

1. Soit k un corps algébriquement clos. On considère $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ des polynômes homogènes de degrés respectifs $d_1, \dots, d_m > 0$ en les indéterminées x_1, \dots, x_n . Le but de l'exercice est de montrer que si $n > m$ alors il existe (dans k^n) un zéro commun non-trivial (c'est-à-dire différent de $(0, \dots, 0)$) à f_1, \dots, f_m . On suppose donc que le seul zéro commun à f_1, \dots, f_m est $(0, \dots, 0)$ et on va montrer $n \leq m$.

(1) Montrer qu'il existe $r \in \mathbb{N}$ tel que tout monôme de degré (total) $\geq r$ en x_1, \dots, x_n appartienne à l'idéal \mathfrak{J} engendré par f_1, \dots, f_m dans $k[x_1, \dots, x_n]$.

(2) En déduire que tout monôme de degré (total) $\geq r$ en x_1, \dots, x_n peut s'écrire $g(x_1, \dots, x_n)$ où g est un polynôme de degré total $< r$ en x_1, \dots, x_n à coefficients dans l'anneau $A = k[f_1, \dots, f_m]$ engendré par f_1, \dots, f_m dans $k[x_1, \dots, x_n]$.

(3) En notant $K = k(f_1, \dots, f_m)$ le corps des fractions de l'anneau intègre A (vu à l'intérieur de $k(x_1, \dots, x_n)$), en déduire que $K[x_1, \dots, x_n]$ est un K -espace vectoriel de dimension finie. Conclure que $k(x_1, \dots, x_n)$ est un K -espace vectoriel de dimension finie.

(4) En raisonnant sur le degré de transcendance, conclure que $n \leq m$.

Corrigé. (1) L'hypothèse faite est que la variété $V(\mathfrak{J})$ définie par $f_1 = \dots = f_m = 0$ est la même que la variété définie par $x_1 = \dots = x_n = 0$. Le Nullstellensatz permet de conclure que pour chaque i il existe r_i tel que $x_i^{r_i}$ appartienne à l'idéal \mathfrak{J} engendré par f_1, \dots, f_m dans $k[x_1, \dots, x_n]$. Si on appelle r la somme des r_i alors tout monôme de degré total au moins r comporte nécessairement un facteur $x_i^{r_i}$ pour un certain i , et appartient donc à \mathfrak{J} .

(2) La conclusion du (1) montre que pour tout monôme q de degré $\geq r$ en les x_i il existe $h_1, \dots, h_m \in k[x_1, \dots, x_n]$ tels que $q = h_1 f_1 + \dots + h_m f_m$. Observons à présent qu'en remplaçant h_i par sa composante homogène de degré (total) $\deg q - d_i$ (ou zéro si $\deg q < d_i$), c'est-à-dire la somme des monômes ayant ce degré, puisque f_i est homogène de degré d_i et q homogène (c'est un monôme !) de degré $\deg q$, on a toujours l'égalité $q = h_1 f_1 + \dots + h_m f_m$ (en effet, on n'a pas changé les monômes de degré $\deg q$). On a donc montré (en décomposant chaque h_i comme somme de monômes) que si q est un monôme de degré $\geq r$ alors il est combinaison linéaire à coefficients dans A des monômes de degré $< \deg q$ (plus petit que lui). Ou, si on préfère, l'égalité $q = h_1 f_1 + \dots + h_m f_m$ se réinterprète comme $q = g(x_1, \dots, x_n)$ où $g \in A[x_1, \dots, x_n]$ (avec $A = k[f_1, \dots, f_m]$) et $\deg g < \deg q$. En réécrivant de nouveau les monômes (dans g) qui sont de plus grand degré $\geq r$ comme combinaison des monômes de degré strictement plus petit qu'eux, et en itérant ce processus (qui termine vu que le degré de g décroît strictement à chaque étape tant qu'il est au moins égal à r), on finit par arriver à $\deg g < r$, d'où la conclusion souhaitée.

