Concours Agrégation, Mathématiques générales

Leçon 62- Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques

Commentaires du jury 2015 : Il semble que cette leçon soit moins choisie par les candidats depuis l'ajout de l'aspect algorithmique dans l'intitulé. A ce sujet, il faut savoir que les techniques liées au simple pivot de Gauss constituent l'essentiel des attendus. La leçon doit impérativement présenter la notion de système échelonné, avec une définition précise et correcte et situer l'ensemble dans le contexte de l'algèbre linéaire (sans oublier la dualité !). Pour les candidats chevronnés, les relations de dépendances linéaires sur les colonnes d'une matrice échelonnée sont claires et permettent de décrire simplement les orbites de l'action à gauche de $GL(n,K)$ sur $M_n(K)$ donnée par $(P,A) \to PA$. Un point de vue opératoire doit accompagner l'étude théorique et l'intérêt pratique (algorithmique) des méthodes présentées doit être expliqué y compris sur des exemples simples où l'on attend parfois une résolution explicite. Des discussions sur la résolution de systèmes sur $\mathbb{Z}$ et la forme normale de Hermite peuvent trouver leur place dans cette leçon.
Commentaires du jury 2016 : Dans cette leçon, les techniques liées au simple pivot de Gauss constituent l'essentiel des attendus. Il est impératif de présenter la notion de système échelonné, avec une définition précise et correcte, et de situer l'ensemble dans le contexte de l'algèbre linéaire (sans oublier la dualité). Un point de vue opératoire doit accompagner l'étude théorique et l'intérêt pratique (algorithmique) des méthodes présentées doit être expliqué y compris sur des exemples simples où l'on attend parfois une résolution explicite. S'ils le désirent, les candidats peuvent aussi présenter les relations de dépendances linéaires sur les colonnes d'une matrice échelonnée qui permettent de décrire simplement les orbites de l'action à gauche de $GL(n,K)$ sur $M_n(K)$ donnée par $(P,A) \to PA$. De même, des discussions sur la résolution de systèmes sur $\mathbb{Z}$ et la forme normale de Hermite peuvent trouver leur place dans cette leçon.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2']Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. B-C-D] Fresnel J. *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)
et
[C. G.] Caldero P., Germoni J. *Histoires hédonistes de groupes et de géométries* (Calvage Mounet 2016)
[Co.] Cohen H., *A course in computational algebraic number theory* Graduate texts in mathematics 138 (Springer 1996)
[Du.] Duverney D. *Théorie des nombres* (Dunod 2007)

Développements conseillés :

(1) Sous-espaces vectoriels de K^n solutions du système linéaire homogène $A\,{}^t(x_1, x_2, ..., x_p) = 0$ et matrice échelonnée normalisée représentant de l'orbite de $A \in M_{n,p}(K)$ pour l'action de $\mathrm{GL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche, [Fr. A] théorème p. 49 et applications p. 73 et 74, 75 et exercices 1 et 2 ci-dessous. Voir aussi [C. G.] tome 1 p. 130.

(2) L'algorithme de décomposition "LU", [F. M. 1] $n°4$. Application à la décomposition de Cholesky, [Fr. B-C-D] p. 211. Application à la signature des matrices symétriques réelles, [F. M. 1] $n°41$.

(3) Le théorème des restes chinois généralisé, [F. M. 2] p. 189 et exercice 7 ci-dessous.

(4) Théorème des zéros et systèmes linéaires, [F. M. 2] p. 271 et exercice 8 ci-dessous.

Exercice 1 Sous-espaces vectoriels de K^n solutions du système linéaire homogène $A\ {}^t(x_1, x_2, ..., x_p) = 0$ et matrice échelonnée normalisée représentant de l'orbite de $A \in M_{n,p}(K)$ pour l'action de $\mathrm{GL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche.

Rappel, [Fr. A] p. 47-49.

Une matrice échelonnée normalisée est nulle ou de rang $r > 0$ et associée à une suite $1 \leq j_1 < j_2 < ... < j_r \leq n$, ce sont alors les matrices $N(a) = [C_1, C_2, ..., C_p] \in M_{n,p}(K)$ de rang r telles que les colonnes $C_{j_k},\ 1 \leq k \leq r-1$ sont les $r-1$ premiers vecteurs de la base canonique $(e_i)_{1\leq i\leq n}$ de K^n, et $C_{j_r} = ae_{j_r}$ avec $a = 1$ si $r < n$ et $a \in K - \{0\}$ si $r = n$. Les autres colonnes étant sujettes à la règle suivante : $C_i = 0$ pour $1 \leq i \leq j_1$, $C_j \in \bigoplus_{1\leq i\leq k} Ke_i$ pour $j_k \leq i \leq j_{k+1}$) et enfin $C_j \in \bigoplus_{1\leq i\leq r} Ke_i$ pour $j_r \leq i$.

Dans ce qui suit les matrices "échelonnée normalisées unité "sont la matrice nulle ou les matrices échelonnées normalisées $N(a)$ avec $a = 1$. Dans [Fr. A] p. 47-49, on montre que les matrices échelonnées normalisées forment un système de représentants des orbites de l'action de $\mathrm{SL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche.

On va montrer que les matrices "échelonnées normalisées unité " forment un système de représentants des orbites de l'action de $\mathrm{SL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche.

(1) Soit $A \in M_{n,p}(K)$ avec $\mathrm{rang}(A) < n$, montrer que les orbites de A sous $\mathrm{GL}_n(K)$ et $\mathrm{SL}_n(K)$ coïncident.

Preuve. On a $\mathrm{SL}_n(K)A = \mathrm{SL}_n(K)N_r(1)$ *où* $N_r(1)$ *est le représentant échelonné normalisé avec* $a = 1$ *puisque* $\mathrm{rang}(A) < n$. *Maintenant si* $b \in K^\times$ *et* $D_n(b)$ *la dilatation de diagonale* $(1, ..., 1, b)$, *alors* $N_r(1) = D_n(b)N_r(1)$; *ainsi* $\mathrm{SL}_n(K)N_r(1) = \mathrm{SL}_n(K)D_n(K^\times)N_r(1)$ *et donc* $\mathrm{SL}_n(K)N_r(1) = \mathrm{GL}_n(K)N_r(1)$ *et* $\mathrm{GL}_n(K)A = \mathrm{SL}_n(K)A$. ///

(2) Soit $A \in M_{n,p}(K)$ avec $\mathrm{rang}(A) = n$. Montrer qu'il existe $P \in \mathrm{GL}_n(K)$ avec $PA = N$ échelonnée normalisée unité.

