Compléments Errata à Algèbre et Géométrie

(Hermann 2011)

de Jean Fresnel et Michel Matignon

(mai 2024)

page de l'ouvrage		page du document ci-après
8	rajouter $U \in M_n(K)$	3
15	monoïde multiplicatif de matrices nilpotentes	3
15	sur les endomorphismes nilpotents	6
20	sur les traces d'un ensemble d'endomorphismes	9
57	sur les polynômes de la forme produit de $X^n - 1$, application au théorème de Brauer, ex. 31	10
87	Ce qui suit remplace le 5.2.1 et le 5.2.2	13
89	ligne 14, $e_i \exp A = e_i e^{a_i}(I_n + \frac{N_i}{1!} + \ldots + \frac{(N_i)^{\alpha_i - 1}}{(\alpha_i - 1)!})$. Alors la formule de 6.1. suit du fait	15
89	ligne 16, 4) Montrons 6.2. . Si $P(X) = (X - a_1)(X - a_2) \ldots (X - a_r)$	15
89	ligne -9, comme $(X - a_i) Q_i(X) = P(X)$, on a donc $e_i (A - a_i I_n) = 0$, i.e. $e_i N_i = 0$ selon les notations de 6.1. , Alors par 6.1. on a bien $\exp(A) = \sum_{i=1}^{r} e_i e^{a_i}$.	15
89	ligne -8, 5) Montrons 6.3. . Comme en 2) si $A' = B' + C'$ avec $B'C' = C'B'$ et	16
89	ligne -3, la formule de 6.3.	16
89	ligne -2, application de 6.3. Soient $A \in M_n(K)$ avec $(A - I_n)^2 (A - 2I_n) = 0$, $t \in K$.	16
92	p. 92, ligne -8, lire $x(t) = \frac{y(t)}{y_0}(x_0 + \frac{y_0}{\lambda} \mathrm{Log}(\frac{y(t)}{y_0}))$	16
147	complément à l'ex.58	16
202	ex. 82, complément	16
209	ligne 9, *sont* θ_j *pour* $1 \leq j < p$ *définies par* $\theta_j(s) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$,	19
220	ligne -8, 13.2.2.3) Conclure de 8.2. que $\rho_0, \rho_1, \rho_2, \rho_3, \theta_1, \theta_2, \ldots, \theta_{p-1}$ sont exactement	19

244	ligne 8, $d \neq n$. Ainsi X'_n est l'ensemble des $x \in X$ pour lesquels n est le plus petit entier m avec $x \in X_m$, au sens de la relation d'ordre définie par d est inférieur ou égal à n si et seulement si $d \mid n$.	19
245	Complément à l'exercice 86 de FM, partie 3, sur la matrice des P.G.C.D.	19
250	Généralisation du déterminant de Vandermonde, applications à un théorème de Chebotarëv, au principe d'incertitude, à la majoration de racines d'un polynôme via la transformée de Fourier discrète	26
252	ligne 4, lire (ex. 87 p. 245 partie 1)	37
258	ligne 3, lire l'ensemble des idempotents de B	37
278	ligne 15, Montrer que $(d_1!)(d_2!)$ divise $(d_1+d_2)!$ (remarquer que $\frac{(d_1+d_2)!}{(d_1!)(d_2!)}$ n'est	37
279	ligne -6, $R(X) := P(z-\lambda X) \in M[X]$, on a donc $R(y) = P(x) = 0$. Montrons que	37
279	ligne-2, On a donc $1 = E(X)A(X) + F(X)B(X)$, $Q(X) = S(X)E(X)$,	37
282	ligne 2, *impair,* $p_i \neq p_j$ *pour* $i \neq j$, $u \geq 0, 1 \geq v_i \geq 0$, $M := \mathbb{Q}[\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n})]$. *Alors les*	37
284	remplacer les lignes 10 à 20 de 2.3) de l'ex.104 par ci-après..	37
318	ligne -9, 2) Montrons 2. Soient $f := \sum_{n \geq 0} u_n X^n$, $g := \sum_{n \geq 0} v_n X^n$, on a donc	38
319	ligne-9, *Démonstration* Soit $f := \sum_{n \geq 0} u_n X^n$, on a donc $P(X) = 1 + p_1 X + ... + p_n X^n$	38
329	ligne 9, lire $a_i = (-1)^i s_i(x_1, x_2, ..., x_n)$	38
349	ligne 7, lire $0 \leq i \leq d$, ligne 13 lire $0 \leq i \leq d$	38
367	complément à l'ellipse de Steiner ex. 126	38
376	ex. 131, une formule élémentaire sur le dénombrement	40
436	ligne 10, peut supposer que $0 \in I$, $1 \in J$. Sachant que $a_i - o = d e + w_i$ avec $w_i \in W$	40

p. 8, rajouter $U \in M_n(K)$

p. 15, complément : **Monoïde multiplicatif de matrices nilpotentes**

Théorème (Köthe, Levitzki) *Soient k un corps commutatif, V un k-espace vectoriel de dimension finie. Soit $\mathcal{S}$ une partie de $\mathrm{End}_k V$ constituée de nilpotents, on suppose en plus que pour tout $u, v \in \mathcal{S}$, on a $uv \in \mathcal{S}$. Alors il existe une base $(e_1, e_2, \dots, e_n)$ de V de façon que pour tout $u \in \mathcal{S}$, la matrice $\mathrm{Mat}(u; e_i)$ soit triangulaire supérieure avec une diagonale nulle. En particulier on a $\mathcal{S}^n = \{0\}$*, i.e. *si $u_1, u_2, \dots, u_n \in \mathcal{S}$, alors $u_1 u_2 \dots u_n = 0$* ([F], ex. 5.7.13. p. 236).

Démonstration

1) Si $\dim V = 1$, on a $\mathcal{S} = \{0\}$, ainsi la proposition est trivialement satisfaite.

Maintenant, on suppose que $n \geq 2$ et que la proposition est satisfaite pour tout espace vectoriel de dimension strictement inférieure à n et pour tout $\mathcal{S}$.

2) On suppose que $\dim V = n \geq 2$. Soit $\mathcal{S}(V)$ le sous-espace vectoriel de V engendré par $\{u(x) \mid u \in \mathcal{S} \text{ et } x \in V\}$, i.e. $\mathcal{S}(V) = \sum_{u \in \mathcal{S}} u(V)$.

On suppose que $\mathcal{S}(V) \neq V$. Soit donc $W := \mathcal{S}(V)$. Clairement W est stable par tout élément de $\mathcal{S}$, ainsi tout $u \in \mathcal{S}$ induit un élément u_W de $\mathrm{End}_k W$. Soit $\mathcal{S}_W := \{u_W \mid u \in \mathcal{S}\}$. Facilement $\mathcal{S}_W$ est un ensemble de nilpotents de $\mathrm{End}_k W$ et si $u_W, v_W \in \mathcal{S}_W$, alors $u_W v_W = (uv)_W \in \mathcal{S}_W$. Ainsi l'hypothèse de récurrence dit qu'il existe une base $(e_1, e_2, \dots, e_r)$ de W de façon que pour tout $u_W \in \mathcal{S}_W$, la matrice $\mathrm{Mat}(u_W; e_1, \dots, e_r)$ soit triangulaire supérieure avec une diagonale nulle.

Soit $\rho : E \to \frac{E}{W}$ la surjection canonique, alors pour tout $u \in \mathcal{S}$ il existe $u_S \in \mathrm{End}_k(\frac{E}{W})$ tel que $\rho u = u_S \rho$. Facilement si $u \in \mathcal{S}$, alors u_S est nilpotent et de plus pour $u, v \in \mathcal{S}$ on a $u_S v_S = (uv)_S$. Soit donc $\mathcal{S}_S := \{u_S \mid u \in \mathcal{S}\}$. Encore ici, on peut appliquer l'hypothèse de récurrence, ce qui veut dire qu'il existe une base $(\rho(e_{r+1}), \rho(e_{r+2}), \dots, \rho(e_n))$ de $\frac{E}{W}$ de façon que pour tout $u \in \mathcal{S}$, la matrice $\mathrm{Mat}(u_S; \rho(e_{r+1}), \dots, \rho(e_n))$ soit triangulaire supérieure avec une diagonale nulle.

Il suit facilement de cela que $(e_1, \dots, e_r, e_{r+1}, \dots, e_n)$ est une base de V et que pour tout $u \in \mathcal{S}$ la matrice $\mathrm{Mat}(u; e_1, e_2, \dots, e_n)$ est triangulaire supérieure avec une diagonale nulle.

3) Il nous reste à montrer que $\mathcal{S}(V)\neq V$.
C'est le plus technique. Supposons le contraire, i.e. $\mathcal{S}(V)=V$.
3.1) *Montrons qu'il existe* $u_1,u_2,\dots,u_t\in\mathcal{S}$ *tels que*

$$V=u_1(V)+u_2(V)+\dots+u_t(V)\ .$$

En effet $V=k\,e_1\oplus k\,e_2\oplus\dots\oplus k\,e_n$ et donc $e_i=\sum_{j\in I_i}u_{j,i}(x_{j,i})$ avec I_i qui est fini, $u_{j,i}\in\mathcal{S}$, $x_{j,i}\in V$. Soit $\{u_1,u_2,\dots,u_t\}=\{u_{j,i}\mid 1\leq i\leq n\mid j\in I_i\}$.
On a donc $\mathcal{S}(V)\subset u_1(V)+u_2(V)+\dots+u_t(V)$ et donc
$V=\mathcal{S}(V)=u_1(V)+u_2(V)+\dots+u_t(V)$.
3.2) Soit donc $T:=\{u_1,u_2,\dots,u_t\}$. Soit $k\geq 1$, on déduit facilement de 3.1) que

$$V=\sum_{(a_1,a_2,\dots,a_k)\in T^k}a_1a_2\ \dots a_k(V)\ .$$

En particulier, pour tout $k\geq 1$, il existe $a_1,a_2,\dots a_k\in T$ avec $a_1a_2\ \dots a_k\neq 0$.
3.3) *On souhaite montrer qu'il existe* $a\in T$ et $z_1,z_2,\dots z_{m-1}\in\mathcal{S}$ *tels que*

$$(a\,z_1)(a\,z_2)\dots(a\,z_{m-1})\,a\neq 0\ \ \textit{avec}\ \ m\geq n\ .$$

Soit $k:=n\,(n-1)\,t$, par 3.2), il existe $w_1,w_2,\dots w_k\in T$ avec
$w_1w_2\ \dots w_k\neq 0$.
Soit $\theta_i:=\mathrm{card}\,\{j\in\{1,2,\dots,k\}\mid w_j=u_i\}$, on a donc

$$\theta_1+\theta_2+\dots+\theta_t=k=n\,(n-1)\,t.$$

En conclusion, il existe i tel que $\theta_i\geq n(n-1)$. On note $a:=u_i$.
Sachant que $a^n=0$ et en regroupant les $w_i\neq a$, on peut écrire
$w:=w_1w_2\ \dots w_k$ sous l'une des quatre formes suivantes.
(1) $w=a^{\alpha_1}y_1a^{\alpha_2}y_2\dots a^{\alpha_m}y_m$ avec $1\leq\alpha_j<n$, $y_j\in\mathcal{S}$,
(2) $w=y_0a^{\alpha_1}y_1a^{\alpha_2}y_2\dots a^{\alpha_m}y_m$ avec $1\leq\alpha_j<n$, $y_j\in\mathcal{S}$,
(3) $w=y_0a^{\alpha_1}y_1a^{\alpha_2}y_2\dots a^{\alpha_{m-1}}y_{m-1}a^{\alpha_m}$ avec $1\leq\alpha_j<n$, $y_j\in\mathcal{S}$,
(4) $w=a^{\alpha_1}y_1a^{\alpha_2}y_2\dots a^{\alpha_{m-1}}y_{m-1}a^{\alpha_m}$ avec $1\leq\alpha_j<n$, $y_j\in\mathcal{S}$.
Comme $\alpha_1+\alpha_2+\dots+\alpha_m\geq n(n-1)$, il suit que $m\geq n$. Comme $w\neq 0$, on a dans tous les cas

$$(a^{\alpha_1}y_1)(a^{\alpha_2}y_2)\dots(a^{\alpha_{m-1}}y_{m-1})\,a^{\alpha_m}\neq 0\ .$$

On peut donc écrire la relation ci-dessus

$$a(a^{\alpha_1-1}y_1)a(a^{\alpha_2-1}y_2)\dots(a^{\alpha_{m-1}-1}y_{m-1}a^{\alpha_m-1})\,a\neq 0\ .$$

En posant $z_i:=a^{\alpha_i-1}y_i$ pour $i\leq m-2$ et $z_{m-1}:=a^{\alpha_{m-1}-1}y_{m-1}a^{\alpha_m-1}$, on obtient la formule recherchée.
3.4) Soit $\mathcal{S}_1:=a\,\mathcal{S}$, alors $\mathcal{S}_1$ est un ensemble de nilpotents qui est stable pour la multiplication. Soit $X:=a(V)$, facilement $v(X)\subset X$ pour tout $v\in\mathcal{S}_1$. Comme a est nilpotent, on a $\dim X<\dim V$.

Si $v \in \mathcal{S}_1$, on note v_X l'endomorphisme de X induit par v. Soit $\mathcal{S}_{1,X} := \{v_X \mid v \in \mathcal{S}_1\}$, facilement $\mathcal{S}_{1,X}$ est une partie de $\mathrm{End}X$ constituée de nilpotents et stable pour la multiplication. Alors par hypothèse de récurrence sur la dimension, on sait en particulier que si $s_1, s_2, \ldots, s_{n-1} \in \mathcal{S}_{1,X}$, on a $s_1 s_2 \ldots s_{n-1} = 0$. Si donc s_i est induit par $t_i \in \mathcal{S}_1$, on a $t_1 t_2 \ldots t_{n-1}(x) = 0$ pour tout $x \in X$. Ca veut dire que $t_1 t_2 \ldots t_{n-1} a(y) = 0$ pour tout $y \in V$.
Il suit en particulier de cela que $(a\, z_1)(a\, z_2) \ldots (a\, z_{m-1})\, a = 0$ puisque $m \geq n$.
Ce qui donne une contradiction.

Commentaires
La démonstration du théorème de **Köthe et Levitzki** sur les monoïdes multiplicatifs de matrices nilpotentes utilise donc des techniques élémentaires de l'algèbre linéaire.
En revanche, le théorème de **Kolchin**, dont l'énoncé est assez proche (voir ci-après) nécessite l'utilisation d'un théorème de **Burnside** (voir ci-après) dont la démonstration utilise des méthodes plus élaborées.

Le théorème de Burnside ([F.] ex. 4.7.18. p.198) *Soient k un corps commutatif, algébriquement clos, V un k-espace vectoriel de dimension $n \geq 1$. Soit $\mathcal{A}$ une sous-algèbre unitaire de $\mathrm{End}\, V$ telle que si W est sous-espace vectoriel de V stable par tout élément de $\mathcal{A}$, alors $W = \{0\}$ ou $W = V$. Alors $\mathcal{A} = \mathrm{End}\, V$.*

Le théorème de Kolchin ([F.], ex. 4.7.20. p. 200) *Soient k un corps commutatif, V un k-espace vectotiel de dimension $n \geq 1$. Soit $\mathcal{G}$ un sous-groupe de $G\ell(V)$ constitué d'éléments unipotents. Alors il existe une base $\mathcal{B}$ de V de façon que pour tout $g \in \mathcal{G}$, la matrice $\mathrm{Mat}(g; \mathcal{B})$ soit triangulaire supérieure avec une diagonale qui est I_n.*

Bibliographie

[F.] **Fresnel J.** *Algèbre des matrices* (Hermann 2011)
[K.] **Köthe G.** *Über maximalenilpotente Unterringe und Nilringe.* Math. Ann. 103, 359-363 (1930)
[L.] **Levitzki J.** *Über nilpotente Unterringe* Math. Ann. 105, 620-627 (1931)

Sur les endomorphismes nilpotents

Proposition 1 *Soient K un corps commutatif, E un K-espace vectoriel de dimension $n\geq 1$. Soient $u\in \mathcal{E}nd E$, un endomorphisme nilpotent, $x\in E-\{0\}$. On suppose que $E:=K[u](x)=\{P(u)(x)\mid P(X)\in K[X]\}$; ce qui veut aussi dire que E est engendré par la famille $\{u^k(x)\mid k\geq 0\}$.*
Alors on a $u^n(x)=0$ et $u^{n-1}(x)\neq 0$. De plus $\{x,u(x),\dots,u^{n-1}(x)\}$ est une base de E et on a

$$\mathrm{Mat}(u;x,u(x),\dots,u^{n-1}(x))=\begin{bmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&1&0\end{bmatrix},$$

ce qui veut aussi dire que $\mathrm{Mat}(u;x,u(x),\dots,u^{n-1}(x))$ *est la matrice compagnon de X^n.*

Démonstration
Comme u est nilpotent, il existe $d\geq 1$ tel que $u^d(x)=0$ et $u^{d-1}(x)\neq 0$.
Il suit alors que si $P(X)\in K[X]$, on a

$$P(u)(x)=a_0x+a_1u^2(x)+\dots+a_{d-1}u^{d-1}(x)$$

avec $a_k\in K$ puisque $u^d(x)=0$ on a donc $u^k(x)=0$ pour $k\geq d$. Ainsi $\{x,u(x),\dots,u^{d-1}(x)\}$ est une famille génératrice de E. On a ainsi $d\geq n$.
Il reste à montrer que cette famille est libre, i.e.
$a_0x+a_1x^2+\dots+a_{d-1}u^{d-1}(x)=0$ implique $a_0=a_1=\dots=a_{d-1}=0$.
Supposons le contraire, il existe donc $t\geq 0$ avec

$$a_tu^t(x)+a_{t+1}u^{t+1}(x)+\dots+a_{d-1}u^{d-1}(x)=0\ ,\ a_t\neq 0\ .$$

En appliquant u^{d-t-1} à cette dernière égalité, on obtient
$a_tu^{d-1}(x)=0$. Sachant que $a_t\neq 0$ et $u^{d-1}(x)\neq 0$, on a une contradiction. Il suit donc que $a_0=a_1=\dots=a_{d-1}=0$.
En conclusion $\{x,u(x),\dots,u^{d-1}(x)\}$ est une base de E; ainsi $d=n$.
Il suit facilement que

$$\mathrm{Mat}(u;(x,u(x),\dots,u^{n-1}(x)))=\begin{bmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&1&0\end{bmatrix}.$$

Proposition 2 *Soient K un corps commutatif, E un K-espace vectoriel de dimension $n\geq 1$. Soient $u\in \mathcal{E}nd E$, un endomorphisme nilpotent, $x\in E-\{0\}$. On suppose que $E:=K[u](x)=\{P(u)(x)\mid P(X)\in K[X]\}$; ce qui veut aussi dire par la proposition 1 que $\{x,u(x),\dots,u^{n-1}(x)\}$ est une base de E. Soient $\lambda\in K-\{0\}$, $\theta(X)\in XK[X]$ et $v:=u(\lambda\,\mathrm{Id}_E-\theta(u))$. Alors il existe $w\in G\ell(E)$ tel que $v=wuw^{-1}$* (i.e. v est semblable à u).