(3) On vient de voir que tout monôme en les x_1, \dots, x_n s'écrit comme combinaison linéaire à coefficients dans A , donc à plus forte raison dans K , des monômes de degré $< r$. Comme il n'y a qu'un nombre fini de monômes de degré $< r$, le K -espace vectoriel engendré (dans $k(x_1, \dots, x_n)$) par tous les monômes en les x_i est de dimension finie, c'est-à-dire exactement que $K[x_1, \dots, x_n]$ est un K -espace vectoriel de dimension finie. Or c'est également un anneau intègre (puisque c'est un sous-anneau du corps $k(x_1, \dots, x_n)$) : et un anneau intègre de dimension finie sur un corps est lui-même un corps (puisque la multiplication par un élément non nul est injective donc bijective). Ainsi, $K[x_1, \dots, x_n]$ est le corps $K(x_1, \dots, x_n)$, qui coïncide donc avec $k(x_1, \dots, x_n)$ (étant contenu dedans...). On a donc prouvé que $k(x_1, \dots, x_n)$ est un K -espace vectoriel de dimension finie.

(4) L'extension de corps $K \subseteq k(x_1, \dots, x_n)$ étant finie, elle est algébrique. On peut alors extraire de f_1, \dots, f_m une base de transcendance sur k de $K = k(f_1, \dots, f_m)$, et celle-ci est encore une base de transcendance sur k de $k(x_1, \dots, x_n)$, donc $\deg \text{tr}_k k(x_1, \dots, x_n) \leq m$. Or manifestement x_1, \dots, x_n est une base de transcendance de $k(x_1, \dots, x_n)$ donc on a

$\deg.\text{tr}_k k(x_1, \dots, x_n) = n$. On a bien prouvé $n \leq m$. ✓

2 (théorème de Tsen). Soit k un corps algébriquement clos, $k(t)$ le corps des fractions rationnelles à une indéterminée sur k . On considère un polynôme $f \in k(t)[x_1, \dots, x_n]$ homogène de degré d à $n + 1$ indéterminées à coefficients dans $k(t)$, où $0 < d < n$ (le degré est strictement inférieur au nombre d'indéterminées). Montrer que f a un zéro non trivial : il existe x_1, \dots, x_n dans $k(t)$, non tous nuls, tels que $f(x_1, \dots, x_n) = 0$. Pour cela, on supposera (quitte à chasser les dénominateurs) que les coefficients de f sont dans $k[t]$, et on cherchera une solution (x_1, \dots, x_n) avec $x_\ell = \sum_{j=0}^N c_{\ell,j} t^j$, où les $c_{\ell,j}$ sont à déterminer et où N est un entier suffisamment grand : en considérant alors $f(x_1, \dots, x_n) = 0$ comme un système en les $c_{\ell,j}$, on appliquera le résultat de l'exercice 1.

Corrigé. Écrivons

$$f(x_1, \dots, x_n) = \sum_{i_1 + \dots + i_n = d} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

Quitte à chasser les dénominateurs, on peut supposer que les a_i sont dans $k[t]$. Soit δ le plus grand de leurs degrés. On cherche un zéro non trivial dans $k[t]$ par la méthode des coefficients indéterminés, en écrivant chaque x_ℓ (pour ℓ allant de 1 à n) comme un polynôme de degré N en t , mettons $x_\ell = \sum_{j=0}^N c_{\ell,j} t^j$. Alors l'équation $f(x_1, \dots, x_n) = 0$ devient un système d'équations homogènes en les $n(N + 1)$ coefficients $c_{\ell,j}$ des polynômes $x_\ell(t)$ exprimant la nullité des coefficients du polynôme en question. (Mieux vaut ne pas essayer d'écrire ce système ! Mais si on y tient, c'est

$$(\forall j) \sum_{\substack{s_{1,0} + \dots + s_{n,N} = d \\ s_{1,1} + \dots + N s_{n,N} + r = j}} \frac{(\sum s_{1,\bullet})! \cdots (\sum s_{n,\bullet})!}{s_{1,0}! \cdots s_{n,N}!} a_{(\sum s_{1,\bullet}), \dots, (\sum s_{n,\bullet}); r} c_{1,0}^{s_{1,0}} \cdots c_{n,N}^{s_{n,N}} = 0$$

