# Un polynôme séparable

## (un exemple d'application du Nullstellensatz formel)

**H. Lombardi & C. Quitté**

Il s'agit ici de généraliser au cas d'un anneau commutatif arbitraire un résultat utile en théorie des corps : *si l'on divise un polynôme $f(x)$ par le pgcd de $f$ et $f'$, on obtient un polynôme séparable.*

Pour un anneau arbitraire, on devra supposer que le pgcd de $f$ et $f'$ existe en un sens fort.

Cet article est écrit dans le style des mathématiques constructives, mais la lectrice ne verra guère de différence avec les articles écrits dans le style usuel. En tout cas elle peut chausser ses lunettes de mathématicienne classique et sauter les passages qui lui paraitraient trop sophistiqués.

On vise ici avant tout à illustrer la puissance du Nullstellensatz formel (y compris sa version constructive).

L'énoncé du Nullstellensatz formel en mathématiques classiques est le suivant.

**Nullstellensatz formel.** (version classique)
*Soit $\mathbf{A}$ un anneau commutatif arbitraire, $f_1$, ..., $f_s$ et $g \in \mathbf{A}[X_1, \ldots, X_n]$.*

1. *On suppose que pour tout homomorphisme $\varphi : \mathbf{A} \to \mathbf{K}$, où $\mathbf{K}$ est un corps algébrique sur $\varphi(\mathbf{A})$, le système $f_1 = \cdots = f_s = 0$ vu dans $\mathbf{K}$ est incompatible. Alors l'idéal $\langle f_1, \ldots, f_s\rangle$ de $\mathbf{A}$ est égal à $\langle 1\rangle$.*
2. *On suppose que pour tout homomorphisme $\varphi : \mathbf{A} \to \mathbf{K}$, où $\mathbf{K}$ est un corps algébrique sur $\varphi(\mathbf{A})$„ le polynôme $g$ s'annule sur les zéros du système $f_1 = \cdots = f_s = 0$ dans $\mathbf{K}$. Alors $g^N \in \langle f_1, \ldots, f_s\rangle$ pour un exposant $N$.*

Notez que dans le Nullstellensatz usuel, $\mathbf{A}$ est un corps et $\mathbf{K}$ est juste une clôture algébrique de $\mathbf{A}$, $\varphi$ étant le morphisme d'inclusion.

Notez aussi que le point *2* résulte du point *1* par ce que l'on appelle le « truc de Rabinovitch ». On introduit une nouvelle variable $Z$ et une nouvelle équation $Zg - 1 = 0$, et l'on applique le point *1* au nouveau système polynomial. Le Nullstellensatz formel se concentre donc sur le point *1*.

Si l'on ne limitait pas $\mathbf{K}$ à être algébrique sur l'image de $\mathbf{A}$, le point *1* du Nullstellensatz formel serait une pure trivialité en mathématiques classiques, au moyen d'un raisonnement par l'absurde et du lemme de Krull. Si l'on avait $1 \notin \langle f_1, \ldots, f_s\rangle$ on prendrait pour $\mathbf{K}$ le corps de fractions du quotient de $\mathbf{A}[\underline{X}]/\langle f_1, \ldots, f_s\rangle$ par un idéal premier (il faut pour cela le lemme de Krull, version faible du lemme de Zorn).

Pour obtenir le Nullstellensatz formel tel que nous l'avons énoncé, il faut prendre un idéal maximal de $\mathbf{A}[\underline{X}]/\langle f_1, \ldots, f_s\rangle$ (supposé non nul), et utiliser le résultat non trivial suivant.

**Nullstellensatz faible.**
*Si $\mathbf{k}$ est un corps et si $\mathbf{L} \supseteq \mathbf{k}$ est à la fois un corps et une $\mathbf{k}$-algèbre de type fini, alors $\mathbf{L}$ est algébrique sur $\mathbf{k}$.*

Ce Nullstellensatz faible admet une preuve entièrement constructive, en supposant que le corps $\mathbf{L}$ admet un test d'égalité à zéro. Voir par exemple une version à peine plus générale en [1, Théorème VI-3.15].

