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

Corrigé. Prouvons d'abord le sens « seulement si » : supposons que $k[x_1, \ldots, x_n]/\mathfrak{I}$ ait un idempotent e différent de 0 et de 1. On a $e^2 = e$, soit $e\,(1-e) = 0$, dans $k[x_1, \ldots, x_n]/\mathfrak{I}$. Alors e se relève en un polynôme (encore noté e) dans $k[x_1, \ldots, x_n]$ 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, $W \cap W' = \varnothing$, 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 $W \cap W' = \varnothing$ 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 $k[x_1, \ldots, x_n]/\mathfrak{I}$ 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 $k[x_1, \ldots, x_n]/\mathfrak{I}$.

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 $k[x_1, \ldots, x_n]/\sqrt{\mathfrak{I}}$ est le quotient de $k[x_1, \ldots, x_n]/\mathfrak{I}$ par ses nilpotents (cf. exercice 4 de la feuille n°6). D'après ce qu'on vient de montrer, il existe $e \in k[x_1, \ldots, x_n]/\sqrt{\mathfrak{I}}$ idempotent non trivial. Relevons e arbitrairement à $k[x_1, \ldots, x_n]/\mathfrak{I}$. 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 $e^{2n} + \cdots + C_{2n}^{n} e^n\,(1-e)^n$ et $1 - e'$ la somme $C_{2n}^{n+1} e^{n-1}\,(1-e)^{n+1} + \cdots + (1-e)^{2n}$, 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 $k[x_1, \ldots, x_n]/\mathfrak{I}$, et il est non trivial car il se réduit sur $e \in k[x_1, \ldots, x_n]/\sqrt{\mathfrak{I}}$, qui n'est ni 0 ni 1. ✓

2. Soit K un corps et k un sous-corps de K. On appelle *famille algébriquement indépendante* sur k d'éléments de K une famille $(x_i)_{i \in I}$ (on pourra se contenter d'imaginer le cas d'une famille finie) d'éléments de K telle que le morphisme naturel $\iota \colon k[(t_i)_{i \in I}] \to K$, où les t_i sont des indéterminées (c'est-à-dire que $k[(t_i)_{i \in I}]$ est l'anneau des polynômes sur les t_i), qui envoie

---

([1]) C'est-à-dire qu'il vérifie les trois propriétés suivantes dont on rappelle qu'elles sont équivalentes : (i) $\mathfrak{I}$ est intersection d'idéaux premiers, (ii) si $f^n \in \mathfrak{I}$ pour un certain $f \in k[x_1, \ldots, x_n]$ et un $n \in \mathbb{N}$ alors $f \in \mathfrak{I}$, et (iii) l'anneau quotient $k[x_1, \ldots, x_n]/\mathfrak{I}$ est réduit (i.e., tout nilpotent est nul).

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

t_i sur x_i, est injectif. Autrement dit, cela signifie qu'il n'existe pas de polynôme $P \in k[(t_i)_{i\in I}]$ tel que $P((x_i)) = 0$. (Notamment, la famille vide est algébriquement indépendante sur k, et une famille à un seul élément $x \in K$ est algébriquement indépendante sur k si et seulement si x est transcendant sur k.) Dans ces conditions, on identifiera le sous-anneau (image de ι) $k[(x_i)_{i\in I}]$ de K engendré par les x_i avec l'anneau des polynômes en les indéterminées x_i (via le morphisme ι) ; de plus, le corps des fractions $k((x_i)_{i\in I})$ de $k[(x_i)_{i\in I}]$ se plonge lui-aussi naturellement dans K (comme le sous-corps de K engendré par tous les x_i).

Si $(x_i)_{i\in I}$ est une famille d'éléments de K algébriquement indépendante sur k, on dira que $(x_i)_{i\in I}$ est une *base de transcendance* de K sur k lorsque K est algébrique sur $k((x_i)_{i\in I})$.