Preuve. Comme rappelé au-dessus il existe $S \in \mathrm{SL}_n(K)$ *avec* $SA = N_n(a)$ *échelonnée normalisée. Ainsi* $P := D_n(\frac{1}{a})$ *convient.*

(3) Mêmes notations que précédemment. Montrer l'unicité d'un représentant échelonné normalisé unité dans l'orbite $\mathrm{GL}_n(K)A$).

Preuve. Soit $P \in \mathrm{GL}_n(K)$ *avec* $PA = N_n(1)$, *alors* $D_n(\frac{1}{\det P})PA = D_n(\frac{1}{\det P})N_n(1)$ *est échelonnée normalisée et* $S := D_n(\frac{1}{\det P})P \in \mathrm{SL}_n(K)$. *Ainsi* $D_n(\frac{1}{\det P})N_n(1) = N_n(a)$ *est le représentant échelonné normalisé dans l'orbite* $\mathrm{SL}_n(K)A$. ///

(4) Montrer par un procédé algorithmique que deux matrices échelonnées normalisées unité sont égales si et seulement si elles ont le même noyau. Ainsi on retrouve la bijection entre les orbites sous $\mathrm{GL}_n(K)$ des matrices de $M_{n,p}(K)$ et les sous-espaces vectoriels V de K^p avec $\dim V \geq p - n$; précisément si $A \in M_{n,p}(K)$ l'espace V correspondant est l'ensemble des solutions du système linéaire homogène $A\ {}^t(x_1, x_2, ..., x_p) = 0$.

Preuve. Soient donc $N = (n_{i,j})$ *et* $N' = (n'_{i,j})$ *deux matrices échelonnées normalisées unité de rang* r *resp.* r' *avec* $\mathrm{Ker}\, N = \mathrm{Ker}\, N'$. *Par le théorème du rang on a* $r = r'$. *On note* $C_{j_k},\ 1 \leq k \leq r$ *resp.* $C'_{j'_k},\ 1 \leq k \leq r$ *la colonne de* N *resp.* N' *qui est égale à* e_k.

Ainsi $e_1, ..., e_{j_1-1} \in \ker N$ *d'où* $j'_1 \geq j_1$ *et par symétrie* $j'_1 = j_1$.

Soit $j_1 < j < j_2$, *montrons que* $n_{1,j} = n'_{1,j}$ *et* $n_{i,j} = n'_{i,j}$ *si* $i > 1$. *Pour cela on remarque que* $n_{1,j}e_{j_1} - e_j \in \mathrm{Ker}\, N = \mathrm{Ker}\, N'$, *il suit que* $0 = N'({}_{1,j}e_{j_1} - e_j) = (n_{1,j} - n'_{1,j})e_1 + \sum_{i>1} n'_{i,j}e_i$ *d'où le résultat. Il suit en sus de cela que* $j'_2 \geq j_2$ *avec égalité par symétrie.*

Si $j_2 < j < j_3$, *alors* $n_{1,j}e_{j_1} + n_{2,j}e_{j_2} - e_j \in \mathrm{Ker}\, N = \mathrm{Ker}\, N'$ *et donc* $0 = (n_{1,j} - n'_{1,j})e_1 + (n_{2,j} - n'_{2,j})e_2 + \sum_{i>2} n'_{i,j}e_i$ *...etc...* . ///

(5) Déduire de la question précédente que si $A, B \in M_{n,p}(K)$ alors $\mathrm{Ker}\, A = \mathrm{Ker}\, B$ si et seulement si il existe $P \in \mathrm{GL}_n(K)$ avec $B = PA$; autrement dit l'ensemble des solutions des systèmes linéaires homogènes $A\ {}^t(x_1, x_2, ..., x_p) = 0$ resp. $B\ {}^t(x_1, x_2, ..., x_p) = 0$ sont les mêmes si et seulement si A et B sont dans la même orbite pour l'action de $\mathrm{GL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche.

Preuve. Seule l'implication $\operatorname{Ker} A = \operatorname{Ker} A'$ *implique l'existence de* $P \in \mathrm{GL}_n(K)$ *avec* $A' = PA$ *mérite justification. On écrit* $A = UN$ *resp.* $A = UN'$ *avec* $U, U' \in \mathrm{GL}_n(K)$ *et* N, N' *des matrices normalisées unité. On a* $\operatorname{Ker} N = \operatorname{Ker} N'$ *et on conclut avec la question précédente. Une preuve directe est proposée dans l'exercice qui suit. ///*

Exercice 2 Une variante de la dernière question de l'exercice précédent.

(1) Si $A, A' \in M_{n,p}(K)$ alors $\operatorname{Ker} A = \operatorname{Ker} A'$ si et seulement si il existe $P \in \mathrm{GL}_n(K)$ avec $A' = PA$; autrement dit l'ensemble des solutions des systèmes linéaires homogènes $A\ {}^t(x_1, x_2, ..., x_p) = 0$ resp. $A'\ {}^t(x_1, x_2, ..., x_p) = 0$ sont les mêmes.

Preuve. On traduit cela en terme d'applications linéaires c'est alors une application du théorème de factorisation : il existe une unique application linéaire v de $\operatorname{Im} A$ dans $\operatorname{Im} A'$ telle que $v \circ A = A'$ et puisque $\operatorname{Ker} A = \operatorname{Ker} A'$, v est bijective. Il faut prolonger v en un automorphisme w de K^n. Pour cela on écrit $K^n = \operatorname{Im} A \bigoplus S = \operatorname{Im} A' \bigoplus S'$ et puisque S, S' ont la même dimension on prolonge v à S en envoyant une base donnée de S sur une base de S'.

(2) Si $K = \mathbb{R}$ ou $\mathbb{C}$ quelle est la fermeture des orbites ?

Preuve. Soit $A \in M_{n,p}(K)$ *et* r *le rang de* A.

Si $r < n$, $\mathrm{GL}_n(K)A = \mathrm{SL}_n(K)D_n(K^\times)A = \mathrm{SL}_n(K)A$, *ainsi l'orbite de* A *est dense dans l'espace vectoriel* $M_n(K)A$ *qui est fermé ...*

Si $r = n$ *et donc* $n \leq p$ *on écrit* $A = P(I_n, 0.., 0)Q$ *avec* P *dans* $\mathrm{SL}_n(K)$ *et* Q *dans* $\mathrm{GL}_n(K)$ *(utiliser une dilatation). Ainsi l'orbite de* A *est homéomorphe à* $\mathrm{SL}_n(K)(I_n, 0.., 0) = (\mathrm{SL}_n(K), 0.., 0)$ *qui est fermé dans* $M_{n,p}(K)$. ///

Exercice 3

La décomposition "LDU" (communément dénommée "LU"), [F. M. 2] p. 28.