Démonstration
On a facilement $v \in uK[u]$ et $uv = vu$, ainsi v est nilpotent et plus précisément $v^n = 0$. Par ailleurs l'élément $\lambda \mathrm{Id}_E - \theta(u)$ est un inversible de $\mathcal{End}E$, en effet
$\lambda(\mathrm{Id}_E - \lambda^{-1}\theta(u))\lambda^{-1}(\mathrm{Id}_E + \lambda^{-1}\theta(u) + (\lambda^{-1}\theta(u))^2 + \ldots$
$+ (\lambda^{-1}\theta(u))^{(n-1)}) = \mathrm{Id}_E$

Il suit de cela que $u^n = 0$ implique $v^n = 0$ et que $u^{n-1} \neq 0$ implique $v^{n-1} \neq 0$. Alors il suit de la proposition 1 que $\{x, v(x), \ldots, v^{n-1}(x)\}$ est une base de $K[v](x)$.
Ainsi $\dim K[v](x) = \dim K[u](x)$. Ainsi $\{x, v(x), \ldots, v^{n-1}(x)\}$ est aussi une base de $K[u](x)$. Il suit que

$$\mathrm{Mat}(v; (x, v(x), \ldots, v^{n-1}(x))) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Ainsi les matrices de u et de v dans des bases différentes sont égales, il suit qu'il existe $w \in G\ell(E)$ tel que $v = wuw^{-1}$. De façon plus précise, on a $w(u^k(x)) = v^k(x)$ pour $0 \leq k \leq n-1$.

Théorème 1 *Soient K un corps commutatif, E un K-espace vectoriel de dimension $n \geq 1$. Soient $u \in \mathcal{End}E$, un endomorphisme nilpotent, $x \in E - \{0\}$. Soient $\lambda \in K - \{0\}$ et $v := u(\lambda \mathrm{Id}_E - \theta(u))$ où $\theta(X) \in XK[X]$. Alors il existe $w \in G\ell(E)$ tel que $v = wuw^{-1}$* (i.e. v est semblable à u).

Démonstration
Il suit du théorème 2 ci-après, qu'il existe $x_1, x_2, \ldots, x_s \in E$ et des entiers $d_1 \geq d_2 \geq \ldots \geq d_s \geq 1$ avec $u^{d_i}(x_i) = 0$, $u^{d_i - 1}(x_i) \neq 0$ pour $1 \leq i \leq s$ et

$$E = K[u](x_1) \oplus K[u](x_2) \oplus \ldots \oplus K[u](x_s) .$$

Facilement, on a $u(K[u](x_i)) \subset K[u](x_i)$ pour $1 \leq i \leq s$. Ainsi u induit un endomorphisme u_i de $K[u](x_i) = K[u_i](x_i)$ qui est nilpotent.
Facilement $v = \lambda u$ induit sur $K[u_i](x_i)$ l'endomorphisme $v_i = \lambda u_i$.
On peut donc appliquer la proposition 2 à l'endomorphisme u_i ; il suit donc qu'il existe $w_i \in G\ell(K[u_i](x_i))$ avec $v_i = w_i u_i w_i^{-1}$. Soit alors w défini par

$$w(y_1 + y_2 + \ldots + y_s) := w_1(y_1) + w_2(y_2) + \ldots + w_s(y_s)$$

pour $y_i \in K[u](x_i) = K[u_i](x_i)$ et pour $1 \leq i \leq s$. Il suit facilement que $w \in G\ell(E)$ avec $v = wuw^{-1}$, sachant que $w_i \in G\ell(K[u_i](x_i))$.
Ainsi, le corollaire est démontré.

Corollaire *Soient K un corps commutatif, E un K-espace vectoriel de dimension $n\geq 1$, d un endomorphisme diagonalisable de E , u un endomorphisme nilpotent de E* avec $d\,u=u\,d$, $\lambda\in K-\{0\}$, $\theta(X)\in XK[X]$.
Alors $d+u(\lambda\,\mathrm{Id}_E-\theta(u))$ est semblable à $d+u$ modulo $G\ell_n(E)$; i.e. il existe $w\in G\ell_n(E)$ tel que $d+u(\lambda\,\mathrm{Id}_E-\theta(u))=w(d+u)w^{-1}$.

Démonstration
Soit $m_d(X)$ le polynôme minimal de d , on a donc
$$m_d(X)=(X-\mu_1)(X-\mu_2)\ldots(X-\mu_s) \text{ avec } \mu_i\in K\,,\ \mu_i\neq\mu_j \text{ si } i\neq j\,.$$
Ainsi
$$E=\ker(d-\mu_1\,\mathrm{Id}_E)\oplus\ker(d-\mu_2\,\mathrm{Id}_E)\oplus\ldots\oplus\ker(d-\mu_s\,\mathrm{Id}_E)$$
et d induit sur $\ker(d-\mu_i\,\mathrm{Id}_E)=:F_i$, l'homothétie $\mu_i\,\mathrm{Id}_{F_i}$.
Comme $d\,u=u\,d$, on a $u(F_i)\subset F_i$, ainsi u induit sur F_i un endomorphisme u_i qui est nilpotent. Cela implique que $d+u$ induit sur F_i l'élément $\mu_i\,\mathrm{Id}_{F_i}+u_i$.
De même $d+u(\lambda\,\mathrm{Id}_E-\theta(u))$ induit sur F_i , l'endomorphisme
$$\mu_i\,\mathrm{Id}_{F_i}+u_i(\lambda\,\mathrm{Id}_{F_i}-\theta(u_i))\,.$$
On sait par la proposition 2 qu'il existe $w_i\in G\ell_n(E_i)$ avec $(\lambda\,\mathrm{Id}_{F_i}-\theta(u_i))=w_i\,u_i\,w_i^{-1}$ ainsi
$$\mu_i\,\mathrm{Id}_{F_i}+u_i(\lambda\,\mathrm{Id}_{F_i}-\theta(u_i))=w_i(\mu_i\,\mathrm{Id}_{F_i}+u_i)\,w_i^{-1}\,.$$
Soit w défini par $w(y_1+y_2+\ldots+y_s)=w_1(y_1)+w_2(y_2)+\ldots+w_s(y_s)$, pour $y_i\in F_i$ et pour $1\leq i\leq s$. Il suit facilement que $w\in G\ell(E)$ avec $v=w\,u\,w^{-1}$, sachant que $w_i\in G\ell(F_i)$.

Remarque Ce corollaire généralise un exercice sur les matrices intitulé "sur une déformation des endomorphismes" ([Fr] ex. 5.7.34 p. 204 (version 1997) ou ex. 5.7.10 p. 234 (version 2011))

Proposition 3
Soient K un corps commutatif, E un *K-espace vectoriel de dimension $n\geq 1$, u un endomorphisme diagonalisable de E avec $u\neq 0$. Alors il existe une partie finie $\mathcal{S}$ de K telle que pour tout $\lambda\in K-\mathcal{S}$, on a $\lambda\,u$ non semblable à u* ; i.e. *pour tout $\lambda\in K-\mathcal{S}$, on a pour tout $w\in G\ell_n(E)$, $\lambda\,u\neq w\,u\,w^{-1}$.*

Démonstration
Comme u est diagonalisable, on a $m_u(X)=(X-\mu_1)(X-\mu_2)\dots(X-\mu_s)$ avec $\mu_i\in K$ et $\mu_i\neq\mu_j$ pour $i\neq j$. Facilement $m_{\lambda u}(X)=(X-\lambda\mu_1)(X-\lambda\mu_2)\dots(X-\lambda\mu_s)$. Facilement si λu est semblable à u, on a $\{\mu_1,\mu_2,\dots,\mu_s\}=\{\lambda\mu_1,\lambda\mu_2,\dots,\lambda\mu_s\}$. Le cas $u=0$ implique $s=1$ et $\mu_1=0$; cela ne demande aucune condition sur λ. Si $u\neq 0$, on a par exemple $\mu_1\neq 0$ et comme $\lambda\mu_1\in\{\mu_1,\mu_2,\dots,\mu_s\}$, il existe i avec $\lambda\mu_1=\mu_i$, ainsi $\lambda\in\mathcal{S}:=\{\frac{\mu_1}{\mu_1},\frac{\mu_2}{\mu_1},\dots,\frac{\mu_s}{\mu_1}\}$. Ce qui montre la proposition.

Théorème 2 *Soient K un corps commutatif, E un $K-$espace vectoriel de dimension $n\geq 1$, u un endomorphisme nilpotent de E. Alors il existe $x_1,x_2,\dots,x_s\in E$, des entiers $d_1\geq d_2\geq\dots\geq d_s\geq 1$ avec $u^{d_i}(x_i)=0$, $u^{d_i-1}(x_i)\neq 0$ pour $1\leq i\leq s$ et*

$$E=K[u](x_1)\oplus K[u](x_2)\oplus\dots\oplus K[u](x_s)\ .$$

Démonstration
C'est le théorème 4.1.1 de [F] p. 130 (1997) ou p. 175 (2011) ou le théorème de [F.M.] p. 15.

[F] **Fresnel J.** *Algèbre des matrices* Hermann (1997 ou 2011)
[F.M] **Fresnel J. Matignon M.** *Algèbre et géométrie* Ellipses (2017)

Sur les traces d'un ensemble d'endomorphismes

Exemple 1 Soit K un corps commutatif, on note E_{ij} la matrice dont tous les éléments sont nuls sauf celui en position (i,j) qui vaut 1.
Soit $\mathcal{S}:=\{E_{ij}\in M_n(K)\mid 1\leq i\leq n\ ,\ 1\leq j\leq n\}\cup\{0\}$.
Facilement $\mathcal{S}$ est stable pour la multiplication de $M_n(K)$, $\mathrm{Tr}(E_{i,j})=\delta_{ij}$ (avec $\delta_{ij}=0$ si $i\neq j$ et $\delta_{ii}=1$) et $\mathrm{card}\,\mathcal{S}=n^2+1$; on a donc $\mathrm{card}\,\mathcal{S}<2^{n^2}$.

Exemple 2 Soient K un corps commutatif, Δ une partie multiplicative finie de K, i.e. que pour $d,d'\in\Delta$, on a $dd'\in\Delta$; on suppose en plus que Δ contient l'élément nul de $M_n(K)$. On note encore E_{ij} la matrice dont tous les éléments sont nuls sauf celui en position (i,j) qui vaut 1.
Soit $\mathcal{S}:=\{dE_{ij}\in M_n(K)\mid d\in\Delta\ ,\ 1\leq i\leq n,1\leq j\leq n\}$. Facilement $\mathcal{S}$ est stable pour la multiplication de $M_n(K)$ et $\mathrm{card}\,\mathcal{S}=((\mathrm{card}\,\Delta)-1)\,n^2+1$.
0n a alors $\mathrm{card}\,\mathcal{S}<(\mathrm{card}\,\Delta)^{n^2}$.

Alors le théorème qui suit, généralise ces deux exemples.

Théorème B ([K.], p. 99)
Soient k *un corps commutatif,* V *un k-espace vectoriel avec* $\dim V = n \geq 1$. *Soit* $\mathcal{S}$ *une partie de* $\mathrm{End}\, V$ *avec* $\mathrm{rang}\, \mathcal{S} = n^2$. *On suppose que* $\mathcal{S}$ *est stable pour la multiplication et que* $A := \{\mathrm{Tr}\, u \mid u \in \mathcal{S}\}$ *est fini . Alors* $\mathrm{card}\, \mathcal{S} \leq (\mathrm{card}\, A)^{n^2}$.

Démonstration
Soit $\mathcal{T} \subset \mathcal{S}$ une partie libre à n^2 éléments. Soient $A := \{\mathrm{Tr}(u) \mid u \in \mathcal{S}\}$, $A^{\mathcal{T}}$ l'ensemble des applications de $\mathcal{T}$ dans A .
Soit $\rho : \mathcal{S} \to A^{\mathcal{T}}$ l'application définie comme il suit. Si $s \in \mathcal{S}$, alors pour tout $t \in \mathcal{T}$ l'application $\rho(s)$ est définie par $\rho(s)(t) := \mathrm{Tr}(st)$ (sachant que $\mathcal{S}$ est sable pour la multiplication, on a bien $\mathrm{Tr}(st) \in A$) .
On a ρ injectif, en effet si $\rho(s) = \rho(s')$, ça veut dire que pour tout $t \in \mathcal{T}$, on a $\mathrm{Tr}(st) = \mathrm{Tr}(s't)$, soit $\mathrm{Tr}((s - s')t) = 0$. Il suit alors que $s - s' = 0$ (Fr proposition 2.1.3.2 , p. 90 (a.v) , p. 116 (n.v))
Ainsi $\mathrm{card}\, \mathcal{S} \leq (\mathrm{card}\, A)^{n^2}$.

Exemple 3 Soit K un corps fini (donc commutatif), $\mathcal{S} := M_n(K)$, $A := \{\mathrm{Tr}\, u \mid u \in M_n(K)\} = K$, alors on a $\mathrm{card}\, \mathcal{S} = (\mathrm{card}\, A)^{n^2}$.

Bibliographie
[F.] **Fresnel J.** *Algèbre des matrices* Hermann (1997 ou 2011)
[K.] **Kaplansky I.** *Fields and Rings* The University of Chicago Press (1969)

Sur les polynômes de la forme produit de $X^n - 1$

Proposition *Soit* K *un corps commutatif avec* $\mathrm{car}\, K = 0$. *Soient*

$$P(X) = (X^{a_1} - 1)(X^{a_2} - 1) \ldots (X^{a_s} - 1) \in K[X]$$

avec $a_1 \geq a_2 \geq \ldots \geq a_s \geq 1$, $s \geq 1$.

$$Q(X) = (X^{b_1} - 1)(X^{b_2} - 1) \ldots (X^{b_t} - 1) \in K[X]$$

avec $b_1 \geq b_2 \geq \ldots \geq b_t \geq 1$, $t \geq 1$.
On suppose que $P(X) = Q(X)$. *Alors* $s = t$ *et* $a_i = b_i$ *pour* $1 \leq i \leq s$.

Démonstration
Ce sera une récurrence sur s .

A. *Initialisation*

Si $s=1$, on a

$$(X^{a_1}-1)=(X^{b_1}-1)(X^{b_2}-1)\dots(X^{b_t}-1)\ .$$

Ainsi $a_1=b_1+b_2+\dots+b_t$, cela prouve que

(1) $\qquad b_i\le a_1$ pour $1\le i\le t$.

Soit $L\supset K$ un corps commutatif qui contient toutes les racines de $X^{a_1}-1$ et donc aussi toutes les racines de $(X^{b_1}-1)(X^{b_2}-1)\dots(X^{b_t}-1)$.

Soit $G:=\{x\in L\mid x^{a_1}=1\}$. Comme $\mathrm{car}\,K=0$, les racines de $X^{a_1}-1$ sont distinctes ; en effet le polynôme dérivé de $X^{a_1}-1$ qui est $a_1X^{a_1-1}$ a pour seule racine 0 parce que $\mathrm{car}\,K=0$ et 0 n'est pas une racine de $X^{a_1}-1$. Il suit de cela que $o(G)=a_1$. On sait alors que G est un sous-groupe fini du groupe multiplicatif $K^\times=K-\{0\}$ qui est cyclique ([F.M.2] corollaire p. 122), disons engendré par ξ avec $o(\xi)=a_1$ (si $K=\mathbb{Q}$, on peut considérer $L=\mathbb{C}$ ainsi G est le sous-groupe engendré par $\xi=e^{i\frac{2\pi}{a_1}}\in\mathbb{C}$)

En particulier $\xi^{a_1}-1=0$ et $(\xi^{b_1}-1)(\xi^{b_2}-1)\dots(\xi^{b_t}-1)=0$.

Ce qui veut dire qu'il existe i avec $1\le i\le t$ et $\xi^{b_i}=1$. Ainsi $a_1\mid b_i$, donc $a_1\le b_i$ et comme $b_i\le b_1$, on a $a_1\le b_1$.

Compte tenu de (1), cela implique $a_1=b_1$, et toujours avec (1), comme $b_i\ge 1$, on a $t=1$ et donc $P(X)=Q(X)$.