Naturellement, d'un point de vue constructif, si l'on ne fait aucune hypothèse plus précise concernant l'anneau $\mathbf{A}$, on n'aura pas accès aux idéaux maximaux de $\mathbf{A}[\underline{X}]/\langle f_1,\ldots,f_s\rangle$, et la démonstration classique ne pourra pas fonctionner.

Avoir accès aux idéaux maximaux de $\mathbf{A}[\underline{X}]/\langle f_1,\ldots,f_s\rangle$ signifierait donner un algorithme de calcul qui, étant donnés l'anneau $\mathbf{A}$ et les polynômes $f_1,\ldots,f_s$, ou bien explicite l'appartenance $1\in\langle f_1,\ldots,f_s\rangle$, ou bien explicite un idéal maximal $\mathfrak{m}$ de $\mathbf{A}$ et un idéal maximal $\mathfrak{M}$ de $\mathbf{A}[\underline{X}]$ contenant $\mathfrak{m}+\langle f_1,\ldots,f_s\rangle$.

On va illustrer dans la fin de l'article le fait suivant. Ce que nous appelons « la version constructive du Nullstellensatz formel », qui semble n'être qu'un cas particulier du Nullstellensatz formel classique, celui où l'anneau $\mathbf{A}$ est $\mathbb{Z}$[1], constitue une version satisfaisante de l'énoncé classique, au sens (informel) suivant.

**Principe des versions constructives**. *Chaque fois que le théorème classique est utilisé pour démontrer un énoncé concret, il suffit de disposer de sa version constructive pour obtenir explicitement le résultat concret.*

Nous donnons tout d'abord l'énoncé de la version constructive du Nullstellensatz formel.

## Nullstellensatz formel. (version constructive) [1, Théorème III-9.9]

*Soient $f_1,\ldots,f_s$ et $g\in\mathbb{Z}[X_1,\ldots,X_n]$.*

1. *Supposons que le système $f_1=\cdots=f_s=0$ est incompatible sur tout corps fini. Alors on a $1\in\langle f_1,\ldots,f_s\rangle$. Plus précisément :*
   - (a) *Ou bien l'idéal $\langle f_1,\ldots,f_s\rangle$ de $\mathbb{Z}[\underline{X}]$ est égal à $\langle 1\rangle$ (et pour tout anneau commutatif $\mathbf{B}$ non nul, le système $f_1=\cdots=f_s=0$ vu sur $\mathbf{B}[\underline{X}]$ est incompatible).*
   - (b) *Ou bien le système $f_1=\cdots=f_s=0$ admet un zéro dans un corps fini.*
2. *Supposons que pour tout corps fini, le polynôme $g$ s'annule sur les zéros du système $f_1=\cdots=f_s=0$. Alors $g^N\in\langle f_1,\ldots,f_s\rangle$ pour un exposant $N$.*

On n'a pas écrit le point *2* sous une forme aussi précise que le point *1*, mais le lecteur devinera sans mal ce qu'il en est précisément (l'anneau $\mathbf{B}$ doit être supposé réduit).

La démonstration de ce théorème est basée sur l'usage bien compris du résultant (qui donne déjà le Nullstellensatz usuel sous forme constructive) et donc fournit un algorithme qui n'utilise pas la théorie sophistiquée des bases de Gröbner sur $\mathbb{Z}$ pour établir l'appartenance $1\in\langle f_1,\ldots,f_s\rangle$ dans la conclusion. En pratique, l'algorithme a pour but de calculer l'appartence souhaitée, et s'il échoue, il fournit un contre-exemple explicite de l'hypothèse (i.e., dans le point *1* une solution du système $f_1=\cdots=f_s=0$ dans un corps fini).

Nous illustrons maintenant le principe des versions constructives sur un exemple non trivial. Il s'agit de résoudre explicitement le point *3* de l'exercice sui suit.