où $\sum s_{\ell,\bullet}$ désigne $s_{\ell,0} + \dots + s_{\ell,N}$ et $a_{i_1, \dots, i_n; r}$ est le coefficient de t^r dans le polynôme $a_{i_1, \dots, i_n} \in k[t]$, et où j parcourt les entiers de 0 à $Nd + \delta$.) Ce système a $Nd + \delta + 1$ équations en $n(N + 1)$ variables, chacune homogène de degré (total) d . Puisque $d < n$, on a $Nd + \delta + 1 < n(N + 1)$ pour N assez grand. On conclut d'après le résultat de l'exercice 1. ✓

3. Soient $k \subseteq K$ deux corps, et soit n un entier naturel. On munit K^n de sa topologie de Zariski¹ : (1) montrer qu'elle induit la topologie de Zariski sur le sous-ensemble k^n . (2) On suppose que k est algébriquement clos : montrer que pour tout fermé de Zariski Z de K^n défini par des équations à coefficients dans k , l'ensemble $Z \cap k^n$ est dense dans Z pour la topologie de Zariski. Ce résultat vaut-il encore si on ne suppose plus k algébriquement clos ?

Corrigé. (1) Il s'agit de montrer que les fermés de k^n pour la topologie de Zariski sont précisément les intersections de k^n avec les fermés de K^n . Or tout fermé de Zariski de k^n peut s'écrire $V_{k^n}(f_1, \dots, f_r)$ pour certains $f_1, \dots, f_r \in k[x_1, \dots, x_n]$ (en effet, tout idéal \mathfrak{J} de $k[x_1, \dots, x_n]$ est engendré par un nombre fini d'éléments : $k[x_1, \dots, x_n]$ est noethérien) ; alors f_1, \dots, f_r peuvent se voir comme des éléments de $K[x_1, \dots, x_n]$ et il est évident que $k^n \cap V_{K^n}(f_1, \dots, f_r)$ coïncide avec $V_{k^n}(f_1, \dots, f_r)$; réciproquement, si $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ sont des éléments définissant un certain fermé de Zariski $V_{K^n}(f_1, \dots, f_r)$ de K^n , considérons une k -base c_1, \dots, c_s du k -espace vectoriel que leurs coefficients engendrent (dans K) : en écrivant $f_i = f_{i,1}c_1 + \dots + f_{i,s}c_s$ avec les $f_{i,j} \in k[x_1, \dots, x_n]$ (uniquement définis !) on voit

⁽¹⁾ On rappelle que c'est celle dont les fermés sont les $V(\mathfrak{J})$, lieu des zéros communs d'un idéal $\mathfrak{J} \subseteq K[x_1, \dots, x_n]$ de polynômes — les équations de ce fermé.

que l'intersection de $V_{K^n}(f_1, \dots, f_r)$ avec k^n est précisément $V_{k^n}(f_{1,1}, \dots, f_{r,s})$, qui est un fermé de Zariski. Ceci prouve le résultat annoncé.

(2) Supposons $Z = V_{K^n}(f_1, \dots, f_r)$ avec $f_1, \dots, f_r \in k[x_1, \dots, x_n]$: comme il a été remarqué ci-dessus, $k^n \cap Z$ coïncide avec $V_{k^n}(f_1, \dots, f_r)$. Si k est algébriquement clos, d'après le Nullstellensatz, tout élément de $k[x_1, \dots, x_n]$ qui s'annule sur $k^n \cap Z$ appartient à l'idéal radical engendré par f_1, \dots, f_r (c'est-à-dire l'idéal constitué des éléments dont une certaine puissance appartient à l'idéal engendré par f_1, \dots, f_r) : en particulier, cet élément s'annule sur Z tout entier. Plus généralement, si g est un élément de $K[x_1, \dots, x_n]$ qui s'annule sur $k^n \cap Z$, écrivons $g = g_1c_1 + \dots + g_sc_s$ où c_1, \dots, c_s est une k -base du k -espace vectoriel engendré par les coefficients de g et où $g_j \in k[x_1, \dots, x_n]$; alors chaque g_j s'annule sur $k^n \cap Z$ donc sur Z par ce qui vient d'être dit, donc g s'annule sur Z . C'est bien la preuve que $k^n \cap Z$ est Zariski-dense dans Z (son adhérence étant, *a priori*, définie comme le lieu des zéros communs de tous les g s'annulant sur $k^n \cap Z$, et évidemment elle est contenue dans Z qui est fermé).

