

1. 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 $\mathfrak{I}$ 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 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. ✓

2. Soit k un corps parfait, et $\bar{k}$ sa clôture algébrique. On appelle *groupe de Galois absolu*² de k le groupe Γ des automorphismes de $\bar{k}$ sur k .

(0) Montrer (comme en degré fini) que pour $x \in \bar{k}$, on a x fixe par Γ si et seulement si $x \in k$.

(1) Soit n un entier naturel. On notera $\mathbb{A}_k^n$ l'ensemble $\bar{k}^n / \Gamma$ des orbites de n -uplets d'éléments de $\bar{k}$ sous l'action de Γ (chacune de ces orbites est finie : pourquoi ?). Pourquoi y a-t-il un sens à se demander si un élément $f \in k[x_1, \dots, x_n]$ s'annule en un point $x \in \mathbb{A}_k^n$?

On appelle *topologie de Zariski* sur $\mathbb{A}_k^n$ la topologie quotient de la topologie de Zariski sur $\bar{k}^n$ par l'action de Γ (c'est-à-dire la topologie dont les fermés sont donnés par des fermés de Zariski de $\bar{k}^n$ stables par Γ).

(2) Si $\mathfrak{I}$ est un idéal de $k[x_1, \dots, x_n]$, on peut considérer l'idéal $\bar{k}\mathfrak{I}$ de $\bar{k}[x_1, \dots, x_n]$ (pourquoi ?) : montrer que $V(\bar{k}\mathfrak{I}) \subseteq \bar{k}^n$ est stable par l'action de Γ , i.e., définit un fermé de Zariski de $\mathbb{A}_k^n$ — qu'on notera $V(\mathfrak{I})$ — et que c'est l'ensemble des $x \in \mathbb{A}_k^n$ où tous les $f \in \mathfrak{I}$ s'annulent.

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

(²) Attention ! L'extension $k \subseteq \bar{k}$ est en général de degré infini, et Γ est en général un groupe infini...

(3) Si B est une partie de $\mathbb{A}_k^n$, on définit $I(B)$ comme l'idéal des éléments $f \in k[x_1, \dots, x_n]$ qui s'annulent en chaque $x \in B$. Montrer que si $B_{\bar{k}}$ désigne l'image réciproque de B dans $\bar{k}^n$, alors $I(B) = I(B_{\bar{k}}) \cap k[x_1, \dots, x_n]$ et $I(B_{\bar{k}}) = \bar{k} I(B)$ (pour ce dernier point, on pourra se ramener à une extension galoisienne finie contenant les coefficients du polynôme considéré, et invoquer l'indépendance linéaire des caractères).

(4) Montrer que I et V définissent des bijections réciproques entre d'une part les idéaux $\mathfrak{J}$ de $k[x_1, \dots, x_n]$ tels que $\bar{k}\mathfrak{J}$ soit radical³ et d'autre part les fermés de Zariski de $\mathbb{A}_k^n$.

Corrigé. (0) Si $x \in k$, il est trivial que x est fixe par Γ . Réciproquement, supposons que $x \in \bar{k}$ ne soit pas dans k : alors (comme k est parfait), x a un conjugué algébrique x' distinct de lui, et l'isomorphisme $k(x) \xrightarrow{\sim} k(x')$ des corps de rupture $k(x)$ et $k(x')$ de k (vus comme sous-corps de $\bar{k}$) se prolonge en un automorphisme de $\bar{k}$ au-dessus de k , définissant ainsi un élément de Γ qui envoie x sur x' , donc x n'est pas fixe par Γ .

(1) Tout d'abord, chaque orbite de $\bar{k}$ sous l'action de Γ est finie, car les éléments de l'orbite d'un élément $x \in \bar{k}$ sont les conjugués algébriques de x sur k (i.e., les autres racines de son polynôme minimal) ; on en déduit que chaque orbite de $\bar{k}^n$ est encore finie. Si $x \in \bar{k}^n$ et $f \in k[x_1, \dots, x_n]$, alors pour tout $\sigma \in \Gamma$ on a $\sigma(f(x)) = f(\sigma(x))$ (puisque les coefficients de f sont fixes par Γ), et en particulier $f(x) = 0$ si et seulement si $f(\sigma(x)) = 0$, donc il y a un sens à dire que f s'annule au point de $\mathbb{A}_k^n$ représenté par x .