Soient $L_s \subset \mathrm{GL}_n(K)$ le groupe triangulaire inférieur strict (Id sur la diagonale) et $U_{s,n} \subset \mathrm{GL}_n(K)$ le groupe triangulaire supérieur strict (Id sur la diagonale), $\mathcal{D} \subset \mathrm{GL}_n(K)$ le sous-groupe des matrices diagonales inversibles et $P \subset \mathrm{GL}_n(K)$ le sous-groupe des matrices de permutations $Q(\sigma)$ avec $\sigma \in \mathcal{S}_n$ le groupe des permutations de $\{1, 2, ..., n\}$. Enfin si $M \in M_n(K)$ et $1 \leq k \leq n$, on note M_k, la matrice principale construite sur les k-premières lignes et colonnes de M et $\Delta_k(M)$ son déterminant.

(1) Soit $M \in \mathrm{GL}_n(K)$, montrer qu'il existe σ une permutation de $\{1, 2, ..., n\}$, $L \in L_{s,n}$, $U \in U_{s,n}$ et $D \in \mathcal{D}$ avec $A = Q(\sigma)LDU$.

Preuve. Cela revient à dire qu'après permutation des lignes et des opérations sur les colonnes de la forme C_j *reçoit* $C_j + \lambda C_i$ *avec* $i < j$, *la matrice devient triangulaire inférieure. Comme* $M = (m_{i,j})$ *est inversible il existe* k *avec* $m_{k,1} \neq 0$. *On permute alors les lignes* L_1 *et* L_k *et ensuite par des opérations convenables de la forme* C_j *reçoit* $C_j + \lambda_j C_1$ *pour* $1 < j \leq n$, *onobtient une matrice* $N = (n_{i,j} \in \mathrm{GL}_n(K)$ *avec* $n_{1,1} \neq 0$ *et* $n_{1,j} = 0$ *pour* $1 < j \leq n$ *; on réitère le procédé pour la matrice* $(n_{i,j}), 2 \leq i, j \leq n$... ///

(2) Soit $M = LU$ avec $L \in M_n(K)$ triangulaire inférieure et , $U \in M_n(K)$ quelconque. Montrer que $M_k = L_k U_k$ pour $1 \leq k \leq n$.

Preuve. Le plus lumineux est de faire un produit par blocs. On écrit $L = \begin{pmatrix} L_{1,1} & L_{1,2} \\ L_{2,1} & L_{2,2} \end{pmatrix}$ *avec* $L_{1,1} \in M_{k,k}$, $L_{1,2} \in M_{k,n-k}$, $L_{2,1} \in M_{n-k,k}$ *et* $L_{2,2} \in M_{n-k,n-k}$ *et de même pour* U. *Alors* $LU = \begin{pmatrix} L_{1,1}U_{1,1} + L_{1,2}U_{2,1} & L_{1,1}U_{1,2} + L_{1,2}U_{2,2} \\ L_{2,1}U_{1,1} + L_{2,2}U_{2,1} & L_{2,1}U_{1,2} + L_{2,2}U_{2,2} \end{pmatrix}$. *Puisque* L *est triangulaire inférieure on a* $L_{1,2} = 0$ *et* $L_{1,1} = L_k$, $U_{1,1} = U_k$, *d'où le résultat. ///*

(3) En déduire que si $M = LDU$ avec $L \in L_{s,n}$, $D \in \mathcal{D}$ et $U \in U_{s,n}$ alors $M_k = L_k D_k U_k$ et que $\Delta_k(M) = \Delta_k(D)$.

Preuve. Puisque L est triangulaire inférieure il suit de la question 1) que $M_k = L_k(DU)_k$ et puisque D est diagonale donc triangulaire inférieure $(DU)_k = D_kU_k$. Le reste est immédiat. ///

(4) Soit $M \in M_n(K)$ avec $\prod_{1\leq i\leq n} \Delta_i(M) \neq 0$. En appliquant le pivot de Gauss aux lignes de la matrice M, montrer qu'il existe $L \in L_{s,n}$, $U \in U_{s,n}$ et $D \in \mathcal{D}$ avec $M = LDU$.

Preuve. Puisque $m_{1,1} = \Delta_1(M)$ la multiplication à gauche par les matrices $B_{i,1}(-\frac{m_{i,1}}{m_{1,1}})$ pour $1 < i \leq n$ donne la matrice M' avec M'_2 triangulaire supérieure de diagonale $m'_{1,1} = m_{1,1},\ m'_{2,2}$. Par la question 1 (il faut remarquer que $B_{i,1}(-\frac{m_{i,1}}{m_{1,1}}) \in L_{s,n}$) on déduit que $\Delta_2(M) = \Delta_2(M') = m_{1,1}m'_{2,2}$, ainsi $m'_{2,2} \neq 0$ et on reitère le procédé jusqu'à l'obtention d'une matrice triangulaire supérieure. ///

(5) On conserve les hypothèses de la question précédente. Montrer que le triplet (L, D, U) est unique.
Preuve. Si $LDU = L'D'U'$ on déduit que $L^{-1}L' = (DU)(D'U')^{-1}$ est dans $L_{s,n}$ et triangulaire supérieure, c'est donc la matrice Id. Il suit que $L = L'$ et $DU = D'U'$. Ainsi $D^{-1}D' = UU'^{-1}$ est diagonale et dans $U_{s,n}$, c'est donc la matrice Id. ///

(6) Dans cette question K est le corps fini à q éléments. Montrer que le nombre de matrices de $M_n(\mathbb{F}_q)$ qui admettent une décomposition "LDU" est $(q-1)^n q^{n(n-1)}$.

Preuve. Puisque décomposition "LDU" est unique il suffit de compter les choix respectivement pour L, D et U.

Dans [C. G.] une solution par récurrence est proposée : Soit $M_n \in M_n(\mathbb{F}_q)$ qui admet une décomposition "LDU" et $M \in M_{n+1}(\mathbb{F}_q)$ une matrice dont la matrice principale construite sur les n premières colonnes coïncide avec M_n. On montre qu'une CNS pour que M admette une décomposition "LDU" est que le coefficient $m_{n+1,n+1}$ évite une valeur fonction des autres coefficients. Précisément il s'agit d'éviter les solutions de l'équation $\Delta_{n+1}(M_{n+1}) = 0$. Puisque les colonnes de la matrices M_n sont linéairement indépendantes il existe des coefficients uniquement définis λ_i pour $i \leq n$ tels que $m_{i,n+1} = \sum_{k\leq n} \lambda_k m_{i,k}$ (les λ_i sont les solutions d'un système de Cramer) ainsi $\det M_{n+1} = (m_{n+1,n+1} - \sum_{k\leq n} \lambda_k m_{n+1,k}) \det M_n$. Alors M_{n+1} admet une décomposition "LDU" si et seulement si $m_{n+1,n+1} \neq \sum_{k\leq n} \lambda_k m_{n+1,k}$. Ainsi si N_n est le nombre de matrices de $M_n(\mathbb{F}_q)$ qui admettent une décomposition "LDU" alors $N_{n+1} = (q-1)q^{2n}N_n$. On conclut avec $N_1 = q-1$. ///

Exercice 4
La décomposition "LDU" générique, [F. M. 2] p. 41.

