Exemple de théories décidables.

Dans ce chapitre, on traite de l'élimination des quantificateurs dans les corps réels clos (et les corps algébriquement clos).

1 De quoi on parle ?

1.1 L'élimination des quantificateurs.

Définition 1. Une théorie T (de la logique du 1er ordre) admet *l'élimination des quantificateurs* si pour toute formule $\varphi(\bar{y})$, il existe une formule sans quantificateurs $\psi(\bar{y})$ telle que $T \vdash \forall \bar{y}\,(\varphi(\bar{y}) \leftrightarrow \psi(\bar{y}))$.

Lemme 1. Une théorie T élimine les quantificateurs ssi pour toute formule $\varphi(x, \bar{y})$ sans quantificateurs, il existe une formule $\psi(\bar{y})$ sans quantificateurs et $T \vdash \forall \bar{y}\,(\exists x\, \varphi(x, \bar{y}) \leftrightarrow \psi(\bar{y})))$.

Preuve. Idée de la preuve :

- ▷ « $\implies$ ». C'est un cas particulier.
- ▷ « $\impliedby$ ». Toute formule est équivalente à une formule prénexe, c'est-à-dire une formule où les quantificateurs sont à la racine :

$$\mathsf{Q}_1 x_1\, \mathsf{Q}_2 x_2\, \ldots\, \mathsf{Q}_n x_n\, \varphi(x_1, \ldots, x_n),$$

où $\varphi(\cdots)$ est sans quantificateurs. Pour démontrer que toute formule est équivalente à une formule prénexe, on procède par induction sur la formule, et on doit potentiellement procéder à des cas d'α-renommage au besoin.

Pour toute formule sous forme prénexe, le lemme est vrai.

$\square$

Exemple 1. La théorie des booléens est la théorie

$$T_{\text{bool}} := \{\forall x\, x = 0 \vee x = 1, 0 \neq 1\},$$

sur le langage $\mathscr{L} = \{0, 1\}$. Cette théorie admet l'élimination des quantificateurs. En effet, par exemple, une formule

$$F := \exists x_1 \; \cdots \; \exists x_n \; (x_1 = 1 \vee x_2 = 0 \vee x_4 = 1) \wedge \cdots),$$

est équivalente à $\top$ ou $\perp$.

Exemple 2. Sur le langage $\mathscr{L}_{\text{co}} = \{0, 1, +, \times, \leq\}$, la théorie $T := \mathbf{Th}(\mathbb{R})$ admet l'élimination des quantificateurs. En effet, par exemple, la formule

$$\varphi(a, b, c) := \exists x\; (a \times x \times x + b \times x + c = 0)$$

est équivalente à la formule sans quantificateurs

$$\psi(a, b, c) := (a \neq 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)\ .$$

1.2 Les corps réels clos et le théorème de Tarski.

Définition 2. Un *corps réel clos* est un corps commutatif ordonné dans lequel on a le théorème des valeurs intermédiaires pour les polynômes à 1 variable.

La théorie T_{CRC} est la théorie du 1er ordre et ses axiomes sont :

- ▷ axiomes de corps commutatifs ;

- axiomes de relation d'ordre total ;
- $1 > 0$;
- axiomes de corps ordonné (compatibilité de $+$ et $\times$ avec $\leq$) :

$$\forall x\, \forall y\, \forall z\ \begin{pmatrix} x \leq y \to x + z \leq y + z \\ \wedge \\ (z \geq 0 \wedge x \leq y) \to x \times y \leq y \times z \\ \wedge \\ (z \leq 0 \wedge x \leq y) \to x \times y \geq y \times z \end{pmatrix} ;$$

- schéma d'axiomes pour le théorème des valeurs intermédiaires : pour $n \in \mathbb{N}$,

$$\begin{gathered} \forall a_0 \dots a_n\, \forall x\, \forall y \\ a_0 + a_1 x + \cdots + a_n x^n \geq 0 \wedge a_0 + a_1 y + \cdots + a_n y^n \leq 0 \\ \downarrow \\ \exists z\ (x \leq z \leq y \vee y \leq z \leq x) \wedge a_0 + a_1 z + \cdots + a_n z^n = 0. \end{gathered}$$

Exemple 3. Exemples de corps réels clos : $\mathbb{R}$ les réels, $\bar{\mathbb{Q}} \cap \mathbb{R}$ les nombres réels algébriquement clos.