(1) Montrer que toute famille algébriquement indépendante sur k d'éléments de K se complète en une base de transcendance et que de toute famille génératrice (de K en tant que corps[3]) on peut extraire une base de transcendance.

(2) Montrer que deux bases de transcendance de K sur k ont toujours le même cardinal. (Pour plus de simplicité, on pourra supposer qu'une des bases est finie.) Pour cela, on pourra montrer le *lemme d'échange* : si $z_1, \ldots, z_m$ est une base de transcendance de K sur k et t un élément de K tel que $z_1, \ldots, z_\ell, t$ soient algébriquement indépendants sur k (pour un certain ℓ), alors il existe j entre $\ell + 1$ et m tel qu'en remplaçant z_j par t dans la base de transcendance $z_1, \ldots, z_m$ on trouve encore une base de transcendance.

Le cardinal commun des bases de transcendance de K sur k est appelé le *degré de transcendance* de K sur k, et noté $\operatorname{deg.tr}_k K$. Ainsi, $\operatorname{deg.tr}_k K = 0$ exactement lorsque K est algébrique sur k.

Corrigé. (1) Le lemme de Zorn montre que toute famille algébriquement indépendante est contenue dans une famille algébriquement indépendante maximale. Montrons qu'une telle famille est une base de transcendance : si $(x_i)_{i\in I}$ est une famille algébriquement indépendante maximale, on veut donc prouver que K est algébrique sur $k((x_i)_{i\in I})$; pour cela, soit $t \in K$, on veut montrer qu'il n'est pas transcendant sur $k((x_i)_{i\in I})$. Mais s'il l'est, on observe que la famille obtenue en rajoutant t à la famille $(x_i)_{i\in I}$ est encore algébriquement indépendante : en effet, si on avait un polynôme $P(t, (x_i))$ qui l'annulât, en considérant P comme polynôme de la seule variable t (dont il dépend effectivement, sinon il donnerait une relation de dépendance algébrique entre les x_i, chose qui n'existe pas) on contredirait la transcendance de t sur $k((x_i)_{i\in I})$. Par maximalité de $(x_i)_{i\in I}$, ceci ne peut pas se produire : donc K est bien algébrique sur $k((x_i)_{i\in I})$ et $(x_i)_{i\in I}$ est une base de transcendance.

Soit maintenant $(x_i)_{i\in J}$ une famille génératrice (i.e., $K = k((x_i)_{i\in J})$) : soit I une partie maximale de J telle que $(x_i)_{i\in I}$ soit algébriquement indépendante (de nouveau on utilise le lemme de Zorn), et on va montrer qu'il s'agit d'une base de transcendance. Si ce n'est pas le cas, l'extension K de $k((x_i)_{i\in I})$ n'est pas algébrique, donc elle ne peut pas être engendrée uniquement par des éléments algébriques, donc il existe $j \in J$ (et évidemment $j \notin I$) tel que x_j soit transcendant sur $k((x_i)_{i\in I})$, et par ce qu'on vient d'expliquer la famille obtenue en rajoutant j à I contredit la maximalité de I.

(2) Prouvons le lemme d'échange proposé par l'énoncé : soit $z_1, \ldots, z_m$ une base de transcendance (finie) et $t \in K$ tel que $z_1, \ldots, z_\ell, t$ soient algébriquement indépendants. Puisque $t \in K$ est algébrique sur $k(z_1, \ldots, z_m)$, on peut trouver une relation de dépendance algébrique $P(t, z_1, \ldots, z_m) = 0$; comme $z_1, \ldots, z_\ell, t$ sont algébriquement indépendants par hypothèse, il le polynôme P ne peut pas dépendre que de ces variables, donc il doit faire intervenir z_j pour un certain j entre $\ell + 1$ et m. Soit z'_i défini par $z'_i = z_i$ si $i \neq j$ et $z'_j = t$. La relation $P(t, z_1, \ldots, z_m) = 0$, ou $P(z_j, z'_1, \ldots, z'_m) = 0$, se lit aussi comme affirmant que z_j est algé-

