Thm 9 ("Lemme de normalisation de E. Noether*", 1926): Soit A une k-algèbre de type fini. Alors il existe des éléments algébriquement indépendants $y_1, \dots, y_m$ dans A tels que A soit une extension finie de $k[y_1, \dots, y_m]$.

Rque: On a donc

$$\text{type fini} \begin{cases} A \\ \text{Ul finie} \\ k[y_1, \dots, y_m] \\ \text{Ul algébrique pure} \\ k \end{cases}$$

Lemme 10: Soit A une k-alg. de type fini engendrée par des éléments $x_1, \dots, x_n$ alg. liés. Alors il existe $x_1', \dots, x_{n-1}'$ dans A t.q. $x_1, \dots, x_n$ alg. liés. Alors il existe $x_1', \dots, x_{n-1}'$ dans A t.q. x_n est entier sur $A' = k[x_1', \dots, x_{n-1}']$ et $A = A'[x_n]$.

Dém. du thm à partir du lemme: Supposons que A est engendrée par des éléments $x_1, \dots, x_n$. On procède par récurrence sur n. Pour $n = 0$, on prend $m = 0$. Supposons $n \geq 1$. Si $x_1, \dots, x_n$ sont alg. indép., on prend $m = n$, $y_i = x_i$, $1 \leq i \leq n$. Sinon, le lemme s'applique: il existe $x_1', \dots, x_{n-1}'$ t.q. x_n est entier sur $A' = k[x_1', \dots, x_{n-1}']$ et que $A = A'[x_n]$. Par l'hypothèse de récurrence, il existe $y_1, \dots, y_m$ alg. indép. dans A' t.q. A' est finie sur $k[y_1, \dots, y_m]$. Alors $A = A'[x_n]$ est finie sur $k[y_1, \dots, y_m]$. ✓

Dém. du lemme: Soit $0 \neq P \in k[X_1, \dots, X_n]$ t.q. $P(x_1, \dots, x_n) = 0$.

Première méthode (Nagata, 1962): On cherche les x_i' sous la forme

$$x_i' = x_i - x_n^{e^i}, \quad 1 \leq i \leq n-1,$$

---

* Emmy Amalie Noether, 1882 (Erlangen) – 1935 (Bryn Mawr, Pennsylvania)

pour un entier e assez grand. Pour tout choix de $e \geq 1$, on a $k[x_1', \dots, x_{n-1}', x_n] = A$. En outre, on a

$$0 = P(x_1, \dots, x_n) = P(x_1' + x_n^e, x_2' + x_n^{e^2}, \dots, x_{n-1}' + x_n^{e^{n-1}}, x_n)$$
$$= Q(x_1', x_2', \dots, x_{n-1}', x_n)$$

pour un $Q \in k[X_1', \dots, X_{n-1}', X_n]$. On aimerait que le coeff. dominant de $Q(x_1', \dots, x_{n-1}', X_n) \in A'[X_n]$ soit une constante inversible (car cela impliquerait que x_n soit entier sur A). Pour tout monôme $X_1^{a_1} \dots X_n^{a_n}$ apparaissant dans P, on a

$$X_1^{a_1} \dots X_n^{a_n} = \left(\prod_{i=1}^{n-1} (X_i' + X_n^{e^i})^{a_i} \right) X_n^{a_n}$$
$$= X_1'^{a_1} \dots X_{n-1}'^{a_{n-1}} X_n^{a_n} + \dots + X_n^{a_1 e + a_2 e^2 + \dots + a_{n-1} e^{n-1} + a_n}$$

Le dernier terme est l'unique terme de plus haut degré en X_n. Si e est strictement plus grand que tous les exposants a_i qui apparaissent dans les monômes de P, alors le degré

$$a_1 e + a_2 e^2 + \dots + a_{n-1} e^{n-1} + a_n \qquad (*)$$

détermine les a_i : ce sont les chiffres de l'écriture de $(*)$ en base e. Donc des monômes distincts de P fournissent des puissances distinctes de X_n dans $Q(x_1', \dots, x_{n-1}', X_n)$. Une seule de ces puissances est maximale et elle apparaît avec un coeff. dans k^*.