[1] Mais qui par contre admet une démonstration constructive, et donc fournit un algorithme explicitant le théorème.

## Exercice.

*1.* Soit $\mathbf{K}$ un corps discret[2], $x$ une indéterminée, $f \in \mathbf{K}[x]$ un polynôme non nul, $h = \text{pgcd}(f, f')$ et $f_1 = f/h$.
On suppose que $f$ se décompose en un produit de facteurs linéaires dans un corps discret contenant $\mathbf{K}$.
Montrer que $\text{Res}_x(f_1, {f_1}') \in \mathbf{K}^\times$, ou, ce qui revient au même[3], que $1 \in \langle f_1, f_1' \rangle \subseteq \mathbf{K}[x]$.
Si en outre $\deg(f) = n$ et $n! \in \mathbf{K}^\times$, alors $f$ divise ${f_1}^n$.

*2.* Démontrer les mêmes résultats sans faire d'hypothèse de factorisation concernant $f$.

*3.* Soit $\mathbf{k}$ un anneau commutatif et $f \in \mathbf{k}[x]$ primitif[4] de degré formel[5] $n$. On suppose que l'idéal $\langle f, f' \rangle$ est engendré par un polynôme $h$ (nécessairement primitif).

*a.* Montrer qu'il existe des polynômes $u$, $v$, $f_2$, $f_1 \in \mathbf{k}[x]$, satisfaisant les égalités

$$uf_1 + vf_2 = 1 \quad \text{et} \quad \begin{bmatrix} u & v \\ -f_2 & f_1 \end{bmatrix} \begin{bmatrix} f \\ f' \end{bmatrix} = \begin{bmatrix} h \\ 0 \end{bmatrix}.$$

*b.* En utilisant le Nullstellensatz formel, montrer que $1 \in \langle f_1, f_1' \rangle \subseteq \mathbf{k}[x]$.

*c.* Si en outre $n! \in \mathbf{k}^\times$, alors peut-on montrer que $f$ divise ${f_1}^n$ ?.

*4.* Question subsidiaire. Donner une démonstration directe du point *3* qui n'utilise pas le Nullstellensatz formel.

## Solution

*1.* On suppose que $f = \prod_k (x - a_k)^{m_k}$, avec les $a_k - a_\ell$ inversibles pour $k \neq \ell$. Le polynôme $f_1$ est un diviseur de $f$. Pour le déterminer, il suffit de savoir, pour chaque $k$, quelle puissance de $(x-a)^k$ divise $f'$. On écrit $f = (x - a_k)^{m_k} g_k$ et l'on a $\langle g_k, x - a_k \rangle = \langle 1 \rangle$. On a :

$$f' = m_k (x - a_k)^{m_k - 1} g_k + (x - a_k)^{m_k} g_k' = (x - a_k)^{m_k - 1}\, u_k.$$

avec

$$u_k = m_k g_k + (x - a_k) g_k'.$$

Si $m_k = 0$ dans $\mathbf{K}$, on obtient que $f'$ est divisible par $(x - a_k)^{m_k}$.
Si $m_k \in \mathbf{K}^\times$, alors $g_k \in \langle u_k, x - a_k \rangle$ donc $\langle u_k, x - a_k \rangle = \langle 1 \rangle$, et l'on obtient que $f'$ est divisible par $(x - a_k)^{m_k - 1}$ mais pas par $(x - a_k)^{m_k}$. En fin de compte, on obtient l'égalité

$$f_1 = \prod_{k : m_k \in \mathbf{K}^\times} (x - a_k).$$

Dans tous les cas, le polynôme $f_1$ est séparable.
Et si tous les $m_k \in \mathbf{K}^\times$, (par exemple si $n! \in \mathbf{K}^\times$), alors $f$ divise $f_1^n$.