La conclusion ne vaut pas si k n'est pas algébriquement clos. Par exemple, si $k = \mathbb{R}$ et $K = \mathbb{C}$, le fermé Z défini dans \mathbb{C}^2 (de coordonnées (x, y)) par $x^2 + y^2 = 0$ intersecte \mathbb{R}^2 en l'unique point $(0, 0)$, dont l'adhérence de Zariski (dans \mathbb{C}^2 ou \mathbb{R}^2 indifféremment) est lui-même et non pas Z tout entier. ✓

4. Soit k un corps algébriquement clos et \mathfrak{J} un idéal de $k[x_1, \dots, x_n]$ qu'on pourra pour plus de simplicité supposer radical. On appelle $V(\mathfrak{J})$ l'ensemble des n -uplets $(x_1, \dots, x_n) \in k^n$ tels que $f(x_1, \dots, x_n) = 0$ pour tout $f \in \mathfrak{J}$, qu'on munit de la topologie de Zariski². Montrer qu'alors $V(\mathfrak{J})$ est connexe (en tant qu'espace topologique) si et seulement si l'anneau quotient $k[x_1, \dots, x_n]/\mathfrak{J}$ n'a pas d'autres idempotents que 0 et 1 (c'est-à-dire que $e^2 = e$ dans $k[x_1, \dots, x_n]/\mathfrak{J}$ implique $e = 0$ ou $e = 1$).

Corrigé. Prouvons d'abord le sens « seulement si » : supposons que $k[x_1, \dots, x_n]/\mathfrak{J}$ ait un idempotent e différent de 0 et de 1. On a $e^2 = e$, soit $e(1 - e) = 0$, dans $k[x_1, \dots, x_n]/\mathfrak{J}$. Alors e se relève en un polynôme (encore noté e) dans $k[x_1, \dots, x_n]$ tel que $e \notin \mathfrak{J}$ et $1 - e \notin \mathfrak{J}$ mais $e(1 - e) \in \mathfrak{J}$. On considère $W = V(\mathfrak{J} + (e))$ le fermé de $V(\mathfrak{J})$ défini par l'idéal $\mathfrak{J} + (e)$ engendré par \mathfrak{J} et e , et $W' = V(\mathfrak{J} + (1 - e))$ le fermé défini de même par l'idéal engendré par \mathfrak{J} et $1 - e$. Autrement dit W est le lieu de $V(\mathfrak{J})$ où e vaut 0 et W' est le lieu où e vaut 1. On a $W \cup W' = V(\mathfrak{J})$: cela résulte immédiatement de $e(1 - e) \in \mathfrak{J}$ (en tout point de $V(\mathfrak{J})(k)$, soit e s'annule soit $1 - e$ s'annule) ; par ailleurs, $W \cap W' = \emptyset$, car e et $1 - e$ ne peuvent s'annuler simultanément. De plus, $W \neq V(\mathfrak{J})$ puisque $e \notin \mathfrak{J}$ et plus généralement $e^n \notin \mathfrak{J}$ (vu que $e^n = e$) pour tout $n \geq 1$ ce qui, d'après le Nullstellensatz (fort), prouve qu'il existe des points de $V(\mathfrak{J})$ où e ne s'annule pas ; de même, $W' \neq V(\mathfrak{J})$. Au final, on a montré que $V(\mathfrak{J})(k)$ s'écrivait comme la réunion de deux fermés disjoints non vides : ceci montre qu'il n'est pas connexe.