Deuxième méthode (E. Noether) : Cette méthode ne s'applique que quand k est infini, ce qu'on suppose maintenant. On cherche les x_i' sous la forme

$$x_i' = x_i - c_i x_n, \quad 1 \leq i \leq n-1,$$

pour des $c_i \in k$ à déterminer. Soit d le degré total de P et soit Q la somme des termes de degré d de P. Alors les coefficients dominants de X_n dans

$$P(x_1' + c_1 X_n, \dots, x_{n-1}' + c_{n-1} X_n, X_n)$$

et $Q(x_1' + c_1 X_n, \dots, x_{n-1}' + c_{n-1} X_n, X_n)$

sont égaux. On a

$$Q(x_1' + c_1 X_n, \dots, x_{n-1}' + c_{n-1} X_n, X_n) = X_n^d Q(c_1, \dots, c_{n-1}, 1) + R,$$

R de degré $< d$ en X_n. Comme $Q(X_1, \dots, X_{n-1}, 1)$ est un polynôme non nul (car le polynôme homogène $Q(X_1, \dots, X_{n-1}, X_n)$ est non nul) il existe des $c_1, \dots, c_{n-1} \in k$ t.q. $Q(c_1, c_2, \dots, c_{n-1}, 1) \neq 0$, par le lemme suivant. ✓

Lemme 11 : Soient k un corps infini et $P \in k[X_1, \dots, X_n]$ un polynôme non nul. Alors il existe $x_1, \dots, x_n \in k$ t.q. $P(x_1, \dots, x_n) \neq 0$.

Dém. : Montrons par récurrence sur n que

$$P(x_1, \dots, x_n) = 0, \ \forall x \in k^n \Longrightarrow P = 0.$$

C'est bien connu pour $n = 1$. Supposons $n \geq 2$. Écrivons $P = \sum_{i=0}^{N} A_i X^i$ où $A_i \in k[X_1, \dots, X_{n-1}]$, $0 \leq i \leq n$. Pour tous $x_1, \dots, x_{n-1} \in k$, le polynôme $P(x_1, \dots, x_{n-1}, X_n) = \sum_{i=1}^{N} A_i(x_1, \dots, x_{n-1}) \cdot X^i$ s'annule en tout $x_n \in k$. Donc les $A_i(x_1, \dots, x_{n-1})$ s'annulent (cas $n = 1$). Donc les A_i s'annulent (récurrence). ✓

1.5 Nullstellensatz (théorème des zéros)

Lemme 1 : Soit $A \subset B$ une extension entière d'anneaux intègres.
Alors A est un corps ssi B est un corps.

Dém. : "$\Rightarrow$" Soit $0 \neq x \in B$. Comme x est entier sur A, le A-espace vectoriel $A[x]$ est de dimension finie. La mult. par x est un endomorphisme injectif donc bijectif de $A[x]$. Elle atteint donc 1.

"$\Leftarrow$" Soit $0 \neq x \in A$. Soit $y \in B$ l'inverse de x. Comme y est entier sur A, on a

$$y^n + a_1 y^{n-1} + \dots + a_n = 0$$

pour des $a_i \in A$. En multipliant par x^{n-1} on trouve

$$y + a_1 + a_2 x + \dots + a_n x^{n-1} = 0$$

ce qui montre que y est dans A. ✓

Théorème 2 (Nullstellensatz faible, Hilbert*, 1893) : Soient k un corps et K une k-algèbre de type fini qui est un corps. Alors l'extension $K \supseteq k$ est finie.

