le 23/11/2018, Compléments et errata à

Algèbre et géométrie

81 thèmes pour l'Agrégation de mathématiques

Jean Fresnel & Michel Matignon

p. 44, ligne 8, remplacer cette ligne par la suivante.

sance du stabilisateur de $DQ(\sigma)$ *dans les cas de la décomposition* $LDQ(\sigma)U$ *que le stabilisa-*

p. 80, paragraphe I.8.

1. Actualité des résultats sur $\mathbb{R}$

Si V est un sous-espace vectoriel de $M_n(\mathbb{R})$ tel que $V-\{0\}\subset G\ell_n(\mathbb{R})$, alors on sait que le maximum possible pour la dimension de V est le nombre de Hurwitz-Radon défini comme il suit.

Si $n=2^{4a+b}(2m+1)$ avec a,b,m entiers $a\geq 0$, $0\leq b\leq 3$, alors

$$\rho(n):=8a+2^b\ .$$

L'existence de sous-espaces vectoriels V de $M_n(\mathbb{R})$ tels que $V-\{0\}\subset G\ell_n(\mathbb{R})$, est associé à l'existence d'algèbres de Clifford qui sont des algèbres d'endomorphismes d'espaces vectoriels sur $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, i.e. les réels, les complexes, les quaternions. Si bien qu'on obtient des dimensions un peu supérieures à celles obtenues en 4. à 11. ([P] p. 272 à 273).

Pour une construction plus élémentaire de ces espaces vectoriels, on peut consulter [A. T.] .

Le problème de la borne maximum de la dimension des espaces vectoriels V a été résolu en 1962 par un article de **J. F. Adams** concernant les champs de vecteurs tangents à la sphère ([A]).

[A] **Adams J. F.** *Vector fields on spheres* Annals of Math. 75 (1962) 603-632

[A. T.] **Antetomaso R. & Tissier A.** *Quel est le maxumum de la dimension d'un sous-espace vectoriel de $M(n,\mathbb{R})$ dont tout élément non nul est inversible ?*, RMS 127-4 (2016-2017) 11-15

[P] **Porteous I. R.** *Topological Geometry* 1969 Van Nostrand Reinhold company

[A. T.] **Antetomaso R. & Tissier A.** *Quel est le maxumum de la dimension d'un sous-espace vectoriel de $M(n,\mathbb{R})$ dont tout élément non nul est inversible ?*, RMS 127-4 (2016-2017) 11-15

[P] **Porteous I. R.** *Topological Geometry* 1969 Van Nostrand Reinhold company

2. Une question plus générale

Soient K un corps commutatif, $n \geq 1$, $1 \leq k \leq n$, V est un sous-espace vectoriel de $M_n(K)$ tel que tout élément de $V-\{0\}$ est de rang supérieur ou égal à k . Alors que peut-on dire de la dimension de V ?

Facilement, on a $\dim V \leq n(n-k+1)$.

En effet, soit $\rho : V \to M_{n-k+1,n}(K)$ définie par $\rho([m_{i,j}]) := \begin{bmatrix} m_{1,1} & m_{1,2} & \cdot & m_{1,n} \\ m_{2,1} & m_{2,1} & \cdot & m_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ m_{n-k+1,1} & \cdot & \cdot & m_{n-k+1,n} \end{bmatrix}$. Si on avait $\dim V > n(n-k+1)$, on aurait alors $\ker \rho \neq \{0\}$; cela veut dire que V contiendrait une matrice non nulle de rang strictement plus petit que k , ce qui est une contradiction.

Remarque 1. On peut considérer le même type de questions en remplaçant sous-espace vectoriel V de $M_n(K)$ par sous-espace vectoriel V de $M_{n,p}(K)$.

Remarque 2. On peut considérer le même type de questions en remplaçant sous-espace vectoriel V par sous-espace affine E de $M_n(K)$.
Dans ce cas les résultats sont plus simples parce qu'ils ne dépendent pas essentiellement de la nature du corps commutatif K (voir [S]).

[S] **de Seguins Pazzis C.** *Large affine spaces of matrices with rank bounded below* Linear Algebra Appl. 437 (2012) 499-512

p. 121 complément à III.1.

Les sous-groupes de $\frac{\mathbb{Q}}{\mathbb{Z}}$

Définition Dans tout ce complément *groupe cyclique* signifie groupe engendré par un élément d'ordre fini.

I. Le groupe $\frac{\mathbb{Q}}{\mathbb{Z}}$

Proposition 0 *Soient* $\rho:\mathbb{Q}\to\frac{\mathbb{Q}}{\mathbb{Z}}$ *la surjection canonique,* $a\geq 1$ *un entier. Alors* $\frac{\mathbb{Q}}{\mathbb{Z}}$ *contient un unique sous-groupe d'ordre* a *, c'est* $\rho(\frac{1}{a}\mathbb{Z})$*; il est cyclique engendré par* $\rho(\frac{1}{a})$.

Démonstration
Il est immédiat que $\rho(\frac{1}{a}\mathbb{Z})$ est un sous-groupe cyclique de $\frac{\mathbb{Q}}{\mathbb{Z}}$ engendré par $\rho(\frac{1}{a})$. Soient maintenant un sous-groupe G de $\frac{\mathbb{Q}}{\mathbb{Z}}$, avec $o(G)=a$. Soit donc $\rho(x)\in G$ avec $x\in\mathbb{Q}$, on a $a\rho(x)=\rho(0)$, ce qui veut dire que $a\,x\in\mathbb{Z}$, ainsi $x\in\frac{1}{a}\mathbb{Z}$. Il suit de cela que $\rho(x)\in\rho(\frac{1}{a}\mathbb{Z})$, donc $G\subset\rho(\frac{1}{a}\mathbb{Z})$ et comme $o(G)=o(\rho(\frac{1}{a}\mathbb{Z}))$, on a bien $G=\rho(\frac{1}{a}\mathbb{Z})$.

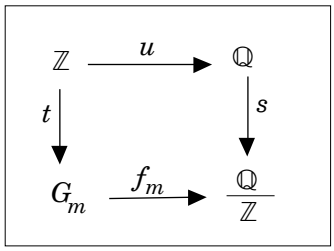
Proposition 1 *Soit G un groupe abélien (noté additivement). Alors les propriétés suivantes sont équivalentes.*
i) Le groupe G est de torsion (i.e. *tout élément de G est d'ordre fini*) *et tout sous-groupe fini de G est cyclique,*
ii) Le groupe G est une réunion croissante de sous-groupes cycliques,
i.e. *il existe une suite $(G_m)_{m\geq 1}$ de sous-groupes cycliques avec $G_m \subset G_{m+1}$ pour tout $m \geq 1$ et $G = \bigcup_{m\geq 1} G_m$,*
iii) le groupe G est isomorphe à un sous-groupe de $\frac{\mathbb{Q}}{\mathbb{Z}}$.

Démonstration
1) Montrons *ii)* implique *i)*.
Comme $G = \bigcup_{m\geq 1} G_m$, il suit que tout élément de G est d'ordre fini.
Soit K un sous-groupe fini de G. Comme $G = \bigcup_{m\geq 1} G_m$ et que la réunion est croissante, il existe m avec $K \subset G_m$, sachant que G_m est cyclique, il suit que K est cyclique. Ainsi *i)* est satisfait.

2) Montrons *i)* implique *ii)*.
Soient $m \geq 1$ et $G_m := \{x \in G \mid o(x) \mid m!\}$. Facilement G_m est un sous-groupe de G. Soit $y \in G_m$ d'ordre maximum, il s'agit de montrer que G_m est engendré par y ; soit $d := o(y)$. Soit donc $y\mathbb{Z}$ le sous-groupe de G_m engendré par y et $\rho : G_m \to \frac{G_m}{y\mathbb{Z}}$ la surjection canonique. Soit $x \in G_m$, soit $d_1 := o(x)$, $d_2 := o(\rho(x))$; on a donc $d_1 \leq d$ et $d_2 \mid d_1$. Par ailleurs, il existe $\alpha \in \mathbb{Z}$ avec $d_2 x = \alpha y$.
Par le lemme 3, ci-après, on sait qu'il existe $u, v \in \mathbb{Z}$ tels que $o(ux + vy) = \text{ppcm}(o(x), o(y)) = \text{ppcm}(d_1, d)$. Or $\text{ppcm}(o(x), o(y)) \mid m!$, ainsi $ux + vy \in G_m$. Par définition de y, on a $\text{ppcm}(d_1, d) \leq d$, ce qui montre que $d_1 \mid d$.

Montrons qu'il existe $\lambda\in\mathbb{Z}$ tel que $d_2(x+\lambda y)=0$, i.e. $\alpha y+d_2\lambda y=0$. Il suffit donc de trouver $\lambda\in\mathbb{Z}$ tel que $\alpha+d_2\lambda=0$. On a les relations $d_2 x=\alpha y$ et $d_1 x=0$; ainsi $\frac{d_1}{d_2}(d_2 x)=0$, i.e. $\frac{d_1}{d_2}(\alpha y)=0$ ce qui veut dire qu'il existe $\theta\in\mathbb{Z}$ tel que $\frac{d_1}{d_2}\alpha=\theta d$. Ainsi $\alpha=d_2(\frac{d}{d_1})\theta$, il suit de cela que $\alpha+d_2\lambda=d_2(\frac{d}{d_1}\theta+\lambda)$. Il suffit de choisir $\lambda=-\frac{d}{d_1}\theta$.
Soit $z=x-\frac{d}{d_1}\theta y$, on a $d_2 z=0$, $\rho(z)=\rho(x)$ et $o(\rho(x))=d_2$, il suit de cela que $o(z)=d_2$. On a alors $\mathbb{Z}y+\mathbb{Z}z=\mathbb{Z}y\oplus\mathbb{Z}z$, en effet si $\lambda y+\mu z=0$, en appliquant ρ on a $\mu\rho(z)=0$ et donc $d_2\mid\mu$, comme $o(z)=d_2$, il suit que $\mu z=0$ et donc aussi $\lambda y=0$.
Ainsi le groupe $\mathbb{Z}y\oplus\mathbb{Z}z$ est d'ordre $d\,d_2$; par ailleurs il suit de *i*) que le groupe $\mathbb{Z}y\oplus\mathbb{Z}z$ est cyclique, ainsi il contient un élément d'ordre $d\,d_2$. Sachant que d est le maximum des ordres des éléments de G_m , il suit que $d_2=1$ et donc $x\in y\mathbb{Z}$.
On a donc montré que G_m est cyclique. Facilement $G_m\subset G_{m+1}$ et $G=\bigcup_{m\geq 1}G_m$. Ce qui est *ii*).

3) On suppose *ii*) satisfait, il s'agit de montrer *iii*).
3.1) Ainsi il existe une famille de sous-groupes cycliques $(G_m)_{m\geq 1}$ avec $o(G_m)=d_m$ et $G_m\subset G_{m+1}$ pour tout $m\geq 1$.
Il suit du lemme 2 ci-après, par récurrence sur m qu'il existe une suite $(x_m)_m$ avec x_m est génétateur de G_m et $\frac{d_{m+1}}{d_m}x_{m+1}=x_m$ pour tout $m\geq 1$.
3.2) Soit $m\geq 1$ et soit le diagramme ci-contre où $u:\mathbb{Z}\to\mathbb{Q}$ est défini par $u(z):=\frac{z}{d_m}$, $t:\mathbb{Z}\to G_m$ esr défini par $t(z)=z\,x_m$ et enfin $s:\mathbb{Q}\to\frac{\mathbb{Q}}{\mathbb{Z}}$ est la surjection canonique.



Facilement, on a $\ker s\,u = \ker t = d_m\,\mathbb{Z}$; ainsi il existe un homomorphisme injectif $f_m : G_m \to \frac{\mathbb{Q}}{\mathbb{Z}}$ tel que $f_m\,t = s\,u$, ainsi $f_m(z\,x_m) = s(\frac{z}{d_m})$.

Facilement $f_{m+1}|_{G_m} = f_m$ et de façon plus générale, si $m' \geq m$, on a $f_{m'}|_{G_m} = f_m$.

3.3) Alors 3.2) montre qu'il existe un unique homomorphisme $f : G \to \frac{\mathbb{Q}}{\mathbb{Z}}$ tel que $f|_{G_m} = f_m$ pour tout $m \geq 1$.

Ce qui est *iii*).

4) Montrons *iii*) implique *ii*).

4.1) Montrons d'abord que $\frac{\mathbb{Q}}{\mathbb{Z}}$ est réunion croissante de sous-groupes cycliques.