Exercice 5 Rang, système linéaire et changement de base.

Soit K un corps commutatif et $M = (m_{i,j}) \in M_{p,n}(K)$. On rappelle que le rang de $M = (C_1, C_2, ..., C_n)$ est la dimension de l'espace vectoriel engendré par les vecteurs colonnes $C_k,\ 1 \leq k \leq n$ de M. Soit $I_s := (i_1, i_2, ..., i_s)$ avec $1 \leq i_1 < i_2 < ... < i_s \leq p$ et $J_s := (j_1, j_2, ..., j_s)$ avec $1 \leq j_1 < j_2 < ... < j_s \leq n$ $M_{I_s,J_s} \in M_s(K)$ la matrice extraite de M en oubliant les lignes d'indices $\notin I_s$ et les colonnes d'indices $\notin J_s$.

(1) On suppose que le rang de M est égal à r. Montrer que pour $s > r$, $\det M_{I_s,J_s} = 0$ (on pourra considérer une projection linéaire convenable)

Preuve. Pour $s > r$ les colonnes $(C_j)_{j\in J_s}$ sont liées il en est donc de même si l'on supprime les lignes de ces colonnes d'indice $\notin I_s$ ainsi la matrice M_{I_s,J_s} n'est pas inversible. ///

(2) En déduire que le rang de M est égal au maximum des entiers s tels qu'il existe une matrice M_{I_s,J_s} extraite de M qui est inversible.

Preuve. Il faut de montrer qu'il existe un déterminant $\det M_{I_r,J_r}$ qui n'est pas nul. On extrait de la famille $C_1, C_2, ..., C_n$, une famille libre maximale $(C_k)_{k\in I_s}$ et puisque c'est une base de l'espace vectoriel engendré par les vecteurs colonnes $C_k,\ 1 \leq k \leq n$ de M on a $s = r$. On est ainsi ramené à une matrices $M \in M_{p,r}(K)$ dont les colonnes sont linéairement indépendantes ; il faut en extraire

une sous-matrice de taille $r \times r$ de déterminant non nul. Pour cela on fait une récurrence sur r. Si $r = 1$, la matrice n'est pas nul et c'est donc fini. Supposons donc que $M = (C_1, C_2, ..., C_{r+1}) = {}^t(L_1, L_2, ..., L_p) \in M_{p,r+1}(K)$ est de rang $r+1$. Quitte à faire une permutation des lignes (donc un changement de base à l'arrivée) on peut supposer pour simplifier l'écriture que la matrice principale construite sur les r-premières lignes et les r premières colonnes $M_r := (C_1(r), C_2(r), ..., C_r(r)) \in M_{r,r}(K)$ est inversible. On suppose maintenant que les matrices $M_r(i) := {}^t(L_1, ..., L_r, L_i) =: (C_1(r,i), C_2(r,i), ..., C_r(r,i), C_{r+1}(r,i)) \in M_{r+1,r+1}(K)$ pour $i > r$ sont de déterminant nul, on doit alors aboutir à une contradiction. Puisque les r-premières colonnes de $M_r(i)$ sont indépendantes, la dernière colonne (*) $C_{r+1}(r,i) = \sum_{1 \leq k \leq r} \lambda_k C_k(r,i)$ et les λ_k sont ainsi uniquement déterminés (ce sont les solutions d'un système de Cramer). Si on projette cette relation (*) sur les r-premières lignes on obtient (**) $C_{r+1}(r) = \sum_{1 \leq k \leq r} \lambda_k C_k(r)$ où $C_{r+1}(r) := {}^t(m_{1,r+1}, ..., m_{r,r+1})$, la $r+1$-ième colonne de M tronquée des lignes de rang $> r$. Puisque les r colonnes $C_k(r)$ sont linéairement indépendantes (hypothèse de récurrence) cela montre que les λ_k sont indépendants de i et donc que $C_{r+1} = \sum_{1 \leq k \leq r} \lambda_k C_k$ d'où une contradiction. ///

(3) Montrer que si $N \in M_m(K)$ alors $\det N = \det {}^t N$ où ${}^t N$ désigne la matrice transposée de N.
Preuve. . On a $\det N = \sum_{\sigma \in \mathcal{S}_n} \epsilon(\sigma) n_{\sigma(1),1} n_{\sigma(2),2} ... n_{\sigma(n),n}$ *et* $\det {}^t N = \sum_{\sigma \in \mathcal{S}_n} \epsilon(\sigma) n_{1,\sigma(1)} n_{2,\sigma(2)} ... n_{n,\sigma(n)}$. *Il suffit de remarquer que pour $\sigma \in \mathcal{S}_n$, $n_{i,\sigma(i)} = n_{\sigma^{-1}(j),j}$ où $j = \sigma(i)$. Ainsi $n_{1,\sigma(1)} n_{2,\sigma(2)} ... n_{n,\sigma(n)} = n_{\sigma^{-1}(1),1} n_{\sigma^{-1}(2),2} ... n_{\sigma^{-1}(n),n}$. Le résultat suit alors du fait que $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$.*
On peut donner une autre preuve. Si $\det N \neq 0$, *on a vu qu'avec la décomposition $N = D_n(\det N) \prod_{i \in I} B_i$ où I est fini et chaque B_i est une matrice élémentaire de transvection . Puisque B_i est triangulaire avec Id sur la diagonale il suit que* $\det B_i = \det {}^t B_i = 1$ *; ainsi* $\det {}^t N = \det D_n(\det N) = \det N$ *puisque la matrice de dilatation est diagonale. De même si* $\det {}^t N \neq 0$ *alors comme précédemment on déduit que* $\det N \neq 0$. ///

(4) En déduire que le rang de $M \in M_{p,n}(K)$ est égal à la dimension de l'espace vectoriel engendré par les vecteurs lignes de M.
Preuve. Puisque le rang de M est le maximum des entiers s tels qu'il existe une matrice M_{I_s,J_s} extraite de M avec $\det M_{I_s,J_s} \neq 0$ *et puisque* $\det {}^t M_{I_s,J_s} = \det M_{I_s,J_s}$ *le rang de M est égal au rang de ${}^t M$. On retrouve ainsi un résultat montré avec la dualité et la transposée d'un endomorphisme. ///*