Qu'en est-il de $\mathbb{C}$? Si on a $i \geq 0$ et on a $1 \leq 2$ donc $i \leq 2i$ et par multiplication par i on a $-1 \leq -2$, absurde ! Le même procédé fonctionne si l'on suppose $i \leq 0$. Il n'y a pas de manière d'ordonner $\mathbb{C}$ de telle sorte à ce qu'il soit un corps réel clos.

Proposition 1.
1. Un corps réel clos est de caractéristique 0.
2. Dans un corps réel clos, on a le théorème de Rolle (entre deux racines d'un polynôme, la dérivée s'annule).

Preuve. Idée de la preuve :

1. On a $1 > 0$ donc $2 > 1 > 0$ donc $3 > 0$, *etc.* On montre, par récurrence, pour tout n que $n > 0$ et donc $n \neq 0$.
2. On montre que si la dérivée est de signe constant alors le

polynôme est monotone d'où le théorème de Rolle. □

À quoi ressemblent les formules dans $\mathscr{L}_{\text{co}}$?

- Les termes représentent des polynômes à plusieurs variables et à coefficients dans $\mathbb{N}$.
- Les formules atomiques représentent des équations et inéquations entre polynômes :

$$P(X) \le Q(X) \text{ ou } P(X) = Q(X),$$

  et même $P(X) \geq 0$ ou $P(X) = 0$ avec P à coefficient dans $\mathbb{Z}$.
- Les formules sans quantificateur sont équivalentes à des formules de la forme

$$\bigvee_i \bigwedge_j (P_{i,j} \; \Delta_{i,j} \; 0),$$

  où $\Delta_{i,j} \in \{<, >, =\}$.
- Les formules sont équivalentes à des formules sous forme prénexe de la forme

$$\mathsf{Q}_1 x_1 \dots \mathsf{Q}_n x_n \; \bigvee_i \bigwedge_j (P_{i,j} \; \Delta_{i,j} \; 0),$$

  avec $\mathsf{Q}_i \in \{\forall, \exists\}$.

Théorème 1 (Tarski). La théorie des corps réels clos admet l'élimination des quantificateurs. Elle est axiome-complète et décidable.

Preuve. En supposant que T_{CRC} admet l'élimination des quantificateurs, alors on a une théorie axiome-récursive ~~qui contient les entiers donc indécidable par Gödel~~. Non ! On ne contient pas $\mathscr{P}_0$! En effet, l'axiome $\mathsf{A1}$ n'est pas vérifié : on n'a pas $\mathsf{S} x \neq 0$!

Soit F une formule close de $\mathscr{L}_{\text{co}}$. Montrer que $T_{\text{CRC}} \vdash F$ ou $T_{\text{CRC}} \vdash \neg F$. Il existe une formule sans quantificateurs G et $T_{\text{CRC}} \vdash F \leftrightarrow G$ et G n'a pas de variable. Ainsi G est équivalent à une conjonction de disjonction de formules équivalentes à

$$\text{ⓝ} > \text{ⓜ} \text{ ou } \text{ⓝ} = \text{ⓜ}.$$

La valeur de vérité ne dépend pas du modèle, d'où $T_{\text{CRC}} \vdash G$ ou $T_{\text{CRC}} \vdash \neg G$, donc $T_{\text{CRC}} \vdash F$ ou $T_{\text{CRC}} \vdash \neg F$, et donc T_{CRC} est axiome-complète.

Comme T_{CRC} est axiome-récursive, pour décider si $T_{\text{CRC}} \vdash F$, il suffit d'énumérer toutes les preuves jusqu'à en trouver une de F ou de $\neg F$. $\square$

2 La méthode d'élimination.

2.1 Rappels et exemples.

Il suffit de montrer le lemme ci-dessous.