Soient $m \geq 1$, $L_m := s(\frac{1}{m!}\mathbb{Z})$; facilement L_m est cyclique d'ordre $m!$, engendré par $s(\frac{1}{m!})$. Tout aussi facilement on a $L_m \subset L_{m+1}$ pour tout $m \geq 1$ et $\frac{\mathbb{Q}}{\mathbb{Z}} = \bigcup_{m \geq 1} L_m$.

4.2) Soient maintenant H un sous-groupe de $\frac{\mathbb{Q}}{\mathbb{Z}}$ et $H_m := H \cap L_m$, alors H_m est cyclique et $H = \bigcup_{m \geq 1} H_m$.

Si donc G est isomorphe à H , il suit bien que G est une réunion croissante de sous-groupes cycliques de G , ce qui veut dire que *ii*) est satisfait.

2. Sur la décomposition en *p*-composantes des sous-groupes de $\frac{\mathbb{Q}}{\mathbb{Z}}$.

Proposition 2 *Soit* $s : \mathbb{Q} \to \frac{\mathbb{Q}}{\mathbb{Z}}$ *la surjection canonique. Soit* $p \geq 2$ *un nombre premier,* K_p *le sous-groupe de* $\frac{\mathbb{Q}}{\mathbb{Z}}$ *constitué des éléments qui sont d'ordre une puissance de* p .

1. *Alors* $K_p = s(\mathbb{Z}[\frac{1}{p}]) \simeq \frac{\mathbb{Z}[\frac{1}{p}]}{\mathbb{Z}}$ *où* $\mathbb{Z}[\frac{1}{p}]$ *est le sous-groupe de* $\mathbb{Q}$ *constitué des fractions dont le dénominateur est une puissance de* p *. En particulier les sous-groupes de* K_p *sont* $\{0\}$, K_p , $s(\frac{1}{p^m}\mathbb{Z})$ *pour* $m \geq 1$; $s(\frac{1}{p^m}\mathbb{Z})$ *est le seul sous-groupe de* K_p *qui est d'ordre* p^m *et* K_p *est le seul sous-groupe de* K_p *qui n'est pas fini.*
Si $\mathcal{P}$ *désigne l'ensemble des nombres premiers* $p \geq 2$ *, alors on a*

$$\frac{\mathbb{Q}}{\mathbb{Z}} = \bigoplus_{p \in \mathcal{P}} K_p .$$

2. *Soit* H *un sous-groupe de* $\frac{\mathbb{Q}}{\mathbb{Z}}$, $p \geq 2$ *un nombre premier,* H_p *le sous-groupe des éléments de* H *qui sont d'ordre une puissance de* p *. Alors* $H = \bigoplus_{p \in \mathcal{P}} H_p$ *et* $H_p = H \cap K_p$ *. On sait par* **1.** *que* H_p *est un groupe cyclique d'ordre une puissance de* p *ou* $H_p = K_p$ *.*

Démonstration

1) Montrons **1.**

1.1) Il est immédiat que $s(\frac{1}{p^m}\mathbb{Z})$ est le groupe cyclique d'ordre p^m , engendré par $s(\frac{1}{p^m})$. Soit $G \neq \{0\}$ un sous-groupe fini de K_p , on a donc

$$G = \{s(\frac{a_i}{p^{n_i}}) \mid p \nmid a_i , 1 \leq i \leq r , n_1 \leq n_2 \leq \ldots \leq n_r\} \cup \{s(0)\} .$$

Par Bézout, il existe $\lambda , \mu \in \mathbb{Z}$ avec $1 = \lambda a_r + \mu p^{n_r}$; ainsi $s(\frac{1}{p^{n_r}}) = s(\lambda \frac{a_r}{p^{n_r}}) + s(\mu) \in G$, comme $s(\mu) = 0$, on a $s(\frac{1}{p^{n_r}}) \in G$. Il suit facilement de cela que $s(\frac{1}{p^{n_r}}\mathbb{Z}\}) \subset G$, l'autre inclusion est immédiate puisque $n_i \leq n_r$.

1.2) Soit G un sous-groupe infini de K_p , on a donc une suite $(s(\frac{a_i}{p^{n_i}}))_i$ avec $p \nmid a_i$ et $\lim_{i \to \infty} n_i = \infty$. Il s'agit de montrer que

$K_p \subset G$. Soit $s(\frac{a}{p^m}) \in K_p$, il existe r tel que $n_r \geq m$. Comme en 1.1) on déduit que $s(\frac{1}{p^{n_r}}) \in G$ et donc $s(\frac{a}{p^m}) = s(a\, p^{n_r - m} \frac{1}{p^{n_r}}) \in G$; cela montre bien que $K_p \subset G$ et donc que $K_p = G$.

1.3) Il reste à montrer que $\frac{\mathbb{Q}}{\mathbb{Z}} = \bigoplus_{p \in \mathcal{P}} K_p$. Clairement on a $\sum_{p \in \mathcal{P}} K_p \subset \frac{\mathbb{Q}}{\mathbb{Z}}$.

Soit $s(\frac{a}{N}) \in \frac{\mathbb{Q}}{\mathbb{Z}}$, si $N = \pm 1$, alors $s(\frac{a}{N}) = s(0) \in \sum_{p \in \mathcal{P}} K_p$. Si $N \neq \pm 1$, alors $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ où les p_i sont des premiers positifs distincts et $\alpha_i > 0$ pour $1 \leq i \leq r$. Soit $q_i := \frac{N}{p_i^{\alpha_i}}$, facilement $1 = \mathrm{pgcd}(q_1, q_2, \ldots, q_r)$, alors par Bézout, il existe $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ tels que $a = a_1 q_1 + a_2 q_2 + \ldots + a_r q_r$. Ainsi $\frac{a}{N} = a_1 \frac{q_1}{N} + a_2 \frac{q_2}{N} + \ldots + a_r \frac{q_r}{N}$, il suit de la définition de q_i que $p_i^{\alpha_i} \frac{q_i}{N} = 1$ et donc que $p_i^{\alpha_i}\, s(a_i \frac{q_i}{N}) = s(0)$, ce qui montre que $s(\frac{a}{N}) \in K_{p_1} + K_{p_2} + \ldots + K_{p_r}$. On a donc $\frac{\mathbb{Q}}{\mathbb{Z}} = \sum_{p \in \mathcal{P}} K_p$, il reste à montrer que la somme est directe.

Soit donc $0 = x_1 + x_2 + \ldots + x_r$ avec $p_i^{\beta_i} x_i = 0$. Comme $1 = \mathrm{pgcd}(p_1^{\beta_1}, p_2^{\beta_2} p_3^{\beta_3} \ldots p_r^{\beta_r})$, par Bézout, il existe $u, v \in \mathbb{Z}$ avec $1 = u\, p_1^{\beta_1} + v\, p_2^{\beta_2} p_3^{\beta_3} \ldots p_r^{\beta_r}$; il suit de cela que $0 = (1 - u\, p_1^{\beta_1})\, x_1 + v\, p_2^{\beta_2} p_3^{\beta_3} \ldots p_r^{\beta_r} (x_2 + x_3 + \ldots + x_r)$, i.e. $0 = x_1$. On montre de même que $0 = x_i$ pour $2 \leq i \leq r$. Ainsi la somme est directe.

2) La démonstration de **2.** est immédiate.

3. Application au sous-groupe de torsion du groupe multiplicatif d'un corps commutatif.

Proposition 3 *Soit* K *un corps commutatif,* $K^\times = K - \{0\}$ *le groupe des inversibles de* K *et* $(K^\times)_{tor}$ *, le sous-groupe de torsion de* $K^\times$, i.e. *le sous-groupe de* $K^\times$ *constitué des éléments de* $K^\times$ *qui sont d'ordre fini.*

1. *Soit* $m \in \mathbb{N}$, $m \geq 1$, $G_m := \{x \in K \mid x^{m!} = 1\}$ *où* $m! := 1.2.\ldots.m$. *Alors on a*

$$(K^\times)_{tor} = \bigcup_{m \geq 1} G_m .$$

Il suit du lemme 1 ci-après que G_m *est cyclique. Il suit alors de la proposition1 que* $(K^\times)_{tor}$ *est isomorphe à un sous-groupe de* $\frac{\mathbb{Q}}{\mathbb{Z}}$.

2. *Soit* $p \geq 2$ *un nombre premier* $(K^\times)_{tor,p}$ *le sous-groupe des éléments* x *de* $(K^\times)_{tor}$ *pour lesquels il existe un entier* n_x *tel que* $x^{p^{n_x}} = 1$, i.e. $(K^\times)_{tor,p}$ *est constitué des éléments de* $(K^\times)_{tor}$ *qui sont d'ordre une puissance de* p . *Il suit de la proposition 2 que* $(K^\times)_{tor,p}$ *est soit un groupe cyclique d'ordre une puissance de* p , *soit isomorphe à* $\frac{\mathbb{Z}[\frac{1}{p}]}{\mathbb{Z}}$ *où* $\mathbb{Z}[\frac{1}{p}]$ *est le sous-groupe de* $\mathbb{Q}$ *constitué des fractions dont le dénominateur est une puissance de* p .

Enfin il résulte de la proposition 2 que $(K^\times)_{tor} = \bigoplus_{p \in \mathcal{P}} (K^\times)_{tor,p}$ *où* $\mathcal{P}$ *est l'ensemble des premiers* $p \geq 2$ *de* $\mathbb{Z}$.

3. *Si* K *est un corps commutatif de caractéristique nulle qui contient toutes les racines de l'unité (par exemple* $\mathbb{C}$*), alors* $(K^\times)_{tor}$ *est isomorphe à* $\frac{\mathbb{Q}}{\mathbb{Z}}$.

Si K *est un corps commutatif de caractéristique* q *qui contient toutes les racines de l'unité, ce qui veut dire que* K *contient* $(\mathbb{F}_q)^{alg}$ *, la clôture algébrique de* $\mathbb{F}_q \simeq \frac{\mathbb{Z}}{q\mathbb{Z}}$. *Alors* $(K^\times)_{tor} \simeq \bigoplus_{p \in \mathcal{P} - \{q\}} \frac{\mathbb{Z}[\frac{1}{p}]}{\mathbb{Z}}$.

Démonstration C'est une conséquence immédiate des propositions 1 et 2.

4. Application au sous-groupe de torsion de $SO_2(\mathbb{R})$ et de $O_2(\mathbb{R})$.

Proposition 4

1. ([Fr. B.C.D.] proposition 4.1.1. p. 76, proposition 4.1.4. p. 78)

On rappelle que $SO_2(\mathbb{R}) := \{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in G\ell_2(\mathbb{R}) \mid a^2+b^2=1 \}$ *et que* $SO_2(\mathbb{R})$ *est un groupe abélien. On sait que l'application* $\rho : \mathbb{R} \to SO_2(\mathbb{R})$ *définie par* $\rho(\theta) := \begin{bmatrix} \cos(2\pi\theta) & -\sin(2\pi\theta) \\ \sin(2\pi\theta) & \cos(2\pi\theta) \end{bmatrix}$ *est un homomorphisme surjectif du groupe* $(\mathbb{R},+)$ *sur le groupe* $SO_2(\mathbb{R})$ *dont le noyau est* $\mathbb{Z}$ *. Ainsi* ρ *induit un isomorphisme de* $\frac{\mathbb{R}}{\mathbb{Z}}$ *sur* $SO_2(\mathbb{R})$ *.*

De même ρ *induit un isomorphisme de* $\frac{\mathbb{Q}}{\mathbb{Z}}$ *sur* $(SO_2(\mathbb{R}))_{tor}$ *où* $(SO_2(\mathbb{R}))_{tor}$ *est le sous-groupe de torsion de* $SO_2(\mathbb{R})$ *.*

On rappelle que $O_2(\mathbb{R}) = SO_2(\mathbb{R}) \cup \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} SO_2(\mathbb{R})$ *.*

Plus généralement, si $B \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ *, on a* $o(B)=2$ *et* $O_2(\mathbb{R}) = SO_2(\mathbb{R}) \cup (B)\, SO_2(\mathbb{R})$ *, et si* $A \in SO_2(\mathbb{R})$ *, on a* $BAB^{-1}=A^{-1}$ *.*

1. *Soit* H *un sous-groupe de* $SO_2(\mathbb{R})$ *qui est de torsion,* i.e. *un sous-groupe de* $SO_2(\mathbb{R})$ *constitué d'éléments qui sont d'ordre fini.*

Soit $m \in \mathbb{N}$ *,* $m \geq 1$*,* $H_m := \{A \in H \mid A^{m!} = I_2\}$ *où* $m! := 1.2.\ldots.m$ *.*

On sait que H_m *est fini et que c'est l'unique sous-groupe cyclique de* $SO_2(\mathbb{R})$ *, d'ordre* $o(H_m)$ *, il est engendré par la rotation de mesure d'angle* $\frac{2\pi}{o(H_m)}$ ([Fr B,C,D] ex. 10.39 p. 155).