(5) Soient $K \subset L$, deux corps commutatifs et $M = (C_1, C_2, ..., C_n) \in M_n(K)$. Montrer que $\dim_K \sum_{1 \leq i \leq n} KC_i = \dim_L \sum_{1 \leq i \leq n} LC_i$.
Preuve. La dimension $\dim_K \sum_{1 \leq i \leq n} KC_i$ *est le rang de la matrice $M \in M_n(K)$ et* $\dim_L \sum_{1 \leq i \leq n} LC_i$ *le rang de $M \in M_n(L)$. Nous avons vu que le rang de $M \in M_n(K)$ est aussi le maximum des entiers s tels qu'il existe une matrice M_{I_s,J_s} extraite de M avec* $\det M_{I_s,J_s} \neq 0$ *c'est donc aussi le rang de $M \in M_n(L)$. ///*

(6) Soient $K \subset L$, deux corps commutatifs et $A, B \in M_n(K)$. On note $S(K) := \{M \in M_n(K) \mid AM = MB\}$ et $S(L) := \{M \in M_n(L) \mid AM = MB\}$. Montrer que $\dim_K S(K) = \dim_L S(L)$ (on pourra considérer la matrice dans la base canonique $(E_{i,j})_{1 \leq i,j \leq n}$ de $M_n(K)$ de l'application linéaire $\varphi_K : M_n(K) \to M_n(K)$ définie par $\varphi_K(M) = AM - MB$).
Preuve. Soit $\Phi_K \in M_{n^2}(K)$ la matrice de l'endomorphisme φ_K dans la base canonique $(E_{i,j})_{1 \leq i,j \leq n}$. Par le théorème du rang $\dim_K S(K) = n^2 - (\Phi_K)$. *Puisque Φ_K est égal à la matrice $\Phi_L \in M_{n^2}(L)$ de l'endomorphisme φ_L dans la base canonique $(E_{i,j})_{1 \leq i,j \leq n}$ et puisque $(\Phi_K) = (\Phi_L)$ (par la question précédente) le résultat suit. ///*

(7) On reprend les notations précédentes. Soit $C \in M_n(K)$. On note $S_C(K) := \{M \in M_n(K) \mid AM - MB = C\}$ et $S_C(L) := \{M \in M_n(L) \mid AM - MB = C\}$. Déduire de la question précédente que si $S_C(L) \neq \emptyset$ il en est de même de $S_C(K)$.
Preuve. L'ensemble $S_C(K) \neq \emptyset$ si et seulement si $C \in \operatorname{Im} \varphi_K$. Soit $\Phi_K(C) \in M_{n^2,n^2+1}(K)$ la matrice obtenue par concaténation de Φ_K et de la colonne des coordonnées de C dans la base

$(E_{i,j})_{1\leq i,j\leq n}$, *alors* $C \in \operatorname{Im}\varphi_K$ *si et seulement si* $\Phi_K = \Phi_K(C)$. *Puisque la nonvacuité de* $S_C(L)$ *se traduit par* $\Phi_L = \Phi_L(C)$ *et que* $\Phi_L = \Phi_K$, $\Phi_L(C) = \Phi_K(C)$ *le résultat suit.* ///

(8) On reprend les notations précédentes avec $K = \mathbb{R}$ et $L = \mathbb{C}$ et on suppose qu'il existe $P \in S(\mathbb{C})$ qui est inversible. Montrer qu'il existe $Q \in S(\mathbb{R})$ qui est inversible.

Preuve. Puisque $\mathbb{C} = \mathbb{R} + i\mathbb{R}$ *on écrit* $P = P_1 + iP_2$ *où* $P_j \in M_n(\mathbb{R})$. *Alors* $P_j \in S(\mathbb{R})$. *On sait seulement que* $\det(P_1 + iP_2) \neq 0$ *ce qui ne garantit pas que* $\det P_j \neq 0$. *Considérons le polynôme* $D(X) := \det(P_1 + XP_2) \in \mathbb{R}[X]$. *Puisque* $D(i) \neq 0$, *il suit que* $D(X)$ *n'est pas identiquement nul. Si* $\deg D = 0$, P_1 *convient et sinon puisque* $\mathbb{R}$ *est infini il existe* $x \in \mathbb{R}$ *qui évite les zéros de* $D(X)$ *et alors* $Q := P_1 + xP_2$ *convient.* ///

(9) On reprend les notations précédentes avec $K \subset L$ deux corps commutatifs infinis et on suppose qu'il existe $P \in S(L)$ qui est inversible. Montrer qu'il existe $Q \in S(L)$ qui est inversible.

Preuve. On remarque que $\dim_K S(K) \leq n^2$, *que* $S(K) \subset S(L)$ *et que* $\dim_K S(K) = \dim_L S(L)$. *Il suit que si* $P_1, ..., P_s$ *est une base du* K*-espace vectoriel* $S(K)$ *c'est aussi une base du* L*-espace vectoriel* $S(L)$. *Soit* $D(X_1, .., X_s) := \det(X_1P_1 + ... + X_sP_s)$. *Par hypothèse il existe* $(x_1, ..., x_s) \in L^s$ *avec* $D(x_1, ..., x_s) \neq 0$, *ainsi* $D(X_1, .., X_s) \neq 0$ *et puisque* K *est infini il existe* $(y_1, ..., y_s) \in L^s$ *avec* $D(y_1, ..., y_s) \neq 0$. ///

Remarque. *Le résultat est encore vrai si* K *est fini. En effet il existe* $P \in S(K)$ *qui est inversible ssi* A *et* B *sont semblables ce qui est le cas ssi* A, B *ont les mêmes invariants de similitude (réduction de Frobenius).*

Exercice 6 Théorème de Rouché-Fontené, [Fr. A] p. 64. Application à l'invariance du polynôme minimal, [Fr. A] exercice 3.5.1. p. 157.

Exercice 7

Un système linéaire diophantien équivalent à la généralisation du théorème des restes chinois, [F. M. 2] p. 189.

On suppose donnés n entiers $a_i \neq 0,\ 1 \leq i \leq n$ et n entiers $c_i,\ 1 \leq i \leq n$. On se propose de résoudre le système de congruences en l'inconnue $x \in \mathbb{Z}$, $x = c_i$ modulo a_i pour $1 \leq i \leq n$. Ce système est équivalent à la recherche des solutions entières du système linéaire suivant :

$A\ {}^t(x, x_1, x_2, ..., x_n) = {}^t(c_1, c_2, ..., c_n)$ avec

$A := Matrix([[1, -a_1, 0, 0, .., 0], [1, 0, -a_2, 0, 0, .., 0], ..., [1, 0, 0, .., 0, -a_n]]) \in M_{n,n+1}(\mathbb{Z})$, et

$(x, x_1, x_2, ..., x_n) \in \mathbb{Z}^{n+1}$.