Prouvons à présent la réciproque. Si $V(\mathfrak{J})$ n'est pas connexe, on peut écrire $V(\mathfrak{J}) = W \cup W'$ où W et W' sont des fermés disjoints chacun non vide. Mettons $W = V(\mathfrak{J})$ et $W' = V(\mathfrak{J}')$ pour certains idéaux $\mathfrak{J}, \mathfrak{J}'$ contenant \mathfrak{J} , qu'on peut supposer radicaux (en appelant \mathfrak{J} l'idéal des fonctions qui s'annulent sur W et de façon semblable pour \mathfrak{J}'). Commençons par traiter le cas où \mathfrak{J} lui-même est radical. Alors $\mathfrak{J} \cap \mathfrak{J}' = \mathfrak{J}$ d'après le Nullstellensatz (fort) car $W \cup W' = V$, et $\mathfrak{J} + \mathfrak{J}' = (1)$ car $W \cap W' = \emptyset$ toujours avec le Nullstellensatz. D'après ce dernier fait, on peut trouver $e \in \mathfrak{J}$ tel que $1 - e \in \mathfrak{J}'$. On a alors $e(1 - e) \in \mathfrak{J} \cap \mathfrak{J}' = \mathfrak{J}$, autrement dit, la classe de e dans $k[x_1, \dots, x_n]/\mathfrak{J}$ est un idempotent. Or $e \notin \mathfrak{J}$ sans quoi on aurait $\mathfrak{J}' = (1)$ (il contiendrait e et $1 - e$), ce qui n'est pas. On a donc bien trouvé un idempotent e non trivial dans

⁽²⁾ La topologie dont les fermés sont les $V(\mathfrak{J})$ pour $\mathfrak{J} \supseteq \mathfrak{J}$.

$k[x_1, \dots, x_n]/\mathfrak{J}$.

Enfin, si \mathfrak{J} n'est pas supposé radical, soit $\sqrt{\mathfrak{J}}$ son radical (l'intersection des idéaux premiers qui le contiennent), c'est-à-dire que $k[x_1, \dots, x_n]/\sqrt{\mathfrak{J}}$ est le quotient de $k[x_1, \dots, x_n]/\mathfrak{J}$ par ses nilpotents (cf. exercice 3 de la feuille n°7). D'après ce qu'on vient de montrer, il existe $e \in k[x_1, \dots, x_n]/\sqrt{\mathfrak{J}}$ idempotent non trivial. Relevons e arbitrairement à $k[x_1, \dots, x_n]/\mathfrak{J}$. On a alors $e(1-e)$ nilpotent. Écrivons maintenant $1 = (e + (1-e))^{2n}$ avec n grand et développons : on peut le réécrire comme $e' + (1-e')$ où e' est la somme des termes $e^{2n} + \dots + C_{2n}^n e^n (1-e)^n$ et $1-e'$ la somme $C_{2n}^{n+1} e^{n-1} (1-e)^{n+1} + \dots + (1-e)^{2n}$, de sorte que $e'(1-e')$ s'écrit comme produit de termes tous multiples de $e^n(1-e)^n$, et pour n assez grand ceci est nul. Ainsi, e' est idempotent dans $k[x_1, \dots, x_n]/\mathfrak{J}$, et il est non trivial car il se réduit sur $e \in k[x_1, \dots, x_n]/\sqrt{\mathfrak{J}}$, qui n'est ni 0 ni 1. ✓

5. Soit k un corps, n un entier naturel, et $(x_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ une famille de n^2 indéterminées. On appelle Δ le déterminant de la matrice (x_{ij}) (c'est-à-dire dont le coefficient sur la i -ième ligne et j -ième colonne est l'indéterminée x_{ij}) : ainsi, Δ est un élément de l'anneau $k[(x_{ij})]$ des polynômes en les n^2 indéterminées considérées.

(1) Montrer ce polynôme est irréductible (autrement dit, si $\Delta = PQ$ avec $P, Q \in k[(x_{ij})]$, alors l'un de P et Q est constant). Pour cela, on pourra étudier le degré de P et Q par rapport à toutes les variables d'une ligne i_0 , puis d'une colonne j_0 .

(2) Si k est algébriquement clos, montrer (sans utiliser (1)) que pour chaque $0 \leq r \leq n$ l'ensemble des matrices de rang $\leq r$ est un fermé algébrique irréductible dans $\mathbb{M}_n(k)$ (identifié à k^{2n}) muni de sa topologie de Zariski. Pour cela, on pourra utiliser l'application $\psi: \mathbb{M}_n(k) \times \mathbb{M}_n(k) \rightarrow \mathbb{M}_n(k)$ qui envoie (a, b) sur aJb où J est une matrice judicieusement choisie.