Alors on a $H_m \subset H_{m+1}$ *pour tout* $m \geq 1$ *et*

$$H = \bigcup_{m \geq 1} H_m .$$

C'est une illustration de la propostion 1.

2. *Soit* $p \geq 2$ *un nombre premier* $H_{(p)}$ *le sous-groupe des éléments* A *de* H *pour lesquels il existe un entier* n_x *tel que* $A^{p^{n_x}} = I_2$, i.e. $H_{(p)}$ *est constitué des éléments de* H *qui sont d'ordre une puissance de* p . *Il suit de la proposition 2 que* $H_{(p)}$ *est soit un groupe cyclique d'ordre une puissance de* p , *soit isomorphe à* $\frac{\mathbb{Z}[\frac{1}{p}]}{\mathbb{Z}}$

où $\mathbb{Z}[\frac{1}{p}]$ *est le sous-groupe de* $\mathbb{Q}$ *constitué des fractions dont le dénominateur est une puissance de* p .

Enfin il résulte de la proposition 2 que $H = \bigoplus_{p \in \mathcal{P}} H_{(p)}$ *où* $\mathcal{P}$ *est l'ensemble des premiers* $p \geq 2$ *de* $\mathbb{Z}$.

3. *Soit* G *un sous-groupe de* $O_2(\mathbb{R})$ *qui est de torsion,* i.e. *un sous-groupe de* $O_2(\mathbb{R})$ *constitué d'éléments qui sont d'ordre fini. Soit* $H := G \cap SO_2(\mathbb{R})$, *on suppose que* $H \neq G$. *Soit* $\sigma \in G - H$, *alors on sait que* $o(\sigma) = 2$ *et que* $G = H \cup \sigma H$.

Soit $m \in \mathbb{N}$, $m \geq 1$, $H_m := \{A \in H \mid A^{m!} = I_2\}$ *où* $m! := 1.2 \ldots m$.

On sait que H_m *est fini et que c'est l'unique sous-groupe cyclique de* $SO_2(\mathbb{R})$, *d'ordre* $o(H_m)$, *il est engendré par la rotation de mesure d'angle* $\frac{2\pi}{o(H_m)}$ ([Fr B,C,D] ex. 10.39 p. 155).

Soit $G_m = H_m \cup \sigma H_m$, *alors* G_m *est un groupe fini avec* $o(G_m) = 2\,o(H_m)$ ([Fr. B,C,D] ex. 10.39 p. 155).

Plus précisément G_m *est un groupe diédral, d'ordre* $2\,o(H_m)$ *et on a* $G_m \subset G_{m+1}$ *pour tout* $m \geq 1$ *et*

$$G = \bigcup_{m \geq 1} G_m .$$

On rappelle ([Fr E] p. 41) *que si* $n \geq 1$, *alors il existe un et un seul groupe, à isomorphisme près, engendré par deux éléments* τ , σ *avec* $\tau \neq \sigma$, $o(\tau) = n$, $o(\sigma) = 2$ *et* $\sigma\,\tau\,\sigma^{-1} = \tau^{-1}$. *Ce groupe est réalisé par le sous-groupe suivant de* $O_2(\mathbb{R})$,

$$\mathfrak{D}_n := \left\{ \begin{bmatrix} \cos 2\pi\frac{k}{n} & -\sin 2\pi\frac{k}{n} \\ \sin 2\pi\frac{k}{n} & \cos 2\pi\frac{k}{n} \end{bmatrix}, \begin{bmatrix} \cos 2\pi\frac{k}{n} & \sin 2\pi\frac{k}{n} \\ \sin 2\pi\frac{k}{n} & -\cos 2\pi\frac{k}{n} \end{bmatrix}, 0 \le k < n \right\}.$$

Soient

$t := \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}$, $s := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, *alors* $o(t) = n$, $o(s) = 2$,

$s\,t\,s^{-1} = t^{-1}$.

Un tel groupe s'appelle le groupe *diédral* d'ordre $2n$.

4. *Soit G un sous-groupe de $O_2(\mathbb{R})$ qui est de torsion,* i.e. *un sous-groupe de $O_2(\mathbb{R})$ constitué d'éléments qui sont d'ordre fini. Soit $H := G \cap SO_2(\mathbb{R})$, on suppose que $H \neq G$. Soit $\sigma \in G - H$, alors on sait que $o(\sigma) = 2$ et que $G = H \cup \sigma H$.*

Soit $p \geq 2$ un nombre premier $(G)_{(p)}$ le sous-ensemble des éléments A de G pour lesquels il existe un entier n_x tel que $A^{p^{n_x}} = 1$, i.e. *$(G)_{(p)}$ est constitué des éléments de G qui sont d'ordre une puissance de p . Si $p \geq 3$ on a $(G)_{(p)} = (H)_{(p)}$ et $G_{(2)} = H_{(2)} \cup \sigma H_{(2)}$. En particulier $(G)_{(p)}$ est un sous-groupe de G pour tout nombre premier p.*

Remarque 1 Soit $B \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$, alors $SO_2(\mathbb{R})_{tor} \cup (B)\, SO_2(\mathbb{R})$ est l'ensemble des éléments de torsion de $O_2(\mathbb{R})$; en particulier cet ensemble n'est pas un sous-groupe de $O_2(\mathbb{R})$. Par ailleurs les sous-groupes de torsion maximaux de $O_2(\mathbb{R})$ sont les groupes de la forme $SO_2(\mathbb{R})_{tor} \cup (B)\, SO_2(\mathbb{R})_{tor}$ où $B \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$.

Remarque 2 Si G un groupe, p un nombre premier et $G_{(p)}$ le sous-ensemble des éléments de G qui sont d'ordre une puissance de p . Si G est abélien, alors $G_{(p)}$ est un sous-groupe de G , mais si n'est pas abélien $G_{(p)}$ peut ne pas être un sous-groupe de G .

Démonstration C'est en partie une conséquence immédiate des propositions 1 et 2.

Lemme 1 *Soit K un corps commutatif, G un sous-groupe fini du groupe $K^{\times}=K-\{0\}$ des inversibles de K. Alors G est cyclique.*

Démonstration C'est le corollaire p. 123 de cet ouvrage.

Lemme 2 *Soient $A\subset B$ deux groupes cycliques (notés additivement) avec $o(A)=a$, $o(B)=b=ac$. Soit $x\in A$ avec $o(x)=a$. Alors il existe $y\in B$ avec $o(y)=b$ et $cy=x$. Ainsi l'application $y\mapsto cx$ de l'ensemble des générateurs de B dans l'ensemble des générateurs de A est surjective.*

Démonstration
1) On considère d'abord le cas particulier suivant. Soient $U\subset V$ deux groupes cycliques (notés additivement) avec $o(U)=u$, $o(V)=v=up$ où p est un nombre premier. Soit $x\in U$ avec $o(x)=u$. Alors on veut montrer qu' il existe $y\in V$ avec $o(y)=v$ et $py=x$.
En effet il existe $z\in V$ avec $o(z)=v=up$, il suit facilement de cela que $o(pz)=u$; ainsi il existe $\alpha\in\mathbb{Z}$ avec $1=\mathrm{pgcd}(\alpha,u)$ et $pz=\alpha x$.
Supposons $1=\mathrm{pgcd}(\alpha,up)$. Il existe donc $\gamma\in\mathbb{Z}$ tel que $\alpha\gamma\equiv 1 \,\mathrm{modulo}\,(up\mathbb{Z})$; ainsi $1=\mathrm{pgcd}(\gamma,up)$ et donc $o(\gamma z)=up$; de plus $p(\gamma z)=x$. Ainsi $y:=\gamma z$ convient.
Supposons $1\neq\mathrm{pgcd}(\alpha,up)$, sachant que $1=\mathrm{pgcd}(\alpha,u)$ cela veut dire que $p\mid\alpha$ et donc $p\nmid u$. Il suit de cela que sachant que $1=\mathrm{pgcd}(\alpha,u)$, cela veut dire que $1=\mathrm{pgcd}(\alpha+u,up)$.
Il existe donc $\gamma\in\mathbb{Z}$ tel que $(\alpha+u)\gamma\equiv 1 \,\mathrm{modulo}\,(up\mathbb{Z})$; ainsi $1=\mathrm{pgcd}(\gamma,up)$; par ailleurs $pz=\alpha x$ implique facilement $pz=(\alpha+u)x$, donc $p(\gamma z)=x$, il suit que $o(\gamma z)=up$ et donc que $y:=\gamma z$ convient.

2) Traitons maintenant le cas général.
On a donc $c=p_1p_2...p_r$ ou les p_i sont des nombres premiers. On sait que si C est un groupe cyclique d'ordre n, pour tout diviseur d de n il existe un et un seul sous-groupe de C qui est d'ordre d. Il suit de cela qu'il existe des sous-groupes cycliques de B, $C_0, C_1, ..., C_r$ avec $C_i \subset C_{i+1}$ pour $0 \leq i < r$, $C_0 = A$, $C_r = B$, $o(C_{i+1}) = p_{i+1} o(C_i)$ pour $0 \leq i < r$.
La partie 1) dit qu'il existe $y_1 \in C_1$ avec $o(y_1) = p_1 a$ et $p_1 y_1 = x$. De la même façon il existe $y_2 \in C_2$ avec $o(y_2) = p_2 (p_1 a)$ et $p_2 y_2 = y_1$. Et de façon générale il existe $y_{i+1} \in C_{i+1}$ avec $o(y_{i+1}) = p_{i+1} (p_1 p_2 ... p_i a)$ et $p_{i+1} y_{i+1} = y_i p_i$ pour $0 \leq i < r$. Il est alors clair que $y := y_r$ convient.

Lemme 3 *Soient G un groupe abélien (noté additivement), $x, y \in G$, deux éléments d'ordre fini. Alors il existe $u, v \in \mathbb{Z}$ tels que* $o(u x + v y) = \mathrm{ppcm}(o(x), o(y))$.

Démonstration C'est la partie A.1 de la démonstration du lemme 1, p. 121 de cet ouvrage.

[Fr. B.C.D.] **Fresnel J** *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999),
[Fr. E.] **Fresnel J** *Groupes* (Hermann 2001),

p. 128 complément : le théorème est encore valable si on suppose seulement que G est un groupe fini (non nécessairement abélien). C'est un résultat de Joseph Ayoub
The direct extension theorem, J. Group Theory 9 (2006), 307-316

Page 130, complément

Sur le nombre minimum de générateurs d'un groupe de type fini

Convention et notation Soit G un groupe de type fini, i.e. engendré par un nombre fini d'éléments. Si $G \neq \{e\}$, on note $r(G)$ le nombre minimum de générateurs de G et par convention $r(\{e\}) = 0$.
On verra (proposition 5) que l'application r est une fonction croissante sur l'ensemble des groupes abéliens de type fini, i.e. si $H \subset G$, alors $r(H) \leq r(G)$.
En revanche, il n'en est rien sur l'ensemble des groupes finis non nécessairement commutatifs.

1. Quelques exemples de calcul de $r(G)$

Proposition 1 *Soit* $G \neq \{0\}$ *, un groupe abélien fini, alors on a* $G = \mathbb{Z} x_1 \oplus \mathbb{Z} x_2 \oplus \ldots \oplus \mathbb{Z} x_r$ *avec* $1 \neq o(x_r) \mid o(x_{r-1}) \mid \ldots \mid o(x_1)$ (*théorème* 1, *p.* 123 *de cet ouvrage*). *Alors* $r(G) = r$, i.e. $r(G)$ *est le nombre d'invariants du groupe abélien fini* G .

Démonstration C'est la partie 2. de l'exercice 8.45. p. 100 de Fr. E.