Lemme 2. Si pour toute formule F de la forme $\exists x \bigvee_i \bigwedge_k P_{i,j} \; \Delta_{i,j} 0$ avec $P_{i,j}$ des polynômes et $\Delta_{i,j} \in \{<, >, =\}$, il existe une formule sans quantificateurs G telle que

$$T_{\text{CRC}} \vdash \forall \bar{y} \, G(\bar{y}) \leftrightarrow F(\bar{y})$$

alors T_{CRC} admet l'élimination des quantificateurs.

Idée de la méthode :

- On part d'un polynôme, par exemple $ax^2 + bx + 1$.
- On calcule des « quantités importantes » (des polynômes de degré 0 en x), ici a et $a^2 - 4a$.
- On trouve des « conditions de signe » qui permettent de satisfaire la formule, ici $a \neq 0 \wedge a^2 - 4a \geq 0$.

Définition 3. Avec $P \in \mathbb{Z}[\bar{Y}][X] = \mathbb{Z}[Y_1, \ldots, Y_n][X]$, les polynômes s'écrivent comme

$$P(X) = a_n X^n + \cdots + a_0 \text{ où } n \geq 1,\ a_n \neq 0 \text{ et } a_i \in \mathbb{Z}[\bar{Y}],$$

et on définit les opérations :

- ▷ *dérivée* $\mathrm{D}(P) := \frac{\partial P(X)}{\partial X}$;
- ▷ *extraction du coefficient dominant* $\mathrm{E}(P) := a_n$;
- ▷ *omission du terme dominant* $\mathrm{O}(P) := a_{n-1}X^{n-1} + \cdots + a_0$;
- ▷ *reste modifié* $\mathrm{MR}(P, Q)$:
  si $P = a_n X^n + \cdots + a_0$ et $Q = b_n X^n + \cdots + b_0$ où

  $$n = \deg P \geq m = \deg Q \geq 1$$

  et $P \neq Q$ alors $\mathrm{MR}(P, Q)$ est l'unique polynôme de $\mathbb{Z}[\bar{Y}][X]$ de degré $r < m$ tel qu'il existe $L \in \mathbb{Z}[\bar{Y}][X]$ et

  $$(b_n)^{nm+1} \times P = Q \times L + R.$$

Exemple 4. Si $P = X^4$ et $Q = 3X^2 + X + 1$ alors

$$\begin{array}{r|l}
X^4 & 3X^2 + X + 1 \\ \cline{2-2}
-X^4 - \frac{1}{3}X^3 - \frac{1}{3}X^2 & \frac{1}{3}X^2 - \frac{1}{9}X - \frac{2}{27} \\ \cline{1-1}
-\frac{1}{3}X^3 - \frac{1}{3}X^2 & \\
\frac{1}{3}X^3 + \frac{1}{9}X^2 + \frac{1}{9}X & \\ \cline{1-1}
-\frac{2}{9}X^2 + \frac{1}{9}X & \\
\frac{2}{9}X^2 + \frac{2}{27}X + \frac{2}{27} & \\ \cline{1-1}
\frac{5}{27}X + \frac{2}{27} &
\end{array}$$

et le reste modifié est $\mathrm{MR}(P, Q) = 3^3(\frac{5}{27}X + \frac{2}{27}) = 5X + 2$.

2.2 Énoncé comme lemme clé.