B. *Hérédité* (passage de s à $s+1$).

On suppose la proposition vraie pour s, il faut alors montrer que la proposition est vraie pour $s+1$. On a donc

$$(X^{c_1}-1)(X^{c_2}-1)\dots(X^{c_{s+1}}-1)=(X^{d_1}-1)(X^{d_2}-1)\dots(X^{d_r}-1)$$

avec $c_1\ge c_2\ge\dots\ge c_{s+1}\ge 1$ et $d_1\ge d_2\dots\ge d_r\ge 1$

Là encore, on considère $L\supset K$, un corps commutatif qui contient toutes les racines de $(X^{c_1}-1)(X^{c_2}-1)\dots(X^{c_{s+1}}-1)$ donc qui contient toutes les racines de $(X^{d_1}-1)(X^{d_2}-1)\dots(X^{d_r}-1)$.

Soit $\xi\in L$ avec $\xi^{c_1}=1$, $o(\xi)=c_1$ (on utilise la même méthode que pour l'initialisation). Il suit qu'il existe $i\ge 1$ avec $\xi^{d_i}-1=0$ (de nouveau si $K=\mathbb{Q}$, on peut considérer $L=\mathbb{C}$ ainsi G est le sous-groupe engendré par $\xi=e^{i\frac{2\pi}{c_1}}\in\mathbb{C}$)

On a donc

(2) $\qquad c_1\mid d_i\le d_1$.

De même il existe $\theta\in L$ avec $o(\theta)=d_1$, en particulier $\theta^{d_1}-1=0$ et aussi il existe i avec $\theta^{c_i}-1=0$, ce qui implique $d_1\mid c_i\le c_1$ et donc

(3) $\qquad d_1\le c_i$

Il suit de (2) et (3) que $d_1=c_1$.

Comme $L[X]$ est intègre, on a

$$(X^{c_2}-1)(X^{c_3}-1)\ldots(X^{c_{s+1}}-1)=(X^{d_2}-1)(X^{d_3}-1)\ldots(X^{d_r}-1)\ .$$

Comme à gauche, on a s facteurs, l'hypothèse de récurrence dit que $s=r-1$ et que $c_2=d_2, c_3=d_3, \ldots, c_{s+1}=d_{s+1}$.
Cela montre bien que la proposition est vraie pour $s+1$.

Remarque 1 La caractéristique 0 est nécessaire. En effet en caractéristique $p\geq 2$, on a par exemple

$$(X-1)^p=X^p-1\text{ , soit }(X-1)(X-1)\ldots(X-1)=X^P-1\ .$$

Ainsi il n'y a pas unicité.

Remarque 2 Concernant l'exercice 31, p. 57 de [F.M.1] (sur un théorème de Brauer) on pourra utiliser cette proposition pour montrer la partie 2.4).
Soient $\sigma=c_1\,c_2\ldots c_s$ la décomposition en cycles à supports disjoints, y compris les cycles longueur 1 et a_i la longueur du cycle c_i avec $a_1\geq a_2\geq\ldots\geq a_s\geq 1$. Si donc $\tilde{\sigma}$ est l'automorphisme associé à $\sigma\in\mathfrak{S}_n$, son polynôme caractéristique est défini par

$$\chi_{\tilde{\sigma}}(X)=(X^{a_1}-1)\,(X^{a_2}-1)\ldots(X^{a_r}-1)\ .$$

De la même façon soit $\tau\in\mathfrak{S}_n$, et soient $\tau=d_1\,d_2\ldots d_t$ sa décomposition en cycles à supports disjoints, y compris les cycles longueur 1 et b_i la longueur du cycle d_i avec $b_1\geq b_2\geq\ldots\geq b_t\geq 1$. Si donc $\tilde{\tau}$ est l'automorphisme associé à $\tau\in\mathfrak{S}_n$, son polynôme caractéristique est défini par

$$\chi_{\tilde{\tau}}(X)=(X^{b_1}-1)\,(X^{b_2}-1)\ldots(X^{b_t}-1)\ .$$

On suppose que $\tilde{\sigma}$ et $\tilde{\tau}$ sont conjugués modulo $G\ell_n(K)$, ainsi il existe $w\in G\ell_n(K)$ avec $\tilde{\tau}=w\,\tilde{\sigma}\,w^{-1}$, ainsi on a $\chi_{\tilde{\sigma}}(X)=\chi_{\tilde{\tau}}(X)$, i.e.

$$(X^{a_1}-1)\,(X^{a_2}-1)\ldots(X^{a_r}-1)=(X^{b_1}-1)\,(X^{b_2}-1)\ldots(X^{b_t}-1)\ .$$

Il suit alors de la proposition que $r=t$ et $a_i=b_i$ pour $1\leq i\leq s$. Ce qui veut dire que σ et τ sont conjugués modulo $\mathfrak{S}_n$.

[F.M.1] Fresnel J. Matignon M. *Algèbre et géométrie* 2011 Hermann.
[F.M.2] Fresnel J. Matignon M. *Algèbre et géométrie* 2017 Ellipses.

p. 87 ce qui suit remplace le 5.2.1. et 5.2.2. avec quelques éléments de démonstration

5.2. Sur "l'injectivité" de l'exponentielle de matrices réelles

5.2.1. *Soient* $N, N' \in M_n(\mathbb{R})$ *, deux matrices nilpotentes. Alors les propriétés suivantes sont équivalentes.*

i) On a $N = N'$ *, ii) on a* $\exp(N) = \exp(N')$.

5.2.2. *Soient* $D, D' \in M_n(\mathbb{R})$ *, deux matrices semi-simples,* $m_D(T)$ (resp. $m_{D'}(T)$) *le polynôme minmal de* D (resp. D'). *On décompose* $m_D(T)$ *sous la forme* $m_D(T) = U_1(T)\, U_2(T)\, U_3(T)\, U_4(T)$ *avec*

$U_1(T) = (T-\lambda_1)(T-\lambda_2)\ldots(T-\lambda_r)$, $\lambda_k \in \mathbb{R}$,

$U_2(T) = (T-\mu_1)(T-\bar{\mu}_1)\,(T-\mu_2)(T-\bar{\mu}_2)\ldots(T-\mu_s)(T-\bar{\mu}_s)$ *avec*

$\mu_k = a_k + i\, b_k$, $a_k, b_k \in \mathbb{R}$, *et* $b_k \equiv 0 \,\text{modulo}\, 2\pi\mathbb{Z}$ *et* $b_k \neq 0$,

$U_3(T) = (T-\nu_1)(T-\bar{\nu}_1)(T-\nu_2)(T-\bar{\nu}_2)\ldots(T-\nu_t)(T-\bar{\nu}_t)$ *avec*

$\nu_k = a_k + i\, b_k$, $a_k, b_k \in \mathbb{R}$, *et* $b_k \equiv \pi \,\text{modulo}\, 2\pi\mathbb{Z}$, *et enfin*

$U_4(T) = (T-\eta_1)(T-\bar{\eta}_1)(T-\eta_2)(T-\bar{\eta}_2)\ldots(T-\eta_u)(T-\bar{\eta}_u)$ *avec*

$\eta_k = a_k + i\, b_k$, $a_k, b_k \in \mathbb{R}$, *et* $b_k \equiv \beta_k \,\text{modulo}\, 2\pi\mathbb{Z}$, *avec* $0 < \beta_k < \pi$.

Soient $\Lambda_1 := \{\, \lambda_k \mid 1 \leq k \leq r \,\}$, $\Lambda_2 := \{\, \mu_k \mid 1 \leq k \leq s \,\}$, $\Lambda_3 := \{\, \nu_k \mid 1 \leq k \leq t \,\}$, $\Lambda_4 := \{\, \eta_k \mid 1 \leq k \leq u \,\}$, $M_i := \{\, e^{\lambda} \mid \lambda \in \Lambda_i \,\}$.

On associe aussi à D' *une décomposition analogue avec des* $U_i'(T)$ *, ainsi que des ensembles* Λ_i' *et* M_i' .

Alors les propriétés suivantes sont équivalentes.

i) On a $\exp(D) = \exp(D')$,

ii) les trois propriétés suivantes sont satisfaites.

1. *On a* $M_1 \cup M_2 = M_1' \cup M_2'$. *Soient* $m \in M_1 \cup M_2$,

$$W_m := \Big(\bigoplus_{e^{\lambda} = m,\, \lambda \in \Lambda_1} \ker_{\mathbb{R}}(D - \lambda I_n) \Big) \oplus \Big(\bigoplus_{e^{\mu} = m,\, \mu \in \Lambda_2} \ker_{\mathbb{R}}((D-\mu I_n)(D-\bar{\mu})\, I_n)) \Big) ,$$

$$W_m' := \Big(\bigoplus_{e^{\lambda} = m,\, \lambda \in \Lambda_1'} \ker_{\mathbb{R}}(D' - \lambda I_n) \Big) \oplus \Big(\bigoplus_{e^{\mu} = m,\, \mu \in \Lambda_2'} \ker_{\mathbb{R}}((D'-\mu I_n)(D'-\bar{\mu}\, I_n)) \Big) ,$$

alors on a $W_m = W_m'$.

2. *On a* $M_3 = M_3'$. *Soient* $m \in M_3$,

$$W_m := \bigoplus_{e^{\nu} = m,\, \nu \in \Lambda_3} \ker_{\mathbb{R}}((D-\nu I_n)(D-\bar{\nu} I_n)) ,$$

$$W_m' := \bigoplus_{e^{\nu} = m,\, \nu \in \Lambda_3'} \ker_{\mathbb{R}}((D'-\nu I_n)(D'-\bar{\nu} I_n)) \text{ , alors on a } W_m = W_m' .$$

3. *On a* $M_4 = M_4'$. *Soient* $m \in M_4$, $m = \rho\, e^{i\theta}$ *avec* $0 < \theta < \pi$,

$$W_m := \bigoplus_{e^{\eta} = m,\, \eta \in \Lambda_4} \ker_{\mathbb{R}}((D-\eta I_n)(D-\bar{\eta} I_n)) ,$$

$$W_m' := \bigoplus_{e^{\eta} = m,\, \eta \in \Lambda_4'} \ker_{\mathbb{R}}((D'-\eta I_n)(D'-\bar{\eta} I_n)) \text{ , alors on a } W_m = W_m' \text{ et il existe}$$

$u_m \in G\ell(W_m)$ *tel que* $(u_m)^2 = -\,\mathrm{Id}_{W_m}$, $u_m D = D\, u_m$, $u_m D' = D'\, u_m$, *et pour* $X \in \ker_{\mathbb{R}}((D-\eta I_n)(D-\bar{\eta} I_n))$, *si* $\eta = a + i\, b \in \Lambda_4$, *on a* $D(X) = a X - b\, u_m(X)$; *et pour* $X \in \ker_{\mathbb{R}}(D'-\eta' I_n)(D'-\bar{\eta}' I_n)$, *si* $\eta' = a' + i\, b' \in \Lambda_4$, *on a*

$D'(X)=a'X-b'u_m(X)$.
(*si* $A\in M_n(\mathbb{R})$, *alors* $\ker_{\mathbb{R}}(A):=\{Z\in\mathbb{R}^n \mid AZ=0\}$).

Plan de la démonstration de 5.2.2.
L'implication $i)\Rightarrow ii)$
1) Le calcul de $\exp(D)$
Soient $\xi\in\mathbb{C}-\mathbb{R}$, $\xi=a+ib$, $\ker_{\mathbb{C}}(D-\xi I_n):=\{Z\in\mathbb{C}^n \mid (D-\xi I_n)(Z)=0\}$,
$Q(T):=(T-\xi)(T-\bar{\xi})=T^2-2aT+(a^2+b^2)$,
$\ker_{\mathbb{R}} Q(D)==\{X\in\mathbb{R}^n \mid Q(D)(X)=0\}$. Alors
$\ker_{\mathbb{R}}(Q(D))\subset\ker_{\mathbb{C}}(D-\mu_j I_n)\oplus\ker_{\mathbb{C}}(D-\bar{\mu}_j I_n)$ et l'application $Y\longmapsto Y+\bar{Y}$ est une bijection $\mathbb{R}$-linéaire de $\ker_{\mathbb{C}}(D-\mu_j I_n)$ sur $\ker_{\mathbb{R}} Q(D)$.
Soit $u\in G\ell(\ker(Q(D))$ défini par $u(Y+\bar{Y}):=i(\bar{Y}-Y)$. Comme $D(Y)=\xi Y$, on a $D(\bar{Y})=\bar{\xi}\bar{Y}$. Il suit facilement que si $\xi=a+ib$, on a $D(Y+\bar{Y})=a(Y+\bar{Y})-b(i(\bar{Y}-Y))$. Ainsi pour $X\in\ker_{\mathbb{R}}(Q(D))$, on a $D(X)=aX-bu(X)$; facilement $u^2=-\mathrm{Id}$ et donc $D(u(X))=bX+au(X)$ et $Du(X)=uD(X)$.
Calculons $\exp(D)(X)$ pour $X\in\ker_{\mathbb{R}} Q(D)$. Par ce qui précède on a
$\begin{bmatrix} D(X) \\ D(u(X)) \end{bmatrix}=\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} X \\ u(X) \end{bmatrix}$ et donc
$\begin{bmatrix} D^k(X) \\ D^k(u(X)) \end{bmatrix}=\begin{bmatrix} a & -b \\ b & a \end{bmatrix}^k\begin{bmatrix} X \\ u(X) \end{bmatrix}$. Il suit que
$\begin{bmatrix} \exp(D)(X) \\ \exp(D)(u(X)) \end{bmatrix}=\exp(\begin{bmatrix} a & -b \\ b & a \end{bmatrix})(\begin{bmatrix} X \\ u(X) \end{bmatrix})$.
Or $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}=aI_2+b\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, donc
$\exp\begin{bmatrix} a & -b \\ b & a \end{bmatrix}=\exp(aI_2)\times\exp(b\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix})$, soit
$\exp\begin{bmatrix} a & -b \\ b & a \end{bmatrix}=e^a I_2\times((\cos b)I_2+(\sin b)\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix})$.
En résumé, on a $\exp(D)(X)=e^a((\cos b)X-(\sin b)u(X))$,
$\exp(D)(u(X))=e^a((\sin b)X+(\cos b)u(X))$.

2) Comme D est une matrice diagonalisable de $M_n(\mathbb{C})$, il suit que $\exp(D)$ est une matrice diagonalisable de $M_n(\mathbb{C})$ et que l'ensemble de ses valeurs propres est exactement $M_1\cup M_2\cup M_3\cup M_4\cup\bar{M}_4$. Les valeurs propres réelles positives sont les éléments de $M_1\cup M_2$, les valeurs propres réelles négatives sont les éléments de M_3 et enfin les valeurs propres non réelles sont les éléments de $M_4\cup\bar{M}_4$. Il suit bien de cela que $M_1\cup M_2=M'_1\cup M'_2$, $M_3=M'_3$, $M_4=M'_4$. Enfin en considérant l'espace propre associé à ces valeurs propres, on déduit que $W_m=W'_m$.

3) Il nous reste à montrer la partie 3.

Soient $m \in M_4$, $V_m := \bigoplus_{e^\eta = m,\, \eta \in \Lambda_4} \ker_{\mathbb{C}}(D - \eta I_n)$,

$V'_m := \bigoplus_{e^\eta = m,\, \eta \in \Lambda'_4} \ker_{\mathbb{C}}(D' - \eta I_n)$, alors V_m est l'espace propre de $\exp(D)$ associé à la valeur propre m, de même V'_m est l'espace propre de $\exp(D')$ associé à la valeur propre m ; comme $\exp(D) = \exp(D')$, on a $V_m = V'_m$. Il suit de 1) que l'application $Y \mapsto Y + \bar{Y}$ est une bijection $\mathbb{R}$-linéaire, notée u_m de $V_m := \bigoplus_{e^\eta = m,\, \eta \in \Lambda_4} \ker_{\mathbb{C}}(D - \eta I_n)$ sur

$W_m := \bigoplus_{e^\eta = m,\, \eta \in \Lambda_4} \ker_{\mathbb{R}}((D - \eta I_n)(D - \bar{\eta} I_n))$. De même l'application

$Y \mapsto Y + \bar{Y}$ est une bijection $\mathbb{R}$-linéaire de $V'_m := \bigoplus_{e^\eta = m,\, \eta \in \Lambda'_4} \ker_{\mathbb{C}}(D' - \eta I_n)$

sur $W'_m := \bigoplus_{e^\eta = m,\, \eta \in \Lambda'_4} \ker_{\mathbb{R}}((D' - \eta I_n)(D' - \bar{\eta} I_n))$, qui est aussi u_m. Il suit encore de 1) que $u_m \in G\ell(W_m)$, $(u_m)^2 = -\mathrm{Id}_{W_m}$, $u_m D = D\, u_m$, $u_m D' = D'\, u_m$, et pour $X \in \ker_{\mathbb{R}}(D - \eta I_n)(D' - \bar{\eta} I_n)$ *on a pour* $\eta = a + i\,b$, $D(X) = aX - b\, u_m(X)$; de même pour $X \in \ker_{\mathbb{R}}((D' - \eta I_n)(D' - \bar{\eta}' I_n))$ on a pour $\eta' = a' + i\,b'$, $D'(X) = a'X - b' u_m(X)$.