Proposition 2 (structure des groupes abéliens de type fini) *Soient* $G \neq \{0\}$ *un groupe abélien de type fini,* G_t *le sous-groupe de torsion de* G *. Alors il existe un entier* $d \geq 0$ *unique tel que* $G \simeq G_t \oplus \mathbb{Z}^d$ *. En*

plus G_t *est un groupe fini et si* $G_t \neq \{0\}$ *, il admet une décomposition sous la forme*
$G_t = \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \ldots \oplus \mathbb{Z}x_r$ *avec* $1 \neq o(x_r) \mid o(x_{r-1}) \mid \ldots \mid o(x_1)$.
Par ailleurs on a $r(G) = d + r$.

Démonstration La première partie est le corollaire 6.2.4. p. 61 de Fr. E.
Pour la seconde partie, on traite seulement le cas où $G_t \neq \{0\}$, $r \geq 1$, en imitant la technique de l'exercice 8.45. p. 100 de Fr. E. En effet si p est un nombre premier avec $p \mid o(x_1)$, alors $\frac{G}{pG}$ est isomorphe à $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{d+r}$. Soient $\rho : G \to \frac{G}{pG}$ la surjection canonique, $(g_1, g_2, \ldots, g_m)$ une famille génératrice de G , alors $(\rho(g_1), \rho(g_2), \ldots, \rho(g_m))$ est une famille génératrice du $\frac{\mathbb{Z}}{p\mathbb{Z}}$-espace vectoriel $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{d+r}$; ainsi $m \geq d + r$. Par ailleurs, si $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_d)$ est une base de $\mathbb{Z}^d$, il suit que $(x_1, x_2, \ldots, x_r, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_d)$ est famille génératrice de G . Ainsi donc $r(G) = d + r$. Les cas $d = 0$ ou $r = 0$ se traitent de la même façon, compte tenu de la convention $r(\{0\}) = 0$.

Proposition 3 (système générateur minimal pour S_n et $\mathfrak{A}_n$)
1. *Le groupe* S_n *est engendré par* $(1, 2, \ldots, n)$ *et* $(n-1, n)$ *; ainsi le nombre minimal de générateurs de* S_n *est* 2 *pour* $n \geq 3$. *Le groupe* S_n *est aussi engendré par* $(2, \ldots, n)$ *et* $(1, 2)$. *Ainsi* $r(\mathrm{S}_n) = 2$ *si* $n \geq 3$.
2. *Si* n *est pair,* $\mathfrak{A}_n$ *est engendré par le cycle* $(2, 3, \ldots, n)$ *et le* 3*-cycle* $(1, 2, 3)$. *Si* n *est impair* $\mathfrak{A}_n$ *est engendré par le cycle* $(1, 2, \ldots, n)$ *et le* 3*-cycle* $(1, 2, 3)$. *Ainsi* $r(\mathfrak{A}_n) = 2$ *si* $n \geq 4$.

Démonstration La partie 1. est le corollaire 2.2.1.3.5. p. 30 de Fr. E.
La partie 2. est l'exercice 64 partie 3.2. p. 155 de F.M.1.

Proposition 4 *Soient p un nombre premier, G un groupe d'ordre $p^n, n \geq 1$. Soit* $\mathrm{Fratt}(G)$ *le sous-groupe de* **Frattini** *de G ,* i.e. *l'intersection des sous-groupes maximaux de G. On sait que dans le cas d'un p-groupe, on* $\mathrm{Fratt}(G) = D(G)\,G^p$ *où $D(G)$ est le groupe dérivé de G et $D(G)\,G^p$ est le sous-groupe de G engendré par $D(G)$ et les x^p où $x \in G$. Ainsi $\frac{G}{\mathrm{Fratt}(G)}$ est isomorphe au groupe additif de $(\mathbb{F}_p)^r$. Soient $\varphi : G \to \frac{G}{\mathrm{Fratt}(G)} \simeq (\mathbb{F}_p)^r$ la surjection canonique $e_1, e_2, \ldots, e_r \in G$ de façon que $\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_r)$ soit un système générateur minimal de $\frac{G}{\mathrm{Fratt}(G)}$;* i.e. *une base du $\mathbb{F}_p$-espace vectoriel $\frac{G}{\mathrm{Fratt}(G)}$. Alors $(e_1, e_2, \ldots, e_r)$ est un système générateur de G et r est le cardinal minimum d'un système générateur de G ,* i.e. $r(G) = r$.

Démonstration C'est les propositions de l'exercice 76 p. 192-193 de F.M.1.

2. Variation du nombre minimal de générateurs pour les groupes abéliens de type fini.

Proposition 5 *Soit G un groupe abélien de type fini, H un sous-groupe de G . Alors H est de type fini et $r(H) \leq r(G)$.*

Démonstration On suppose que G est noté additivement.
Si $G = \{0\}$, on a $H = \{0\}$ et donc $0 = r(G) = r(H)$.
On suppose désormais que $G \neq \{0\}$.
1) On suppose que $r(G) = 1$, i.e. $G = \mathbb{Z}\,x_1$ avec $x_1 \neq 0$. Soit $\theta : \mathbb{Z} \to \mathbb{Z}\,x_1$ la surjection définie par $\theta(z) := z\,x_1$. Si H est un sous-groupe de $\mathbb{Z}\,x_1$, on a $\theta(\theta^{-1}(H)) = H$, comme $\theta^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$, il existe $a \in \mathbb{Z}$ avec $\theta^{-1}(H) = a\,\mathbb{Z}$. Ainsi $H = \theta(\theta^{-1}(H)) = \mathbb{Z}\,a\,x_1$. Cela montre que $r(H) \leq 1$. Ainsi la proposition est satisfaite pour $r(G) = 1$.

2) *On suppose que* $r(G)\geq 2$ *et que la proposition est satisfaite pour tout groupe abélien* G' *tel que* $r(G')<r(G)$.
On a $r(G)=n\geq 2$ et donc $G=\mathbb{Z}\,x_1+\mathbb{Z}\,x_2+\ldots+\mathbb{Z}\,x_n$. Soit $\rho: G\to\frac{G}{\mathbb{Z}\,x_1}$ la surjection canonique. On a donc
$\frac{G}{\mathbb{Z}\,x_1}=\mathbb{Z}\,\rho(x_2)+\mathbb{Z}\,\rho(x_3)+\ldots+\mathbb{Z}\,\rho(x_n)$. Tout d'abord $\frac{G}{\mathbb{Z}\,x_1}\neq\{0\}$, sinon on aurait $G=\mathbb{Z}\,x_1$, cela contredit
$r(G)=n\geq 2$. On a donc $1\leq r(\frac{G}{\mathbb{Z}\,x_1})\leq n-1$; il suit de l'hypothèse de récurrence que $r(\rho(H))=k\leq n-1$. Si $\rho(H)=\{0\}$, cela veut dire que $H\subset\mathbb{Z}\,x_1$ et la partie 1) dit que $r(H)\leq 1$; ainsi la proposition est satisfaite.
On suppose maintenant que $\rho(H)\neq\{0\}$, ainsi $1\leq k$ et donc $\rho(H)=\mathbb{Z}\,\rho(h_1)+\mathbb{Z}\,\rho(h_2)+\ \ldots+\mathbb{Z}\,\rho(h_k)$. Enfin il suit de la partie 1) qu'l existe $a\in\mathbb{Z}$ avec $H\cap\mathbb{Z}\,x_1=\mathbb{Z}\,a\,x_1$. Il reste à montrer que $H=\mathbb{Z}\,a\,x_1+\mathbb{Z}\,h_1+\mathbb{Z}\,h_2+\ \ldots+\mathbb{Z}\,x_k$. L'inclusion
$\mathbb{Z}\,a\,x_1+\mathbb{Z}\,h_1+\mathbb{Z}\,h_2+\ \ldots+\mathbb{Z}\,h_k\subset H$ est immédiate.
Maintenant si $h\in H$, on a
$\rho(h)=\lambda_1\rho(h_1)+\lambda_2\rho(h_2)+\ldots+\lambda_k\rho(h_k)$, avec $h_i\in H$, ainsi
$h-(\lambda_1h_1+\lambda_2h_2+\ldots+\lambda_kh_k)\in H\cap(\ker\rho)=H\cap\mathbb{Z}\,x_1=\mathbb{Z}\,a\,x_1$,
ce qui veut dire que $h-(\lambda_1h_1+\lambda_2h_2+\ldots+\lambda_kh_k)=\mu\ (a\,x_1)$. Cela montre $H\subset\mathbb{Z}\,a\,x_1+\mathbb{Z}\,h_1+\mathbb{Z}\,h_2+\ \ldots+\mathbb{Z}\,x_k$.
En conclusion, on a $r(H)\leq k+1\leq n$. Ce qui est la proposition.

3. Variation du nombre minimal de générateurs pour les groupes finis non nécessairement commutatifs.

La question naturelle qui se pose est de savoir si la proposition 5 est encore vraie lorsque le groupe G n'est plus commutatif. La réponse est trivialement non.

2.1. L'exemple le plus immédiat est le suivant. Soit $H := (\frac{\mathbb{Z}}{2\mathbb{Z}})^n$, il suit de la proposition 1 ques $r((\frac{\mathbb{Z}}{2\mathbb{Z}})^n) = n$. Soit $\rho : H \to \mathfrak{S}(H)$ définie comme il suit. Si $h \in H$, alors $\rho(h)$ est la bijection de H définie par $x \longmapsto h\,x$; facilement ρ est un homomorphisme injectif. Par ailleurs on sait que $\mathfrak{S}(H) \simeq \mathfrak{S}_{2^n}$ est engendré par deux éléments si $n \geq 2$ (proposition 3) et il n'est pas commutatif, on a $r(\mathfrak{S}(H)) = 2$. Si donc $n \geq 3$, on a $r(\rho(H)) > r(\mathfrak{S}(H))$.

2.2. Dans l'exemple 2.1. l'indice de $\rho(H)$ dans $\mathfrak{S}(H)$ est grand. On peut obtenir des exemples avec un indice plus petit de la façon qui suit.
On rappelle que $r(\mathfrak{S}_n) = 2$ si $n \geq 3$ (proposition 3) et $r(\mathfrak{A}_n) = 2$ si $n \geq 4$ (proposition 3) .
Par exemple, soit $G = \mathfrak{S}_6$ et H le sous-groupe engendré par les transpositions $(1,2),(3,4),(5,6)$; facilement H est isomorphe à $(\frac{\mathbb{Z}}{2\mathbb{Z}})^3$. Ainsi $r(G) = 2$ et $r(H) = 3$. On peut généraliser cet exemple avec $G = \mathfrak{S}_{2m}$ et $H \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^m$.
Autre exemple, soient $G = \mathfrak{A}_9$ et H est le sous-groupe engendré par les 3-cycles $(1,2,3),(4,5,6),(7,8,9)$. Facilement $H \simeq (\frac{\mathbb{Z}}{3\mathbb{Z}})^3$, ainsi $r(H) = 3$ et $r(G) = 2$. On peut généraliser cet exemple avec $G = \mathfrak{A}_{3m}$ et $H \simeq (\frac{\mathbb{Z}}{3\mathbb{Z}})^m$.

2.3. Notre objectif est maintenant de trouver le plus petit exemple. C'est un certain groupe à 16 éléments.

Proposition 6 *Il existe un groupe G engendré par a, b, c et avec $o(G) = 16$, $o(a) = 4$, $o(b) = o(c) = 2$, $a\,b = b\,a$, $b\,c = c\,b$ et $c\,a\,c^{-1} = a\,b$.*
Ce groupe est engendré par a et c et on a $r(G) = 2$, i.e. 2 est le nombre minimum de générateurs de G . Enfin le sous-groupe H engendré par a^2, b, c est isomorphe à $(\frac{\mathbb{Z}}{2\mathbb{Z}})^3$, ainsi $r(H) = 3$.

Démonstration
1) Soient $G:=(\frac{\mathbb{Z}}{4\mathbb{Z}})\times(\frac{\mathbb{Z}}{2\mathbb{Z}})\times(\frac{\mathbb{Z}}{2\mathbb{Z}})$ et $s:(\frac{\mathbb{Z}}{4\mathbb{Z}})\to(\frac{\mathbb{Z}}{2\mathbb{Z}})$ la surjection canonique.
On définit sur G une loi interne par
(1) $(x,y,z)*(x',y',z'):=(x+x',y+y'+s(x')\,z,z+z')$.
Facilement $(G,*)$ est un groupe avec $o(G)=16$. Désormais si $u,v\in G$, on notera uv l'élément $u*v$.
Soient $a:=(1,0,0)$, $b:=(0,1,0)$, $c:=(0,0,1)$, alors on a bien $o(a)=4$, $o(b)=o(c)=2$, $ab=ba$, $bc=cb$ et $cac^{-1}=ab$.