Lemme 3 (Informel). À partir d'un ensemble de polynômes S, on obtient en temps fini un ensemble fini de polynômes BCS de degré 0 en appliquant les quatre opérations D, E, O et MR. [1]

Exemple 5. À partir de $S = \{\overbrace{aX^2 + bX + 1}^{p_0}\}$, on a

- ▷ on commence par ajouter p_0 ;
- ▷ d'abord les dérivées, omissions et extractions : on ajoute les polynômes $2aX + a$, a et $aX + 1$, $2a$, 1 et 0 ;
- ▷ ensuite on calcule le reste modifié
$$\mathrm{MR}(aX^2 + aX + 1, 2aX + a) = 4a^2 - a^3,$$
et on l'ajoute ;
- ▷ on calcule le reste modifié
$$\mathrm{MR}(aX^2 + aX + 1, aX + 1) = a,$$
et on l'ajoute (il y est déjà) ;
- ▷ on calcule le reste modifié
$$\mathrm{MR}(3aX + a, aX + 1) = a^2 - 2a,$$
et on l'ajoute ;
- ▷ on ne conserve que les polynômes de degré 0.

Dans l'exemple on obtient (après suppression des termes inutiles pour les comparaisons à 0),

$$\mathrm{BC}S = \{a, 4a^2 - a^3, a^2 - 2a\}.$$

On a, en théorie, 27 conditions de signe possibles ($3^{|\mathrm{BC}S|}$) :

- ▷ $a > 0$ et $4a^2 - a^3 > 0$ et $A^2 - 2a < 0$,
- ▷ $a > 0$ et $4a^2 - a^3 < 0$ et $a^2 - 2a < 0$,
- ▷ $a = 0$ et $a^2 - a^3 > 0$ et $a^2 - 2a > 0$,
- ▷ *etc* pour les 24 autre cas.

1. I ♡ le lemme de König.

On traite deux cas : $a > 0$ et $4a^2 - a^3$ et $a^2 - 2a$.

X	$-\infty$		γ_2		γ_1		$+\infty$
a		$>$	$>$	$>$	$>$	$>$	
$4a^2 - a^3$		$>$	$>$	$>$	$>$	$>$	
$a^2 - 2a$		$<$	$<$	$<$	$<$	$<$	
$aX + 1$	$-\infty$	$<$	$<$	$<$	0	$>$	$+\infty$
$2aX + a$	$-\infty$	$<$	0	$>$	$>$	$>$	$+\infty$
$aX^2 + aX + 1$	$+\infty$	$>$	$>$	$>$	$>$	$>$	$+\infty$

.

3 Corps algébriquement clos.

Définition 4. Un *corps algébriquement clos* est un corps commutatif dans lequel tout polynôme a une racine.

Exemple 6. Le corps $\mathbb{C}$ est algébriquement clos. En effet, il s'agit du *théorème fondamental de l'algèbre*, *i.e.* un polynôme de degré n a n racines comptées avec multiplicité.

Tout polynôme est ainsi un produit de polynômes de degré 1.

Définition 5. La *théorie des corps algébriquement clos* est la théorie formée des :

- ▷ axiomes de corps ;
- ▷ du schémas d'axiomes, noté Clos_n, pour tout $n \in \mathbb{N}$,

$$\forall a_0 \dots \forall a_n \, (a_1 \neq 0 \vee \cdots \vee a_n \neq 0 \to \exists b \, a_0 + a_1 b + \cdots + a_n b^n = 0).$$

Définition 6. Un corps est de *caractéristique* $p \in \mathbb{N}^\star$ s'il est modèle de l'ensemble Car_p définie par

$$\{(1 \neq 0) \wedge (1+1 \neq 0) \wedge \cdots \wedge (\underbrace{1 + \cdots + 1}_{p-1} \neq 0) \wedge (\underbrace{1 + \cdots + 1}_{p} = 0)\}.$$

Un corps est de *caractéristique* 0 s'il est modèle de l'ensemble Car_0 définie par

$$\{1 \neq 0, 1+1 \neq 0, 1+1+1 \neq 0, \ldots\}.$$

La *théorie des corps algébriquement clos de caractéristique* $p \in \mathbb{N}$ est :

$$\mathrm{ACF}_p := \{\text{Axiomes des corps}\} \cup \{\, \mathrm{Clos}_n \mid n \in \mathbb{N}\,\} \cup \mathrm{Car}_p.$$

Exemple 7. Les corps $\mathbb{C}$ et $\bar{\mathbb{Q}}$ sont modèles de cette théorie. ***Attention***, $\mathbb{F}_p$ ne l'est pas (et $\mathbb{F}_{p^n}$ non plus), il faut prendre sa clôture algébrique $\bar{\mathbb{F}}_p$ et $\bar{\mathbb{F}}_{p^n}$.