Alors qu'il y a une solution générale élémentaire avec les congruences ; les méthodes de résolution algorithmique (forme normale d'Hermite ou forme de Smith) ne semblent appropriées que pour résoudre des systèmes numériques.

(1) Résolution par les congruences.

(a) Montrer qu'une condition nécessaire pour l'existence d'une solution au système de congruences est que (a_i, a_j) divise $c_i - c_j$ pour tout $1 \leq i < j \leq n$

(b) Réciproquement on va montrer que cette condition est suffisante. Supposons donc que les c_i sont des entiers tels que (a_i, a_j) divise $c_i - c_j$ pour tout $1 \leq i < j \leq n$.

On note μ le PPCM des $a_i,\ 1 \leq i \leq n$ et $d_i := \frac{\mu}{a_i}$.

(i) Montrer que $\operatorname{PGCD}(d_i,\ 1 \leq i \leq n) = 1$ (on pourra raisonner avec les valuations p-adiques).

(ii) Soient $u_i \in \mathbb{Z}$ avec $\sum_{1\leq i\leq n} u_i d_i = 1$. Montrer que a_j divise $d_j \operatorname{PGCD}(a_i, a_j)$ pour $j \neq i$ (remarquer que $\operatorname{PPCM}(a_i, a_j) \operatorname{PGCD}(a_i, a_j) = a_i a_j$ et que $\operatorname{PPCM}(a_i, a_j)$ divise μ) et en déduire que $x_0 = \sum_{1\leq i\leq n} c_i u_i d_i$ est solution du système.

(iii) Montrer que $x_0 + \mathbb{Z}\mu$ est l'ensemble des solutions du système de congruences.

(2) Résolution avec la forme normale d'Hermite, [Fr. A] exercice 1.4.38 p. 103 et inspiré de [Co.].
La matrice A est de rang n puisque les a_i sont supposés non nuls, alors $AU = H$ avec $U_i n\,\mathrm{GL}_n(\mathbb{Z})$ et $H = (h_{i,j}) \in M_{n,n+1}(\mathbb{Z})$ est triangulaire supérieure avec $h_{i,j} = 0$ pour $i \geq j$, $0 \leq h_{i,j} < h_{i,i+1} > 0$ pour $1 \leq i < j \leq n+1$. La résolution du système diophantien $A\ {}^t(x, x_1, x_2, ..., x_n) = {}^t(c_1, c_2, ..., c_n)$ est alors équivalente à celle du système $H\ {}^t(y_0, y_1, y_2, ..., y_n) = {}^t(c_1, c_2, ..., c_n)$ avec ${}^t(x, x_1, x_2, ..., x_n) = U\ {}^t(y_0, y_1, y_2, ..., y_n)$. On dit que H est la forme normale d'Hermite de la matrice A et elle est unique. En d'autres termes les matrices H décrivent un système de représentants des orbites des matrices $A \in M_{n,n+1}(\mathbb{Z})$ de rang n.
Exemple numérique avec $a_1 = 15, a_2 = 21, a_3 = 35$. On suppose donc que
$A := Matrix([[1, -15, 0, 0], [1, 0, -21, 0], [1, 0, 0, -35]])$.
Alors $H = Matrix([[0, 15, 10, 1], [1, 0, 7, 1], [0, 0, 0, 1]])$ et
$U = Matrix([[105, 0, -35, 1], [7, -1, -3, 0], [5, 0, -2, 0], [3, 0, -1, 0])$ (attention Maple anglais pratiquant les actions à gauche il faut chercher la forme normale d'Hermite de la transposée de A et on obtient en transposant une matrice triangulaire inférieure ; la discussion fonctionne sur le même mode que ce qui suit). On doit alors résoudre le système diophantien $0y_0+15y_1+10y_2+y_3 = c_1,\ 7y_2+y_3 = c_2,\ y_3 = c_3$ en les inconnues $y_0, ..., y_3$. Ainsi $y_0 \in \mathbb{Z},\ y_3 = c_3,\ 7y_2 = c_2 - c_3,\ 15y_1 = (c_1 - c_3) - 10y_2$ d'où il suit les conditions nécéssaires pour l'existence d'une solution $7 \mid (c_2 - c_3)$ et $5 \mid (c_1 - c_3)$. Si ces dernières conditions sont satisfaites on a donc $y_2 = \frac{c_2-c_3}{7}$ et donc $15y_1 = (c_1 - c_3) - 10\frac{c_2-c_3}{7} = (c_1 - c_2) - 3\frac{c_2-c_3}{7}$ d'où une autre condition nécessaire $3 \mid (c_2 - c_1)$. On a donc retrouvé les conditions nécessaires vues dans le théorème des chinois généralisé. Supposons donc ces conditions réalisées alors $3y_1 = \frac{c_1-c_3}{5} - 2\frac{c_2-c_3}{7}$ et $5y_1 = \frac{c_1-c_2}{3} - \frac{c_2-c_3}{7}$ d'où $y_1 = 2 * 3y_1 - 5y_1 = 2\frac{c_1-c_3}{5} - 3\frac{c_2-c_3}{7} - \frac{c_1-c_2}{3}$, ainsi ${}^t(x, x_1, x_2, x_3) = U\ {}^t(y_0, y_1, y_2, y_3)$ d'où $x = 105y_0 - 5c_2 + 6c_3$ avec $y_0 \in \mathbb{Z}$.
Remarque. Même si la condition nécessaire et suffisante pour l'existence d'une solution i.e. $\mathrm{PGCD}(a_i, a_j) \mid (c_i - c_j)$ est facile à vérifier cela n'est pas satisfaisant pour caractériser les n uplets $(c_1, ..., c_n)$ pour lesquels l'ensemble des solutions n'est pas vide. Dans l'exemple il s'agit de résoudre le système d'équations diophantiennes $c_2 - c_1 = 3a,\ c_3 - c_1 = 5b,\ c_3 - c_2 = 7c$ i.e. $c_2 = c_1 + 3a,\ c_3 = c_1 + 5b$ et $3a - 5b + 7c = 0$. Pour résoudre cette dernière équation on projette les solutions sur la première coordonnée a et puisque $(a, b, c) := (1, 9, 6)$ est solution il suit que si (a, b, c) est solution alors $(a, b, c) - a(1, 9, 6) = (0, -9a + b, -6a + c)$ est encore solution d'où l'ensmble des solutions $(a, 9a + 7d, 6a + 5d)$ avec $(a, d) \in \mathbb{Z}^2$. D'où la paramétrisation des triplets (c_1, c_2, c_3) pour lesquels le théorème des restes chinois avec $(a_1, a_2, a_3) = (15, 21, 35)$ a un ensemble non vide de solutions $(c_1, c_2, c_3) = (e, e+3a, e+45a+35d)$ avec $(a, d, e) \in \mathbb{Z}^3$. C'est un sous-groupe S de $\mathbb{Z}^3$ dont les facteurs invariants sont $1, 1, 105$, ainsi $\frac{\mathbb{Z}^3}{S} \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{7\mathbb{Z}}$.