2) Soit $H:=(2\frac{\mathbb{Z}}{4\mathbb{Z}})\times(\frac{\mathbb{Z}}{2\mathbb{Z}})\times(\frac{\mathbb{Z}}{2\mathbb{Z}})$, il suit de (1) que H est un sous-groupe commutatif de G engendré par a^2,b,c et isomorphe à $(\frac{\mathbb{Z}}{2\mathbb{Z}})^3$, ainsi $r(H)=3$ (proposition 1). Facilement G est engendré par a et c et la relation $cac^{-1}=ab$ montre qu'il n'est pas commutatif, ce qui implique qu'il ne peut être engendré par un élément, ainsi $r(G)=2$.

Proposition 7 *Soient $H\subset G$ deux groupes finis avec $r(H)>r(G)$. On suppose que G est d'ordre minimum avec la propriété précédente. Alors G est isomorphe au groupe d'ordre* 16 *défini par la proposition 6.*

Démonstration
1) *On a $r(G)\geq 2$ et donc $r(H)\geq 3$* . En effet, si $r(G)=1$, ça veut dire que le groupe G est cyclique, il en est de même de H , ainsi $r(H)=1$; ce n'est pas possible. Le cas $r(G)=0$ est trivial.

2) Comme $r(H)\geq 3$, alors le lemme 1 ci-après dit que $o(H)\geq 2^3$ (on pourrait aussi dire qu'on connaît tous les groupes d'ordre au plus 7 et que ceux-ci sont engendrés par deux ou un éléments). Comme $r(H)\neq r(G)$, on a $H\neq G$ et donc $[G:H]\geq 2$. Il suit de

tout cela que $o(G) \geq 16$; sachant que G est d'ordre minimal, il suit de la proposition 6 que $o(G) = 16$ et $o(H) = 2^3$.

3) Si donc $o(H) = 2^3$, il suit du lemme 1 que $r(H) \leq 3$. Si on avait $r(H) \leq 2$, cela impliquerait $r(G) \leq 1$, ce qui est exclu par 1). Ainsi $o(H) = 2^3$ et $r(H) = 3$. Si H était non commutatif, cela veut dire que H est le groupe dihédral à 8 éléments ou le groupe des quaternions, mais dans ce cas, on a $r(H) = 2$ (5.4. p. 43, Fr. E.). Ainsi H est commutatif et le théorème de structure des groupes abéliens finis nous dit que la seule possibilité est $H \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^3$.
Alors le lemme 2 ci-après permet de conclure.

Lemme 1 *Soit G un groupe fini, $n := r(G)$, $(x_1, x_2, \dots, x_n)$ une famille génératrice de G . Comme $r(G) = n$, on a $o(x_i) \geq 2$, soit a_i l'infimum des premiers p qui divisent l'ordre de x_i . Alors on a $o(G) \geq a_1 a_2 \dots a_n$; en particulier on a toujours $o(G) \geq 2^n$.*

Démonstration
Soient $A_i := \{0, 1, \dots, a_i - 1\}$, $\theta : A_1 \times A_2 \times \dots \times A_n \to G$ définie par $\theta(\alpha_1, \alpha_2, \dots, \alpha_n) := (x_1)^{\alpha_1} (x_2)^{\alpha_2} \dots (x_n)^{\alpha_n}$. Il s'agit de montrer que θ est injectif. Supposons le contraire, on a donc
(1) $\qquad (x_1)^{\alpha_1} (x_2)^{\alpha_2} \dots (x_n)^{\alpha_n} = (x_1)^{\beta_1} (x_2)^{\beta_2} \dots (x_n)^{\beta_n}$.
On peut supposer qu'il existe k avec
$\alpha_1 = \beta_1, \alpha_2 = \beta_2, \dots, \alpha_{k-1} = \beta_{k-1}$ et par exemple $\alpha_k > \beta_k$. Il suit alors de la relation (1) la relation (2) ci-après
$(x_k)^{\alpha_k - \beta_k} = (x_{k+1})^{\beta_{k+1}} (x_{k+2})^{\beta_{k+2}} \dots (x_n)^{\beta_n} ((x_{k+1})^{\alpha_{k+1}} \dots (x_n)^{\alpha_n})^{-1}$.
Il suit de cela que $(x_k)^{\alpha_k - \beta_k}$ appartient au sous-groupe engendré par $\{x_{k+1}, x_{k+2}, \dots, x_n\}$. Comme $1 \leq \alpha_k - \beta_k < a_k$, il suit que $\text{pgcd}(\alpha_k - \beta_k, o(x_k)) = 1$, ainsi il existe $N \geq 1$ avec

$N(\alpha_k - \beta_k) = 1 + \lambda\, o(x_k)$, $\lambda \in \mathbb{Z}$. Ainsi en élevant la relation (2) à la puissance N , on déduit que x_k appartient au sous-groupe engendré par $\{x_{k+1}, x_{k+2}, \dots, x_n\}$. Il suivrait donc de cela que la famille $(x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n)$ engendre G ; ce qui contredit le fait que $r(G) = n$.

Lemme 2 *Soit G un groupe non commutatif, d'ordre 16 qui contient un sous-groupe H isomorphe à $(\frac{\mathbb{Z}}{2\mathbb{Z}})^3$. On note e l'élément neutre de G .*
1. *On suppose qu'il existe $a \in G - H$ tel que $o(a) = 2$. Alors G est produit semi-direct de $\{e, a\}$ par H . De plus $r(G) \geq 3$.*
2. *On suppose que pour tout $a \in G - H$, on a $o(a) = 4$. Alors $a^2 \in H$ et il existe $b, c \in H$ avec les propriétés suivantes : le groupe H est engendré par a^2, b, c et $ab = ba$, $bc = cb$, $cac^{-1} = ab$. Ainsi le couple (G, H) n'est autre chose que le couple défini selon la proposition 3.*

Démonstration
1) Comme H est d'indice 2 dans G , il est distingué dans G , il suit que G est produit semi-direct de $\{e, a\}$ par H .
Si le produit est direct, alors G est commutatif, c'est exclu.
On suppose maintenant que le produit n'est pas direct. Comme H est distingué, l'élément a opère sur le $\frac{\mathbb{Z}}{2\mathbb{Z}}$-espace vectoriel H , par $h \longmapsto a\,h\,a^{-1}$. Appelons u cet isomorphisme. Comme $u^2 = \mathrm{id}_H$, et sachant que $\mathrm{car}(\frac{\mathbb{Z}}{2\mathbb{Z}}) = 2$, il suit que $\chi_u(X) = (X+1)^3$.
Par ailleurs, comme le produit n'est pas direct, on a $u \neq \mathrm{id}_H$, ainsi la réduction de Jordan dit qu'il existe une base (e_1, e_2, e_3) du $\frac{\mathbb{Z}}{2\mathbb{Z}}$-espace vectoriel H , avec $u(e_1) = e_1$, $u(e_2) = e_2, u(e_3) = e_2 + e_3$.
Cela se traduit en notation multiplicative par
(1) $\quad ae_1 = e_1 a$, $ae_2 = e_2 a$, $ae_3 = e_2 e_3 a$.

En particulier le sous-groupe K engendré par e_2 est dans le centre de G, donc distingué. Soit $\rho : G \to \frac{G}{K}$ la surjection canonique, alors les relations (1) montrent que $\frac{G}{K}$ est commutatif, engendré par $\rho(a), \rho(e_1), \rho(e_3)$ avec $\rho(a)^2 = \rho(e), \rho(e_1)^2 = \rho(e), \rho(e_3)^2 = \rho(e)$; comme $o(\frac{G}{K}) = 2^3$, cela veut dire que $\frac{G}{K} \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^3$. En conclusion $r(G) \geq 3$.

2) Comme H est d'indice 2 dans G, il est distingué dans G, l'élément a opère sur le $\frac{\mathbb{Z}}{2\mathbb{Z}}$-espace vectoriel H, par $h \mapsto a\,h\,a^{-1}$. Appelons u cet isomorphisme. Comme H est d'indice 2 dans G, il est distingué dans G, ainsi $a^2 \in H$ qui est commutatif, cela implique que $u^2 = \mathrm{id}_H$, et sachant que $\mathrm{car}(\frac{\mathbb{Z}}{2\mathbb{Z}}) = 2$, il suit que $\chi_u(X) = (X+1)^3$.
Sachant que le groupe G n'est pas commutatif, il suit que $u \neq \mathrm{id}_H$.
Ainsi la réduction de Jordan dit qu'il existe une base (e_1, e_2, e_3) du $\frac{\mathbb{Z}}{2\mathbb{Z}}$-espace vectoriel H, avec

$$u(e_1) = e_1\ ,\ u(e_2) = e_2, u(e_3) = e_2 + e_3\ .$$

Comme H est d'indice 2 dans G, il est distingué dans G, ainsi $a^2 \in H$ et $a^2 \neq e$ puisque $o(a) = 4$.
Montrons que $a^2 \neq e_2$. Sinon la relation $u(e_3) = e_2 + e_3$ en notation multiplicative donnerait $a\,e_3\,a^{-1} = e_2\,e_3 = a^2\,e_3$. Soit donc $a\,e_3 = a^2\,e_3\,a$ et alors $(a\,e_3)^2 = (a^2\,e_3\,a)(a\,e_3) = a^2\,e_3\,(a\,a)\,e_3$, comme H est commutatif, on a $(a\,e_3)^2 = e$; c'est contraire à l'hypothèse puisque $a\,e_3 \in G - H$.
Comme $\frac{\mathbb{Z}}{2\mathbb{Z}} e_1 \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} e_2 = \ker(u - \mathrm{id}_H)$ et que $u(a^2) = a^2$, comme $a^2 \neq e_2$ on a $\frac{\mathbb{Z}}{2\mathbb{Z}} e_1 \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} e_2 = \frac{\mathbb{Z}}{2\mathbb{Z}} a^2 \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} e_2$.

Soient maintenant $b := e_2, d := e_3$. On a
$o(a)=4, o(b)=2, o(c)=2$, $ab=ba$, $bc=cb$ et $acа^{-1}=bc$.
Or $acа^{-1}=bc$ dit que $ca^{-1}c^{-1}=a^{-1}b$, donc $cac^{-1}=ba$.
Enfin avec la relation $ab=ba$, on obtient $cac^{-1}=ab$.
Sachant que $G=H\cup aH$, il suit que l'application
$\theta: (\frac{\mathbb{Z}}{4\mathbb{Z}})\times(\frac{\mathbb{Z}}{2\mathbb{Z}})\times(\frac{\mathbb{Z}}{2\mathbb{Z}})\to G$ définie par $\theta(x,y,z) := a^x b^y c^z$, avec une interprétation évidente pour a^x, b^y, c^z , est clairement surjective, donc bijective.
Il suit facilement des relations $ab=ba$, $bc=cb$ et $acа^{-1}=bc$ que
(2) $(a^x b^y c^z)(a^{x'} b^{y'} c^{z'}) = a^{x+x'} b^{y+y'+s(x')z} c^{z+z'}$ où
$s: (\frac{\mathbb{Z}}{4\mathbb{Z}}) \to (\frac{\mathbb{Z}}{2\mathbb{Z}})$ est la surjection canonique.
Cela montre bien que le couple (G,H) n'est autre chose que le couple défini selon la proposition 3.

Bibliographie

[Fr. E.] **Fresnel J.** *Groupes* (Hermann 2001)
[F. M.1] **Fresnel J.** , **Matignon M.** *Algèbre et Géométrie* (Hermann 2011)

Page 145, complément

Famille de transpositions génératrice de $\mathfrak{S}_n$ et connexité du graphe associé

Définition du graphe associé à une famille finie de transpositions

Soit $n \geq 2$, $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$. Soit $\Lambda \neq \emptyset$ une famille finie de transpositions de $\mathfrak{S}_n$. Alors le graphe $G(\Lambda)$ associé à Λ est le graphe dont l'ensemble des *sommets* est $S := \bigcup_{t \in \Lambda} \text{support}(t)$, sachant que si t est la transposition $t = (a, b)$, alors $\text{support}(t) = \{a, b\}$.

Par ailleurs les *arêtes du graphe* $G(\Lambda)$ sont définies comme il suit : si $x, y \in S$, il y a une arête qui relie x et y si et seulement si $x \neq y$ et si la transposition (x, y) est élément de Λ . Ainsi donc l'ensemble des arêtes du graphe $G(\Lambda)$ s'identifie aux parties $\{x, y\}$ à deux éléments de S telles que la transposition (x, y) est un élément de Λ .