(2) Si $\mathfrak{J}$ est un idéal de $k[x_1, \dots, x_n]$ alors $\bar{k}\mathfrak{J}$ est un sous- $\bar{k}$ -espace vectoriel de $\bar{k}[x_1, \dots, x_n]$ et il est stable par multiplication par chacun des x_i , donc c'est un idéal de $\bar{k}[x_1, \dots, x_n]$. Si $x \in V(\bar{k}\mathfrak{J})$ et $\sigma \in \Gamma$ alors pour tout $f \in \mathfrak{J}$ on a $f(\sigma(x)) = 0$ puisque $(\sigma^{-1}f)(x) = 0$ (car $\sigma^{-1}f \in \bar{k}\mathfrak{J}$), donc $\sigma(x) \in V(\bar{k}\mathfrak{J})$ ce qui prouve que $V(\bar{k}\mathfrak{J})$ est stable sous Γ . Enfin, si tous les $f \in \mathfrak{J}$ s'annulent en un $x \in \bar{k}^n$, on peut conclure que tous les $f \in \bar{k}\mathfrak{J}$ s'y annulent aussi, puisque ce sont des combinaisons linéaires (à coefficients dans $\bar{k}$) des premiers.

(3) Le fait qu'un $f \in k[x_1, \dots, x_n]$ s'annule en $x \in \mathbb{A}_k^n$ signifie simplement qu'il s'annule en un quelconque de ses représentants dans $\bar{k}^n$, donc $I(B) = I(B_{\bar{k}}) \cap k[x_1, \dots, x_n]$ est trivial. Dans l'autre sens, si $f \in \bar{k}[x_1, \dots, x_n]$ appartient à $I(B_{\bar{k}})$, montrons qu'on peut l'écrire comme combinaison $\bar{k}$ -linéaire d'éléments de $k[x_1, \dots, x_n]$ s'annulant sur B . Soit E une extension galoisienne finie de k , contenue dans $\bar{k}$, et contenant tous les coefficients de f (pour pouvoir se ramener à une situation de degré fini), et soit $G = \text{Gal}(E/k)$ le groupe de Galois de E sur k : alors pour tout $c \in E$ on a $\sum_{\sigma \in G} \sigma(cf) \in k[x_1, \dots, x_n]$, et ce polynôme s'annule en tout point de B (i.e., en tout point de $B_{\bar{k}}$) puisque c'est le cas de chaque terme. Or si $c_1, \dots, c_s$ forme une base de E et $\sigma_1, \dots, \sigma_s$ une énumération des éléments de G , l'indépendance linéaire des caractères montre que la matrice $(\sigma_j(c_i))$, matrice $s \times s$ à coefficients dans E , a des colonnes indépendantes (il n'existe pas de relation $\sum_j \lambda_j \sigma_j(c_i) = 0$, où $\lambda_j \in E$, pour tout i), c'est-à-dire qu'elle est inversible : donc f peut se retrouver comme combinaison E -linéaire des $\sum_j \sigma_j(c_i f)$, et on a expliqué que ces polynômes sont dans $I(B)$.