---

[2]Un corps discret est un corps dans lequel la disjonction « $a = 0$ ou $a$ inversible » est explicite. Notez que $\mathbb{R}$ n'est pas un corps discret, mais que le point *3* de l'exercice fournit une version constructive satisfaisante du résultat pour $\mathbb{R}$.

[3]Le résultant peut être calculé sans ambigüité car le degré de $f_1$ est connu, parce que $\mathbf{K}$ est un corps discret. La formulation $1 \in \langle f_1, f_1' \rangle \subseteq \mathbf{K}[x]$, qui ne présuppose pas connu le degré de $f_1$ est ici plus uniforme, et préférable comme on va le voir dans le point *3*

[4]Un polynôme est dit primitif si ses coefficients engendrent l'idéal $\langle 1 \rangle$

[5]On ne suppose pas que l'anneau possède un test pour « $a = 0$ ? ». En conséquence on ne suppose pas connu le degré de $f$. Néanmoins, comme $f$ est un élément explicite de $\mathbf{k}[x]$, il n'y a qu'un nombre fini de coefficients qui apparaissent dans son écriture, et le degré formel de $f$ est défini comme le plus grand degré d'un monôme dans une telle écriture.

*2.* Cette question ne se comprend que d'un point de vue constructif, car en mathématiques classiques tout polynôme possède un corps de racines, et il suffit alors de se reporter au point *1.*

En lisant le chapitre VII de [1] on se convaincra que l'on peut toujours « faire comme si » l'on disposait d'un corps de racines pour le polynôme $f$.

Voici comment cela fonctionne.

On considère d'abord les zéros $x_k$ dans l'algèbre de décomposition universelle $\mathbf{A}$ de $f$ sur $\mathbf{K}$. Si $x_1 - x_2 \in \mathbf{A}^\times$, le polynôme $f$ est séparable, $h = 1$ et $f_1 = f$.

Sinon, on remplace $\mathbf{A}$ par un quotient de Galois $\mathbf{B}$ de $\mathbf{A}$. Dans ce quotient $\mathbf{B}$, on a par exemple $x_1 = x_2$.

On considère ensuite $x_1 - x_3$ dans $\mathbf{B}$. S'il est nul ou inversible, tout est OK (et on continue en comparant les autres paires de racines).

Sinon, il faut considèrer un quotient de Galois plus poussé.

En fin de compte, après avoir renuméroté les $x_i$ on est certain d'obtenir dans un un quotient de Galois $\mathbf{C}$ de l'algèbre de décomposition universelle une égalité

$$f(x) = \prod_{k=1}^{\ell} (x - x_k)^{m_k}, \text{ avec les } x_k - x_j \in \mathbf{C}^\times \text{ pour } k \neq j.$$

La démonstration donnée au point *1* fonctionne alors dans ce nouveau cadre. On obtient effet

$$f_1 = \prod_{k:k\leq\ell,\, m_k\in\mathbf{K}^\times} (x - x_k).$$

Puis le résultant $\mathrm{Res}_x(f_1, f_1')$ peut être calculé dans $\mathbf{C}$, où il est égal à $\pm\prod_{j<k\in S}(x_j - x_k)^2$ (avec $S = \{\, k \in [\![1..\ell]\!] \mid m_k \in \mathbf{K}^\times \,\}$). C'est donc un élément de $\mathbf{K} \cap \mathbf{C}^\times = \mathbf{K}^\times$.
Et si tous les $m_k \in \mathbf{K}^\times$, (par exemple si $n! \in \mathbf{K}^\times$), alors $f$ divise $f_1^n$.