Soit $x, y \in S$, un *chemin qui relie* x *à* y est une suite finie $(a_1, a_2, \ldots, a_r)$ d'éléments de S telle que $a_1 = x$, $a_r = y$ et $\{a_k, a_{k+1}\}$ est une arête pour $1 \leq k < r$.

Soit $x \in S$, on appelle *composante connexe de* x l'ensemble des $y \in S$ pour lesquels il existe un chemin qui relie x à y . En particulier, on dit que le graphe $G(\Lambda)$ est *connexe*, s'il existe un point $x \in S$ tel que la composante connexe de x soit S ; c'est équivalent de dire que pour tout $x, y \in S$, $x \neq y$, il existe un chemin qui relie x à y .

Théorème *Soient* $n \geq 2$, $\mathfrak{S}_n$ *le groupe des permutations de l'ensemble* $\{1, 2, \ldots, n\}$, Λ *une famille finie, non vide de transpositions de* $\mathfrak{S}_n$ *et* $G(\Lambda)$ *le graphe associé à* Λ *selon la définition ci-dessus.*
Alors les propriétés suivantes sont équivalentes.
i) La famille Λ *engendre le groupe* $\mathfrak{S}_n$,
ii) le graphe $G(\Lambda)$ *a pour ensemble de sommets* $\{1, 2, \ldots, n\}$ *et le graphe* $G(\Lambda)$ *est connexe selon la définition ci-dessus.*

Démonstration
1) *Montrons i) implique ii).*
1.1) Montrons que 1 est un sommet du graphe $G(\Lambda)$.
Sinon $1 \notin \text{support}(t)$ pour tout $t \in \Lambda$, ainsi $t(1) = 1$ pour tout $t \in \Lambda$. Comme Λ engendre $\mathfrak{S}_n$, il suit que $\sigma(1) = 1$ pour tout $\sigma \in \mathfrak{S}_n$; ce qui est une contradiction, en particulier pour le cycle $\sigma = (1, 2, \ldots, n)$.
De la même façon k est un sommet si $1 \leq k \leq n$.
1.2) Montrons que $G(\Lambda)$ est connexe.
Soit A la composante connexe de 1 , selon la définition ci-dessus. Il s'agit de montrer que $A = \{1, 2, \ldots, n\}$. Supposons le contraire, on a donc $\{1, 2, \ldots, n\} = A \cup B$ avec $B \neq \emptyset$. Il suit de la définition de la composante connexe de 1 que pour tout $t \in \Lambda$, on a $\text{support}(t) \subset A$ ou $\text{support}(t) \subset B$. Il suit de cela que pour tout $t \in \Lambda$, on a $t(A) = A$ et $t(B) = B$. Comme Λ engendre $\mathfrak{S}_n$, on a aussi pour tout $\sigma \in \mathfrak{S}_n$, $\sigma(A) = A$ et $\sigma(B) = B$. Cela donne une contradiction en considérant $\sigma = (1, 2, \ldots, n)$ et $\sigma^k(1)$ pour $1 \leq k \leq n$.

2) *Montrons ii) implique i) .*
Soit H le sous-groupe de $\mathfrak{S}_n$ engendré par Λ . Il suffit de montrer que $(1,k)\in H$ pour $2\leq k\leq n$ puisque l'on sait que la famille $\{(1,k) \mid 2\leq k\leq n\}$ engendre $\mathfrak{S}_n$ (Fr.E. corollaire 2.2.1.3.4.).
Il suit du lemme ci-après qu'il existe un chemin $(b_1, b_2, \ldots, b_s)$ qui relie 1 à k avec $1=b_1$, $k=b_s$, $b_1\notin\{b_2, b_3, \ldots, b_s\}$ et $(b_i, b_{i+1})\in\Lambda$ pour $1\leq i<s$. On a donc $(b_1, b_2)\in H$, et sachant que b_1 est invariant par (b_2, b_3) , on a

$$(b_2, b_3)\,(b_1, b_2)(b_2, b_3)^{-1}=(b_1, b_3)\in H\ .$$

De même $(b_3, b_4)\,(b_1, b_3)(b_3, b_4)^{-1}=(b_1, b_4)\in H$. Ainsi par récurrence, on a $(b_1, b_s)\in H$, i.e. $(1,k)\in H$.

Lemme *Soient x, y deux sommets de $G(\Lambda)$ avec $x\neq y$. On suppose en plus qu'il existe un chemin qui relie x à y . Alors il existe un chemin $(b_1, b_2, \ldots, b_s)$ avec $b_1=x$, $b_s=y$ et $b_1\notin\{b_2, b_3, \ldots, b_s\}$.*

Démonstration Soit $(a_1, a_2, \ldots, a_r)$ un chemin qui relie x à y , i.e. $x=a_1$, $y=a_r$ et $(a_i, a_{i+1})\in\Lambda$ pour $1\leq i<r$. Comme $a_1\neq a_r$, il existe un plus grand entier $j<r$ tel que $a_j=a_1$. Ainsi $a_j\notin\{a_{j+1}, a_{j+2}, \ldots, a_r\}$ et $(a_{j+1}, a_{j+2}, \ldots, a_r)$ est un chemin qui relie $a_1=a_j=x$ à $a_r=y$ avec les propriétés du lemme.

Remarque Les propriétés suivantes sont équivalentes.
i) L'ensemble des sommets du graphe $G(\Lambda)$ est $\{1, 2, \ldots, n\}$,
ii) $\{k\in\{1, 2, \ldots, n\} \mid t(k)=k$ pour tout $t\in\Lambda\}=\emptyset$.

[Fr. E.] **Fresnel J.** *Groupes* (Hermann 2001)

p.216 IV.4. complément

Existence de polynômes homogènes à deux variables, à coefficients dans un anneau A et prenant des valeurs inversibles sur une partie finie de A^2

Introduction

Soit A un anneau commutatif, unitaire, $A^\times$ le groupe des inversibles de A, $m \geq 1$,
$P(X,Y) = a_0 Y^m + a_1 X Y^{m-1} + \ldots + a_m X^m \in A[X,Y]$, un polynôme homogène à coefficients dans A, de degré m.
Soit $(x,y) \in A^2$, avec $P(x,y) \in A^\times$, alors on a $xA + yA = A$; sinon il existe un idéal maximal $\mathfrak{M}$ de A tel que $xA + yA \subset \mathfrak{M}$, il suit facilement de cela que $P(x,y) \in \mathfrak{M}$, ce qui est en contradiction avec $P(x,y) \in A^\times$. Réciproquement si $xA + yA = A$, on a $u, v \in A$ avec $ux + vy = 1$, si donc $W(X,Y) := uX + vY$, alors $W(X,Y)$ est un polynôme homogène de degré 1 avec $W(x,y) = 1$. En termes simples, si un couple $(x,y) \in A^2$ satisfait une relation de Bézout, c'est équivalent à l'existence d'un polynôme homogène $W(X,Y) \in A[X,Y]$, de degré 1 tel que $W(x,y) = 1$ et en particulier $W(x,y) \in A^\times$.
Le premier problème que l'on traite ici se généralise de la façon qui suit.
Quels sont les anneaux A pour lesquels la propriété ci-après est toujours satifaite.
Soient $n \geq 1$, $(x_i, y_i) \in A^2$ avec $1 \leq i \leq n$, et $x_i A + y_i A = A$ pour $1 \leq i \leq n$. Alors il existe $P(X,Y) \in A[X,Y]$ avec $P(X,Y)$ homogène, $\deg P(X,Y) \geq 1$ *et $P(x_i, y_i) \in A^\times$ pour $1 \leq i \leq n$.*
Nous répondons à cela avec la proposition 1 qui suit.

Le second problème que l'on traite ici se généralise de la façon qui suit.
Quels sont les anneaux A *pour lesquels la propriété ci-après est toujours satifaite.*
Soient $n \geq 1$, $(x_i, y_i) \in A^2$ *avec* $1 \leq i \leq n$, *et* $x_i A + y_i A = A$ *pour* $1 \leq i \leq n$. *Alors il existe* $P(X,Y) \in A[X,Y]$ *avec* $P(X,Y)$ *homogène,* $\deg P(X,Y) \geq 1$ *et* $P(x_i, y_i) = 1$ *pour* $1 \leq i \leq n$.
Nous répondons à cela avec la proposition 2 qui suit.

Proposition 1 *Soient* A *un anneau commutatif, unitaire,* $A^\times$ *le groupe des inversibles de* A . *Alors les propriétés suivantes sont équivalentes.*
i) Pour tout $z \in A$, *soit* $\rho_z : A \to \frac{A}{zA}$ *la surjection canonique, alors le groupe quotient* $\frac{(\rho_z(A))^\times}{\rho_z(A^\times)}$ *est de torsion ; ici* $(\rho_z(A))^\times$ *désigne le groupe des inversibles de* $\rho_z(A)$,
ii) pour tout $a, b \in A$ *avec* $aA + bA = A$, *il existe* $N \geq 1$, $\lambda \in A$ *avec* $b^N - \lambda a \in A^\times$,
iii) pour tout $n \geq 1$ *et pour toute famille finie* $(x_i, y_i)_{1 \leq i \leq n}$ *d'éléments de* A^2 *avec* $x_i A + y_i A = A$ *pour* $1 \leq i \leq n$, *il existe un polynôme* $P(X,Y) \in A[X,Y]$ *(qui dépend de la famille) avec* $P(X,Y)$ *homogène,* $\deg P(X,Y) \geq 1$ *et* $P(x_i, y_i) \in A^\times$, *pour* $1 \leq i \leq n$.

Démonstration (par récurrence sur n)
0) L'équivalence entre *i*) et *ii*) est immédiate.

1) Montrons *ii*) implique *iii*) (par récurrence sur n).

1.1) Le cas $n = 1$, c'est la relation $x_1 A + y_1 A = A$ qui dit qu'il existe $u, v \in A$ avec $u x_1 + v y_1 = 1$; ainsi $P(X,Y) = uX + vY$ convient.

On suppose l'implication ii) donne iii) satisfaite pour n .
On a donc $P(X,Y)\in A[X,Y]$ *homogène,* $\deg P(X,Y)\geq 1$ *et* $P(x_i,y_i)\in A^\times$ *pour* $1\leq i\leq n$.
Quitte à changer $P(X,Y)$ *en* $P(X,Y)^\alpha$, $\alpha\geq 1$, *on peut supposer que* $\deg P(X,Y)\geq n$ *; en effet, sachant que* $P(X,Y)$ *est homogène et que* $P(x_1,y_1)^\alpha\in A^\times$, *donc* $P(X,Y)^\alpha\neq 0$, *on a* $\deg P(X,Y)^\alpha=\alpha\deg P(X,Y)$.

1.2) Soit $(x_{n+1},y_{n+1})\in A^2$ et $x_{n+1}A+y_{n+1}A=A$.
On a donc $W(X,Y)\in A[X,Y]$ homogène de degré 1 avec $W(x_{n+1},y_{n+1})=1$. Soit $Q(X,Y):=\prod_{i=1}^{n}(y_iX-x_iY)$.
Soient $b:=P(x_{n+1},y_{n+1})$, $a:=Q(x_{n+1},y_{n+1})$.
Montrons que $aA+bA=A$.
Supposons le contraire, il existe donc un idéal maximal $\mathfrak{M}$ de A tel que $aA+bA\subset\mathfrak{M}$.
Soit $\rho:A\to\frac{A}{\mathfrak{M}}$ la surjection canonique, on a donc $\rho(a)=0$, ce qui veut dire que $\prod_{i=1}^{n}\rho(y_ix_{n+1}-x_iy_{n+1})=0$, sachant que $\frac{A}{\mathfrak{M}}$ est un corps , cela veut dire qu'il existe i avec $1\leq i\leq n$ tel que $\rho(y_ix_{n+1}-x_iy_{n+1})=0$. Alors il existe $\lambda\in A$ tel que
(1) $\qquad(\rho(x_{n+1},\rho(y_{n+1}))=\rho(\lambda)(\rho(x_i),\rho(y_i))$ avec $\rho(\lambda)\neq 0$.
En effet, comme $x_iA+y_iA=A$, on a $\rho(x_i)\rho(A)+\rho(y_i)\rho(A)=\rho(A)$, cela implique $(\rho(x_i),\rho(y_i))\neq(0,0)$; ainsi il existe $\lambda\in A$ tel que
$$(\rho(x_{n+1},\rho(y_{n+1}))=\rho(\lambda)(\rho(x_i),\rho(y_i))\ .$$
Comme $x_{n+1}A+y_{n+1}A=A$, on a on a $u,v\in A$ avec $x_{n+1}u+y_{n+1}v=1$, donc $\rho(x_{n+1})\rho(u)+\rho(y_{n+1})\rho(v)=1$ et alors $\rho(\lambda)(\rho(x_i)\rho(u)+\rho(y_i)\rho(v))=1$; ce qui montre que $\rho(\lambda)\neq 0$.
Sachant que $P(x_i,y_i)=\varepsilon_i\in A^\times$, on a donc $\rho(P(x_i,y_i))=\rho(\varepsilon_i)\in(\rho(A))^\times$; il suit facilement de (1) que

(2) $\rho(P(x_{n+1},y_{n+1}))=\rho(\lambda)^{\deg P}\rho(P(x_i,y_i))=\rho(\lambda)^{\deg P}\rho(\varepsilon_i)\neq 0$, où $\varepsilon_i=P(x_i,y_i)\in A^\times$.
Ainsi $\rho(b)\neq 0$ et donc $b\notin\mathfrak{M}$; ce qui est une contradiction.
On a bien $aA+bA=A$.