(4) Tout d'abord, il est clair que si $B \subseteq \mathbb{A}_k^n$ est une partie quelconque, alors $\bar{k} I(B) = I(B_{\bar{k}})$ est un idéal radical (de $k[x_1, \dots, x_n]$). Si Z est un fermé de Zariski de $\mathbb{A}_k^n$, mettons $Z = V(\mathfrak{J})$, alors $V(I(Z)) = V(I(V(\mathfrak{J})))$ est à la fois contenu et contenant $V(\mathfrak{J}) = Z$, donc $V(I(Z)) = Z$. Si maintenant $\mathfrak{J}$ est un idéal de $k[x_1, \dots, x_n]$ tel que $\bar{k}\mathfrak{J}$ soit radical, alors en posant $Z = V(\mathfrak{J})$, on voit que $I(Z) = I(Z_{\bar{k}}) \cap k[x_1, \dots, x_n] = \bar{k}\mathfrak{J} \cap k[x_1, \dots, x_n] = \mathfrak{J}$ (le fait que $I(Z_{\bar{k}}) = I(V(\bar{k}\mathfrak{J})) = \bar{k}\mathfrak{J}$ est une conséquence du Nullstellensatz puisque $\bar{k}\mathfrak{J}$ est radical, et le fait que $\bar{k}\mathfrak{J} \cap k[x_1, \dots, x_n] = \mathfrak{J}$ est une généralité d'algèbre linéaire : si $W' \subseteq W$ sont deux k -espaces vectoriels alors $\bar{k}W' \cap W = W'$ comme on le voit en prenant des bases). ✓

(³) Il se trouve en fait que, le corps k étant supposé parfait, $\bar{k}\mathfrak{J} \subseteq \bar{k}[x_1, \dots, x_n]$ est radical si et seulement si $\mathfrak{J} \subseteq k[x_1, \dots, x_n]$ l'est.

3. Soit k un corps algébriquement clos et $\mathfrak{I}$ un idéal de $k[x_1, \dots, x_n]$ qu'on pourra pour plus de simplicité supposer radical. On appelle $V(\mathfrak{I})$ l'ensemble des n -uplets $(x_1, \dots, x_n) \in k^n$ tels que $f(x_1, \dots, x_n) = 0$ pour tout $f \in \mathfrak{I}$, qu'on munit de la topologie de Zariski⁴. Montrer qu'alors $V(\mathfrak{I})$ est connexe (en tant qu'espace topologique) si et seulement si l'anneau quotient $k[x_1, \dots, x_n]/\mathfrak{I}$ n'a pas d'autres idempotents que 0 et 1 (c'est-à-dire que $e^2 = e$ dans $k[x_1, \dots, x_n]/\mathfrak{I}$ implique $e = 0$ ou $e = 1$).

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

Enfin, si $\mathfrak{I}$ n'est pas supposé radical, soit $\sqrt{\mathfrak{I}}$ son radical (l'intersection des idéaux premiers qui le contiennent), c'est-à-dire que $k[x_1, \dots, x_n]/\sqrt{\mathfrak{I}}$ est le quotient de $k[x_1, \dots, x_n]/\mathfrak{I}$ par ses nilpotents. D'après ce qu'on vient de montrer, il existe $e \in k[x_1, \dots, x_n]/\sqrt{\mathfrak{I}}$ idempotent non trivial. Relevons e arbitrairement à $k[x_1, \dots, x_n]/\mathfrak{I}$. 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 $C_{2n}^{m+1} e^{n-1} (1 - e)^{n+1} + \dots + (1 - e)^{2n}$, 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 $k[x_1, \dots, x_n]/\mathfrak{I}$, et il est non trivial car il se réduit sur $e \in k[x_1, \dots, x_n]/\sqrt{\mathfrak{I}}$, qui n'est ni 0 ni 1. ✓

4. 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

⁽⁴⁾ La topologie dont les fermés sont les $V(\mathfrak{J})$ pour $\mathfrak{J} \supseteq \mathfrak{I}$.

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 $(x_{i_0j})_{1 \leq j \leq n}$, 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_0j})) 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 dépende pas des (x_{i_0j}) ; quant à P , il est de degré non nul (c'est-à-dire exactement 1) en chacune des variables x_{i_0j} , 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 $(x_{ij_0})_{1 \leq i \leq n}$. Comme P est de degré 1 en l'indéterminée $x_{i_0j_0}$, c'est forcément encore P qui est homogène de degré 1 dans les (x_{ij_0}) et Q qui ne dépend pas d'elles. Mais alors Q ne dépend pas de x_{ij_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). ✓