*3a.* Si $\langle f, f' \rangle = \langle h \rangle$, on a des polynômes $u$, $v$, $f_2$ et $f_1$ tels que

$$uf + vf' = h,\ hf_1 = f \text{ et } hf_2 = f'.$$

Cela donne $h(uf_1 + vf_2) = h$. Puisque $h$ divise $f$, il est primitif donc régulier, d'où $uf_1 + vf_2 = 1$. Et l'égalité matricielle du point *3a* est bien satisfaite :

$$\begin{bmatrix} u & v \\ -f_2 & f_1 \end{bmatrix} \begin{bmatrix} f \\ f' \end{bmatrix} = \begin{bmatrix} h \\ 0 \end{bmatrix}.$$

*3b.* On considère l'anneau $\mathbb{Z}[(c_i)_{i\in[\![1..\ell]\!]}]$, où les $c_i$ sont d'une part des indéterminées que l'on prend pour les coefficients des polynômes $f$, $h$, $u$, $v$, $f_2$ et $f_1$, et d'autre part des indéterminées pour obtenir une combinaison linéaire des coefficients de $f$ égale à 1. On a choisi pour les polynômes en $x$ les degrés formels correspondant aux équations que l'on a par hypothèse dans $\mathbf{k}[x]$.

On considère le système polynomial sur les indéterminées $(c_i)$ qui correspond aux équations suivantes dans $\mathbb{Z}[(c_i)][x]$ :

$$f \text{ est primitif},\ uf_1 + vf_2 = 1,\ hf_1 = f,\ hf_2 = f'.$$

Soit alors $\mathfrak{a}$ l'idéal de $\mathbb{Z}[(c_i)]$ engendré par ce système polynomial de $\mathbb{Z}[(c_i)]$. On obtient ainsi l'anneau « générique » de la situation considérée :

$$\boxed{\mathbf{A} = \mathbb{Z}[(c_i)]/\mathfrak{a}.}$$

Il est clair que tout se passe dans le sous-anneau $\mathbf{k}'$ (de $\mathbf{k}$) quotient de l'anneau générique $\mathbf{A}$, obtenu en spécialisant les indéterminées $c_i$ en leurs valeurs dans $\mathbf{k}$.

Si l'on évalue cette situation dans un corps fini $\mathbf{F}$, i.e. si l'on considère un homomorphisme $\mathbf{A} \to \mathbf{F}$, on a $1 \in \langle f_1(x), f_1'(x)\rangle \subseteq \mathbf{F}[x]$ en vertu du point *1.* En effet, comme on a forcé $f(x)$ à être primitif, son image dans $\mathbf{F}[x]$ est un polynôme non nul, et l'on peut appliquer le point *1*, en notant que tout corps fini possède une clôture algébrique. Notons que si au contraire $f(x)$ était le polynôme nul de $\mathbf{F}[x]$, les équations que l'on impose n'interdiraient pas d'avoir $f_1 = 0$.

Notons $\mathfrak{b} = \mathfrak{a} + \langle f_1(x), f_1'(x)\rangle \subseteq \mathbb{Z}[x, (c_i)_{i\in[\![1..\ell]\!]}]$. On a donc obtenu que le système polynomial qui correspond à l'idéal $\mathfrak{b}$ n'a de solution dans aucun corps fini.

Par le Nullstellensatz formel on en déduit que $1 \in \mathfrak{b}$, ce qui veut aussi dire que $1 \in \langle f_1(x), f_1'(x)\rangle \subseteq \mathbf{A}[x]$. Et ceci implique que $1 \in \langle f_1(x), f_1'(x)\rangle \subseteq \mathbf{k}[x]$, car cette appartenance est déjà certifiée avec le sous-anneau $\mathbf{k}'$ de $\mathbf{k}$ qui est un quotient de $\mathbf{A}$.

Notez que l'on n'a pas besoin de démontrer le point *2* pour obtenir le résultat général du point *3b* (qui contient le point *2* comme cas particulier).

*3c.* Voyons la dernière question : *si en outre* $n! \in \mathbf{k}^\times$*, alors* $f$ *divise* ${f_1}^n$ *?* Ici $n$ est a priori le degré formel de $f$, qui peut être son vrai degré si on le connaît.

On doit introduire une indéterminée supplémentaire $z$ pour l'inverse de $n!$.