1.3) Il suit alors de l'hypothèse *ii*) qu'il existe $N\geq 1$, $\varepsilon\in A^\times$, $\lambda\in A$ avec
$b^N-\lambda a=\varepsilon$.
Soit alors $R(X,Y):=P(X,Y)^N-\lambda Q(X,Y)\,W(X,Y)^{N\deg P-n}$.
Facilement $R(x_i,y_i)\in A^\times$ pour $1\leq i\leq n$. Cela montre d'une part que $R(X,Y)\neq 0$ et que $R(X,Y)$ est homogène de degré $N\deg P(X,Y)\geq 1$. De plus
$R\ (x_{n+1},y_{n+1})=b^N-\lambda a=\varepsilon$; ce qui montre *iii*) pour $n+1$.

2) Pour montrer que *iii*) implique *ii*) , il suffit de montrer que non *ii*) implique non *iii*).
On suppose donc qu'il existe $a,b\in A$ avec $aA+bA=A$ et que pour tout $N\geq 1$ et pour tout $\lambda\in A$, on a $b^N-\lambda a\notin A^\times$. Suposons qu'il existe un polynôme homogène $P(X,Y)\in A[X,Y]$, de degré $n\geq 1$ avec $P(0,1)\in A^\times$ et $P(a,b)\in A^\times$. On a donc $P(X,Y)=a_0Y^n+a_1XY^{n-1}+...+a_nX^n$. Alors $P(0,1)=\varepsilon_1\in A^\times$ veut dire que $\varepsilon_1=a_0\in A^\times$ et en plus $P(a,b)=\varepsilon_2\in A^\times$ impliquent que $\varepsilon_2=\varepsilon_1b^n+\mu a$ avec $\mu\in A$; cela montre que $b^n+(\varepsilon_1)^{-1}\mu a=\varepsilon_2(\varepsilon_1)^{-1}$; ce qui est une contradiction.

Proposition 2 *Soit A un anneau commutatif, unitaire, $A^\times$ le groupe des inversibles de A . Alors les propriétés suivantes sont équivalentes.*
i) Pour tout $z\in A$, le groupe des inversibles de $\frac{A}{zA}$ est de torsion, i.e. *tout élément du groupe des inversibles de $\frac{A}{zA}$ est d'ordre fini,*

ii) pour tout $a,b\in A$ *avec* $aA+bA=A$ *, il existe* $N\geq 1$, $\lambda\in A$ *avec* $b^N-\lambda a=1$,
iii) pour tout $n\geq 1$ *et pour toute famille finie* $(x_i,y_i)_{1\leq i\leq n}$ *d'éléments de* A^2 *avec* $x_iA+y_iA=A$ *pour* $1\leq i\leq n$ *, il existe un polynôme* $P(X,Y)\in A[X,Y]$ *(qui dépend de la famille) avec* $P(X,Y)$ *homogène,* $\deg P(X,Y)\geq 1$ *et* $P(x_i,y_i)=1$, *pour* $1\leq i\leq n$.

Démonstration (par récurrence sur n)
0) L'équivalence entre *i*) et *ii*) est immédiate.

1) Montrons *ii*) implique *iii*) (par récurrence sur n).

1.1) Le cas $n=1$, c'est la relation $x_1A+y_1A=A$ qui dit qu'il existe $u,v\in A$ avec $ux_1+vy_1=1$; ainsi $P(X,Y)=uX+vY$ convient.
On suppose l'implication ii) donne iii) satisfaite pour n .
On a donc $P(X,Y)\in A[X,Y]$ *homogène,* $\deg P(X,Y)\geq 1$ *et* $P(x_i,y_i)=1$ *pour* $1\leq i\leq n.$
Quitte à changer $P(X,Y)$ *en* $P(X,Y)^\alpha$, $\alpha\geq 1$, *on peut supposer que* $\deg P(X,Y)\geq n$ *; en effet, sachant que* $P(X,Y)$ *est homogène et que* $P(x_1,y_1)^\alpha=1$, *donc* $P(X,Y)^\alpha\neq 0$, *on a* $\deg P(X,Y)^\alpha=\alpha\deg P(X,Y)$.

1.2) Soit $(x_{n+1},y_{n+1})\in A^2$ et $x_{n+1}A+y_{n+1}A=A$.
On a donc $W(X,Y)\in A[X,Y]$ homogène de degré 1 avec $W(x_{n+1},y_{n+1})=1$. Soit $Q(X,Y):=\prod_{i=1}^{n}(y_iX-x_iY)$.
Soient $b:=P(x_{n+1},y_{n+1})$, $a:=Q(x_{n+1},y_{n+1})$.
Montrons que $aA+bA=A$.
Le démonstration est analogue à celle de la proposition 1.

1.3) Il suit alors de l'hypothèse *ii*) qu'il existe $N \geq 1$, $\varepsilon \in A^{\times}$, $\lambda \in A$ avec $b^N - \lambda a = 1$.
Soit alors $R(X,Y) := P(X,Y)^N - \lambda Q(X,Y)\, W(X,Y)^{N \deg P - n}$.
Facilement $R(x_i, y_i) = 1$ pour $1 \leq i \leq n$. Cela montre d'une part que $R(X,Y) \neq 0$ et que $R(X,Y)$ est homogène de degré $N \deg P(X,Y) \geq 1$. De plus
$R(x_{n+1}, y_{n+1}) = b^N - \lambda a = 1$; ce qui montre *iii*) pour $n+1$.

2) Pour montrer que *ii*) implique *iii*) , il suffit de montrer que non *ii*) implique non *iii*).
On suppose donc qu'il existe $a, b \in A$ avec $aA + bA = A$ et que pour tout $N \geq 1$ et pour tout $\lambda \in A$, on a $b^N - \lambda a \neq 1$. Suposons qu'il existe un polynôme homogène $P(X,Y) \in A[X,Y]$, de degré $n \geq 1$ avec $P(0,1) = 1$ et $P(a,b) = 1$. On a donc $P(X,Y) = a_0 Y^n + a_1 X Y^{n-1} + \ldots + a_n X^n$. Alors $a_0 = P(0,1) = 1$ et en plus $P(a,b) = 1$ impliquent qu'il existe $\mu \in A$ avec $b^n = 1 + \mu a$; ce qui est une contradiction.

Remarque 1 *Exemples d'anneaux satisfaisant le i*) *de la proposition 1, on dira satisfaisant* P1.

0. Un corps satisfait P1.
1. Soit $A = \underset{k \geq 1}{\cup} A_k$ avec $A_k \subset A_{k+1}$ pour $k \geq 1$ et A_k satisfaisant P1 pour tout $k \geq 1$. Alors A satisfait P1. Plus généralement une limite inductive d'anneaux satisfaisant P1 , satisfait P1.
2. La clôture intégrale de $\mathbb{Z}$ dans un corps extension finie de $\mathbb{Q}$ satifait P1.
La clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}^{alg}$ satifait P1.
3. Si les anneaux $A_1, A_2, \ldots, A_r$ satisfont P1, il en est de même de $A_1 \times A_2 \times \ldots \times A_r$.

Remarque 2 *Exemples d'anneaux satisfaisant le i) de la proposition 2, on dira satisfaisant* P2.

1. L'anneau $\mathbb{Z}$ des entiers.
2. L'anneau A des entiers d'une extension quadratique imaginaire de $\mathbb{Q}$; en effet le théorème de Dirichlet montre que $A^\times$ est fini et par ailleurs, si $z \neq 0$, l'anneau $\frac{A}{zA}$ est fini.
3. Soient $\mathbb{F}_p$ le corps fini à p éléments, $(\mathbb{F}_p)^{alg}$ une clôture algébrique de $\mathbb{F}_p$, L un sous-corps de $(\mathbb{F}_p)^{alg}$.
Alors L satifait P2.
4. Soit L comme ci-dessus, alors l'anneau des polynômes $L[T]$ satisfait P2.
5. Soit $A = \underset{k\geq 1}{\cup} A_k$ avec $A_k \subset A_{k+1}$ pour $k \geq 1$ et A_k satisfaisant P2 pour tout $k \geq 1$. Alors A satisfait P2. Plus généralement une limite inductive d'anneaux satisfaisant P2 , satisfait P2.
6. Si les anneaux $A_1, A_2, \ldots, A_r$ satisfont P2, il en est de même de $A_1 \times A_2 \times \ldots \times A_r$.
7. (un exemple non noethérien en caractéristique nulle) Soit A le sous-anneau de $\mathbb{Z}^{\mathbb{N}}$ constitué des suites constantes à partir d'un certain rang ; clairement cet anneau est unitaire. Si x est la suite $(x_k)_{k\geq 0}$, alors $\frac{A}{xA} \simeq \prod_{k\geq 0} \frac{\mathbb{Z}}{x_k\mathbb{Z}}$. Comme tous les $\frac{\mathbb{Z}}{x_k\mathbb{Z}}$ sont tous égaux à partir d'un certain rang, il suit que le groupe des inversibles de $\frac{A}{xA}$ est de torsion.
Par ailleurs, soit $\mathfrak{A}$ l'idéal des suites nulles à partir d'un certain rang ; facilement cet idéal n'est pas de type fini.
8. (un exemple non noethérien en caractéristique p) Soient K un corps fini et $A := K^{\mathbb{N}}$. Soit $x = (x_k)_{k\geq 0}$, $S := \{k \in \mathbb{N} \mid x_k = 0\}$, alors $\frac{A}{xA} \simeq K^S$, il suit de cela que le groupe des inversibles de $\frac{A}{xA}$ est de torsion.

Par ailleurs, soit $\mathfrak{A}$ l'idéal des suites nulles à partir d'un certain rang ; facilement cet idéal n'est pas de type fini.

Remarque 3 *Exemples d'anneaux qui ne satisfont pas* P2.
L'anneau A des entiers d'une extension quadratique réelle de $\mathbb{Q}$; en effet le théorème de Dirichlet montre que $A^\times$ n'est pas de torsion.
L'anneau A des entiers d'une extension de $\mathbb{Q}$ de degré ≥ 3 ; là encore le théorème de Dirichlet montre que $A^\times$ n'est pas de torsion.
Tout corps de caractéristique nulle.
Tout corps de caractéristique p qui n'est pas algébrique sur $\mathbb{F}_p$.
L'anneau des polynômes $\mathbb{Z}[T]$. Par exemple pour $z := 1-2T$, l'image de 2 dans $\frac{\mathbb{Z}[T]}{z\mathbb{Z}[T]}$ est un inversible d'ordre infini ; pour $z := T^2$, l'image de $1+T$ dans $\frac{\mathbb{Z}[T]}{z\mathbb{Z}[T]}$ est un inversible d'ordre infini.

p.246 IV.8.1. même complément que p. 121

p.247, ligne 5, lire
que $\rho e^{i\theta} \in \mathbb{U}_d$, ainsi $G \subset \mathbb{U}_d$ et comme $o(G) = o(\mathbb{U}_d)$, on a $G = \mathbb{U}_d$.

p. 249 complément à IV.8.2.
Dans la partie 2 du théorème on montre que la somme des racines du n-ième polynôme cyclotomique est $\mu(n)$, i.e. la valeur en n de la fonction de Möbius.
De façon plus générale, on peut évaluer la somme des puissances h-ièmes des racines du n-ième polynôme cyclotomique.
C'est ce qui suit

Sommes de Newton relatives aux racines du polynôme cyclotomique

Soit $n>0$ un entier. On note U_n le sous-groupe de $\mathbb{C}^\times$ constitué des racines n-ièmes de l'unité et U'_n le sous-ensemble de U_n constitué des éléments d'ordre n . Par définition le n-ième polynôme cyclotomique est $\Phi_n(X) := \prod_{z\in U'_n} (X-z)$.