(3) Résolution sur un exemple avec la réduction à la forme de Smith. Cas $a_1 = 15, a_2 = 21, a_3 = 35$.
Par ce qui précède la CNS est $(\frac{c_1-c_2}{3}, \frac{c_1-c_3}{5}, \frac{c_2-c_3}{7}) \in \mathbb{Z}^3$.
On résout le système $A\ {}^t(x, y, z, w) = (c_1, c_2, c_3)$ où
$A := Matrix([[1, -15, 0, 0], [1, 0, -21, 0], [1, 0, 0, -35]])$; Maple donne
$S = Matrix([[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 105, 0]])$ (c'était prévisible avec le pgcd des mineurs de taille donnée) et
$U = Matrix([[0, 0, 1], [-3, 1, 2], [14, -5, -9]])$ avec $det\ U = 1$ et
$V = Matrix([[1, -35, -735, 105], [0, -2, -42, 7], [0, -1, -20, 3], [0, -1, -21, 5]])$ avec $det\ V = 1$ et $UAV = S$. Cela revient à résoudre $S\ {}^t(X, Y, Z, W) = U\ {}^t(c_1, c_2, c_3)^t$ avec ${}^t(x, y, z, w) = V\ {}^t(X, Y, Z, W)$. Ainsi on obtient la CNS $105Z = 14c_1 - 5c_2 - 9c_3$. On vérifie que la condition $(\frac{c_1-c_2}{3}, \frac{c_1-c_3}{5}, \frac{c_2-c_3}{7}) \in \mathbb{Z}^3$ implique bien la divisibilité par $3 * 5 * 7 = 105$ de $14c_1 - 5c_2 - 9c_3$ (remarquer que $14c_1 - 5c_2 - 9c_3 = 14(c_1 - c_2) + 9(c_2 - c_3) = 14(c_1 - c_3) + 5(c_3 - c_2)$)...

Exercice 8 Théorème des zéros et systèmes linéaires, [F. M. 2] p. 271.

(1) *Rappels.*

Soit k un corps algébriquement clos, $A := k[X_1, ..., X_n]$ et $I \subset A$ un idéal.

(a) L'idéal I est de type fini i.e. il existe $P_1, ..., P_s \in A$ avec $I = \sum_{1 \leq i \leq s} AP_i$ (propriété noethérienne des anneaux de polynômes).

(b) Soit $\underline{a} := (a_1, a_2, ..., a_n) \in k^n$ et $eval_{\underline{a}} : A \to k$ avec $eval_{\underline{a}}(P) = P(\underline{a})$. Alors $\ker eval_{\underline{a}} = \sum_{1 \leq i \leq n} A(X_i - a_i)$. Réciproquement les idéaux maximaux de A sont de cette forme (k est algébriquement clos).

(c) Soit $I = \sum_{1 \leq i \leq s} AP_i$ et $V(I) := \{\underline{a} := (a_1, a_2, ..., a_n) \in k^n \ | \forall i, eval_{\underline{a}}(P_i) = 0\}$. Le "théorème des zéros de Hilbert" dit que $P \in A,\ P(V(I)) = 0$ si et seulement si il existe $t > 0$ tel que $P^t \in I$.

(d) Avec les mêmes notations, $V(I) = \emptyset$ si et seulement si $I = A$ autrement dit si il existe $U_i \in A$ avec $\sum_{1 \leq i \leq s} U_i P_i = 1$ (cela provient de la caractérisation des idéaux maximaux).

(2) *Le problème*

On donne $A_{s,n} \in M_{s,n}(k)$ et $A_{s,n+1} = (a_{i,j}) \in M_{s,n+1}(k)$ qui est la concaténation de $A_{s,n}$ pour les n premières colonnes et du vecteur colonne ${}^t(a_{1,n+1}, ..., a_{s,n+1})$.

Pour $1 \leq i \leq s$, on définit $P_i := \sum_{1 \leq j \leq n} a_{i,j} X_j - a_{i,n+1}$. Soit $S(k) := \{\underline{x} := (x_1, x_2, ..., x_n) \in k^n,\ |\forall i, P_i(\underline{x}) = 0\}$. Il s'agit de montrer que $S(k) = \emptyset$ si et seulement si il existe $\mu_i \in k$ avec $\sum_{1 \leq i \leq s} \mu_i P_i = 1$.

(3) *Par l'algèbre linéaire*

(a) Montrer que $S(k) = \emptyset$ si et seulement si $(A_{s,n}) < (A_{s,n+1})$.

Preuve. $S(k) = \emptyset$ *ssi* ${}^t(a_{1,n+1}, ..., a_{s,n+1})$ *n'est pas dans l'image de* $A_{s,n}$ *ce qui compte tenu de l'inclusion* $\operatorname{Im} A_{s,n} \subset \operatorname{Im} A_{s,n+1}$ *équivaut à* $(A_{s,n}) < (A_{s,n+1})$.///

(b) On suppose que $S(k) = \emptyset$, montrer en utilisant le pivot de Gauss sur les lignes qu'il existe $\mu_i \in k$ avec $\sum_{1 \leq i \leq s} \mu_i L_i = 0$ et $\sum_{1 \leq i \leq s} \mu_i a_{i,n+1} \neq 0$, où L_i est la i-ième ligne de $A_{s,n}$ et conclure.