Enfin *ii*) implique *i*) est sans difficulté.

p. 89 , ligne 14

$e_i \exp A = e_i e^{a_i} (I_n + \frac{N_i}{1!} + \ldots + \frac{(N_i)^{\alpha_i - 1}}{(\alpha_i - 1)!})$. Alors la formule de 6.1. suit du fait

ligne 16

4) Montrons 6.2. . Si $P(X) = (X - a_1)(X - a_2) \ldots (X - a_r)$ est le polynôme minimal de A, on sait que $a_i \neq a_j$ pour $i \neq j$. Il s'agit d'abord de montrer la formule $1 = u_1 Q_1 + u_2 Q_2 + \ldots + u_r Q_r$. Posons

$Q(X) := u_1 Q(X) + u_2 Q_2(X) + \ldots + u_r Q_r(X)$, facilement, on a $Q(a_i) = 1$ pour $1 \leq i \leq r$; sachant que $\deg Q \leq r - 1$ et que les a_i sont distincts, on a $Q(X) - 1 = 0$, i.e. la formule de Bézout.

ligne -9

Comme $(X - a_i)\, Q_i(X) = P(X)$, on a donc $e_i (A - a_i I_n) = 0$, i.e. $e_i N_i = 0$ selon les notations de 6.1. , Alors par 6.1. on a bien $\exp(A) = \sum_{i=1}^{r} e_i e^{a_i}$.

ligne -8
5) Montrons 6.3. Comme en 2) si $A'=B'+C'$ avec $B'C'=C'B'$ et

ligne -3
la formule de 6.3.

ligne -2
Application de 6.3. Soient $A\in M_n(K)$ avec $(A-I_n)^2(A-2I_n)=0$, $t\in K$.

p. 92 , ligne -8, lire

$$x(t)=\frac{y(t)}{y_0}\left(x_0+\frac{y_0}{\lambda}\mathrm{Log}\left(\frac{y(t)}{y_0}\right)\right)$$

p. 147, ex. 58, complément

Par cet exercice, on sait que si G opère transitivement sur X qui est fini, alors il existe $g\in G$ tel que $\mathrm{Fix}(g):=\{x\in X\mid g(x)=x\}=\emptyset$; en particulier $\mathrm{Fix}(G):=\{x\in X\mid$ pour tout $g\in G$, on a $g(x)=x\}=\emptyset$.

Question. On suppose que $\mathrm{Fix}(G)=\emptyset$, existe-t-il $g\in G$ avec $\mathrm{Fix}(g)=\emptyset$?

Un exemple qui dit NON.

Soit G le sous-groupe de $\mathfrak{S}(\{1,2,3,4,5\})$ défini comme il suit. Pour tout $g\in G$, on a $g(\{1,2,3\})=\{1,2,3\}$ et donc $g(\{4,5\})=\{4,5\}$. Ainsi g induit un élément $u(g)$ de $\mathfrak{S}(\{1,2,3\})$ et un élément $v(g)$ de $\mathfrak{S}(\{4,5\})$. On suppose que $u:G\to\mathfrak{S}(\{1,2,3\})$ est surjectif et que pour tout $g\in G$, on a $v(g)=(4)(5)$ si $\mathrm{sgn}(u(g))=1$ et $v(g)=(4,5)$ si $\mathrm{sgn}(u(g))=-1$.
Facilement $\mathrm{Fix}(G)=\emptyset$ et $\mathrm{Fix}(g)\neq\emptyset$ pour tout $g\in G$.

p.202, ex. 82, complément

Soient k un corps commutatif, $\mathcal{G}$ et $\mathcal{G}'$ deux sous-groupes de $G\ell_n(k)$ et $f:\mathcal{G}\to\mathcal{G}'$ un homomorphisme de groupes.
On suppose que pour tout $g\in\mathcal{G}$, il existe $A_g\in G\ell_n(k)$ tel que

$$f(g)=A_g g A_g^{-1}.$$

Alors la question est la suivante.
Existe-t-il $B\in G\ell_n(k)$ tel que pour tout $g\in\mathcal{G}$, on ait

$$f(g)=B g B^{-1}\ ?$$

0) *Si $\mathcal{G}$ est engendré par un élément, la réponse est trivialement oui.*

1) *La réponse est oui, si $\mathcal{G}$ est fini.*
Soit $\rho:\mathcal{G}\to G\ell_n(k)$, l'injection canonique, i.e. $\rho(g)=g$.
Soit $\mu:\mathcal{G}'\to G\ell_n(k)$, l'injection canonique et $\rho':=\mu f$, i.e. $\rho'(g)=\mu f(g)$ pour tout $g\in\mathcal{G}$.
Ainsi ρ et ρ' sont deux représentations linéaires de $\mathcal{G}$.
Il suit de l'hypothèse sur f qu'il existe $A_g\in G\ell_n(k)$ avec $\rho'(g)=A_g g A_g^{-1}$; en conséquence $\chi_{\rho'(g)}(X)=\chi_{\rho(g)}(X)$, où $\chi_{\rho'(g)}(X)$ (resp. $\chi_{\rho(g)}(X)$) est le polynôme caractéristique de $\rho'(g)$ (resp. $\rho(g)$) .
Compte tenu de FM1, n°10, p. 208 et n°12, p. 208 il suit que les représentations ρ et ρ' sont isomorphes. Ce qui veut dire qu'il existe $B\in G\ell_n(k)$ tel que pour tout $g\in\mathcal{G}$, on a $\rho'(g)=B\rho(g)B^{-1}$.

2) *La réponse est oui, si $\mathcal{G}$ est limite inductive de sous-groupes finis.*
On fera la démonstration dans le cas plus simple où $\mathcal{G}$ est réunion croissante d'une suite de sous-groupes finis de $\mathcal{G}$, i.e. $\mathcal{G}=\bigcup_{i\geq 0}\mathcal{G}_i$ avec $\mathcal{G}_i$ qui est fini et $\mathcal{G}_i\subset\mathcal{G}_{i+1}$ pour tout $i\geq 0$.
2.1) En considérant l'isomorphisme $f_i:\mathcal{G}_i\to f(\mathcal{G}_i)$ défini par $f_i(g):=f(g)$ pour $g\in\mathcal{G}_i$, il suit de 1) qu'il existe $B_i\in G\ell_n(k)$ tel que pour tout $g\in\mathcal{G}_i$, on a $f(g)=B_i g B_i^{-1}$.
2.2) Soit $\mathcal{E}_i:=\{M\in M_n(k)\mid$ pour tout $g\in\mathcal{G}_i$, on a $f(g)M=Mg\}$. Il suit facilement que $\mathcal{E}_i$ est un k-espace vectoriel et que par 2.1) , on a $\dim\mathcal{E}_i\geq 1$.
2.3) Facilement, si $j\geq i$, on a $\mathcal{E}_j\subset\mathcal{E}_i$, ainsi $\dim\mathcal{E}_i\geq\dim\mathcal{E}_j$, il suit que la suite décroissante $(\dim\mathcal{E}_i)_i$ est stationnaire et donc que la suite $(\mathcal{E}_i)_i$ est stationnaire.
Ainsi, il existe k avec $\mathcal{E}_i=\mathcal{E}_k$ pour tout $i\geq k$.
Il suit de cela que pour tout $g\in\mathcal{G}$, on a $f(g)=B_k g B_k^{-1}$.

3) *Un exemple avec $\mathcal{G}=\mathcal{G}'$, un sous-groupe de $G\ell_2(k)$ et $f:\mathcal{G}\to\mathcal{G}$ un automorphisme du groupe $\mathcal{G}$, tel que pour tout $g\in\mathcal{G}$, il existe $A_g\in G\ell_2(k)$ avec*

$$f(g)=A_g g A_g^{-1},$$

et tel qu'il n'existe pas $B\in G\ell_n(k)$ avec $f(g)=BgB^{-1}$ pour tout $g\in G$.

Soit k un corps contenant $\mathbb{Q}$ et $x,y\in k$ de façon que la famille (x,y) soit $\mathbb{Q}$-libre. Soient

$$\mathcal{G}:=\{\begin{bmatrix}1 & \alpha x+\beta y\\ 0 & 1\end{bmatrix}\mid(\alpha,\beta)\in\mathbb{Z}^2\}\ ,\ .$$

Facilement l'application

$$(\alpha,\beta)\mapsto\begin{bmatrix}1 & \alpha x+\beta y\\ 0 & 1\end{bmatrix}$$

est un isomorphisme du groupe additif $\mathbb{Z}^2$ sur $\mathcal{G}$. Comme $(\alpha,\beta)\mapsto(\alpha+\beta,\beta)$ est un automorphisme de $\mathbb{Z}^2$, il suit que l'application $f:\mathcal{G}\to\mathcal{G}$ définie par $f(\begin{bmatrix}1 & \alpha x+\beta y\\ 0 & 1\end{bmatrix}):=\begin{bmatrix}1 & (\alpha+\beta)x+\beta y\\ 0 & 1\end{bmatrix}$ est un automorphisme de $\mathcal{G}$.

Soient $(\alpha,\beta)\in\mathbb{Z}^2$, $(\alpha,\beta)\neq(0,0)$, sachant que (x,y) est $\mathbb{Q}$-libre, on a $(\alpha+\beta)x+\beta y\neq 0$, soit $d:=\dfrac{\alpha x+\beta y}{(\alpha+\beta)x+\beta y}$ et $A(\alpha,\beta):=\begin{bmatrix}1 & 0\\ 0 & d\end{bmatrix}$.

Sachant que (x,y) est $\mathbb{Q}$-libre, on a $\alpha x+\beta y\neq 0$, ce qui veut dire que $A(\alpha,\beta)\in G\ell_2(k)$. Facilement

$$\begin{bmatrix}1 & \alpha(x+1)+\beta y\\ 0 & 1\end{bmatrix}A(\alpha,\beta)=A(\alpha,\beta)\begin{bmatrix}1 & \alpha x+\beta y\\ 0 & 1\end{bmatrix}.$$

Il suit de cela que pour tout $g\in\mathcal{G}$, il existe $A_g\in G\ell_2(k)$ avec

$$f(g)=A_g g A_g^{-1}.$$

Il reste à montrer qu'il n'existe pas $B=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in G\ell_2(k)$ avec

$$\begin{bmatrix}1 & (\alpha+\beta)x+\beta y\\ 0 & 1\end{bmatrix}B=B\begin{bmatrix}1 & \alpha x+\beta y\\ 0 & 1\end{bmatrix}.$$

Sachant que cette dernière égalité est vraie pour tout $(\alpha,\beta)\in\mathbb{Z}^2$, avec $(\alpha,\beta)\neq(0,0)$, on déduit que

(1) $\quad d((\alpha+\beta)x+\beta y)=a(\alpha x+\beta y)$,

(2) $\quad c(\alpha x+\beta y)=0$.

Comme $\alpha x+\beta y\neq 0$ si $(\alpha,\beta)\neq(0,0)$, on a $c=0$. Ensuite (1) pour $\alpha=1$, $\beta=0$, donne $dx=ax$. De même (1) pour $\alpha=0$, $\beta=1$, donne $d(x+y)=ay$. Ainsi $dx=ax$ et $d(x+y)=ay$ impliquent $a=d=0$. Il suit que $B\notin G\ell_2(k)$.

Remarque. Cette question évoque un "principe local-global" ou encore un "principe de Hasse" pour un groupe qui s'énonce comme il suit.

Soit G un groupe, $f:G\to G$ un automorphisme. On suppose que pour tout $g\in G$, il existe $x_g\in G$ tel que $f(g)=x_g g(x_g)^{-1}$.

On dit alors que le principe de Hasse est satisfait, s'il existe $x\in G$ tel que pour tout $g\in G$, on a $f(g)=x\,g\,x^{-1}$; i.e. f est un automorphisme intérieur.

A ce propos on pourra consulter [K.] pour une liste de groupes satisfaisant le principe de Hasse. Par exemple les groupes $S\ell_n(D)$ ou $G\ell_n(D)$ avec D un anneau commutatif euclidien satisfont le principe de Hasse ([W. 1] , [W. 2]). Burnside a construit un groupe d'ordre 3^6 qui ne satisfait pas le principe de Hasse et Wall a construit un sous-groupe de $\mathfrak{S}_8$ d'ordre 2^5 qui ne satisfait pas le principe de Hasse ([W. 3])

Dans notre exemple 3) la situation est différente puisque $\mathcal{G} \subset G\ell_2(k)$ et que l'on considère les automorphismes intérieurs de $G\ell_2(k)$.

[K.] Kunyavskii Boris *Local-global invariants of finite and infinite groups: around Burnside from another side* Expo. Math. 31 (2013), n° 3, 256-273.
[W. 1] Wada Hideo *"Hasse principle" for* $S\ell_n(D)$ Proc. Japan Acad. Ser. A Math. Sci. 75 (1999), n° 5, 67-69.
[W. 2] Wada Hideo *"Hasse principle" for* $G\ell_n(D)$ Proc. Japan Acad. Ser. A Math. Sci. 76 (2000), n° 3, 44-46.
[W. 3] Wall G.E. *Finite groups with class-preserving outer automorphisms* J. London Math. Soc. 22 (1947) 315-320.

p. 209, ligne 9,
sont θ_j *pour* $1 \leq j < p$ *définies par* $\theta_j(s) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$,

p. 220, ligne -8,
13.2.2.3) Conclure de 8.2. que $\rho_0, \rho_1, \rho_2, \rho_3, \theta_1, \theta_2, \ldots, \theta_{p-1}$ sont exactement

p. 244, ligne 8,

$d \neq n$. Ainsi X'_n est l'ensemble des $x \in X$ pour lesquels n est le plus petit entier m avec $x \in X_m$, au sens de la relation d'ordre définie par d est inférieur ou égal à n si et seulement si $d \mid n$.

Complément à l'exercice 86 de FM, partie 3, p. 245

Sur la matrice des P.G.C.D.

0. Introduction

L'exemple historique est celui de la matrice de Smith (1976). Il s'agit de la matrice $M = [m_{i,j}] \in M_n(\mathbb{Z})$ avec $m_{i,j} = \text{pgcd}(i,j)$. Alors Smith ([S.]) a montré que $\det M = \varphi(1)\,\varphi(2) \ldots \varphi(n)$ où φ est l'indicateur d'Euler. Smith a lui-même généralisé ce résultat au cas où $X = (x_1, x_2, \ldots, x_n)$ est une suite de $\mathbb{N}_+ := \mathbb{N} - \{0\}$ telle que $\{x_1, x_2, \ldots, x_n\}$ est un ensemble fermé pour la factorisation ; ce qui veut dire que pour tout i,j le $\text{pgcd}(x_i, x_j)$ est élément de $\{x_1, x_2, \ldots, x_n\}$. Si donc $M = [m_{i,j}] \in M_n(\mathbb{Z})$ avec $m_{i,j} = \text{pgcd}(x_i, x_j)$ alors $\det M = \varphi(x_1)\,\varphi(x_2) \ldots \varphi(x_n)$.
En 1989 Beslin et Ligh ([B. L. 3]) ont tout d'abord considéré la matrice ci-dessus sans supposer que $\{x_1, x_2, \ldots, x_n\}$ est un ensemble fermé pour la

factorisation. Alors ils ont montré que la matrice symétrique M est symétrique définie positive.
Pour notre complément la généralisation est assez profonde puisque l'on considère une suite $X=(x_1,x_2,\dots,x_n)$, sachant que $\{x_1,x_2,\dots,x_n\}$ est un ensemble fermé ou non pour la factorisation. Ensuite, on considère une application $F\colon \mathbb{N}_+\to A$ où A est un anneau commutaif et $\psi\colon \mathbb{N}_+\to A$ est défini par $\psi(m)=\sum_{d\mid m} F(d)\,\mu(\frac{m}{d})$ où μ est la fonction de Möbius. Et enfin $M(X,F):=[m_{i,j}]\in M_n(A)$ avec $m_{i,j}=F(\text{pgcd}(i,j))$, qu'on appellera encore la matrice des P.G.C.D.
Le théorème principal dit qu'il existe une matrice rectangulaire $Z\in M_{n,m}(\mathbb{Z})$ telle que $M=Z\Delta\,{}^tZ$ où Δ est une matrice diagonale, de diagonale $(\psi(d_1),\psi(d_2),\dots,\psi(d_m))$, avec $\{d_1,d_2,\dots,d_m\}$ qui est la fermeture pour la factorisation de $\{x_1,x_2,\dots,x_n\}$.
Si de plus $\{x_1,x_2,\dots,x_n\}$ est un ensemble fermé pour la factorisation, alors on peut choisir $Z\in G\ell_n(\mathbb{Z})$.
Dans le cas où $F\colon \mathbb{N}_+\to\mathbb{Z}$ satisfait $F(m)=m$ (resp. $\psi(m)=1$, $\psi(m)=m$) , on retrouve le théorème Smith et quelques autres.

Si $A=\mathbb{R}$, sous la condition $\psi(m)>0$ pour tout m , on trouve que M est symétrique définie positive. Si $\{x_1,x_2,\dots,x_n\}$ est un ensemble fermé pour la factorisation, alors la signature de M est le couple (p,q) où p (resp. q) est le nombre de i tels que $\psi(x_i)>0$ (resp. $\psi(x_i)<0$).

1. La matrice des P.G.C.D.
Soient $\mathbb{N}_+:=\mathbb{N}-\{0\}$, $n\geq 1$, $X:=(x_1,x_2,\dots,x_n)$ une suite finie d'éléments de $\mathbb{N}_+$ avec $x_i\neq x_j$ si $i\neq j$, A un anneau commutatif, $F\colon \mathbb{N}_+\to A$ une application.
Soit $M(X,F)=[m_{i,j}]_{\substack{1\leq i\leq n\\ 1\leq j\leq n}}\in M_n(A)$, la matrice définie par

$$m_{i,j}:=F(\text{pgcd}(x_i,x_j)).$$

On l'appelle *la matrice des* P.G.C.D. *associée à* X *et* F .
Si μ est la fonction de Möbius, alors les relations (1) et (2) suivantes sont équivalentes

(1) $$\psi(m)=\sum_{d\mid m} F(d)\,\mu(\frac{m}{d}),$$

(2) $$F(m)=\sum_{d\mid m}\psi(d),$$

ce qui veut dire que si $F\colon \mathbb{N}_+\to A$ une application et si ψ est défini par (1) , alors F satisfait la relation (2) ; de même si $\psi\colon \mathbb{N}_+\to A$ est une application

et si F est défini par (2) , alors ψ satisfait la relation (1) ([FM 1], ex. 86, partie 1.2. et 1.3. p. 243).