Soit $h\in\mathbb{N}$, on appelle h-ième somme de Newton relative aux racines du polynôme cyclotomique Φ_n , l'expression $p_h(n) := \sum_{z\in U'_n} z^h$; l'expression $p_h(n)$ est aussi appelée somme de Ramanujan.

Proposition *Soient* $n>0$, $h\geq 0$ *des entiers* , $p_n(h)$ *la* h*-ème somme de Newton relative aux racines du polynôme cyclotomique* Φ_n *. Alors on a*

$$p_h(n) = \sum_{d\,|\,\mathrm{pgcd}(n,h)} d\,\mu(\frac{n}{d}) = \frac{\mu(\frac{n}{\mathrm{pgcd}(n,h)})\,\varphi(n)}{\varphi(\frac{n}{\mathrm{pgcd}(n,h)})}\,.$$

Démonstration
On s'intéresse tout d'abord à la formule $p_h(n) = \sum_{d\,|\,\mathrm{pgcd}(n,h)} d\,\mu(\frac{n}{d})$.
1) Facilement, on a $U_n = \bigcup_{d\,|\,n} U'_d$. Il suit de cela que $\sum_{d\,|\,n} p_h(d) = \sum_{z\in U_n} z^h$. Il suit de cela que $\sum_{d\,|\,n} p_h(d) = 0$ si $h\nmid n$ et que $\sum_{d\,|\,n} p_h(d) = n$ si $h\,|\,n$. Alors la formule $p_h(n) = \sum_{d\,|\,\mathrm{pgcd}(n,h)} d\,\mu(\frac{n}{d})$

est conséquence de la formule d'inversion de Möbius (F. M.] p. 243).

Nous allons ensuite montrer l'égalité $p_h(n)=\dfrac{\mu(\frac{n}{\mathrm{pgcd}(n,h)})\,\varphi(n)}{\varphi(\frac{n}{\mathrm{pgcd}(n,h)})}$.

Posons $\theta(n):=\dfrac{\mu(\frac{n}{\mathrm{pgcd}(n,h)})\,\varphi(n)}{\varphi(\frac{n}{\mathrm{pgcd}(n,h)})}$. Si $1=\mathrm{pgcd}(n,m)$ on a facilement
$\theta(n\,m)=\theta(n)\,\theta(m)$ (on dit souvent que la fonction θ est multiplicative). On va montrer que sous les mêmes hypothèses, on a de même
$p_h(n\,m)=p_h(n)\,p_h(m)$. Il suffira alors de vérifier que $\theta(q^k)=p_h(q^k)$ pour tout premier q et tout entier $k\geq 0$.

2) Montrons que p_h est une fonction multiplicative. Soit $m,n\in\mathbb{N}$, $m\geq 1$, $n\geq 1$ et $1=\mathrm{pgcd}(m,n)$. Soit $f:U_m\times U_n\to U_{mn}$ l'application définie par $f(z,z'):=zz'$. Facilement f est un homomorphisme de groupes. Montrons que f est injectif. Soit $(z,z')\in\ker f$, i.e. $zz'=1$. On considère une relation de Bézout $1=u\,m+v\,n$, on a donc $z^{(1-u\,m)}(z')^{v\,n}=1$, i.e. $z=1$ et aussi $z'=1$.
Montrons que f induit une bijection de $U'_m\times U'_n$ sur U'_{mn}. Tout d'abord montrons que $f(U'_m\times U'_n)\subset U'_{mn}$. Soient $z\in U'_m$, $z'\in U'_n$ il faut montrer
que $o(zz')=mn$. Facilement $(zz')^{mn}=1$, supposons que $(zz')^d=1$, on a donc $(zz')^{dm}=1$ et donc $(z')^{dm}=1$, comme $o(z')=n$, on a $n\mid dm$, et comme $1=\mathrm{pgcd}(m,n)$ il suit que $n\mid d$. De façon analogue $m\mid d$ et comme $1=\mathrm{pgcd}(m,n)$ il suit que $mn\mid d$; ce qui montre que
$o(z\,z')=m\,n$. Ainsi f induit une injection de $U'_m\times U'_n$ dans U'_{mn}.
Sachant que

$$\mathrm{card}(U'_m\times U'_n)=\mathrm{card}(U'_m)\mathrm{card}(U'_n)=\mathrm{card}(U'_{mn}),$$

il suit que f induit une bijection de $U'_m \times U'_n$ sur U'_{mn}.
Soit toujours $m, n \in \mathbb{N}$, $m \geq 1$, $n \geq 1$ et $1 = \text{pgcd}(m,n)$. Alors $p_h(m)\, p_h(n) = (\sum_{z \in U'_m} z^h)(\sum_{z \in U'_n} (z')^h) = \sum_{(z,z') \in U'_m \times U'_n} (z z')^h$;
or la bijection de $U'_m \times U'_n$ sur U'_{mn} montre que

$$\sum_{(z,z') \in U'_m \times U'_n} (z z')^h = p_h(mn).$$

Ainsi l'application p_h est multiplicative.

3) Soit q un nombre premier, $k \geq 0$ un entier, calculons $p_h(q^k)$. On a

$$p_h(q^k) = \sum_{z \in U_{q^k}} z^h - \sum_{z \in U_{q^{k-1}}} z^h .$$

Il suit alors facilement de cette expression que $p_h(q^k) = 0$ si $q^{k-1} \nmid h$, $p_h(q^k) = -q^{k-1}$ si $q^{k-1} \mid h$ et $q^k \nmid h$ et enfin $p_h(q^k) = q^k - q^{k-1}$ si $q^k \mid h$.
On vérifie facilement qu'on a les mêmes formules pour la fonction θ.

Remarque 1 On pourra vérifier directement que l'expression $\dfrac{\mu(\frac{n}{\text{pgcd}(n,h)})\, \varphi(n)}{\varphi(\frac{n}{\text{pgcd}(n,h)})}$ est un élément de $\mathbb{Z}$; en effet cela résulte simplement du fait que si $a \mid b$, alors $\varphi(a) \mid \varphi(b)$.

Remarque 2 Les formules de Newton permettent de calculer les coefficients du n-ième polynôme cyclotomique en fonction de sommes de Ramanujan $p_1(n), p_2(n), \ldots, p_{\varphi(n)}(n)$ ([F. M.] p. 327). Toutefois l'expression obtenue ne semble pas être facilement utilisable ; en particulier elle ne saurait permettre d'obtenir le résultat de Schur au 5. du théorème de la page 249.

[F. M.] **Fresnel J. & Matignon M.** *Algèbre et Géométrie,* Hermann 2011

p. 302 paragraphe V.2.1.

La démonstration de 2) de la ligne -4 p. 302 à la ligne 16 p. 303.

On peut avantageusement remplacer cette démonstration (qui est juste) par la suivante.

Par ([Fr. F] théorème 7.7.1.7. p. 268) on sait que
$$R(X)=F(X,Y)\,U(X,Y)+G(X,Y)\,V(X,Y)$$
avec $(U(X,Y),V(X,Y)\neq(0,0)$ et $\deg_Y U(X,Y)<m$,
$\deg_Y V(X,Y)<n$.
Supposons $R(X)=0$, on a donc
(1) $F(X,Y)\,U(X,Y)=-G(X,Y)\,V(X,Y)$.
Sachant que $\mathbb{C}[X,Y]$ est intègre, on a donc $U(X,Y)\neq 0$ et $V(X,Y)\neq 0$. Et de plus
(2) $\deg_Y F(X,Y)+\deg_Y U(X,Y)=\deg_Y G(X,Y)+\deg_Y V(X,Y)$.
Sachant de plus que $\mathbb{C}[X,Y]$ est factoriel, et que $F(X,Y)$ et $G(X,Y)$ n'ont pas de facteur irréductible en commun, il suit de (1) que $G(X,Y)$ divise $U(X,Y)$ dans $\mathbb{C}[X,Y]$.
Sachant que $U(X,Y)\neq 0$, cela veut dire que
$$\deg_Y G(X,Y)\leq\deg_Y U(X,Y)\ ,$$
ce qui est une contradiction.
Ainsi l'hypothèse $R=0$ est à rejeter.

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

p. 306 paragraphe V.2.2.

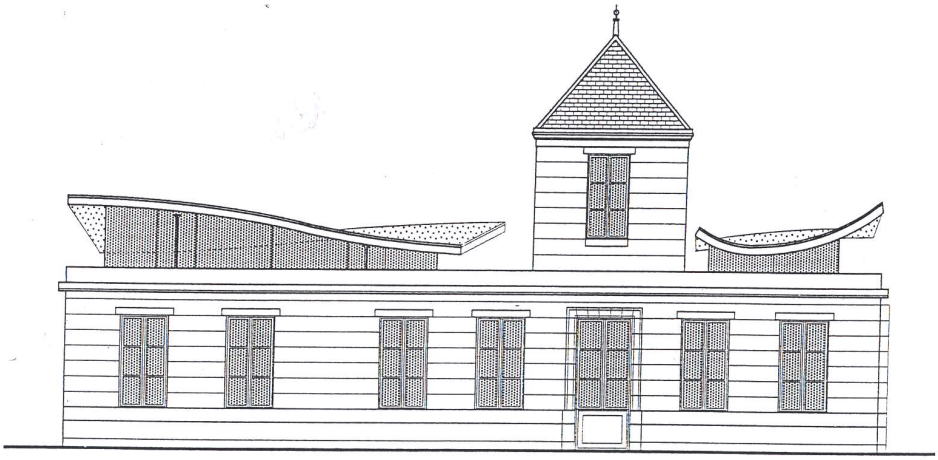
La démonstration de 3) de la ligne 3 p. 306 à la ligne -2 p. 306.

On peut avantageusement remplacer cette démonstration (qui est juste) par la suivante.

3) Soit $R(X,Y,Z)$ le résultant de $\widetilde{F}$, $\widetilde{G}$ en degré n et m considérés comme polynômes de la variable T à coefficients dans $\mathbb{C}[X,Y,Z]$.
Montrons que $R(X,Y,Z)\neq 0$ et que $\deg R(X,Y,Z)=n\,m$. En

Par ([Fr. F] théorème 7.7.1.7. p. 268) on sait que
$R(X,Y,Z)=\widetilde{F}(X,Y,Z,T)\,U(X,Y,Z,T)+\widetilde{G}(X,Y,Z,T)\,V(X,Y,Z,T)$
avec $(U(X,Y,Z,T),V(X,Y,Z,T)\neq(0,0)$ et
$\deg_T U(X,Y,Z,T)<m$, $\deg_T V(X,Y,Z,T)<n$.
Supposons $R(X,Y,Z)=0$, on a donc
(1) $\widetilde{F}(X,Y,Z,T)\,U(X,Y,Z,T)=-\widetilde{G}(X,Y,Z,T)\,V(X,Y,Z,T)$.
Sachant que $\mathbb{C}[X,Y,Z,T]$ est intègre, on a donc
$U(X,Y,Z,T)\neq 0$ et $V(X,Y,Z,T)\neq 0$. Et de plus
(2) $\deg_T\widetilde{F}(X,Y,Z,T)+\deg_T U(X,Y,Z,T)=$
$\deg_T\widetilde{G}(X,Y,Z,T)+\deg_{YT}V(X,Y,Z,T).$
Sachant de plus que $\mathbb{C}[X,Y,Z,T]$ est factoriel, et par 2) que $\widetilde{F}(X,Y,Z,T)$ et $\widetilde{G}(X,Y,Z,T)$ n'ont pas de facteur irréductible en commun, il suit de (1) que $\widetilde{G}(X,Y,Z,T)$ divise $U(X,Y,Z,T)$ dans $\mathbb{C}[X,Y,Z,T]$.
Sachant que $U(X,Y,Z,T)\neq 0$, cela veut dire que
$$\deg_T\widetilde{G}(X,Y,Z,T)\leq\deg_T U(X,Y,Z,T)\ ,$$
ce qui est une contradiction.
Ainsi l'hypothèse $R=0$ est à rejeter.

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



Bibliothèque Diophante d'Alexandrie
de l'Ecole mathématique et informatique de l'Université de Bordeaux