Preuve. Le pivot de Gauss sur les lignes de la matrice $A_{s,n+1}$ *aboutit à* s *lignes* $(L'_i, a'_{i,n+1})$ *où* $L'_i := \sum_{1 \leq j \leq n} \mu_{j,i} L_j$ *et* $a'_{i,n+1}) := \sum_{1 \leq j \leq n} \mu_{j,i} a_{j,n+1}$ *avec les* r *premières lignes* L'_i *linéairement indépendantes et les suivantes nulles, ainsi* $r = (A_{s,n})$ *et enfin* $a'_{r+1,n+1}) \neq 0$ *puisque* $(A_{s,n}) < (A_{s,n+1})$. *Ainsi* $\sum_{1 \leq j \leq s} \mu_{j,r+1} P_j = -\sum_{1 \leq j \leq s} \mu_{j,r+1} a_{j,n+1} = -a'_{r+1,n+1} \neq 0$. *On conclut donc en divisant cette égalité par* $a'_{r+1,n+1}$.///

(4) *Par le Nullstellensatz*

Preuve. Remarque. Notons que la partie d) du rappel fournit une CNS pour que $S(k) = \emptyset$ *: Il existe* $U_i \in A = k[X_1, ..., X_n]$ *avec* $\sum_{1 \leq i \leq s} U_i P_i = 1$, *mais il ne semble pas possible d'en déduire une relation avec des* $U_i \in k$.///

(a) Soit $f_1, ..., f_t \in A$ des polynômes homogènes de degré 1. Montrer que l'idéal $\sum_{1 \leq i \leq t} Af_i$ est un idéal premier de A.

Preuve. Quitte à réordonner on peut supposer que $f_1, ..., f_r$ *sont* k*-linéairement indépendants et qu'ils engendrent tous les* f_i *alors l'idéal* $I := \sum_{1 \leq i \leq r} f_i = \sum_{1 \leq i \leq t} f_i$. *On peut alors compléter la famille libre* $(Y_i := f_i,\ 1 \leq i \leq r)$ *par* $(Y_i,\ r+1 \leq i \leq n)$ *en une base du* k*-espace vectoriel* $H_{1,n} := \sum_{1 \leq i \leq n} X_i$ *des polynômes homogènes de degré* 1. *Alors* $A = k[Y_1, ..., Y_n]$ *et donc* $\frac{A}{I} \simeq k[Y_{r+1}, ..., Y_n]$ *est intègre.*///

(b) Soit $\tilde{P}_i := \sum_{1 \leq j \leq n} a_{i,j} Y_j - a_{i,n+1} Y_{n+1} \in k[Y_1, ..., Y_{n+1}]$. Montrer que $S(k) = \emptyset$ si et seulement si $V(\tilde{P}_i) \subset V(Y_{n+1})$.

Preuve. On a $V(\tilde{P}_i) = \{(y_1, ..., y_{n+1})\}$ *avec* $y_{n+1} = 0$ *et* $\sum_{1 \leq j \leq n} a_{i,j} y_j = 0$ *union* $y_{n+1} \neq 0$ *et* $(\frac{y_1}{y_{n+1}}, ..., \frac{y_n}{y_{n+1}}) \in S(k)$.///

(c) En déduire que $S(k) = \emptyset$ si et seulement si il existe $m > 0$ avec $Y_{n+1}^m \in \sum_{1 \leq i \leq s} \tilde{P}_i k[Y_1, ..., Y_{n+1}]$.

Preuve. Cela suit immédiatement de la question précédente et du Nullstellensatz qui reste vrai si k n'est pas algébriquement clos.

(d) Déduire de a) que l'on peut supposer que $m = 1$

Preuve. Par a) il suit que l'idéal $\sum_{1 \leq i \leq s} \tilde{P}_i k[Y_1, ..., Y_{n+1}]$ *est premier , ainsi* $Y_{n+1} \in \sum_{1 \leq i \leq s} \tilde{P}_i k[Y_1, ..., Y_{n+1}]$.///

(e) Conclure.

Preuve. Ainsi $Y_{n+1} = \sum_{1 \leq i \leq s} U_i \tilde{P}_i$ *avec* $U_i \in k[Y_1, ..., Y_{n+1}]$. *Par l'unicité de la décomposition en composantes homogènes il suit que* $Y_{n+1} = \sum_{1 \leq i \leq s} \mu_i \tilde{P}_i$ *où* $\mu_i \in k$ *est la composante homogène de degré* 0 *de* U_i. *On conclut en spécialisant à* $Y_{n+1} = 1$.///

Exercice 9 Utilisable dans la leçon 90 Méthodes combinatoires, dénombrement : Systèmes linéaires à coefficients entiers, le lemme de Siegel et son application à la transcendance de e et π, [Du.] p. 158-160.

Lemme. Soient $A := (A_{ij}) \in M_{m,n}(\mathbb{Z})$, $n > m$. Soit $C \in \mathbb{N}$ avec $max\ |A_{ij}| \leq C$. Alors il existe $(x_1, ..., x_n) \in \mathbb{Z}^n$ avec $0 < max_i\ |x_i| \leq (nC)^{\frac{m}{n-m}}$ et $A\ {}^t(x_1, ..., x_n) = 0$.

Preuve. Pour $1 \leq j \leq m$, soit $-V_j$ (resp. W_j) la somme des éléments négatifs (resp. positifs) de $\{A_{1j}, ..., A_{nj}$. On a $V_j + W_j \leq nC$. Soit $X \in N$ et $(x_1, ..., x_n) \in \mathbb{Z}^n$ avec $0 \leq x_i \leq X$. Soit $(y_1, ..., y_m) \in \mathbb{Z}^m$ avec $y_j = \sum_j A_{ij} x_i$. On a $-V_j X \leq y_j \leq W_j X$. L'ensemble E des $(x_1, ..., x_n)$ compte $(X+1)^n$ éléments alors que l'ensemble F des $(y_1, ..., y_m)$ en compte au plus $(nCX+1)^m$. On vérifie que pour $X = [(nC)^{\frac{m}{n-m}}]$ on a $|E| > |F|$. Ainsi l'application $(x_1, ..., x_n) \in E \to (y_1, ..., y_m) \in F$ n'est pas injective il existe $x' := (x'_1, ..., x'_n) \neq x'' := (x''_1, ..., x''_n)$ dans E qui ont la même image, alors $x := x' - x''$ convient.

Application à la transcendance de e^α lorsque α est algébrique sur $\mathbb{Q}$.

L'idée : En utilisant le lemme de Siegel, on construit pour $n \in \mathbb{N}$ assez grand, une fonction $F_n(x) = \sum_{0 \leq i \leq p} \sum_{0 \leq j \leq q} a_{ij} x^i e^{jx}$ avec $a_{ij} \in \mathbb{Z}$, $p = \lfloor \frac{n}{Log\ n} \rfloor$, $q = \lfloor (Log\ n)^2 \rfloor$ et $F_n(0) = F'_n(0) = ... = F_n^{(n-1)}(0) = 0$, $F_n(\alpha) = F'_n(\alpha) = ... = F_n^{(n-1)}(\alpha) = 0$, $0 < max_{i,j}\ |a_{ij}| \leq e^n$. On en tire une contradiction.