*Première solution partielle.*
Notons $R$ le reste de la division de ${f_1}^n$ par $f$ (que l'on suppose ici unitaire). Alors on sait que pour tout zéro de l'idéal $\mathfrak{c} = \mathfrak{a} + \langle zn! - 1\rangle$ dans un corps fini, les coefficients de $R$ sont nuls. Le Nullstellensatz formel nous dit alors que les coefficients de $R$ sont dans le nilradical $\sqrt{\mathfrak{c}}$ de $\mathfrak{c}$.
En conclusion, dans un anneau $\mathbf{k}$ tel que $n! \in \mathbf{k}^\times$, si les hypothèses sont satisfaites, et si $f$ est unitaire, on peut affirmer que les coefficients de $R$ sont nilpotents. Comme conséquence, une certaine puissance de $R = {f_1}^n - fq$ est nulle, et donc $f$ divise une puissance de $f_1$.

*Deuxième solution partielle.*
On va obtenir la même conclusion finale sans supposer $f$ unitaire.
On introduit une indéterminée $z$ et l'on considère l'idéal

$$\mathfrak{d} = \mathfrak{a} + \langle f(x), zn! - 1\rangle \subseteq \mathbb{Z}[x, z, (c_i)_{i\in[\![1..\ell]\!]}].$$

D'après le point *1*, le polynôme $f_1(x)$ s'annule en tout zéro de $\mathfrak{d}$ dans tout corps fini. Le Nullstellensatz formel implique qu'une puissance de $f_1$ est dans $\mathfrak{d}$, d'où il suit que dans $\mathbf{k}[x]$, $f$ divise une puissance de $f_1$.

*4.* Merci à la lectrice qui résoudra cette question, et qui éclaircira complètement le dernier point de la question *3.*

## Concernant une amélioration éventuelle du résultat

On peut se demander s'il est possible de renforcer le résultat du point *3* comme suit. On suppose toujours le polynôme $f$ primitif, mais on ne suppose plus que l'idéal $\langle f, f'\rangle$ est principal. On pose

$$I = (\langle f, f'\rangle : f') = (\langle f\rangle : f'),\ I' = \langle g' \mid g \in I\rangle\ ,\ J = I + I',$$

et la conclusion serait que $1 \in J$.

Lorsque $\langle f, f'\rangle$ est principal, on obtient en reprenant les notations précédentes $J = \langle f_1, {f_1}'\rangle$, et l'on retrouve le point *3b.* En fait, pour un corps $\mathbf{K}$, on a $1 \in J$ même si $f$

est nul. Mais le résultat n'est pas valable avec le plus simple des anneaux : $\mathbb{Z}$. Comme le montre l'exemple suivant.

On prend $f = 5x^2 + x - 3$. On a $f' = 10x + 1$ et $\mathrm{disc}(f) = 61$.

Donc $61 \in \langle f, f' \rangle$. En fait, modulo 61, on a $f = 5(x-6)^2$ et $\langle f, f' \rangle = \langle x - 6 \rangle$, ce qui force sur $\mathbb{Z}$ l'égalité $\langle f, f' \rangle \cap \mathbb{Z} = 61\mathbb{Z}$. Comme le pgcd de $f$ et $f'$ dans $\mathbb{Z}[x]$ est 1, leur ppcm est $ff'$, par suite $I = \langle f \rangle$, mais $1 \notin J = \langle f, f' \rangle$.

Un exemple plus général serait donné par $f = x^2 + bx + c$ lorsque le discriminant est non nul, on obtient $I = \langle f \rangle$, $J = \langle f, f' \rangle$ avec

$$\langle f, f' \rangle \cap \mathbb{Z} = \frac{b^2 - 4c}{\mathrm{pgcd}(b, 2)}\,\mathbb{Z},$$

et le seul cas pour lequel $1 \in \langle f, f' \rangle$ est lorsque $b^2 - 4c = 1$.

## Références

1. H. Lombardi, C. Quitté. *Algèbre Commutative, Méthodes Constructives.* Calvage & Mounet, (2011).