Remarque 1.

- ▷ Tous les corps finis sont de la forme $\mathbb{F}_{p^n}$ avec p premier.
- ▷ Un élément a est dit *algébrique* sur le corps $\Bbbk$ si c'est la racine d'un polynôme à coefficient dans $\Bbbk$. On dit que a est *algébrique de degré* q si le polynôme minimal dont a est racine est de degré q.

Exemple 8.

- ▷ Le nombre $\sqrt{3}$ est algébrique sur $\mathbb{Q}$ de degré 2.
- ▷ Le nombre i est algébrique sur $\mathbb{Q}$ de degré 2.
- ▷ Le nombre $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ de degré 3.
- ▷ Le nombre π n'est pas algébrique sur $\mathbb{Q}$.

Remarque 2. Si a est algébrique de degré q sur $\Bbbk$ alors $\Bbbk(a)$ est le corps engendré par $\Bbbk$ et a. C'est l'ensemble des polynômes de degré $\leq q-1$ sur $\Bbbk$, et on définie le produit modulo un polynôme minimal de a.

Exemple 9. On a $\mathbb{R}(i) = \mathbb{R}[X]/(X^2 - 1) \cong \mathbb{C}$. Le produit est :

$$\begin{aligned}(aX + b)(cX + d) &= acX^2 + X(ad + bc) + bd\\ &= (ad + bc)X + bd - ac.\end{aligned}$$

En particulier, si a est de degré q sur $\mathbb{F}_{p^n}$ alors $\mathbb{F}_{p^n}(a) = \mathbb{F}_{p^{qn}}$.

Théorème 2 (Tarski–bis). Pour tout p, la théorie des corps algébriquement clos de caractéristique p admet l'élimination des quantificateurs. Elle est complète et décidable.

Preuve. Comme la dernière fois, il suffit de montrer pour toute formule de la forme

$$\exists x\ (P_1(x) = 0 \wedge \cdots \wedge P_n(x) = 0 \wedge Q(x) \neq 0),$$

il existe une formule sans quantificateurs équivalente dans ACF_p. On continue la preuve sur un exemple. □

Exemple 10. On élimine les quantificateurs sur

$$\exists x\ (ax^2 + ax + 1 = 0 \wedge ax + 1 \neq 0),$$

avec la caractéristique $p = 0$. On a les polynômes suivants :

- ▷ $p_0(X) = aX^2 + aX + 1$
- ▷ $p_1(X) = \mathrm{D}p_0(X) = 2aX + a$
- ▷ $p_2(X) = \mathrm{E}p_0 = a$
- ▷ $p_3(X) = aX + 1$
- ▷ $p_4(X) = \mathrm{MR}(p_0, p_1) = 4a^2 - a^3$
- ▷ $p_2(X) = \mathrm{MR}(p_0, p_3) = a$
- ▷ $p_5(X) = \mathrm{MR}(p_1, p_3) = a^2 - 2a.$

Les « conditions de signe » sont $= 0$ ou $\neq 0$ (notés 0 et $\neq$).

On se place dans un cas exemple :

	autres	γ_1	γ_2	γ_3	γ_4
a	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$
$4a^2 + a^3$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$
$a^2 - 2a$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$
$aX + 1$	$\neq$	0	$\neq$	$\neq$	$\neq$
$2aX + a$	$\neq$	$\neq$	0	$\neq$	$\neq$
$aX^2 + aX + 1$	$\neq$	$\neq$	$\neq$	0	0

.