(3) ...ou même toute famille génératrice d'un sous-corps de K sur lequel K est algébrique...

brique sur $k(z'_1, \ldots, z'_m)$: il s'ensuit que K est algébrique sur $k(z'_1, \ldots, z'_m)$ (puisqu'il est algébrique sur $k(z_1, \ldots, z_m)$ et qu'on vient de voir que ce dernier est algébrique sur $k(z'_1, \ldots, z'_m)$). D'autre part, les z'_i sont algébriquement indépendants : car s'ils ne l'étaient pas, comme les $z_1, \ldots, z_m$ le sont, ce serait t qui serait algébrique sur les autres z'_i, donc z_j serait algébrique sur les autres $z'_i = z_i$, par hypothèse ce n'est pas le cas. On a bien prouvé que les z'_i forment une base de transcendance de K sur k.

Venons-en au résultat recherché : tout d'abord, s'il existe une base de transcendance finie $z_1, \ldots, z_m$, alors toute famille algébriquement indépendante $x_1, \ldots, x_n$ vérifie $n \leq m$. En effet, le lemme d'échange permet de remplacer un des z_i, mettons z_1, par x_1, puis un des z_i autre que z_1, mettons z_2, par x_2, et ainsi de suite, toujours en obtenant des bases de transcendance. Finalement, on voit que $x_1, \ldots, x_m$ est une base de transcendance, donc $n \leq m$. (Ici, on a supposé la famille $x_1, \ldots, x_n$ finie, mais de façon générale on voit que toute sous-famille finie d'une famille algébriquement indépendante doit avoir au plus m éléments donc toute famille algébriquement indépendante est finie.)

Enfin, si on a une base de transcendance infinie $(x_i)_{i \in I}$, d'après ce qu'on vient de voir, toute autre base de transcendance $(y_j)_{j \in J}$ est également infinie ; par ailleurs, tout élément y_j de K est algébrique sur le sous-corps engendré par une sous-famille *finie* des x_i, donc on a une application de J vers les parties finies de I telle que l'image réciproque d'une partie finie donnée de I soit finie, et ceci prouve bien que I et J ont même cardinal (en utilisant le fait que, pour I infini, I est équipotent à l'ensemble de ses parties finies). ✓

3. Soit k un corps algébriquement clos. On considère $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ des polynômes homogènes de degrés respectifs $d_1, \ldots, d_m > 0$ en les indéterminées $x_1, \ldots, x_n$. 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 $(0, \ldots, 0)$) à $f_1, \ldots, f_m$. On suppose donc que le seul zéro commun à $f_1, \ldots, f_m$ est $(0, \ldots, 0)$ 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 $x_1, \ldots, x_n$ appartienne à l'idéal $\mathfrak{I}$ engendré par $f_1, \ldots, f_m$ dans $k[x_1, \ldots, x_n]$.

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

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

(4) En utilisant les résultats de l'exercice 2, conclure que $n \leq m$.

Corrigé. (1) L'hypothèse faite est que la variété $V(\mathfrak{I})$ définie par $f_1 = \ldots = f_m = 0$ est la même que la variété définie par $x_1 = \ldots = x_n = 0$. Le Nullstellensatz permet de conclure que pour chaque i il existe r_i tel que $x_i^{r_i}$ appartienne à l'idéal $\mathfrak{I}$ engendré par $f_1, \ldots, f_m$ dans $k[x_1, \ldots, x_n]$. 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 $\mathfrak{I}$.

