Notes de l'exposé du 20 novembre à l'ENS Lyon, au Séminaire des doctorants et doctorantes.

Le 17ième problème de Hilbert : une preuve modèle-théorique.

Prérequis : Langage, théorie, formule, modèle-complétude, structure.

Plan :

I – Corps ordonnable.
  1) Corps ordonné – Exemple.
  2) Corps ordonnable – Extension – Ex. Corps formellement réel.

II – Corps réel clos
  1) Définition alg – Clôture réelle
  2) Équivalents – RCF – Modèle-complétude.

III – 17ième Hilbert : Énoncé & preuve.

IV – Pour aller plus loin.
  – Positivstellensatz –.

. Christian d'Elbée .

En 1900 lors du Deuxième international des mathématiciens à Paris, David Hilbert présenta une liste des 23 problèmes qui - selon lui - devait marquer le cours des mathématiques du 20ème siècle. Le 17ème problème s'énonce ainsi : Toute fonction rationnelle réelle ne prenant que des valeurs positives est une somme de carrés.

C'est en 1927 que Emil Artin proposa une preuve à cette conjecture. Elle était basée sur un raisonnement sur le monde des réels et met des outils de l'algèbre réelle, ou géométrie semi-algébrique.

Le théoricien des modèles Abraham Robinson proposa une preuve plus tard, avec des outils de base de théorie des modèles. C'est cette preuve que nous présentons dans cet exposé.

I - Corps ordonnable.

1) Corps ordonnés - Exemples

Un corps, j'espère que tout le monde sait de quoi il s'agit. On dit que un corps $(K, +, \cdot, 0, 1)$ est <u>ordonné</u> si l'on dispose d'une relation d'ordre $<$ totale, stricte telle que

$$\forall a, b, c \qquad a < b \Rightarrow a + c < b + c$$

$$a < b \text{ et } c > 0 \Rightarrow ac < bc.$$

<u>Exemple</u> : $(\mathbb{R}, +, \cdot, 0, 1, <)$, $(\mathbb{Q}, +, \cdot, 0, 1)$, tout sous corps K de $\mathbb{R}$ hérite de l'ordre naturel sur $\mathbb{R}$.

<u>Remarques</u> : On retrouve dans les corps ordonnés les propriétés suivantes :

(1) $-1 < 0$ et $1 > 0$:

Si 1 était négatif : alors, $1 - 1 < -1$
donc $-1 > 0$ donc $1 < 0 \Rightarrow -1 < 0$ ↯
donc $1 > 0$, $-1 < 0$.

(1') car $K = 0$.

(2) Un carré est positif, de même pour les sommes de carrés.

(si $a < 0$ et $a^{-1} > 0$ alors $a \cdot a^{-1} = 1 < 0$ de $a^{-1} > 0$)
si $a > 0$ et $a^{-1} < 0$ ———— $a^{-1} < 0$
donc a et a^{-1} sont de même "signe".

Ensuite si $a^2 < 0$. si $a \geq 0$ ce n'est pas possible.
sinon $(-a)^2 < 0$ où $-a > 0$ et ce n'est pas possible.

$a^2 = (-a)^2$ et l'un des 2 a ou $-a$ est > 0 donc le produit de 2 positifs est > 0.

($a < 0 \Rightarrow a - a < -a$ donc $-a > 0$).

2) Corps Ordonnable.

C'est un corps $(R, +, \cdot, 0, 1)$ tel qu'il existe un ordre $<$ sur R tq $(R, +, \cdot, 0, 1, <)$ est un corps ordonné.

<u>Exemple</u> : (1) $\mathbb{Q}$, $\mathbb{R}$, l'ordre est unique.

(2) $\mathbb{Q}(X)$: admet $2^{\aleph_0}$-ordres non isomorphes.

[illegible] $\mathbb{Q}(X)$ alg. corps ord. $\mathbb{Q}$ $\mathbb{Q}$

$x \in \mathbb{R}$ transcendant, $f : \mathbb{Q}(X) \to \mathbb{Q}(x)$ et on définit l'ordre sur $\mathbb{Q}(X)$ par le pullback de l'ordre sur $\mathbb{Q}(x) \subseteq \mathbb{R}$.

Comme $\{q \in \mathbb{Q} \mid q < x\}$ est différent pour chaque transcendant $x \in \mathbb{R}$ et qu'on a que sur le corps fixe $\mathbb{Q}$ chaque transcendant définit un ordre non isomorphe.

On peut même ordonner $\mathbb{Q}(X)$ en mettant X à l'infini ou infinitésimal.

Un corps $(R, +, \cdot)$ est <u>formellement réel</u> si -1 n'est pas une somme de carrés d'élt de R.
$(-1 \notin \Sigma \square)$.

