \vDash \phi(\overline{x})$ et on conclut par compacité.

Application aux corps réels clos

Théorème

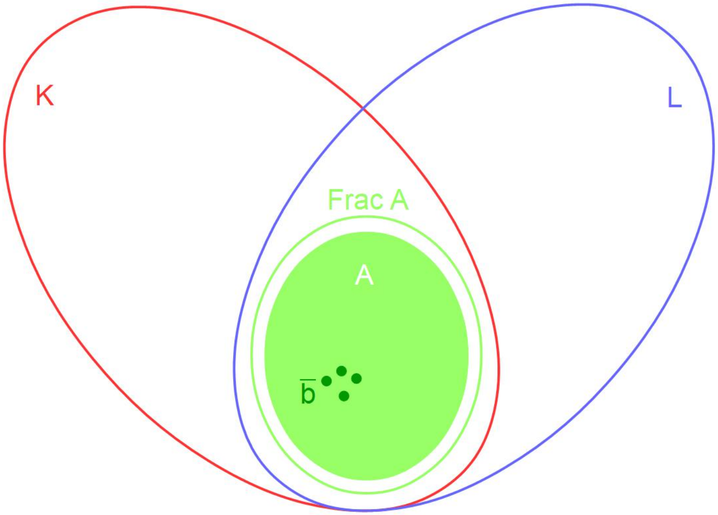
Soit $\phi(\overline{x})$ une formule. Alors pour tous corps réels clos $\mathbb{K}, \mathbb{L}$ avec un sous-anneau commun A, pour tout $\overline{a} \subset A$, on a $\mathbb{K} \vDash \phi(\overline{a})$ si et seulement si $\mathbb{L} \vDash \phi(\overline{a})$.

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

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

On pose $\mathbb{K}$ et $\mathbb{L}$ deux corps réels clos avec un sous-anneau commun A, et $\overline{b} \subset A$ tel que $\mathbb{K} \vDash \phi(\overline{b})$. Montrons que $\mathbb{L} \vDash \phi(\overline{b})$.
Il existe $a \in \mathbb{K}$ tel que $\mathbb{K} \vDash \psi(a, \overline{b})$.

Application aux corps réels clos



Clôture réelle

Théorème

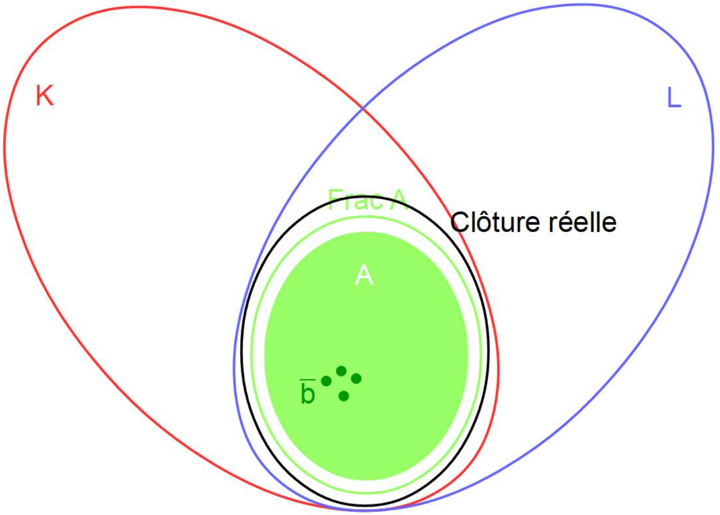
Soit $\mathbb{K}$ un corps ordonné. Il existe une extension $\mathbb{L}/\mathbb{K}$ telle que $\mathbb{L}$ est algébrique sur $\mathbb{K}$ et réel clos.
Cette extension est unique à isomorphisme près.
Enfin, toute extension réelle close de $\mathbb{K}$ contient $\mathbb{L}$.

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 $\mathbb{K}$.

Application aux corps réels clos



Application aux corps réels clos

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

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

Application aux corps réels clos

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

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

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

Avantage de la preuve

- 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 $\phi(\overline{x})$ une formule et $\overline{a} \subset \overline{\mathbb{Q}} \cap \mathbb{R}$:

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

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.