Lemme *Soient* $X:=(x_1,x_2,\dots,x_n)$ *une suite finie d'éléments de* $\mathbb{N}_+$ *avec* $x_i\neq x_j$ *si* $i\neq j$, A *un anneau commutatif,* $F:\mathbb{N}_+\to A$ *une application,* $M(X,F)$ *la matrice des P.G.C.D. associée à* X *et* F *comme ci-dessus.*
Soient $\sigma\in\mathfrak{S}_n$ *une permutation,* Y *la suite* $(x_{\sigma(1)},x_{\sigma(2)},\dots,x_{\sigma(n)})$ *et* $Q(\sigma)=[\varepsilon_{\sigma(1)},\varepsilon_{\sigma(2)},\dots,\varepsilon_{s(n)}]$ *la matrice associée à* σ *où* $(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_n)$ *est la base canonique de* A^n *. Alors on a*

$$^tQ(\sigma)\,Q(\sigma)=I_n \quad et \quad M(X,F)\,Q(\sigma)=Q(\sigma)\,M(Y,F)\ .$$

2. Le théorème principal sur la matrice des P.G.C.D.

Théorème *Soient* $X:=(x_1,x_2,\dots,x_n)$ *une suite finie d'éléments de* $\mathbb{N}_+$ *avec* $x_i\neq x_j$ *si* $i\neq j$, A *un anneau commutatif,* $F:\mathbb{N}_+\to A$ *une application,* $M(X,F)$ *la matrice des P.G.C.D. associée à* X *et* F *.*
Soit D *la fermeture de* $\{x_1,x_2,\dots,x_n\}$ *pour la factorisation,* i.e.
$D:=\{d\in\mathbb{N}_+\mid$ *il existe* x_i *avec* $d\mid x_i\}$ *. Notons* $D=\{d_1,d_2,\dots,d_m\}$ *avec* $d_i\neq d_j$ *pour* $i\neq j$ *.*
Soit $Z:=[z_{i,j}]_{\substack{1\le i\le n\\1\le j\le m}}\in M_{n,m}(A)$ *avec* $z_{i,j}=1_A$ *si* $d_j\mid x_i$ *et* $z_{i,j}=0$ *autrement.*
Soit Δ *la matrice diagonale, de diagonale* $(\psi(d_1),\psi(d_2),\dots,\psi(d_m))$ *où* ψ *est défini en* (1)*. Alors on a*

$$M(X,F)=Z\Delta\,{}^tZ\ .$$

Démonstration
Soit $u_{i,j}$ le terme en position (i,j) de la matrice $Z\Delta\,{}^tZ$. On a

$$u_{i,j}=\sum_{k=1}^{m} z_{i,k}z_{j,k}\psi(d_k)\ ,$$

donc

$$u_{i,j}=\sum_{\substack{d_k\mid x_i\\ d_k\mid x_j}}\psi(d_k)=\sum_{d_k\mid \mathrm{pgcd}(x_i,x_j)}\psi(d_k)\ ,$$

il suit alors de (2) que

$$u_{i,j}=F(\mathrm{pgcd}(x_i,x_j))\ .$$

Cela montre bien que $Z\Delta\,{}^tZ=M(X,F)$.

3. Le cas des ensembles fermés pour la factorisation

Définition 1 Soit E une partie finie de $\mathbb{N}_+$, on dit que E *est fermé pour la factorisation* si pour tout $x \in E$ et pour tout $d \in \mathbb{N}_+$ tel que $d \mid x$, alors $d \in E$.

Exemple 1 L'ensemble $\{1, 2, \dots, n\}$ est fermé pour la factorisation.

Exemple 2 Soit p un nombre premier, alors l'ensemble $\{1, p, p^2 \dots, p^n\}$ est fermé pour la factorisation.

Corollaire 1 *Soient* $X := (x_1, x_2, \dots, x_n)$ *une suite finie d'éléments de* $\mathbb{N}_+$ *avec* $x_i \neq x_j$ *si* $i \neq j$, *on suppose que* $\{x_1, x_2, \dots, x_n\}$ *est fermé pour la factorisation. Soient* A *un anneau commutatif,* $F : \mathbb{N}_+ \to A$ *une application,* $M(X, F)$ *la matrice des P.G.C.D. associée à* X *et* F. *Alors il existe* $\sigma \in \mathfrak{S}_n$, T *une matrice triangulaire inférieure de* $M_n(\mathbb{Z}\, 1_A)$ *avec des* 1_A *sur la diagonale de façon que*

$$T\, {}^t Q(\sigma)\, M(X, F)\, Q(\sigma)\, {}^t T = \Delta,$$

où Δ *est la matrice diagonale, de diagonale* $(\psi(x_{\sigma(1)}), \psi(x_{\sigma(2)}), \dots, \psi(x_{\sigma(n)}))$ *et où* ψ *est défini en* (1).

Démonstration
Soient $\sigma \in \mathfrak{S}_n$ tel que $x_{\sigma(1)} < x_{\sigma(2)} < \dots < x_{\sigma(n)}$ et $y_i := x_{\sigma(i)}$. Enfin, soit Y la suite $(y_1, y_2, \dots, y_n)$, il suit du lemme que ${}^t Q(\sigma)\, Q(\sigma) = I_n$ et $M(X, F)\, Q(\sigma) = Q(\sigma)\, M(Y, F)$.
Soit $Z := [z_{i,j}]_{\substack{1 \le i \le n \\ 1 \le j \le n}} \in M_n(A)$ avec $z_{i,j} = 1_A$ si $y_j \mid y_i$ et $z_{i,j} = 0$ autrement. Il suit que Z est une matrice triangulaire inférieure avec des 1_A sur la diagonale.
Il suit alors du théorème que $M(Y, F) = Z\, \Delta\, {}^t Z$ où Δ est la matrice diagonale, de diagonale $(\psi(y_1), \psi(y_2), \dots, \psi(y_n))$. Si donc $T := Z^{-1}$, on a

$$T\, {}^t Q(\sigma)\, M(X, F)\, Q(\sigma)\, {}^t T = \Delta,$$

où Δ est la matrice diagonale, de diagonale $(\psi(x_{\sigma(1)}), \psi(x_{\sigma(2)}), \dots, \psi(x_{\sigma(n)}))$ et où ψ est défini en (1).

4. Le cas $A = \mathbb{Z}$ (historiquement le plus riche)

Corollaire 2 (résultat historique de H.J.S. Smith, 1876)
Soit φ *l'indicateur d'Euler,* i.e. $\varphi(1) = 1$ *et pour* $n \geq 2$,
$\varphi(n) := \operatorname{card}\{i \mid 0 \leq i < n \text{ et } 1 = \operatorname{pgcd}(i, n)\}$.
1. *Soit* $M := [\operatorname{pgcd}(i, j)]_{\substack{1 \le i \le n \\ 1 \le j \le n}} \in M_n(\mathbb{Z})$, *alors on a* $\det M = \varphi(1)\, \varphi(2) \dots \varphi(n)$.

2. *Soient* $\{x_1, x_2 \dots, x_n\}$ *un ensemble fermé de* $\mathbb{N}_+$ *pour la factorisation,* $M := [\text{pgcd}(x_i, x_j)]_{\substack{1 \le i \le n \\ 1 \le j \le n}} \in M_n(\mathbb{Z})$, *alors on a* $\det M = \varphi(x_1)\,\varphi(x_2) \dots \varphi(x_n)$.

Démonstration
1) Soit X la suite finie $(1, 2, \dots, n)$ et $F : \mathbb{N}_+ \to \mathbb{Z}$ défini par $F(k) = k$. On sait alors que $\varphi(m) = \sum_{d \mid m} d\,\mu(\frac{m}{d})$ ([F. M. 1] partie 2.3., p. 244). Ainsi la partie 1. du corollaire 2 est conséquence du corollaire 1.
2) Soit X la suite finie $(x_1, x_2, \dots, x_n)$ et $F : \mathbb{N}_+ \to \mathbb{Z}$ défini par $F(k) = k$. On sait alors que $\varphi(m) = \sum_{d \mid m} d\,\mu(\frac{m}{d})$ ([F. M. 1] partie 2.3., p. 244). Ainsi la partie 2. du corollaire 2 est conséquence du corollaire 1.

Remarque 1 La matrice définie à la partie 1 du corollaire est souvent appelée la matrice de Smith.

Remarque 2 On pourra trouver une application du déterminant de Smith lors de la démonstration d'un théorème Brauer ([F.M.2] théorème 10.1. partie 1.2.3 de la démonstration p. 162).

Corollaire 3
Soit φ *l'indicateur d'Euler,* i.e. $\varphi(1) = 1$ *et pour* $n \ge 2$,
$\varphi(n) := \text{card}\{i \mid 0 \le i < n \text{ et } 1 = \text{pgcd}(i, n)\}$.
1. *Soit* $M := [m_{i,j}]_{\substack{1 \le i \le n \\ 1 \le j \le n}}$, *où* $m_{i,j}$ *est le nombre de diviseurs dans* $\mathbb{N}_+$ *de* $\text{pgcd}(i, j)$. *Alors* $\det M = 1$.
Soit $M := [m_{i,j}]_{\substack{1 \le i \le n \\ 1 \le j \le n}}$, *où* $m_{i,j}$ *est la somme des diviseurs dans* $\mathbb{N}_+$ *de* $\text{pgcd}(i, j)$. *Alors* $\det M = n!$.
2. *Soient* $\{x_1, x_2 \dots, x_n\}$ *un ensemble fermé de* $\mathbb{N}_+$ *pour la factorisation.*
Soit $M := [m_{i,j}]_{\substack{1 \le i \le n \\ 1 \le j \le n}}$, *où* $m_{i,j}$ *est le nombre de diviseurs dans* $\mathbb{N}_+$ *de* $\text{pgcd}(x_i, x_j)$. *Alors* $\det M = 1$.
Soit $M := [m_{i,j}]_{\substack{1 \le i \le n \\ 1 \le j \le n}}$, *où* $m_{i,j}$ *est la somme des diviseurs dans* $\mathbb{N}_+$ *de* $\text{pgcd}(x_i, x_j)$. *Alors* $\det M = x_1 x_2 \dots x_n$.

Démonstration
Il est clair que 2. est conséquence de 1.
Soient X la suite finie $(x_1, x_2, \dots, x_n)$ et $\psi : \mathbb{N}_+ \to \mathbb{Z}$ défini par $\psi(k) = 1$ pour tout $k \in \mathbb{N}_+$, il suit de l'équivalence de (1) et (2) que $F(k)$ est le nombre de diviseurs de k qui sont dans $\mathbb{N}_+$. Il suit alors du corollaire 1 que

$\det M = \psi(x_1)\psi(x_2)\ \ldots\ \psi(x_n) = 1$.
Soit X la suite finie $(x_1, x_2, \ldots, x_n)$ et $\psi : \mathbb{N}_+ \to \mathbb{Z}$ défini par $\psi(k) = k$ pour tout $k \in \mathbb{N}_+$, il suit de l'équivalence de (1) et (2) que $F(k)$ est la somme des diviseurs de k qui sont dans $\mathbb{N}_+$. Il suit alors du corollaire 1 que
$\det M = \psi(x_1)\psi(x_2)\ \ldots\ \psi(x_n) = x_1 x_2 \ldots x_n$.

5. Le cas où $A = \mathbb{R}$

Corollaire 4 *Soit $\psi : \mathbb{N}_+ \to \mathbb{R}$ une application telle que pour tout $m \in \mathbb{N}_+$, on a $\psi(m) > 0$. Soit $F : \mathbb{N}_+ \to \mathbb{R}$ défini par $F(m) = \sum_{d \mid m} \psi(d)$.*
Soient $X := (x_1, x_2, \ldots, x_n)$ une suite finie de $\mathbb{N}_+$ avec $x_i \neq x_j$ pour $i \neq j$ et $M(X,F) := [m_{i,j}]_{\substack{1 \le i \le n \\ 1 \le j \le n}} \in M_n(\mathbb{R})$ avec $m_{i,j} := F(\mathrm{pgcd}(x_i, x_j))$.
Alors $M(X,F)$ est une matrice symétrique définie positive.

Démonstration
Soit $\sigma \in \mathfrak{S}_n$ une permutation telle que $x_{\sigma(1)} < x_{\sigma(2)} < \ldots < x_{\sigma(n)}$ et Y la suite finie $(y_1, y_2, \ldots, y_n)$ avec $y_i := x_{\sigma(i)}$, il suit du lemme que
(3) $$ {}^t Q(\sigma)\, M(X,F)\, Q(\sigma) = M(Y,F) \ , $$
en particulier $\mathrm{rang}\, M(X,F) = \mathrm{rang}\, M(Y,F)$.
Soit $\{d_1, d_2, \ldots, d_m\}$ la fermeture de $\{y_1, y_2, \ldots, y_n\}$ pour la factorisation et on choisit $d_1, d_2, \ldots, d_n$ tels que $d_i = y_i$ pour $1 \le i \le n$.
Soit $Z := [z_{i,j}]_{\substack{1 \le i \le n \\ 1 \le j \le m}} \in M_{n,m}(\mathbb{Z})$ avec $z_{i,j} = 1$ si $d_j \mid y_i$ et $z_{i,j} = 0$ autrement.
Soit Δ la matrice diagonale, de diagonale $(\psi(d_1), \psi(d_2), \ldots, \psi(d_m))$ où ψ est défini en (1). Alors il suit du théorème que
(4) $$ M(Y,F) = Z \Delta\, {}^t Z \ . $$
Si $m > n$, la matrice Z se décompose en deux blocs $Z = [E_1, E_2]$ où $E_1 \in M_n(\mathbb{Z})$, $E_2 \in M_{n,m-n}(\mathbb{Z})$, de plus E_1 est triangulaire inférieure avec des 1 sur la diagonale. Il suit de cela que $\mathrm{rang}\, Z = n$. Si $m = n$, on a facilement $\mathrm{rang}\, Z = n$.
Soit Δ_1 la matrice diagonale dont les coefficients diagonaux sont positifs et telle que $(\Delta_1)^2 = \Delta$. Soit $H := Z \Delta_1$, on a $\mathrm{rang}\, H = n$ et
(5) $$ M(Y,F) = H\, {}^t H \ , $$
il suit de la décomposition de Cartan ([Fr. B.C.D.] ex. 10.18 p. 142) que $\mathrm{rang}\, M(Y,F) = n$.
Il suit de (5) que pour tout $L \in \mathbb{R}^n$, on a ${}^t L\, M(Y,F)\, L \ge 0$, ce qui veut dire que $M(Y,F)$ est symétrique positif, et comme $\mathrm{rang}\, M(Y,F) = n$, il suit bien que $M(Y,F)$ est une matrice symétrique définie positive. Il suit alors de (3) que $M(X,F)$ est une matrice symétrique définie positive.

Corollaire 5 *Soit la suite finie* $X=(x_1,x_2,\dots,x_n)$ *de* $\mathbb{N}_+$ *avec* $x_i\neq x_j$ *pour* $i\neq j$ *, on suppose que* $\{x_1,x_2,\dots,x_n\}$ *est fermé pour la factorisation. Soit* $F:\mathbb{N}_+\to\mathbb{R}$ *une application et* $\psi:\mathbb{N}_+\to\mathbb{R}$ *défini par* $\psi(m)=\sum_{d\mid m}F(d)\,\mu(\frac{m}{d})$, $M(X,F):=[m_{i,j}]_{\substack{1\le i\le n\\1\le j\le n}}\in M_n(\mathbb{R})$ *avec* $m_{i,j}:=F(\mathrm{pgcd}(x_i,x_j))$. *Alors on a*

$\mathrm{sgn}(M(X,F))=(p,q)$ *avec* $p:=\mathrm{card}\{\,i\mid\psi(i)>0\}$, $q:=\mathrm{card}\{\,i\mid\psi(i)<0\}$.

Démonstration

Il suit du corollaire 1 qu'il existe $\sigma\in\mathfrak{S}_n$, T une matrice triangulaire inférieure de $M_n(\mathbb{Z})$ avec des 1 sur la diagonale de façon que

$$T\,{}^tQ(\sigma)\,M(X,F)\,Q(\sigma)\,{}^tT=\Delta\,,$$

où Δ est la matrice diagonale, de diagonale $(\psi(x_{\sigma(1)}),\psi(x_{\sigma(2)}),\dots,\psi(x_{\sigma(n)}))$. Cela montre bien le corollaire.