Ainsi, pour $a \neq 0$, $4a^2 - a^3 \neq 0$, $a^2 - 2a \neq 0$ alors on a

$$\exists x \; (ax^2 + ax + 1 = 0 \land ax + 1 \neq 0).$$

Avec les autres cas, on peut en déduire que

$$\exists x \; (ax^2 + ax + 1 = 0 \land ax + 1 \neq 0)$$

est équivalente à

$$\bigvee_{\substack{\text{tableau de la condition de signe} \\ \text{a une colonne qui convient}}} \text{(conditions de signe)}.$$

Exercice 1. En déduire que ACF_p est complète et décidable.

Remarque 3. En 2010, une preuve ~~Coq~~ Rocq de l'élimination des quantificateurs de cette théorie a été publiée par Cyril Cohen et Assia Mahboubi.

3.1 Applications aux mathématiques.

Théorème d'Ax–Grothendieck.

Théorème 3 (Ax–Grothendieck). Si P est un polynôme de $\mathbb{C}^n$ dans $\mathbb{C}^n$ injectif alors il est bijectif (et son inverse est un polynôme !).

On va prouver ce théorème en trois lemmes.

Lemme 4. Si φ est une formule qui admet comme modèle un corps algébriquement clos de caractéristique arbitrairement grande, alors φ admet comme modèle un corps algébriquement clos de caractéristique 0.

Preuve. On utilise le théorème de compacité de la logique du 1er ordre. Soit $T := \mathrm{ACF}_0 \cup \{\varphi\}$. Montrons que T a un modèle. Pour cela, on montre que T est finiment satisfiable. Soit $T' \subseteq_{\text{fini}} T$. Soit n le plus grand entier tel que

$$(\underbrace{1 + 1 + \cdots + 1}_{n} \neq 0) \in T'.$$

Soit $p > n$ un nombre premier tel que φ admet comme modèle un corps algébriquement clos $\mathbb{k}$ de caractéristique p (qui existe par hypothèse). D'où $\mathbb{k} \models \varphi$, et

$$\mathbb{k} \models \{\text{Axiomes des corps}\} \cup \{\, \mathrm{Clos}_n \mid n \in \mathbb{N} \,\}.$$

D'où, $\mathbb{k} \models \mathrm{ACF}_p$, et donc $\mathbb{k} \models T'$. Ainsi T finiment satisfiable donc T satisfiable. On en déduit que φ admet un modèle de caractéristique 0. $\square$

Lemme 5. Soit $\mathbb{k}$ un corps fini et soient $n \in \mathbb{N}^\star$ et $P : \mathbb{k}^n \to \mathbb{k}^n$ un polynôme injectif. Alors P est bijectif.

Preuve. Comme $\mathbb{k}^n$ est fini alors P est bijectif. $\square$

Lemme 6. Soit $\mathbb{k}$ un corps fini et soient $n \in \mathbb{N}^\star$ et $\bar{\mathbb{k}}$ la clôture algébrique de $\Bbbk$. Soit $P : \bar{\Bbbk}^n \to \bar{\Bbbk}^n$ un polynôme injectif. Alors P est bijectif.

Preuve. On suppose P non surjectif, il existe donc $\bar{b} = (b_1, \dots, b_n) \in \bar{\Bbbk}^n \setminus P(\bar{\Bbbk}^n)$ des nombres algébriques dans $\Bbbk$. Ils sont raciles de polynômes minimaux à coefficients dans $\Bbbk$. Soient $\bar{a} = (a_1, \dots, a_m)$ les coefficients de ces polynômes, ce sont des éléments de $\bar{\Bbbk}$. Soient $\bar{c}$ les coefficients de P.

Soit $\Bbbk' := \Bbbk(\bar{a}, \bar{b}, \bar{c})$, c'est un corps fini. On a $P : \Bbbk'^n \to \Bbbk'^n$ injectif pas surjectif, qui est impossible d'après le lemme précédent. □

On peut donc montrer le théorème d'Ax–Grothendieck.