Dém. : Par le lemme de normalisation, il existe $y_1, \dots, y_m$ algébriquement indépendants dans K tels que K est fini sur $k[y_1, \dots, y_m]$. Par le lemme 1, $k[y_1, \dots, y_m]$ doit être un corps. Donc $m = 0$ et K est fini sur k. ✓

Rques : 1) Si k est non dénombrable, ce théorème est "une trivialité" : Si K n'est pas fini sur k, il n'est pas algébrique. Donc il existe

---

* David Hilbert, 1862 (Königsberg = Kaliningrad) – 1943 (Göttingen)

$x \in K$ qui est transcendant sur k. Mais alors les éléments

$$\frac{1}{x-\alpha}, \quad \alpha \in k,$$

sont linéairement indépendants sur k (unicité de la décomposition en éléments simples). Donc K est de dimension non dénombrable sur k. C'est absurde car K est quotient d'une algèbre de polynômes en un nombre fini de variables.

2) Le Nullstellensatz affirme : les idéaux maximaux de $k[X_1, \dots, X_n]$ sont de codimension finie. Si k est alg. clos, ils sont même de codimension 1 (car alors k n'admet pas d'extension finie non triviale).

Cor. 3 : Si k est un corps alg. clos, les idéaux maximaux de $k[X_1, \dots, X_n]$ sont exactement les idéaux

$$m_x = (X_1 - x_1, X_2 - x_2, \dots, X_n - x_n)$$

associés aux points $x = (x_1, x_2, \dots, x_n)$ de k^n.

Dém. : Pour $x \in k^n$, l'évaluation

$$k[X_1, \dots, X_n] \longrightarrow k, \quad P \longmapsto P(x)$$

induit un isomorphisme

$$k[X_1, \dots, X_n]/m_x \xrightarrow{\sim} k.$$

Donc les m_x sont bien maximaux. Si m est maximal quelconque, on a un isomorphisme

$$\varphi : k[X_1, \dots, X_n]/m \xrightarrow{\sim} k$$

grâce au Nullstellensatz et au fait que k soit alg. clos. Soit $x_i = \varphi(X_i)$, $1 \le i \le n$. Alors clairement $m_x \subseteq m$. Donc $m_x = m$ par maximalité. ✓

Cor. 4 : Un système d'équations polynomiales

$$\left.\begin{aligned} F_1(x_1,\dots,x_n) &= 0 \\ &\vdots \\ F_r(x_1,\dots,x_n) &= 0 \end{aligned}\right\} (*)$$

à coeff. dans un corps alg. clos k n'admet aucune solution $x \in k^n$ ssi il existe des $G_i \in k[X_1,\dots,X_n]$, $1 \le i \le r$, t.q.

$$\sum_{i=1}^{r} G_i F_i = 1.$$

Dém. : Soit I l'idéal de $k[X_1,\dots,X_n]$ engendré par les F_i.

Alors

$(*)$ n'a pas de solution $\Leftrightarrow$ $I \not\subset m_x$, $\forall x \in k^n$

$\Leftrightarrow$ $I \not\subset m$, $\forall m$ max. de $k[X_1,\dots,X_n]$

$\Leftrightarrow$ $I = k[X_1,\dots,X_n]$

$\Leftrightarrow$ $1 \in I$. ✓

2. Variétés algébriques affines

2.1 Parties algébriques et idéaux

Soit k un corps.

Déf : Une partie $X \subseteq k^n$ est algébrique (ou : est une ss-variété alg. fermée de k^n) s'il existe une famille de polynômes P_i, $i \in I$, $P_i \in k[X_1,\dots,X_n]$, t.q.

$$X = \{x \in k^n \mid P_i(x) = 0, \ \forall i \in I\}.$$

Si J est un idéal de $k[X_1,\dots,X_n]$, le lieu d'annulation de J est la partie algébrique

$$V(J) = \{x \in k^n \mid P(x) = 0, \ \forall P \in J\} \subseteq k^n$$

(V = "variété" = "vanishing set"). Si $Y \subseteq k^n$ est une partie

quelconque, <u>l'idéal associé à Y</u> est

$$I(Y) = \{ P \in k[X_1, \dots, X_n] \mid P(y) = 0, \forall y \in Y \}.$$

<u>Rques</u> : 1) Une famille de polynômes $(P_i)_{i \in I}$ et l'idéal J qu'elle engendre ont même lieu d'annulation. Donc toute partie algébrique de k^n est de la forme $V(J)$ pour un idéal J.