Références

[B. L. 1] Beslin Scott and Ligh Steve *Another Generalisation of Smith's Determinant* Bull. Austral. Math. Soc. Vol. 40 (1989) p. 413-415

[B. L. 2] Beslin Scott and Ligh Steve *GCD-closed Sets and the Determinants of GCD Matrices* Fibonacci Q. 30, n° 2, p. 157-160 (1992)

[B. L. 3] Beslin Scott and Ligh Steve *Greatest Common Divisor Matrices* Linear Algebra and Applications 118 : p. 69-76 (1989)

[Fr. B.C.D.] Fresnel J *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)

[F. M. 1] Fresnel J. et Matignon M. *Algèbre et Géométrie* (Hermann 2011)

[F. M. 2] Fresnel J. et Matignon M. *Algèbre et Géométrie* (Ellipses 2017)

[Li.] Li Zhongshan *The Determinants of GCD Matrices* Linear Algebra and Applications 134 : p. 137-143 (1990)

[S.] Smith Henry J. Stephen *On the Value of a Certain Arithmetical Determinant* Proc. London Math. Soc. 7 (1875-1876) p. 208-212

p.250, ex. 89, complément

Généralisation du déterminant de Vandermonde, applications à un théorème de Chebotarëv, au principe d'incertitude, à la majoration de racines d'un polynôme via la transformée de Fourier discrète

0. Introduction

Le déterminant de Vandermonde générique est le déterminant de la matrice $[(X_i)^j]_{\substack{1\le i\le r\\ 0\le j\le r-1}}$ où $X_1, X_2, .., X_r$ sont des variables sur $\mathbb{Z}$. On sait que $V(X_1, X_2, \dots, X_r) := \det([(X_i)^j]_{\substack{1\le i\le r\\ 0\le j\le r-1}}) = \prod_{1\le i<j\le r}(X_j - X_i)$.

Une généralisation de ce déterminant consiste à considérer des polynômes $P_1(T), P_2(T), \dots, P_r(T) \in A[T]$ où A est un anneau commutatif unitaire et où $X_1, X_2, .., X_r$ sont des variables sur A. Alors notre généralisation est $\Delta(X_1, X_2, \dots, X_r) := \det([(P_j(X_i)]_{\substack{1\le i\le r\\ 1\le j\le r}})$. Alors, on a

$\Delta(X_1, X_2, \dots, X_r) = V(X_1, X_2, \dots, X_r)\,\Gamma(X_1, X_2, \dots, X_r)$ avec

$\Gamma(X_1, X_2, \dots, X_r) \in A[X_1, X_2, \dots, X_r]$. On peut même calculer explicitement $\Gamma(X_1, X_2, \dots, X_r)$ en fonction des polynômes $P_1(T), P_2(T), \dots, P_r(T)$. La méthode n'est autre chose que la technique de Gauss qui consiste à ajouter à une ligne, un multiple d'une autre ligne.

Ce résultat admet plusieurs corollaires.

Le premier est une formule de Polyá et Szegö qui permet d'évaluer $\Gamma(1, 1, \dots, 1)$ ([P. S.]).

Le deuxième corollaire s'applique aux polynômes $P_i(T) := T^{n_i}$ pour $1 \le i \le r$. Là encore on obtient explicitement $\Gamma(1, 1, \dots, 1)$.

Le troisième corollaire est un résultat de Chebotarëv ([S. L.]). On considère $\xi \in \mathbb{C}^\times$ avec $o(\xi) = p$, un nombre premier et $M := [\xi^{ij}]_{\substack{0\le i<p\\ 0\le j<p}}$. Alors le résultat est que tous les mineurs de M sont non nuls.

Une dernière application concerne les fonctions $f : \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$ et leur transformée de Fourier $\hat{f}$. Le résultat est que $\mathrm{card}(supp(f)) + \mathrm{card}(supp(\hat{f})) \ge p+1$, où $supp(f)$ (resp. $supp(\hat{f})$) désigne le support de f (resp. $\hat{f}$). Cet énoncé est souvent appellé le principe d'incertitude.

Une application de ce résultat est la majoration du nombre de racines p-èmes de l'unité qui sont racines d'un polynôme unitaire à coefficients dans $\mathbb{C}$, non nul et de degré au plus $p-1$.

Théorème 1 *Soient A un anneau commutatif, unitaire, $X_1, X_2, \dots, X_r$ des variables sur A. Soient $1 \le m \le r$, $1 \le i_1 < i_2 < \dots < i_m \le r$, $k \ge 1$, on définit le polynôme $T_k(X_{i_1}, X_{i_2}, \dots, X_{i_m})$ par*

$$T_k(X_{i_1}, X_{i_2}, \dots, X_{i_m}) := \sum_{\substack{(\alpha_1, \alpha_2, \dots, \alpha_m) \in \mathbb{N}^m \\ \alpha_1 + \alpha_2 + \dots + \alpha_m = k}} (X_{i_1})^{\alpha_1} (X_{i_2})^{\alpha_2} \dots (X_{i_m})^{\alpha_m}$$ *et par*

convention $T_0(X_{i_1}, X_{i_2}, \dots, X_{i_m}) = 1$.

Soient $P_i(X) \in A[X]$ *pour* $1 \le i \le r$, $t := \max_{1 \le i \le r} \deg P_i(X)$, *et*

$$P_i(X) = a_{0,i} + a_{1,i} X + a_{2,i} X^2 + \dots + a_{t,i} X^t .$$

Soient $0 \le k \le r-1$ *et*

$$R_{k,i} := \sum_{\ell=k}^{t} a_{\ell,i} T_{\ell-k}(X_1, X_2, \dots, X_{k+1}) .$$

Soient maintenant

$$\Delta(X_1, X_2, \dots, X_r) := \det \begin{bmatrix} P_1(X_1) & P_2(X_1) & \dots & P_r(X_1) \\ P_1(X_2) & P_2(X_2) & \dots & P_r(X_2) \\ . & . & \dots & . \\ P_1(X_r) & P_2(X_r) & \dots & P_r(X_r) \end{bmatrix},$$

$$V(X_1, X_2, \dots, X_r) := \prod_{1 \le i < j \le r} (X_j - X_i) = \det \begin{bmatrix} 1 & X_1 & X_1^2 \dots & X_1^{r-1} \\ 1 & X_2 & X_2^2 \dots & X_2^{r-1} \\ . & . & \dots & . \\ 1 & X_r & X_r^2 \dots & X_r^{r-1} \end{bmatrix} .$$

Alors, on a

$$\Delta(X_1, X_2, \dots, X_r) = V(X_1, X_2, \dots, X_r)\, \Gamma(X_1, X_2, \dots, X_r)$$

où

$$\Gamma(X_1, X_2, \dots, X_r) := \det \begin{bmatrix} R_{0,1} & R_{0,2} & \dots & R_{0,r} \\ R_{1,1} & R_{1,,2} & \dots & R_{1,r} \\ . & . & \dots & . \\ R_{r-1,1} & R_{r-1,2} & \dots & R_{r-1,r} \end{bmatrix}.$$

En particulier, on a $\Gamma(X_1, X_2, \dots, X_r) \in A[X_1, X_2, \dots, X_r]$ *et*

$$\Gamma(0, 0, \dots, 0) := \det \begin{bmatrix} a_{0,1} & a_{0,2} & \dots & a_{0,r} \\ a_{1,1} & a_{1,,2} & \dots & a_{1,r} \\ . & . & \dots & . \\ a_{r-1,1} & a_{r-1,2} & \dots & a_{r-1,r} \end{bmatrix}.$$

Démonstration

1) Soient $k \ge 1$, $1 \le s < m$, on a

(1) $$T_k(X_m) - T_k(X_s) = (X_m)^k - (X_s)^k = (X_m - X_s)\, T_{k-1}(X_s, X_m) .$$

Soient $k \ge 1$, $2 \le s < m$, on a

(2) $$T_k(X_1, X_2, \dots, X_{s-1}, X_m) - T_k(X_1, X_2, \dots, X_{s-1}, X_s) = (X_m - X_s) T_{k-1}(X_1, X_2, \dots, X_{s-1}, X_s, X_m) .$$

En effet

$$T_k(X_1,X_2,\dots,X_{s-1},X_m)=\sum_{\ell=0}^{k} T_{k-\ell}(X_1,X_2,\dots,X_{s-1})(X_m)^{\ell},$$

$$T_k(X_1,X_2,\dots,X_{s-1},X_s)=\sum_{\ell=0}^{k} T_{k-\ell}(X_1,X_2,\dots,X_{s-1})(X_s)^{\ell}.$$

On sait par (1) que

$$(X_m)^{\ell}-(X_s)^{\ell}=(X_m-X_s)\,T_{\ell-1}(X_s,X_m).$$

Ainsi

$$T_k(X_1,X_2,\dots,X_{s-1},X_m)-T_k(X_1,X_2,\dots,X_{s-1},X_s)=$$
$$(X_m-X_s)\sum_{\ell=0}^{k} T_{k-\ell}(X_1,X_2,\dots,X_{s-1})T_{\ell-1}(X_s,X_m).$$

Facilement

$$T_{k-1}(X_1,X_2,\dots,X_{s-1},X_s,X_m)=\sum_{\ell=0}^{k} T_{k-\ell}(X_1,X_2,\dots,X_{s-1})T_{\ell-1}(X_s,X_m).$$

2) Soient $b_0,b_1,\dots,b_t\in A$, $1<m<r$,

$$U=b_0+b_1T_1(X_1)+b_2T_2(X_1)+\dots,b_t\ T_t(X_1),$$
$$V=b_0+b_1T_1(X_m)+b_2T_2(X_m)+\dots,b_t\ T_t(X_m).$$

Il suit de (1) que

(3) $V-U=(X_m-X_1)(b_1T_0(X_1,X_m)+b_2T_1(X_1,X_m)+\dots+b_tT_{t-1}(X_1,X_m))$.

On suppose que $2\le s<m$. Alors il suit de (2) que

(4) $V-U=(X_m-X_1)(b_1T_0(X_1,X_2,\dots,X_s,X_m)+$
$b_2T_1(X_1,X_2,\dots,X_s,X_m)+\dots+b_tT_{t-1}(X_1,X_2,\dots,X_s,X_m))$.

3) Soient $1\le k<j$,

$Q_{k,j,i}:=\sum_{\ell=k}^{t} a_{\ell,i}T_{\ell-k}(X_1,\dots,X_k,X_j)$, on a donc pour $k\ge 1$, $R_{k,i}=Q_{k,k+1,i}$.

Soit la matrice

$$M_0:=\begin{bmatrix} P_1(X_1) & P_2(X_1) & \dots & P_r(X_1)\\ P_1(X_2) & P_2(X_2) & \dots & P_r(X_2)\\ \cdot & \cdot & \dots & \cdot\\ P_1(X_r) & P_2(X_r) & \dots & P_r(X_r)\end{bmatrix}.$$

Appelons $L_0,L_1,\dots,L_{r-1}$ les lignes de M_0. Considérons les opérations L_1 reçoit L_1-L_0, L_2 reçoit $L_2-L_0,\dots,$ L_{r-1} reçoit $L_{r-1}-L_0$.

Soit $j>1$, on a

$$P_i(X_1)=a_{0,i}+a_{1,i}X_1+a_{2,i}X_1^2+\dots+a_{t,i}X_1^t,$$
$$P_i(X_j)=a_{0,i}+a_{1,i}X_j+a_{2,i}X_j^2+\dots+a_{t,i}X_j^t.$$

Il suit de (1) que

$P_i(X_j)-P_i(X_1)=(X_j-X_1)(a_{1,i}+a_{2,i}T_1(X_1,X_j)+\dots+a_{t,i}T_{t-1}(X_1,X_j))$,

et donc que

$$P_i(X_j)-P_i(X_1)=(X_j-X_1)\,Q_{1,j,i}.$$

Par ailleurs $P_i(X_1)=R_{0,i}$.
Après cette première étape M_0 devient $(X_2-X_1)(X_3-X_1)\dots(X_r-X_1)M_1$, avec

$$M_1:=\begin{bmatrix} R_{0,1} & R_{0,2} & \cdot\ \cdot & R_{0,r} \\ R_{1,1} & R_{1,2} & \cdot\ \cdot & R_{1,r} \\ Q_{1,3,1} & Q_{1,3,1} & \cdot\ \cdot & Q_{1,3,r} \\ \cdot & \cdot & \cdot\ \cdot & \cdot \\ Q_{1,r,1} & Q_{1,r,1} & \cdot\ \cdot & Q_{1,r,r,} \end{bmatrix}.$$

Appelons encore $L_0, L_1, \dots, L_{r-1}$ les lignes de M_1 . On effectue maintenant les opérations suivantes : L_3 reçoit L_3-L_2, L_4 reçoit $L_4-L_2, \dots,$ L_{r-1} reçoit $L_{r-1}-L_2$.
On a

$$Q_{1,2,i}=R_{1,i}=\sum_{\ell=1}^{t} a_{\ell,i}\ T_{\ell-1}(X_1,X_2)$$

et pour $j\geq 3$

$$Q_{1,j,i}=\sum_{\ell=1}^{t} a_{\ell,i}\ T_{\ell-1}(X_1,X_j)\ .$$

Alors (4) dit que
$Q_{1,j,i}-Q_{1,2,i}=(X_j-X_2)\ (a_{2,i}+a_{3,i}T_1(X_1,X_2,X_j)+\dots+a_{t,i}T_{t-2}(X_1,X_2,X_j)$.
Ainsi

$$Q_{1,j,i}-Q_{1,2,i}=(X_j-X_2)\ Q_{2,j,i}\ .$$

Après ces opérations M_1 devient
$(X_2-X_1)(X_3-X_1)\dots(X_r-X_1)(X_3-X_2)(X_4-X_2)\dots(X_r-X_2)M_2$, avec

$$M_2:=\begin{bmatrix} R_{0,1} & R_{0,2} & \cdot\ \cdot\ \cdot & R_{0,r} \\ R_{1,1} & R_{1,2} & \cdot\ \cdot\ \cdot & R_{1,r} \\ R_{2,1} & R_{2,2} & \cdot\ \cdot\ \cdot & R_{2,r,} \\ Q_{2,4,1} & Q_{2,4,2} & \cdot\ \cdot\ \cdot & Q_{2,4,r} \\ \cdot & \cdot & \cdot\ \cdot\ \cdot & \cdot \\ Q_{2,r,1} & Q_{2,r,2} & \cdot\ \cdot\ \cdot & Q_{2,r,r,} \end{bmatrix}.$$

Alors le lecteur voit comment continuer en appliquant la formule (4) .

Remarque Le fait que $\Gamma(X_1,X_2,\dots,X_r)\in A[X_1,X_2,\dots,X_r]$ peut se montrer assez facilement.
1. *On considère d'abord le cas où* $A=B$ *avec* B *factoriel et où* $X_1,X_2,\dots,X_r$ *sont des variables sur* B .
Soient $P_{1,i}(Z)\in B[Z]$ pour $1\leq i\leq r$,

$$\Delta_1(X_1,X_2,\dots,X_r):=\text{dét}\begin{bmatrix} P_1(X_1) & P_2(X_1) & \dots & P_r(X_1) \\ P_1(X_2) & P_2(X_2) & \dots & P_r(X_2) \\ \cdot & \cdot & \dots & \cdot \\ P_1(X_r) & P_2(X_r) & \dots & P_r(X_r) \end{bmatrix},$$

Il faut montrer que $(X_j - X_i)$ divise $\Delta_1(X_1, X_2, \ldots, X_r)$ dans $B[X_1, X_2, \ldots, X_r]$. Soit $\rho : B[X_1, X_2, \ldots, X_r] \to B[X_2, X_3, \ldots, X_r]$ défini par $\rho(X_i) = X_i$ si $i \geq 2$ et $\rho(X_1) = X_2$. Facilement $\rho(\Delta_1(X_1, X_2, \ldots, X_r)) = 0$ et $\rho(U) = U$ si $U \in B[X_2, X_3, \ldots, X_r]$. Par division euclidienne de $\Delta_1(X_1, X_2, \ldots, X_r)$ par le polynôme unitaire $X_1 - X_2$ en X_1, on a

(5) $\Delta_1(X_1, X_2, \ldots, X_r) = (X_1 - X_2)\, Q(X) + R(X)$

où $Q(X) \in B[X_1, X_2, \ldots, X_r]$ et $R(X) \in B[X_2, X_3, \ldots, X_r]$. En appliquant ρ à l'égalité (5), on obtient $0 = R(X)$ et comme $\rho(R) = R$, on a bien $X_1 - X_2$ qui divise $\Delta_1(X_1, X_2, \ldots, X_r)$ dans $B[X_1, X_2, \ldots, X_r]$.

De la même façon, si $i \neq j$, on a $X_i - X_j$ qui divise $\Delta_1(X_1, X_2, \ldots, X_r)$ dans $B[X_1, X_2, \ldots, X_r]$.

Clairement pour $i < j$, les $X_i - X_j$ sont des irréductibles non associés de l'anneau factoriel $B[X_1, X_2, \ldots, X_r]$. Il suit donc de cela que l'image canonique de $V(X_1, X_2, \ldots, X_r)$ dans $B[X_1, X_2, \ldots, X_r]$, notée $V_1(X_1, X_2, \ldots, X_r)$, divise $\Delta_1(X_1, X_2, \ldots, X_r)$ dans $B[X_1, X_2, \ldots, X_r]$, ce qui veut dire que

(6) $\Delta_1(X_1, X_2, \ldots, X_r) = V_1(X_1, X_2, \ldots, X_r)\, \Gamma_1(X_1, X_2, \ldots, X_r)$

avec $\Gamma_1(X_1, X_2, \ldots, X_r) \in B[X_1, X_2, \ldots, X_r]$.

2. *On considère maintenant le cas où A est un anneau commutatif unitaire quelconque.*

Soient $A_{j,i}$, X_k, $1 \leq j \leq t$, $1 \leq i \leq r$, $1 \leq k \leq r$ des variables sur $\mathbb{Z}$; soit $B := \mathbb{Z}[\{A_{j,i}, X_k \mid 1 \leq j \leq t,\ 1 \leq i \leq r,\ 1 \leq k \leq r\}]$. Soient $\varphi : \mathbb{Z} \to A$ l'homomorphisme canonique et $\psi : B \to A$ défini par $\psi(A_{j,i}) := a_{j,i}$, $\psi(z) := \varphi(z)$ si $z \in \mathbb{Z}$. Alors en appliquant ψ à la relation (6), on obtient

(7) $\Delta(X_1, X_2, \ldots, X_r) = V(X_1, X_2, \ldots, X_r)\, \psi(\Gamma_1(X_1, X_2, \ldots, X_r))$

où $\psi(\Gamma_1(X_1, X_2, \ldots, X_r)) \in A[X_1, X_2, \ldots, X_r]$.