Pour un degré d fini et un entier n fixé, on va construire la formule $\phi_{n,d}$ qui exprime qu'un polynôme de degré $\le d$ de $\Bbbk^n$ dans $\Bbbk^n$ qui est injectif et surjectif. Soit $M(n,d)$ l'ensemble fini des monômes unitaires de degré $\le d$ avec n variables $x_1, \dots, x_n$:

$$M(n,d) := \{1, x_1, x_2, x_1x_2, \dots, x_1^d, x_1^{d-1}x_2, \dots\}.$$

On pose la formule, notée $\varphi_{n,d}$.

$$\begin{gathered}\forall (a_{m,i})_{m \in M(n,d), i \in [\![1,n]\!]} \\ \left(\forall x_1 \dots x_n \forall y_1 \dots y_n \bigwedge_{i=1}^n \sum_{m \in M(n,d)} a_{m,i} m(x_i) = \sum_{m \in M(n,d)} a_{m,i} m(y_i) \to \bigwedge_{i=1}^n x_i = y_i\right) \\ \downarrow \\ \forall y_1 \dots y_n \exists x_1 \dots x_n \bigwedge_{i=1}^n y_i = \sum_{m \in M(n,d)} a_{m,i} m(x_i).\end{gathered}$$

Par le troisième lemme, pour tout corps fini $\Bbbk$, on a $\bar{\Bbbk} \models \varphi_{n,d}$ donc pour tout p premier, on a $\bar{\mathbb{F}}_p \models \varphi_{n,d}$. Par le premier lemme, il existe donc $\Bbbk$ de caractéristique 0 telle que $\Bbbk \models \varphi_{n,d}$. Par la complétude de la théorie des corps algébriquement clos, on a que $\mathbb{C} \models \varphi_{n,d}$.

Conjecture de la Jacobienne (1939).

C'est une question encore ouverte. On reçoit plein de preuves fausses.

Définition 7. Soit $P : \mathbb{C}^n \to \mathbb{C}^n$ un polynôme. Son *jacobien* est le déterminant de la matrice jacobienne

$$\operatorname{Jac} P = \left| \left(\frac{\partial P_i}{\partial x_j} \right)_{1 \le i \le n, 1 \le j \le n} \right|.$$

C'est un polynôme.

Proposition 2. Si P est injectif sur $\mathbb{C}^n$ alors P est localement injectif. Et donc, pour tout x (théorème des fonctions implicites), $\operatorname{Jac}(P)$ n'est jamais nul, d'où $\operatorname{Jac} P$ est un polynôme constant non nul.

Remarque 4 (Conjecture (problème 16 de la liste de Steve Smale)). En caractéristique 0, on a $\operatorname{Jac} P$ non nul implique P injectif.

Remarque 5. En caractéristique p, c'est faux : $P(x) := x - x^p$ est non-inversible et $P'(x) = 1 - px = 1$.

Exemple 11. ▷ Avec $n = 1$ et $d = 1$, on considère

$$\begin{aligned} P : \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\longmapsto P(x) := ax + b. \end{aligned}$$

On a $\operatorname{Jac} P = a$ et, $a \neq 0$ implique P injectif.

- Avec $n = 1$ et $d = 2$, on considère

$$\begin{aligned} P : \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\longmapsto P(x) := ax^2 + bx + c. \end{aligned}$$

  On a, si $\operatorname{Jac} P = 2ax + b$ non nul, alors $a = 0$ et $b \neq 0$. C'est le cas précédent !
- Avec $n = 2$ et $d = 1$, on considère

$$\begin{aligned} P : \mathbb{C}^2 &\longrightarrow \mathbb{C}^2 \\ x &\longmapsto P(x, y) := (ax + by + c, dx + ey + f). \end{aligned}$$

  On a $\operatorname{Jac} P = \begin{vmatrix} a & b \\ d & e \end{vmatrix} = ae - bd$. On a $\operatorname{Jac} P$ non nul implique $ae - bd \neq 0$ ce qui implique que le système

$$\begin{cases} ax + bj + c = 0 \\ dx + ej + f = 0 \end{cases}$$

  est inversible, donc la conjecture est vrai.

On a montré quelques résultats partiels :

- pour $d \leq 2$ en 1980 ;
- pour $d \leq 3$ dans le cas général.