3) Les applications

$$\{\text{parties de } k^n\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{idéaux de } k[X_1, \dots, X_n]\}$$

sont décroissantes. On a

$$I(\emptyset) = k[X_1, \dots, X_n], \quad I(k^n) = (0) \text{ si } k \text{ est infini (L1.4.11)}$$

$$V(k[X_1, \dots, X_n]) = \emptyset, \quad V((0)) = k^n$$

4) Pour toute partie $X \subseteq k^n$, on a $V(I(X)) \supseteq X$ et on a l'égalité ssi X est algébrique ("$\Rightarrow$" clair, "$\Leftarrow$" : si $X = V(J)$, alors $J \subseteq I(X)$ donc $V(I(X)) \subseteq V(J) = X \subseteq V(I(X))$)

2) Tout idéal J de $k[X_1, \dots, X_n]$ est de type fini (car $k[X_1, \dots, X_n]$ est noethérien). Donc toute partie alg. de k^n est le lieu d'annulation d'une famille <u>finie</u> de polynômes.

5) Soit J un idéal de $k[X_1, \dots, X_n]$. On a $I(V(J)) \supseteq J$.

Deux obstructions à l'égalité :

- si k n'est pas alg. clos, on peut avoir $J \subsetneq k[X_1, \dots, X_n]$ et $V(J) = \emptyset$ donc $I(V(J)) = k[X_1, \dots, X_n] \supsetneq J$.
- on a $V(J) = V(\sqrt{J})$, donc $J \subseteq \sqrt{J} \subseteq I(V(J))$ et $J = \sqrt{J}$ est une cond. nécessaire pour avoir $J = I(V(J))$.

Thm 1 (Nullstellensatz fort) : Supposons k alg. clos. Alors on a $I(V(J)) = \sqrt{J}$ pour tout idéal J de $k[X_1, \dots, X_n]$.

Dém (astuce de Rabinowitch, 1929) : Soient $F_1, \dots, F_m$ des générateurs de J et soit $P \in I(V(J))$. Alors les polynômes

$$F_1, \dots, F_m, \quad X_{n+1} \cdot P - 1 \in k[X_1, \dots, X_{n+1}]$$

n'ont pas de racine commune dans k^{n+1}. Donc (cor. 1.5.4), il existe $G_1, \dots, G_{m+1}$ dans $k[X_1, \dots, X_{n+1}]$ tels que

$$1 = G_1 F_1 + \dots + G_m F_m + G_{m+1} \cdot (X_{n+1} P - 1). \qquad (*)$$

On a un homomorphisme d'anneaux

$$\begin{aligned} k[X_1, \dots, X_{n+1}] &\longrightarrow k(X_1, \dots, X_n) \\ X_i &\longmapsto X_i \quad , \quad 1 \le i \le n \\ X_{n+1} &\longmapsto 1/P \,. \end{aligned}$$

L'image de l'équation $(*)$ par cet homomorphisme est

$$1 = G_1(X_1, \dots, X_n, 1/P) \cdot F_1 + \dots + G_m(X_1, \dots, X_n, 1/P) \cdot F_m \,.$$

Si on multiplie des deux côtés par une puissance assez élevée P^N, on obtient une équation dans $k[X_1, \dots, X_n]$ qui montre que P^N est dans l'idéal engendré par $F_1, \dots, F_m$. ✓