Cela veut bien dire que $V(X_1, X_2, \ldots, X_r)$ divise $\Delta(X_1, X_2, \ldots, X_r)$ dans l'anneau $A[X_1, X_2, \ldots, X_r]$.

Si l'on sait que $V(X_1, X_2, \ldots, X_r)$ n'est pas un diviseur de zéro dans $A[X_1, X_2, \ldots, X_r]$, on peut en conclure que

$$\psi(\Gamma_1(X_1, X_2, \ldots, X_r)) = \Gamma(X_1, X_2, \ldots, X_r) .$$

3. *Montrons que $V(X_1, X_2, \ldots, X_r)$ ne divise pas zéro dans $A[X_1, X_2, \ldots, X_r]$.*

Si $0 = (X_2 - X_1)(a_0 X_1^0 X_2^n) + a_1 X_1^1 X_2^{n-1}) + \ldots + a_n X_1^n X_2^0)$ avec $a_k \in A[X_3, X_4, \ldots, X_r]$. Il suit de cela que

(8) $0 = a_0 X_2^{n+1} + (a_1 - a_0)(X_1^1 X_2^n) + \ldots + (a_n - a_{n-1})(X_1^n X_2^1) - a_n X_1^{n+1}$,

ainsi $a_0 = a_1 = \ldots = a_n = 0$. Donc $(X_2 - X_1)$ ne divise pas zéro, de la même façon $(X_j - X_i)$ ne divise pas zéro pour $j > i$, ce qui montre que $V(X_1, X_2, \ldots, X_r)$ ne divise pas zéro dans $A[X_1, X_2, \ldots, X_r]$.

Application à une formule de Polyá et Szegö ([P. S.])

Corollaire 1 *Soient* A *un anneau commutatif, unitaire,* $r \geq 1$, $T_1, T_2, \ldots, T_r$ *des variables sur* A , $R_i(Z) \in A[Z]$ *pour* $1 \leq i \leq r$. *Soit*

$$\Delta(T_1, T_2, \ldots, T_r) := \det \begin{bmatrix} R_1(T_1) & R_2(T_1) & \ldots & R_r(T_1) \\ R_1(T_2) & R_2(T_2) & \ldots & R_r(T_2) \\ . & . & \ldots & . \\ R_1(T_r) & R_2(T_r) & \ldots & R_r(T_r) \end{bmatrix}.$$

Alors on a

$$\Delta(T_1, T_2, \ldots, T_r) = V(T_1, T_2, \ldots, T_r) F(T_1, T_2, \ldots, T_r)$$

avec

$$V(T_1, T_2, \ldots, T_r) := \prod_{1 \leq i < j \leq r} (T_j - T_i) = \det \begin{bmatrix} 1 & T_1 & T_1^2 \ldots & T_1^{r-1} \\ 1 & T_2 & T_2^2 \ldots & T_2^{r-1} \\ 1 & T_r & T_r^2 \ldots & T_r^{r-1} \end{bmatrix},$$

et

$$F(T_1, T_2, \ldots, T_r) \in A[T_1, T_2, \ldots, T_r] .$$

Si $R_i(1+X_i) := a_{0,i} + a_{1,i} X_i + a_{2,i} X_i^2 + \ldots + a_{t,i} X_i^t$, alors on a

$$F(1, 1, \ldots, 1) := \det \begin{bmatrix} a_{0,1} & a_{0,2} & \ldots & a_{0,r} \\ a_{1,1} & a_{1,,2} & \ldots & a_{1,r} \\ . & . & \ldots & . \\ a_{r-1,1} & a_{r-1,2} & \ldots & a_{r-1,r} \end{bmatrix}.$$

Remarque Si A est de caractéristique nulle, on a $(a_{k,i})\ k! = R_i^{(k)}(1)$ où $R_i^{(k)}$ désigne la dérivée k-ème de R_i .

Corollaire 2 *Soient* A *un anneau commutatif, unitaire,* $r \geq 1$, $T_1, T_2, \ldots, T_r$ *des variables sur* A , $0 \leq m_1 \leq m_2 \leq \ldots \leq m_r$ *des entiers. Soient*

$$\Delta(T_1, T_2, \ldots, T_r) = \det \begin{bmatrix} T_1^{m_1} & T_1^{m_2} & \ldots & T_1^{m_r} \\ T_2^{m_1} & T_2^{m_2} & \ldots & T_2^{m_r} \\ . & . & \ldots & . \\ T_r^{m_1} & T_r^{m_2} & \ldots & T_r^{m_r} \end{bmatrix},$$

$$V(T_1, T_2, \ldots, T_r) := \prod_{1 \leq i < j \leq r} (T_j - T_i) = \det \begin{bmatrix} 1 & T_1 & T_1^2 \ldots & T_1^{r-1} \\ 1 & T_2 & T_2^2 \ldots & T_2^{r-1} \\ 1 & T_r & T_r^2 \ldots & T_r^{r-1} \end{bmatrix}.$$

Alors, on a

$$\Delta(T_1, T_2, \ldots, T_r) = V(T_1, T_2, \ldots, T_r) F(T_1, T_2, \ldots, T_r) .$$

Et comme $(1+X_j)^{m_i} = 1 + \binom{m_i}{1} X_j + \binom{m_i}{2} X_j^2 + \ldots + \binom{m_i}{m_i} X_j^{m_i}$, *il suit du corollaire 1 que*

$$F(1,1,\ldots,1) = \text{dét} \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \binom{m_1}{1} & \binom{m_2}{1} & \ldots & \binom{m_r}{1} \\ \binom{m_1}{2} & \binom{m_2}{2} & \ldots & \binom{m_r}{2} \\ . & . & \ldots & . \\ \binom{m_1}{r-1} & \binom{m_2}{r-1} & \ldots & \binom{m_r}{r-1} \end{bmatrix}.$$

Si $\text{car} A = 0$, *on a*

$$1!\,2!\ldots(r-1)!\,F(1,1,\ldots,1) = V(m_1, m_2, \ldots, m_r) .$$

Corollaire 3 (Chebotarëv) *Soit* p *un nombre premier. Soient des entiers avec* $0 \le m_1 < m_2 < \ldots < m_r < p$ *et* $0 \le n_1 < n_2 < \ldots < n_r < p$. *Soit* $\xi \in \mathbb{C}^\times$ avec $o(\xi) = p$. *Alors*

$$\text{dét}[\xi^{n_i m_j}]_{\substack{1 \le i \le r \\ 1 \le j \le r}} \neq 0 .$$

Démonstration

Soit $\varphi : \mathbb{Z}[T_1, T_2, \ldots, T_r] \to \mathbb{Z}[T]$ l'unique homomorphisme défini par $\varphi(T_i) := T^{n_i}$. Soient $\Delta_1(T) := \varphi(\Delta(T_1, T_2, \ldots, T_r)) = \text{dét}[T^{n_i m_j}]_{\substack{1 \le i \le r \\ 1 \le j \le r}}$,

$V_1(T) := \varphi(V(T_1, T_2, \ldots, T_r)) = \prod_{1 \le i < j \le r} (T^{n_j} - T^{n_i})$,

$F_1(T) := \varphi(F(T_1, T_2, \ldots, T_r)) = F(T^{n_1}, T^{n_2}, \ldots, T^{n_r})$.

Il s'agit donc de montrer que $\Delta_1(\xi) \neq 0$.

Supposons le contraire, i.e. $\Delta_1(\xi) = 0$. Il suit donc du corollaire 2 que $\Delta_1(T) = V_1(T) F_1(T)$ et donc que $0 = V_1(\xi) F_1(\xi)$. Or $V_1(\xi) = \prod_{1 \le i < j \le r} (\xi^{n_j} - \xi^{n_i})$, sachant que $o(\xi) = p$ et que $0 \le n_1 < n_2 < \ldots < n_r < p$, on a $V_1(\xi) \neq 0$; il suit de cela que $F_1(\xi) = 0$. Soit $\Phi_p(T) := 1 + T + \ldots + T^{p-1}$, on sait que $\Phi_p(T)$ est le générateur unitaire de l'idéal des polynôme de $\mathbb{Z}[T]$ qui s'annulent en ξ ([F. 2] ex. 7.9.6 p. 280). Il existe donc $A(T) \in \mathbb{Z}[T]$ tel que $F_1(T) = A(T) \Phi_p(T)$; en particulier $F_1(1) = A(1) \Phi_p(1)$, ce qui montre que $F_1(1) \in p\mathbb{Z}$. Or il suit du corollaire 2 que $1!\,2!\ldots(r-1)!\,F(1,1,\ldots,1) = V(m_1, m_2, \ldots, m_r)$; i.e. $1!\,2!\ldots(r-1)!\,F_1(1) = \prod_{1 \le i < j \le r} (m_j - m_i)$. Sachant que $r < p$ et que $0 \le m_1 < m_2 < \ldots < m_r < p$, on déduit que $F_1(1) \notin p\mathbb{Z}$; ce qui donne une contradiction.

Remarque On suit là, essentiellement la démonstration de Dieudonné ([D.]). On notera que ce dernier ne savait pas que le résultat était déjà connu de Chebotarëv.

Sur la transformée de Fourier discrète

Définition et notation Soient p un nombre premier, $\xi \in \mathbb{C}^\times$ avec $o(\xi) = p$, $\rho : \mathbb{Z} \to \frac{\mathbb{Z}}{p\mathbb{Z}}$ la surjection canonique. Alors l'application $u : \mathbb{Z} \to \mathbb{C}$ définie par $u(z) := \xi^z$, induit une application $v : \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$ telle que $u = v\rho$. Pour simplifier les notations, *on notera* $v(x)$ par ξ^x.
Soient $f : \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$, $\hat{f} : \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$, défini par $\hat{f}(y) := \sum_{x \in \frac{\mathbb{Z}}{p\mathbb{Z}}} f(x)\,\xi^{xy}$. Alors $\hat{f}$ s'appelle *la transformée de Fourier discrète de* f.

Corollaire 4 *Soient* p *un nombre premier,* A *et* B *deux parties non vides de* $\frac{\mathbb{Z}}{p\mathbb{Z}}$ *avec* $\mathrm{card}(A) = \mathrm{card}(B)$. *Soient* $\mathbb{C}^A$ (resp. $\mathbb{C}^B$) *le* $\mathbb{C}$*-espace vectoriel des applications de* A (resp. B) *dans* $\mathbb{C}$, $\theta : \mathbb{C}^A \to \mathbb{C}^B$ *défini pour* $y \in B$ *par* $\theta(f)(y) = \sum_{x \in A} f(x)\xi^{xy}$. *Alors* θ *est une bijection* $\mathbb{C}$*-linéaire de* $\mathbb{C}^A$ *sur* $\mathbb{C}^B$.

Démonstration
On a $A = \{a_1, a_2, \ldots, a_s\}$, $B = \{b_1, b_2, \ldots, b_s\}$. Soit $\{u_1, u_2, \ldots, u_s\}$ (resp. $\{v_1, v_2, \ldots, v_s\}$ les éléments de $\mathbb{C}^A$ (resp. $\mathbb{C}^B$) définis par $u_i(a_j) = \delta_{i,j}$ (resp. $v_i(b_j) = \delta_{i,j}$) pour $1 \le i \le s$ et $1 \le j \le s$, i.e. u_i (resp. v_j) est la fonction caractéristique de $\{a_i\}$ (resp. $\{b_j\}$). On a donc

$$\theta(u_i)(b_j) = \sum_{x \in A} u_i(x)\xi^{x b_j},$$

soit donc

$$\theta(u_i)(b_j) = u_i(a_i)\xi^{a_i b_j} = \xi^{a_i b_j} v_j(b_j).$$

Ce qui veut dire que

$$\theta(u_i) = \sum_{j=1}^{s} \xi^{a_i b_j} v_j.$$

Il suit de cela que $\mathrm{Mat}(\theta; u_i, v_j) = [\xi^{a_i b_j}]_{\substack{1 \le i \le s \\ 1 \le j \le s}}$. Or il suit du corollaire 3 que $\det [\xi^{a_i b_j}]_{\substack{1 \le i \le s \\ 1 \le j \le s}} \neq 0$; ce qui montre que θ est bijectif.

Théorème 2 (le principe d'incertitude) *Soient* p *un nombre premier* $f: \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$ *une fonction non nulle,* $\hat{f}$ *sa transformée de Fourier discrète. Alors*

$$\mathrm{card}(supp(f)) + \mathrm{card}(supp(\hat{f})) \geq p+1 ,$$

où $supp(f) := \{x \in \frac{\mathbb{Z}}{p\mathbb{Z}} \mid f(x) \neq 0\}$ (resp. $supp(\hat{f}) := \{y \in \frac{\mathbb{Z}}{p\mathbb{Z}} \mid \hat{f}(y) \neq 0\}$) .

Réciproquement, soient A *et* B *deux parties non vides de* $\frac{\mathbb{Z}}{p\mathbb{Z}}$ *avec* $\mathrm{card}A + \mathrm{card}B \geq p+1$. *alors il existe* $f: \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$ *une fonction non nulle, telle que* $supp(f) = A$ *et* $supp(\hat{f}) = B$.

Démonstration

1) Supposons que $f \neq 0$ et $\mathrm{card}(supp(f)) + \mathrm{card}(supp(\hat{f})) \leq p$.
Soit donc $A := supp(f)$, il existe donc une partie B de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec $B \cap supp(\hat{f}) = \emptyset$ et $\mathrm{card}A = \mathrm{card}B$. Si donc $\theta: \mathbb{C}^A \to \mathbb{C}^B$ est l'application défini par le corollaire 4, on a $\theta(f_{|A}) = 0$ et donc $f_{|A} = 0$, ce qui contredit $A := supp(f)$.

2) Montrons la réciproque.

2.1) On suppose la réciproque montrée pour les parties A, B avec $\mathrm{card}A + \mathrm{card}B = p+1$.
Supposons maintenant que $\mathrm{card}A + \mathrm{card}B > p+1$. Soit
$\Theta := \{(A', B') \mid A' \subset A , B' \subset B , A' \neq \emptyset , B' \neq \emptyset$ et $\mathrm{card}A' + \mathrm{card}B' = p+1\}$.
Si donc $\theta = (A', B') \in \Theta$, il existe $f_\theta: \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$ tel que $supp(f_\theta) = A'$ et $supp(\hat{f_\theta}) = B'$.

(1) En particulier, on a $f_\theta(a) \neq 0$ si $a \in A'$, $f_\theta(a) = 0$ si $a \notin A'$; de même $\hat{f_\theta}(b) \neq 0$ si $b \in B'$ et $\hat{f_\theta}(b) = 0$ si $b \notin B'$.
Soit $a \in A$ et $G_a := \{\lambda \in \mathbb{C}^\Theta \mid \sum_{\theta \in \Theta} \lambda(\theta) f_\theta(a) = 0\}$.
Il existe $\theta = (A', B')$ avec $a \in A'$, ainsi $f_\theta(a) \neq 0$; cela montre que G_a est un hyperplan de $\mathbb{C}^\Theta$.
Soit $b \in B$ et $H_b := \{\lambda \in \mathbb{C}^\Theta \mid \sum_{\theta \in \Theta} \lambda(\theta) \hat{f_\theta}(b) = 0\}$. De même H_b est un hyperplan de $\mathbb{C}^\Theta$. On sait alors que $(\bigcup_{a \in A}) G_a) \cup (\bigcup_{b \in B}) H_b) \neq \mathbb{C}^\Theta$ ([F. 1] ex. 1.4.3. p. 77).
Soit donc $\mu \in \mathbb{C}^\Theta$ et $\mu \notin (\bigcup_{a \in A}) G_a) \cup (\bigcup_{b \in B}) H_b)$.
Soient $f := \sum_{\theta \in \Theta} \mu(\theta) f_\theta$, on a alors $\hat{f} := \sum_{\theta \in \Theta} \mu(\theta) \hat{f_\theta}$.

Il suit du choix de μ que $f(a)\neq 0$ pour tout $a\in A$ et que $\hat{f}(b)\neq 0$ pour tout $b\in B$. Ensuite, il suit de (1) que $f(a)=0$ si $a\notin A$ et que $\hat{f}(b)=0$ si $b\notin B$.
Alors on a bien $supp(f)=A$ et $supp(\hat{f})=B$.

2.2) On suppose que $\mathrm{card}A+\mathrm{card}B=p+1$.
On peut trouver une partie C de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ telle que

(2) $\{c\}=B\cap C$ et $\frac{\mathbb{Z}}{p\mathbb{Z}}=B\cup(C-\{c\})$.
Soit $\theta\colon \mathbb{C}^A\to\mathbb{C}^C$ défini par $\theta(g)(y):=\sum_{a\in A} g(a)\,\xi^{xy}$ avec $y\in C$.
Par le corollaire 4, on sait que θ est surjectif, il existe donc $g\in \mathbb{C}^A$ avec $\theta(g)$ qui est la fonction caractéristique de $\{c\}$, i.e. $\theta(g)(y)=0$ si $y\in C-\{c\}$ et $\theta(g)(c)=1$.
Soit $f\colon \frac{\mathbb{Z}}{p\mathbb{Z}}\to\mathbb{C}$ défini par $f(x)=g(x)$ si $x\in A$ et $f(x)=0$ si $x\notin A$.
(3) Facilement, on a $\theta(g)(y)=\hat{f}(y)$ si $y\in C$. Il suit de la définition de f que $\mathrm{supp}(f)\subset A$ et de (2) et (3) que $\mathrm{supp}(\hat{f})\subset B$.
Comme par 1) on a $\mathrm{card}(\mathrm{supp}(f))+\mathrm{card}(\mathrm{supp}(\hat{f}))\geq p+1$, il suit que $\mathrm{supp}(f)=A$ et $\mathrm{supp}(\hat{f})=B$.