(2) La conclusion du (1) montre que pour tout monôme q de degré $\geq r$ en les x_i il existe $h_1, \ldots, h_m \in k[x_1, \ldots, x_n]$ tels que $q = h_1 f_1 + \cdots + h_m f_m$. 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 $q = h_1 f_1 + \cdots + h_m f_m$ (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 $q = h_1 f_1 + \cdots + h_m f_m$ se réinterprète comme $q = g(x_1, \ldots, x_n)$ où $g \in A[x_1, \ldots, x_n]$ (avec $A = k[f_1, \ldots, f_m]$) et $\deg g < \deg q$. En récrivant 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 $x_1, \ldots, x_n$ 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 $k(x_1, \ldots, x_n)$) par tous les monômes en les x_i est de dimension finie, c'est-à-dire exactement que $K[x_1, \ldots, x_n]$ est un K-espace vectoriel de dimension finie. Or c'est également un anneau intègre (puisque c'est un sous-anneau du corps $k(x_1, \ldots, x_n)$) : 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, $K[x_1, \ldots, x_n]$ est le corps $K(x_1, \ldots, x_n)$, qui coïncide donc avec $k(x_1, \ldots, x_n)$ (étant contenu dedans...). On a donc prouvé que $k(x_1, \ldots, x_n)$ est un K-espace vectoriel de dimension finie.

(4) L'extension de corps $K \subseteq k(x_1, \ldots, x_n)$ étant finie, elle est algébrique. D'après les résultats de l'exercice 2, on peut extraire de $f_1, \ldots, f_m$ une base de transcendance sur k de $K = k(f_1, \ldots, f_m)$, et celle-ci est encore une base de transcendance sur k de $k(x_1, \ldots, x_n)$, donc $\operatorname{deg.tr}_k k(x_1, \ldots, x_n) \leq m$. Or manifestement $x_1, \ldots, x_n$ est une base de transcendance de $k(x_1, \ldots, x_n)$ donc $\operatorname{deg.tr}_k k(x_1, \ldots, x_n) = n$. On a bien prouvé $n \leq m$. ✓

4 (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 $f \in k(t)[x_1, \ldots, x_n]$ 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 $x_1, \ldots, x_n$ dans $k(t)$, non tous nuls, tels que $f(x_1, \ldots, x_n) = 0$. Pour cela, on supposera (quitte à chasser les dénominateurs) que les coefficients de f sont dans $k[t]$, et on cherchera une solution $(x_1, \ldots, x_n)$ 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 $f(x_1, \ldots, x_n) = 0$ comme un système en les $c_{\ell,j}$, on appliquera le résultat de l'exercice 3.

Corrigé. Écrivons

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

Quitte à chasser les dénominateurs, on peut supposer que les $a_{\underline{i}}$ 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 $f(x_1, \ldots, x_n) = 0$ 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

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

où $\Sigma s_{\ell,\bullet}$ désigne $s_{\ell,0} + \cdots + s_{\ell,N}$ et $a_{i_1, \ldots, i_n; r}$ est le coefficient de t^r dans le polynôme $a_{i_1, \ldots, i_n} \in k[t]$, 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 3. ✓

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 $\psi\colon \mathbb{M}_n(k) \times \mathbb{M}_n(k) \to \mathbb{M}_n(k)$ 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 dépende 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 $(x_{ij_0})_{1\leq i\leq n}$. 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_{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 $k^{2\,n^2}$), 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). ✓

Motivations : L'exercice 1 est un exemple de traduction algébrique de propriétés géométriques. L'exercice 2 est à comparer avec l'introduction des bases et de la dimension pour un espace vectoriel (on peut, d'ailleurs, donner un formalisme abstrait de bases et de dimension qui recouvre ces deux situations — par exemple dans le cadre de la théorie des modèles). L'exercice 3 constitue la situation non triviale la plus simple de la théorie de la dimension : il faut imaginer la situation dans l'espace projectif $\mathbb{P}^{n-1}$ de dimension $n-1$ sur k : chaque f_i découpe une hypersurface dans ce projectif, qui fait chuter la dimension de 1, mais tant qu'il y a moins de $n-1$ hypersurfaces l'intersection ne peut pas être vide. L'exercice 4 exprime le fait que le corps $k(t)$ des fonctions rationnelles à une indéterminée sur un corps algébriquement clos est « C_1 » (la définition d'un corps C_1 étant précisément la conclusion de l'exercice). L'exercice 5 est un classique.