(3) Quel rapport entre les questions (1) et (2) ?

Corrigé. (1) Supposons qu'on ait une écriture $\Delta = PQ$ avec $P, Q \in k[(x_{ij})]$.

Fixons un $1 \leq i_0 \leq n$. Considéré comme polynôme sur les n seules indéterminées $(x_{i_0 j})_{1 \leq j \leq n}$, on a Δ homogène de degré 1 (ceci se voit en développant par rapport à la i_0 -ième ligne ou bien en définissant le déterminant comme forme multilinéaire alternée sur les lignes). Par conséquent, l'un des deux polynômes P et Q doit être (toujours par rapport aux indéterminées $(x_{i_0 j})$) homogène de degré 1 et l'autre homogène de degré 0 — c'est-à-dire qu'il ne dépend pas des variables en question. Mettons que ce soit Q qui ne dépend pas des $(x_{i_0 j})$; quant à P , il est de degré non nul (c'est-à-dire exactement 1) en chacune des variables $x_{i_0 j}$, puisque c'est le cas de Δ lui-même (le déterminant dépend effectivement de chacun des coefficients de la matrice...) et que Q n'en dépend pas.

Appliquons maintenant le même raisonnement pour un $1 \leq j_0 \leq n$ par rapport à la colonne des indéterminées $(x_{i j_0})_{1 \leq i \leq n}$. Comme P est de degré 1 en l'indéterminée $x_{i_0 j_0}$, c'est forcément encore P qui est homogène de degré 1 dans les $(x_{i j_0})$ et Q qui ne dépend pas d'elles. Mais alors Q ne dépend pas de $x_{i j_0}$ pour i et j_0 arbitraires : c'est dire que Q est constant.

Ceci démontre bien l'irréductibilité de Δ .

(2) L'ensemble V_r des matrices $n \times n$ de rang $\leq r$ est un fermé algébrique car il est défini par l'annulation des déterminants de toutes les sous-matrices carrées $r \times r$, et chacun de ces déterminants est un polynôme.

Soit J la matrice $n \times n$ diagonale dont les r premiers coefficients diagonaux sont des 1 et tous les autres des 0. Alors $(a, b) \mapsto aJb$ définit une application polynomiale surjective ψ de $\mathbb{M}_n(k) \times \mathbb{M}_n(k)$ vers l'ensemble V_r des matrices de rang $\leq r$. (Le fait que l'application est polynomiale se voit directement par les formules de multiplication de matrices ; le fait que son image dans $\mathbb{M}_n(k)$ soit exactement V_r est un fait bien connu d'algèbre linéaire.) Puisque ψ est

continue pour la topologie de Zariski et que sa source est irréductible (c'est k^{2n^2}), on en déduit que son image est irréductible (si on pouvait écrire $V_r = W \cup W'$ avec W et W' deux fermés stricts de V_r , on aurait $\mathbb{M}_n(k) \times \mathbb{M}_n(k) = \psi^{-1}(W) \cup \psi^{-1}(W')$ réunion de deux fermés stricts).

(3) L'ensemble des matrices de rang $\leq n - 1$ est l'ensemble des matrices de déterminant nul, c'est-à-dire $V(\Delta)$ où Δ est le polynôme déterminant dont on a prouvé en (1) qu'il était irréductible. L'idéal qu'il engendre est donc premier, et l'ensemble des matrices de rang $\leq n - 1$ est bien irréductible. Ainsi, le (1) prouve le (2) pour $r = n - 1$. Réciproquement, le (2) prouve que $V(\Delta)$ est irréductible, ce qui montre d'après le Nullstellensatz que Δ est puissance d'un polynôme irréductible, et comme il est évident que Δ n'est pas une puissance non triviale (si on veut, l'idéal qu'il engendre est radical) on conclut que Δ est irréductible. Ainsi, le (2) prouve le (1). ✓