<u>Lemme</u> (Artin-Schreier) 1

Si R est formellement réel et que $a \in R$ est tel que $-a \notin \Sigma \square$, alors il existe un ordre $<$ sur R tel que $a > 0$.

En particulier

<u>Corollaire</u> : $(R, +, \cdot)$ est formellement réel ssi $(R, +, \cdot)$ est ordonnable.

On a donc une caractérisation algébrique de l'existence d'un ordre, il suffit que -1 ne soit pas une somme. Par exemple un corps algébriquement clos n'est pas ordonnable, même si cela n'utilise que le sens trivial de l'implication.

Digression : • Unicité des extensions de corps ordonnés : On voit que si d'un point de vue strictement algébrique, l'extension $\begin{array}{c}\mathbb{Q}(x)\\ | \\ \mathbb{Q}\end{array}$ est unique. Alors d'un point de vue des corps ordonnés il existe $2^{\aleph_0}$ ext de corps ordonnés $\begin{array}{c}\mathbb{Q}(x)\\ | \\ \mathbb{Q}\end{array}$. On peut aussi voir que $\begin{array}{c}\mathbb{Q}(\sqrt{2})\\ | \\ \mathbb{Q}\end{array}$ admet deux ordres sur $\mathbb{Q}(\sqrt{2})$ en mettant $\sqrt{2} > 0$ ou $\sqrt{2} < 0$, donc non clair.

• Q(X) peut être ordonné de façon non archimédienne.

Soit $f(X) \in \mathbb{Q}(X)$ et on écrit $f(X) = \frac{P(X)}{Q(X)}$ avec $Q(X)$ unitaire. On note $cd(f)$ le coefficient dominant de $P(X)$.

On pose alors $f(X) > 0$ ssi $cd(f) > 0$.

Autrement dit

$$f(X) < g(X) \quad \text{ssi} \quad cd\,(f(X) - g(X)) < 0$$

On montre alors que cet ordre fait de $\mathbb{Q}(X)$ un corps ordonné non archimédien puisque

$$\mathrm{cd}\,(X - n) = 1 > 0$$

donc $\quad X > n \quad \forall n \in \mathbb{N}.$

X est un élément infini; $1/X$ un infinitésimal.

II - Corps réels clos :

1) Définition alg. - Exemples.

Pour motiver la définition, penchons nous sur la question : comment peut-on étendre l'ordre d'un corps K sur une extension algébrique.

Pour $\mathbb{R}$, toute extension algébrique non triviale n'est pas formellement réelle, puisque c'est $\mathbb{C} = \mathbb{R}(i)$. Donc $\mathbb{R}$ n'a pas d'extension algébrique formellement réelle et stricte.

- Un corps formellement réel qui n'a pas d'extension algébrique stricte et formellement réel est dit <u>réel-clos</u>.

- Pour n'importe quel corps formellement réel k, en prenant la classe :

$$\mathcal{C} = \left\{ \begin{array}{l} \text{~~extension~~ } L \text{ de } k \text{ algébrique} \\ \text{et formellement réel} \end{array} \right\}$$

C'est - ordonné par l'inclusion de corps - un ensemble inductif et en appliquant le lemme de Zorn il existe un élément maximal. C'est un corps formellement réel et même réel-clos qui est une extension algébrique de k, on le note $\tilde{k}$, appelée la <u>clôture réelle</u> de k.

L'ordre sur un corps réel clos est unique, il est donné par l'ensemble des carrés :

$$x > 0 \text{ ssi } \exists y\ x = y^2.$$

On n'a évidemment pas unicité de la clôture réelle : $\mathbb{Q}(\sqrt{X}) \not\cong \mathbb{Q}(\sqrt{-X})$, $\supseteq \mathbb{Q}$, les clôtures réelles ne sont pas isomorphes.

mieux

<u>Théorème</u> (Artin-Schreier) Soit $(R,<)$ un corps ordonné et $(\tilde{R}^1, <_1)$ ~~et~~ $(\tilde{R}^2, <_2)$ deux clôtures réelles qui ~~etc~~ t.q. $<_1 \restriction R = <_2 \restriction R$, alors

$$(\tilde{R}^1, <_1) \simeq (\tilde{R}^2, <_2) \text{ sont isomorphes}$$

en tant que corps ordonnés.
Autrement dit, si on fixe l'ordre, la clôture réelle est fixée (à iso près).

On parle donc de <u>la</u> clôture réelle d'un corps ordonné.