Corollaire 5 *Soit p un nombre premier et soit le polynôme $P(X)=\sum_{j=0}^{k} c_j X^{n_j}$ avec $c_j\in\mathbb{C}-\{0\}$, $0\leq n_0<n_1<\ldots<n_k<p$. Alors*

$$\mathrm{card}\{z\in\mathbb{C}\mid z^p=1 \text{ et } P(z)=0\}\leq k\ .$$

Démonstration
Soit toujours $\rho:\mathbb{Z}\to\frac{\mathbb{Z}}{p\mathbb{Z}}$ la surjection canonique. Soit $f:\mathbb{Z}\to\mathbb{C}$ défini par $f(\rho(n_j)):=c_j$ pour $0\leq j\leq k$ et $f(x))=0$ pour $x\in\{\rho(0),\rho(1),\ldots,\rho(p-1)\}-\{\rho(n_0),\rho(n_1),\ldots,\rho(n_k)\}$. Sachant que $c_j\neq 0$, on a $\mathrm{card}(\mathrm{supp}(f))=k-1$. Il suit de la définition de $\hat{f}$ que pour $y\in\frac{\mathbb{Z}}{p\mathbb{Z}}$ on a $\hat{f}(y)=\sum_{x\in\frac{\mathbb{Z}}{p\mathbb{Z}}}\sum_{j=0}^{k} f(x)\ (\xi^x)^y$ avec la convention que ξ^x signifie ξ^z si $\rho(z)=x$. Compte tenu de la définition de f on a

$$\hat{f}(y)=\sum_{j=0}^{k} c_j\,\xi^{(n_j)y}=P(\xi^y)\ .$$

En conséquence $y\notin(\mathrm{supp}(\hat{f})$ si et seulement si $P(\xi^y)=0$. Ainsi

$$\mathrm{card}(supp(\hat{f}))=p-\mathrm{card}\{z\in\mathbb{C}\mid z^p=1 \text{ et } P(z)=0\}\ .$$

Sachant par le théorème 2 que

$$\mathrm{card}(supp(f))+\mathrm{card}(supp(\hat{f}))\geq p+1\ ,$$

on déduit que

(4) $\qquad p-\text{card}(supp(\hat{f}))\leq k$.

ce qui veut bien dire que

$$\text{card}\{z\in\mathbb{C}\mid z^p=1 \ \ et \ \ P(z)=0\}\leq k\ .$$

Facilement le corollaire 5 est équivalent au corollaire 6, ci-après.

Corollaire 6 *Soient* p *un nombre premier, k un entier avec* $1\leq k<p$. Soient $P(X)\in\mathbb{C}[X]-\{0\}$ *un polynôme avec* $P(X)=v_0+v_1X+...+v_{p-1}X^{p-1}$. *Alors*

$$\text{card}\{z\in\mathbb{C}\mid z^p=1 \ \ et \ \ P(z)=0\}\leq \text{card}\{j\in\mathbb{N}\mid o\leq j\leq p-1 \ \text{ et } \ v_j\neq 0\}-1.$$

Remarque Il s'agit de savoir si l'inégalité du corollaire 5 ou 6 est optimale. La réponse est oui.
Soient les entiers $0\leq a_1<a_2<...<a_k<p$ avec $1\leq k\leq p-1$ et
$P(X):=(X-\xi^{a_1})(X-\xi^{a_2})...(X-\xi^{a_k})$ où $\xi\in\mathbb{C}^x$ avec $o(\xi)=p$.
Clairement, on a $\text{card}\{z\in\mathbb{C}\mid z^p=1 \text{ et } P(z)=0\}=k$
Par ailleurs degré $P(X)=k$, si donc $P(X)=v_0+v_1X+...+v_{p-1}X^{p-1}$, on a

$$\text{card}\{j\in\mathbb{N}\mid 0\leq j\leq p-1 \ \text{ et } \ v_j\neq 0\}\leq k+1\ .$$

Il suit alors du corollaire 6 que

$$k\leq \text{card}\{j\in\mathbb{N}\mid 0\leq j\leq p-1 \ \text{ et } \ v_j\neq 0\}-1\ ,$$

ce qui veut dire que

$$v_o\neq 0, v_1\neq 0, ..., v_k\neq 0\ .$$

Ainsi l'inégalité du corollaire 5 ou 6 est optimale pour ce polynôme $P(X)$.

Bibliographie

[D.] **Dieudonné J.** *Une propriété des racines de l'unité* Collection of articles dedicaced to Alberto González on his sixty-fifth birthday. Rev. Un. Mat. Argentina 25 (1970/71), 1-3

[E. I.] **Evans R. J. Isaacs J. M.** *Generalized Vandermonde determinants and roots of unity of prime order* Proc. Amer. Math. Soc. 58 (1976) 51-54

[F.] **Frenkel P.** *Simple proof of Chebotarev's theorem on roots of unity,* preprint AC/0312398v3

[F. 1] **Fresnel J.** *Algèbre des matrices* (Hermann 2011)

[F. 2] **Fresnel J.** *Anneaux* (Hermann 2001)

[H.] **Heineman E. R.** *Generalized Vandermonde determinants* Trans. Amer. Math. Soc. 31 (1929) n° 3, 464-476

[P. S.] **Polyá G. , Szegö G.** *Aufgaben und Lehresätze aus der Analysis, vol. 2 p. 56 et 240* (Berlin (Springer), 1925)

[S. L.] **Stevenhagen P. , Lenstra H. W.** *Chebotarëv and his density theorem* Math. Intelligencer 18 (1996) n° 2 26-37

[T.] **Tao T.** *An uncertainty principle for cyclic groups of prime order* Mathematical Research Letter 12. 121-127 (2005)

p. 252, ligne 4, lire (ex. 87 p. 245 partie 1)

p. 258, ligne 3, lire l'ensemble des idempotents de B .

p. 278, ligne 15,
Montrer que $(d_1!)(d_2!)$ divise $(d_1+d_2)!$ (remarquer que $\frac{(d_1+d_2)!}{(d_1!)(d_2!)}$ n'est

p. 279, ligne -6,
$R(X):=P(z-\lambda X)\in M[X]$, on a donc $R(y)=P(x)=0$. Montrons que

p. 279, ligne-2,
On a donc $1=E(X)A(X)+F(X)B(X)$, $Q(X)=S(X)E(X)$,

p. 282, ligne 2,
impair, $p_i\neq p_j$ *pour* $i\neq j$, $u\geq 0$, $1\geq v_i\geq 0$, $M:=\mathbb{Q}[\cos(\frac{2\pi}{n}),\sin(\frac{2\pi}{n})]$. *Alors les*

p.284 , il faut remplacer les lignes 10 à 20 de 2.3) par ce qui suit.

On suppose *i)* satisfait. On a donc $n=2^u p_1 p_2 \ldots p_s$ avec $p_i=1+2^{\beta_i}$, si p_i est un premier impair. Il s'agit donc de montrer que $\mathbb{Q}[\cos(\frac{2\pi}{n}),\sin(\frac{2\pi}{n})]$ est contenu dans une tour quadratique (réelle) ; ce qui veut dire qu'il existe $s\geq 0$, des corps commutatifs K_i avec $0\leq i\leq s$, $K_0=\mathbb{Q}$,
$K_s=\mathbb{Q}[\cos(\frac{2\pi}{n}),\sin(\frac{2\pi}{n})]$ et $K_i\subset K_{i+1}$ pour $0\leq i\leq s-1$ et $[K_{i+1}:K_i]\leq 2$.
1) De la formule $\cos(a)^2-\frac{\cos(2a)}{2}-\frac{1}{2}=0$, un déduit facilement par récurrence sur u que $\mathbb{Q}[\cos(\frac{2\pi}{2^u})]$ est une tour quadratique et de la formule $(\sin(\frac{2\pi}{2^u}))^2=1-(\cos(\frac{2\pi}{2^u}))^2$, que $\mathbb{Q}[\cos(\frac{2\pi}{2^u}),\sin(\frac{2\pi}{2^u})]$ est une tour quadratique.
2) Si $p_i=1+2^{\beta_i}$, on sait que $\mathbb{Q}[\cos(\frac{2\pi}{p_i})]$ est une tour quadratique (c'est la partie 2.2. du même exercice). Sachant que $(\sin(\frac{2\pi}{p_i}))^2=1-(\cos(\frac{2\pi}{p_i}))^2$, il suit que $\mathbb{Q}[\cos(\frac{2\pi}{p_i}),\sin(\frac{2\pi}{p_i})]$ est une tour quadratique.

3) Facilement $\text{pgcd}(\frac{n}{2^u}, \frac{n}{p_1}, \frac{n}{p_2}, \dots, \frac{n}{p_s}) = 1$, alors il suit de Bézout qu'il existe des entiers $a_0, a_1, a_2, \dots, a_s$ avec $1 = a_0 \frac{n}{2^u} + a_1 \frac{n}{p_1} + a_2 \frac{n}{p_2} + \dots + a_s \frac{n}{p_s}$. Ce qui veut dire que $\frac{2\pi}{n} = a_0 \frac{2\pi}{2^u} + a_1 \frac{2\pi}{p_1} + a_2 \frac{2\pi}{p_2} + \dots + a_s \frac{2\pi}{p_s}$. Il suit des formules trigono-métriques que $\cos(\frac{2\pi}{n})$ (resp. $\sin(\frac{2\pi}{n})$) est une forme polynomiale en $\cos(\frac{2\pi}{2^u}), \cos(\frac{2\pi}{p_1}), \cos(\frac{2\pi}{p_2}), \dots, \cos(\frac{2\pi}{p_s})$, et aussi en $\sin(\frac{2\pi}{2^u}), \sin(\frac{2\pi}{p_1}), \sin(\frac{2\pi}{p_2}), \dots, \sin(\frac{2\pi}{p_s})$. Par suite $\cos(\frac{2\pi}{n})$ et $\sin(\frac{2\pi}{n})$ appartiennent au compositum des tours quadratiques définies en 1) et 2). Sachant qu'un compositum de tours quadratiques est une tour quadratique, il suit que $\mathbb{Q}[\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n})]$ est contenu dans une tour quadratique ; ce qui est *ii)*.

p. 318, ligne -9,
2) Montrons 2. Soient $f := \sum_{n \geq 0} u_n X^n$, $g := \sum_{n \geq 0} v_n X^n$, on a donc

p. 319, ligne-9,
Démonstration Soit $f := \sum_{n \geq 0} u_n X^n$, on a donc $P(X) = 1 + p_1 X + \dots + p_m X^n$

p. 329, ligne 9, lire $a_i = (-1)^i s_i(x_1, x_2, \dots, x_n)$

p. 349, ligne 7, lire $0 \leq i \leq d$,
ligne 13, lire $0 \leq i \leq d$

p. 367, Commentaire sur l'ellipse de Steiner (F.M.1, ex. 126,)

Soit $\mathcal{C} := \{\frac{1}{2} e^{i\theta} \mid 0 \leq \theta < 2\pi\}$, le cercle inscrit au triangle $(1, j, j^2)$
Soit f la bijection affine du $\mathbb{R}$-espace affine $\mathbb{C}$ définie par
(0) $\qquad f(1) = a$, $f(j) = b$, $f(j^2) = c$.
On a donc $f(z) = uz + v\bar{z} + w$, où $u, v, w \in \mathbb{C}$, et comme

$$f(0) = f(\tfrac{1}{3}1 + \tfrac{1}{3}j + \tfrac{1}{3}j^2) = w = \tfrac{1}{3}(a + b + c) ,$$

cela veut dire que
(1) $\qquad 3w = a + b + c$.
En suivant les calculs de F.M. 1, ex. 136 , on a

$$\mathscr{E} := f(\mathscr{C}) = w + \{\frac{1}{2} u e^{i\theta} + \frac{1}{2} v e^{-i\theta} \mid 0 \leq \theta < 2\pi\}.$$

En posant

(2) $$u = \rho_1 e^{i\omega_1}\ ,\ v = \rho_2 e^{i\omega_2}\ ,$$

on a

$$\mathscr{E} := f(\mathscr{C}) = w + e^{i\frac{(w_1+w_2)}{2}} \{\frac{1}{2}\rho_1 e^{i\mu} + \frac{1}{2}\rho_2 e^{-i\mu} \mid 0 \leq \mu < 2\pi\}.$$

Soit $\mathscr{F} := \{\frac{1}{2}\rho_1 e^{i\mu} + \frac{1}{2}\rho_2 e^{-i\mu} \mid 0 \leq \mu < 2\pi\} =$

$$\{\frac{1}{2}(\rho_1+\rho_2)\cos\mu + \frac{i}{2}(\rho_1-\rho_2)\sin\mu \mid 0 \leq \mu < 2\pi\}.$$

Ainsi $\mathscr{F}$ dans le repère cartésien orthonormé $(0;1,i)$ est défini par le polynôme $\frac{X^2}{\alpha^2} + \frac{Y^2}{\beta^2} - 1$ avec $\alpha = \frac{1}{2}(\rho_1+\rho_2)\ ,\beta = \frac{1}{2}(\rho_1-\rho_2)$. Ainsi $\mathscr{F}$ est une ellipse et on sait que les foyers sont $\pm\sqrt{\rho_1\rho_2}$.

Soit $g : \mathbb{C} \to \mathbb{C}$ défini par $g(z) = w + e^{i\frac{(w_1+w_2)}{2}} z$. Alors g est une isométrie (positive) et $\mathscr{E} = g(\mathscr{F})$. Il suit de cela que $\mathscr{E}$ est une ellipse et que les foyers de $\mathscr{E}$ sont $g(\sqrt{\rho_1\rho_2})$ et $g(-\sqrt{\rho_1\rho_2})$; i.e.

(3) $$w + e^{i\frac{(w_1+w_2)}{2}}\sqrt{\rho_1\rho_2})\ ,\ w - e^{i\frac{(w_1+w_2)}{2}}\sqrt{\rho_1\rho_2})\ .$$

Il reste à montrer que ce sont les racines du polynôme dérivé de $P(X) = (X-a)(X-b)(X-c)$. Facilement

(4) $$P'(X) = 3X^2 - 2(a+b+c)X + (ab+ba+ca)\ .$$

On sait par (0) que

(5) $$a = u+v+w\ ,\ b = uj+vj^2+w,\ \ c = uj^2+vj+w$$

Par (1) on a

$$3w = a+b+c\ .$$

Ensuite

$$(a+b+c)^2 = (a^2+b^2+c^2) + 2(ab+bc+ca)$$

et donc compte tenu de (5) , on a

(6) $$ab+bc+ca = \frac{1}{2}((3w)^2 - (a^2+b^2+c^2))\ .$$

Or

$$a^2 = (u+v+w)^2 = u^2+v^2+w^2+2(uv+vw+wu)\ ,$$
$$b^2 = (ju+j^2v+w)^2 = j^2u^2+jv^2+w^2+2(uv+j^2vw+jwu)\ ,$$
$$c^2 = j^2u+jv+w)^2 = ju^2+j^2v^2+w^2+2(uv+jvw+j^2wu)\ .$$

Ainsi par addition, on a

(7) $$a^2+b^2+c^2 = 3w^2+6uv\ .$$

Il suit alors de (6) que

(8) $$ab+bc+ca = 3w^2-3uv\ .$$

Cela permet d'écrire $P'(X)$ sous la forme

(9) $$P'(X)=3X^2-6wX+(3w^2-3uv)\ .$$

Or, on sait par (2) que

(10) $$uv=\rho_1\rho_2 e^{i(w_1+w_2)}$$

Facilement

$$P'(X)=3\,(X-(w+e^{i\,\frac{(w_1+w_2)}{2}}\sqrt{\rho_1\rho_2}))(X-(w-e^{i\,\frac{(w_1+w_2)}{2}}\sqrt{\rho_1\rho_2})).$$

Ce qui montre bien que

(11) $$w+e^{i\,\frac{(w_1+w_2)}{2}}\sqrt{\rho_1\rho_2}\ \text{ et }\ w-e^{i\,\frac{(w_1+w_2)}{2}}\sqrt{\rho_1\rho_2}$$

sont les foyers de $\mathscr{C}$.

p. 376, ex. 131

Une formule sur le dénombrement, élémentaire et souvent utilisée (en particulier pour la démonstration p.379).

1. Soient A,B deux ensembles, $f:A\to B$ une application.
Alors on a

(1) $$A=\underset{b\in B}{\cup} f^{-1}(\{b\})\ .$$

2. Si en plus de l'hypothèse 1. , l'ensemble A est fini, on a

(2) $$\mathrm{card}A:\sum_{b\in B}\mathrm{card}\,f^{-1}(\{b\})$$

(dans cette formule le nombre de $b\in B$ avec $f^{-1}(\{b\})\neq\phi$ est fini).

3. Un cas particulièrement intéressant est le suivant.
Si en plus des hypothèses 1. et 2. , on suppose qu'il existe un entier β tel que pour tout $b\in B$, on a $\beta=\mathrm{card}\,(\mathrm{f}^{-1}(\{b\})$, alors

(3) $$\mathrm{card}A=\beta\times\mathrm{card}\,B\ .$$

p. 436, ligne 9

peut supposer que $0\in I$, $1\in J$. Sachant que $a_i-o=de+w_i$ avec $w_i\in W$