<u>Exemple</u> : (non unicité) $F = \mathbb{Q}(X)$

$F(\sqrt{X})$ — $\sqrt{X}$ n'est pas somme de carrés dans

$F(\sqrt{-X})$ — $\sqrt{-X}$ n'est pas $\Sigma\square$

on peut les ordonner et les clôt. réelles ne sont pas iso/F car X est un carré dans l'un et ne l'est pas dans l'autre.

2) Théorie RCF :

On a les équivalents suivants :

(1) k est réel-clos ($<$ sa unique ordre)

(2) • $\forall x$ x ou $-x$ $\in k^2$

• tout polynôme de degré impair admet une racine dans k

(3) (TVI) $a < b$, $P \in k[X]$,

$P(a) \cdot P(b) < 0$

$\longrightarrow \exists c \in]a,b[\ P(c) = 0$.

(4) $k^{alg} = k(i)$ où $i^2 = -1$.

(5) $[k^{alg} : k]$ est fini (Théorème d'Artin-Schreier).

La caractérisation (2) nous permet de donner une axiomatique à la classe des corps réels clos, car c'est exprimable.

• $\forall x\ \exists y\ (x = y^2) \vee (-x = y^2)$

• Pour tout n $\forall x_0 \dots x_{2n+1}\ \exists y$

$$\sum_{i=0}^{2n+1} x_i y^i = 0$$

On note cette théorie RCF.

Théorème : • RCF est complète

• RCF est modèle-complète.

Exemples de corps réels clos :

- $\mathbb{R}$: on a vu.

- $\mathbb{Q}^{alg} \cap \mathbb{R}$: Par le critère (3) : $P \in \mathbb{Q}^{alg} \cap \mathbb{R}$

  $a < b$ $\quad P(a) \cdot P(b) < 0$

  $\exists\ c \in \,]a, b[_{\mathbb{R}}$ tq

  $P(c) = 0$

  donc $c \in \mathbb{Q}^{alg} \cap \mathbb{R}$, de

  $c \in \,]a, b[_a$

  En particulier $(\mathbb{Q}^{alg} \cap \mathbb{R})(i) = \mathbb{Q}^{alg}$.

- corps superréels :

  X espace de Tychonov (1)

  $C(X)$ l'algèbre des fct continues $X \to \mathbb{R}$

  P idéal premier. Alors $\left(C(X)/P\right)^{Frac}$ peut être muni d'un ordre total, en formant un corps réel clos

- Nombres surréels de Conway.

III – 17ième Problème de Hilbert

Énoncé: Si $f(X) \in R(X) = R(X_1 \dots X_n)$ et

$R \models RCF$.

Si $\forall a \in R,\ f(a) \geq 0$, alors

$\exists\ g_1 \dots g_n \in R(X)$ tel que

$$f = \sum_i g_i .$$

Preuve: On suppose que f n'est pas une somme de carrés. ~~donc~~

Par le lemme 1 il existe un ordre sur $R(X)$ tel que $-f > 0$ donc $f < 0$. En effet $R(X)$ est formellement réel car si

$$-1 = \sum g_i^2 ,$$ ~~par indépendance des X_i~~

les termes constants forment une $\Sigma\square$ de $R = -1$.

$$\left[\quad -1 = \sum_i \Big(\sum_j \alpha_j^i X^{M_j}\Big)^2 = \underset{\substack{\parallel \\ 0}}{Q(X)} + \sum \alpha_e^{0\,2} \right]$$

De plus l'ordre $<_1$ sur $R(X)$ étend celui de R puisque $<_1 \restriction R$ est l'unique ordre sur R.

Ensuite $(R(X), <_1)$ admet une clôture réelle

$$\widetilde{R(X)} \models \exists x\ f(x) < 0$$

$$|$$

$$R(X)$$

$$|$$

$$R \models \exists x\ f(x) < 0 .$$

contradiction.

IV - Positivstellensatz

En 1964, Jean Louis Krivine a prouvé un analogue au Nullstellensatz au moyen d'outils modèle-théoriques très proche de ce que l'on a présenté. Soit R un corps ~~réel clos~~.

$X = X_1 \ldots X_n$. On rappelle les notations classiques de géométrie algébrique :

$$J \text{ idéal de } R[X] \ : \ V(J) = \{a \in R^n, f(a) = 0 \ \forall f \in J\}$$

$$V \subseteq R^n \ : \ I(V) = \{P \in R[X] \ P(a) = 0 \ \forall a \in R^n\}$$

On dit qu'un idéal J de $R[X]$ est positif si $\forall \lambda_i \in R^2 \setminus \{0\}$ $f_1 \cdots f_s \in R[X]$

$$\sum \lambda_i f_i^2 \in J \Rightarrow f_1 \ldots f_s \in J$$

Théorème : Si R est réel clos ~~alors~~ J idéal de $R[X]$

alors $J = I(V(J))$ ssi J est positif.